EUROPÄISCHES PARLAMENT

1999 *2004*

Nichtständiger Ausschuss über das Abhörsystem Echelon

VORLÄUFIG

18. Mai 2001

ENTWURF EINES BERICHTS

über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON)

Nichtständiger Ausschuss über das Abhörsystem Echelon

Berichterstatter: Gerhard Schmid

DE

INHALT

Seite

GESCHÄFTSORDNUNGSSEITE

In der Sitzung vom 5. Juli 2000 beschloss das Europäische Parlament die Einsetzung eines nichtständigen Ausschusses über das Abhörsystem Echelon. Zur Erfüllung seines Mandats ernannte der nichtständige Auschuss in seiner konstitutierenden Sitzung vom 5. Juli 2000 Herrn Gerhard Schmid als Berichterstatter.

Der Ausschuss prüfte den Berichtsentwurf in seiner/seinen Sitzung(en) vom ….

In dieser Sitzung/In der letztgenannten Sitzung nahm der Ausschuss den Entschließungsantrag mit … Stimmen bei … Gegenstimmen und … Enthaltungen/einstimmig an.

Bei der Abstimmung waren anwesend: …, Vorsitzende(r)/amtierende(r) Vorsitzende(r); … und … stellvertretende(r) Vorsitzende(r); …, Berichterstatter(in); …, … (in Vertretung von …), … (in Vertretung von … gemäß Art. 153 Abs. 2 der Geschäftsordnung), … und ….

Der Bericht wurde am ... eingereicht.

Die Frist für die Einreichung von Änderungsanträgen wird im Entwurf der Tagesordnung für die Tagung angegeben, auf der der Bericht geprüft wird/wurde auf …, … Uhr festgesetzt.

ENTSCHLIESSUNGSANTRAG

Entschließung des Europäischen Parlaments zu der Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON)

Das Europäische Parlament,

– unter Hinweis auf den Beschluss der Europäischen Parlaments vom 5. Juli 2000, einen nichtständigen Ausschuss über das Abhörsystem Echelon einzusetzen, und dessen Mandat,

– unter Hinweis auf den EG-Vertrag, der auf die Errichtung eines Gemeinsamen Marktes mit einem hohen Grad an Wettbewerbsfähigkeit abzielt,

– unter Hinweis auf den Vertrag der Europäischen Union, insbesondere auf seinen Art 6 Abs 2, der die Verpflichtung der EU zur Achtung der Grundrechte festschreibt, und auf seinen Titel V, der Bestimmungen für eine Gemeinsame Aussen- und Sicherheitspolitik trifft,

– unter Hinweis auf die Charta der Grundrechte der EU, deren Art 7 die Achtung des Privat- und Familienlebens schützt, und ausdrücklich das Recht auf Achtung der Kommunikation normiert,

– unter Hinweis auf die Europäische Konvention der Menschenrechte, insbesondere ihren Artikel 8, der die Privatsphäre schützt, und die zahlreichen anderen internationalien Verträge, die den Schutz der Privatsphäre vorsehen,

– in Kenntnis des Berichts über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem Echelon) des nichtständigen Ausschusses über das Abhörsystem Echelon (A5-..../2001),

zur Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON)

A. in der Erwägung, dass an der Existenz eines weltweit arbeitenden Kommunikationsabhörsystems, das durch anteiliges Zusammenwirken der USA, des Vereinigten Königreichs, Kanadas, Australiens und Neuseelands im Rahmen des UKUSA agreements funktioniert, nicht mehr gezweifelt werden kann; dass es aufgrund der vorliegenden Indizien wahrscheinlich erscheint, dass sein Deckname tatsächlich "ECHELON" ist, letzteres allerdings von nachrangiger Bedeutung ist,

B. in der Erkenntnis, dass das System nicht zum Abhören militärischer, sondern privater und wirtschaftlicher Kommunikation dient, aber die im Bericht vorgenommene Analyse gezeigt hat, dass die Mächtigkeit dieses Systems bei Weitem nicht so umfangreich sein kann, wie von den Medien teilweise angenommen,

zu den Grenzen des Abhörsystems

C. in der Erwägung, dass das Überwachungssystem auf dem globalen Abhören von Satellitenkommunikation aufbaut, dass Kommunikation aber in Gebieten mit hoher Kommunikationsdichte nur zu einem sehr geringen Teil über Satelliten vermittelt wird; dass

somit der überwiegende Teil der Kommunikation nicht durch Bodenstationen abgehört werden kann, sondern nur durch Anzapfen von Kabeln und Abfangen von Funk, was - wie die im Bericht vorgenommenen Untersuchungen gezeigt haben - nur in eng gesteckten Grenzen möglich ist; dass der Personalaufwand für die letztendliche Auswertung von abgefangener Kommunikation weitere Beschränkungen bedingt; dass folgerichtig die ECHELON-Staaten nur auf einen sehr beschränkten Teil der kabel- und funkgebundenen Kommunikation Zugriff haben und nur einen beschränkten Teil der Kommunikation auswerten können,

zur möglichen Existenz anderer Abhörsysteme

D. in der Überlegung, dass das Abhören von Kommunikation ein unter Nachrichtendiensten übliches Spionagemittel ist und ein solches System auch von anderen Staaten betrieben werden könnte, sofern sie über die entsprechenden finanziellen Mittel und die geographischen Voraussetzungen verfügen; dass Frankreich - zumindest was die geographischen Voraussetzungen betrifft - aufgrund seiner Territorien in Übersee als einziger EU-Mitgliedstaat sogar in der Lage wäre, alleine ein globales Abhörsystem zu errichten, und dass es darüber hinaus Hinweise gibt, dass auch Russland ein solches System betreiben könnte,

zur Vereinbarkeit mit EU-Recht

E. in der Überlegung, dass betreffend der Frage der Vereinbarkeit eines Systems des Typs ECHELON mit EU-Recht zwei Fälle zu unterscheiden sind: Wird das System nur zu nachrichtendienstlichen Zwecken verwendet, so ergibt sich kein Widerspruch zu EU-Recht, da Tätigkeiten im Dienste der Staatssicherheit vom EGV nicht erfasst sind, sondern unter Titel V EUV (GASP) fallen würden, es derzeit dort aber noch keine einschlägigen Regelungen gibt, und es somit an Berührungspunkten fehlt. Wird das System hingegen zur Konkurrenzspionage missbraucht, so steht das System im Widerspruch zur Loyalitätspflicht der Mitgliedstaaten und zum Konzept eines gemeinsamen Marktes mit freiem Wettbewerb, so dass ein Mitgliedstaat, der sich daran beteiligt, EG-Recht verletzt,

zur Vereinbarkeit mit dem Grundrecht auf Privatsphäre (Art. 8 EMRK)

F. in dem Bewusstsein, dass jedes Abhören von Kommunikation einen tief greifenden Eingriff in die Privatsphäre des Einzelnen darstellt; dass Art. 8 EMRK, der die Privatsphäre schützt, Eingriffe nur zur Gewährleistung der nationalen Sicherheit zulässt, sofern die Regelungen im innerstaatlichen Recht niedergelegt und allgemein zugänglich sind und festlegen, unter welchen Umständen und Bedingungen die Staatsgewalt sie vornehmen darf; dass Eingriffe darüber hinaus verhältnismäßig sein müssen, daher eine Interessenabwägung vorgenommen werden muss, und nach der Rechtsprechung des EGMR ein reines "nützlich oder wünschenswert sein" nicht genügt,

G. in der Erwägung, dass ein nachrichtendienstliches System, das ohne Gewährleistung der Einhaltung des Verhältnismäßigkeitsprinzips jedwede Kommunikation abfangen würde, mit der EMRK nicht vereinbar wäre; dass in gleicher Weise ein Verstoß gegen die EMRK vorläge, wenn die Regelung, nach der Kommunikationsüberwachung erfolgt, keine Rechtsgrundlage hat, wenn diese nicht allgemein zugänglich ist oder wenn sie so formuliert ist, dass ihre Konsequenzen für den Einzelnen nicht vorhersehbar sind; dass die Regelungen, nach denen amerikanische Nachrichtendienste im Ausland tätig werden, großteils klassifiziert sind, die Wahrung des Verhältnismäßigkeitsprinzips somit zumindest fraglich

ist, und ein Verstoß gegen die vom EGMR aufgestellten Prinzipien der Zugänglichkeit des Rechts und der Voraussehbarkeit seiner Wirkung wohl vorliegt,

H. in der Erwägung, dass sich die Mitgliedstaaten ihrer aus der EMRK erwachsenden Verpflichtungen nicht dadurch entziehen können, dass sie die Nachrichtendienste anderer Staaten auf ihrem Territorium tätig werden lassen, die weniger strengen Bestimmungen unterliegen, da sonst das Legalitätsprinzip mit seinen beiden Komponenten der Zugänglichkeit und Voraussehbarkeit seiner Wirkung beraubt und die Rechtssprechung des EGMR in ihrem Inhalt ausgehöhlt würde,

I. in Anbetracht der Tatsache, dass die Grundrechtskonformität gesetzlich legitimierter Tätigkeit von Nachrichtendiensten zudem verlangt, dass ausreichende Kontrollsysteme vorhanden sind, um einen Ausgleich zur Gefahr zu schaffen, die das geheime Agieren eines Teiles der Verwaltung mit sich bringt; dass der Europäische Gerichtshof für Menschenrechte ausdrücklich die Bedeutung eines effizienten Kontrollsystems im Bereich nachrichtendienstlicher Tätigkeit hervorhob und es deshalb bedenklich erscheint, dass einige Mitgliedstaaten über keine eigenen parlamentarischen Kontrollorgane für Geheimdienste verfügen,

zur Frage, ob EU-Bürger ausreichend vor Nachrichtendienste geschützt sind

J. in der Erwägung, dass der Schutz der EU-Bürger von der Rechtslage in den einzelnen Mitgliedstaaten abhängt, diese aber sehr unterschiedlich gestaltet sind, teilweise sogar gar keine parlamentarischen Kontrollorgane bestehen und deshalb kaum von einem ausreichenden Schutz gesprochen werden kann; dass die europäischen Bürger ein fundamentales Interesse daran haben, dass ihre nationalen Parlamente mit einem formell strukturierten speziellen Kontrollausschuss ausgestattet sind, der die Aktivitäten der Nachrichtendienste überwacht und kontrolliert; dass selbst dort, wo es Kontrollorgane gibt, für diese der Anreiz groß ist, sich mehr um die Tätigkeit von Inlandsnachrichtendiensten als von Auslandsnachrichtendiensten zu kümmern, da in der Regel nur im ersten Fall die eigenen Bürger betroffen sind,

K. in dem Bewusstsein, dass im Falle einer Zusammenarbeit der Nachrichtendienste im Rahmen der GASP die Institutionen gefordert sind, ausreichende Schutzbestimmungen zugunsten der europäischen Bürger zu schaffen,

zur Wirtschaftsspionage

L. in dem Bewusstsein, dass es Bestandteil des Aufgabengebiets von Auslandsnachrichtendiensten ist, sich für wirtschaftliche Daten wie Branchenentwicklungen, Entwicklung von Rohstoffmärkten, Einhaltung von Wirtschaftsembargos, Einhaltung der Lieferregeln für Dual-use-Güter etc. zu interessieren, und dass aus diesen Gründen einschlägige Unternehmen oftmals überwacht werden,

M. in der Überzeugung, dass es jedenfalls nicht tolerierbar ist, wenn sich Nachrichtendienste für Konkurrenzspionage instrumentalisieren lassen, indem sie ausländische Unternehmen ausspionieren, um inländischen einen Wettbewerbsvorteil zu verschaffen, dass es allerdings keinen belegten Fall dafür gibt, dass das globale Abhörsystem dafür eingesetzt wurde, auch wenn dies vielfach behauptet wurde,

N. im Hinblick darauf, dass sich sensible Unternehmensdaten vielfach in den Unternehmen

selbst befinden, so dass Konkurrenzspionage in erster Linie dadurch erfolgt, dass versucht wird, über Mitarbeiter oder eingeschleuste Personen Informationen zu bekommen oder in die internen Computernetzwerke einzudringen; dass nur wenn sensible Daten über Leitungen oder via Funk (Satellit) nach außen gelangen, ein Kommunikationsüberwachungssystem zur Konkurrenzspionage eingesetzt werden kann und dies systematisch nur in folgenden drei Fällen zutrifft:
- bei Unternehmen, die in 3 Zeitzonen arbeiten, so dass die Zwischenergebnisse von Europa nach Amerika und weiter nach Asien gesandt werden;
- im Falle von Videokonferenzen in multinationalen Konzernen, die über V-Sat oder Kabel laufen;
- wenn wichtige Aufträge vor Ort verhandelt werden (wie im Anlagenbau, Aufbau von Telekommunikationsinfrastruktur, Neuerrichtung von Transportsystemen, etc.) und von dort aus Rücksprachen mit der Firmenzentrale gehalten werden müssen,

zu den Möglichkeiten, sich selbst zu schützen

O. unter dem Hinweis, dass Sicherheit für Unternehmen nur dann erzielt werden kann, wenn das gesamte Arbeitsumfeld abgesichert sowie alle Kommunikationswege geschützt sind, auf denen sensible Informationen übermittelt werden; dass es ausreichend sichere Verschlüsselungssysteme zu erschwinglichen Preisen auf dem europäischen Markt gibt; dass auch Privaten dringend zur Verschlüsselung von E-Mails geraten werden muss; dass ein unverschlüsseltes Mail gleich einem Brief ohne Umschlag ist; dass sich im Internet relativ benutzerfreundliche Systeme finden, die sogar für den Privatgebrauch unentgeltlich zur Verfügung gestellt werden,

zu einer Zusammenarbeit der Nachrichtendienste innerhalb der EU

P. in der Erwägung, dass sich die EU darauf verständigt hat, nachrichtendienstliche Informationssammlung im Rahmen der Entwicklung einer eigenen Sicherheits- und Verteidigungspolitik zu koordinieren, dabei aber die Zusammenarbeit mit anderen Partneren in diesen Bereichen fortzusetzen,

Q. in der Erwägung, dass eine Zusammenarbeit der Nachrichtendienste innerhalb der EU auch wünschenswert erscheint, da einerseits eine Gemeinsame Sicherheitspolitik ohne Einbeziehung der Geheimdienste sinnwidrig wäre, andererseits damit zahlreiche Vorteile in professioneller, finanzieller und politischer Hinsicht verbunden wären; dass es auch eher der Idee eines gleichberechtigten Partners der USA entsprechen würde und sämtliche Mitgliedstaaten in ein System einbinden könnte, das in voller Konformität zur EMRK erstellt wird; dass eine entsprechende Kontrolle der Zusammenarbeit durch das Europäische Parlament dann natürlich gesichert sein muss,

R. in der Erwägung, dass das Europäische Parlament im Begriff ist, eigene Regelungen betreffend den Zugriff auf vertrauliche und sensible Informationen und Dokumente aufzustellen,

betreffend Abschluss und Änderung internationaler Verträge zum Schutz der Bürger und Unternehmen

1. fordert den Generalsekretär des Europarats auf, dem Ministerkomitee eine Untersuchung zu unterbreiten, ob die Anpassung des in Art 8 EMRK garantierten Schutzes der Privatsphäre an die modernen Kommunikationsmethoden und Abhörmöglichkeiten in einem Zusatzprotokoll

oder gemeinsam mit der Regelung des Datenschutzes im Rahmen einer Revision der Datenschutzkonvention sinnvoll wäre, unter der Voraussetzung, dass dadurch weder eine Minderung des durch den Gerichtshof entwickelten Rechtsschutzniveaus noch eine Minderung der für die Anpassung an weitere Entwicklungen notwendigen Flexibilität bewirkt wird;

2. fordert die Mitgliedstaaten auf, eine europäische Plattform zu schaffen, um die gesetzlichen Regelungen zur Gewährleistung von Brief- und Fernmeldegeheimnis zu überprüfen, sich überdies auf einen gemeinsamen Text zu veständigen, der den Schutz der Privatsphäre, so wie er in Art. 7 der Europäischen Charta der Grundrechte definiert ist, allen europäischen Bürgern auf dem Staatsterritorium der Mitgliedstaaten in seiner Gesamtheit gewährleistet und darüber hinaus garantiert, dass die Tätigkeit der Nachrichtendienste grundrechtskonform erfolgt, somit den in Kapitel 8 des Berichts, insbesondere in 8.3.4 aus Art 8 EMRK abgeleiteten Bedingungen entspricht;

3. ersucht die Mitgliedstaaten des Europarats, ein Zusatzprotokoll zu beschließen, das den Europäischen Gemeinschaften den Beitritt zur EMRK ermöglicht, oder über andere Maßnahmen nachzudenken, die Konflikte in der Rechtsprechung zwischen dem Straßburger und dem Luxemburger Gerichtshof ausschließen;

4. fordert den Generalsekretär der UNO auf, den verantwortlichen Ausschuss mit der Vorlage von Vorschlägen zu beauftragen, die auf eine Anpassung des Art 17 des Internationalen Paktes über bürgerliche und politische Rechte, der den Schutz der Privatsphäre garantiert, an die technischen Neuerungen abzielen;

5. fordert die USA auf, das Zusatzprotokoll zum Internationalen Pakt über bürgerliche und politische Rechte zu unterzeichnen, damit Individualbeschwerden gegen die USA wegen seiner Verletzung vor dem konventionellen Menschenrechtsausschuss zulässig werden; die einschlägigen amerikanischen NGOs, insbesondere ACLU (American Civil Liberties Union) und EPIC (Electronic Privacy Information Center) werden ersucht, auf die amerikanische Regierung entsprechenden Druck auzuüben;

betreffend nationale gesetzgeberische Maßnahmen zum Schutze von Bürgern und Unternehmen

6. fordert die Mitgliedstaaten auf, ihre eigene Gesetzgebung betreffend die Tätigkeit von Nachrichtendiensten auf ihre Grundrechtskonformität zu überprüfen;

7. fordert die Mitgliedstaaten auf, ein gemeinsames Schutzniveau gegenüber nachrichtendienstlicher Tätigkeit anzustreben, das sich am höchsten mitgliedstaatlichen Schutz orientiert, da die von der Tätigkeit eines Auslandsnachrichtendienstes betroffenen Bürger in der Regel die anderer Staaten und daher auch die anderer Mitgliedstaaten sind;

8. fordert die EU-Institutionen auf, im Falle einer Zusammenarbeit der Nachrichtendienste im Rahmen der GASP ausreichende Schutzbestimmungen zugunsten der europäischen Bürger zu schaffen; das Europäische Parlament als logisches Kontrollorgan muss seinerseits die für die Überwachung dieses hoch sensiblen Bereichs notwendigen Voraussetzungen schaffen, damit es realistisch, aber auch verantwortbar ist, die notwendigen Kontrollrechte einzufordern;

betreffend besondere rechtliche Maßnahmen zur Bekämpfung der Wirktschaftsspionage

9. fordert die Mitgliedstaaten auf, Überlegungen anzustellen, inwieweit durch Regelungen im europäischen und internationalen Recht Wirtschaftsspionage und Bestechung zum Zweck der Auftragsbeschaffung bekämpft werden können, insbesondere ob eine Regelung im Rahmen der WTO möglich wäre, die der wettbewerbsverzerrenden Wirkung eines derartigen Vorgehens Rechnung trägt, z.B. indem sie die Nichtigkeit solcher Verträge festlegt;

10. fordert die Mitgliedstaaten auf, sich in einer gemeinsamen eindeutigen Erklärung selbst zu verpflichten, keine Wirtschaftsspionage gegeneinander zu betreiben, und damit ihren Einklang mit dem Geiste und den Bestimmungen des EG-Vertrags zu signalisieren;

betreffend Maßnahmen in Rechtsanwendung und ihrer Kontrolle

11. appelliert an die nationalen Parlamente, die über keine eigenen paralementarischen Kontrollorgane zur Überwachung der Nachrichtendienste verfügen, solche einzurichten;

12. ersucht die nationalen Kontrollausschüsse der Geheimdienste, bei der Ausübung der ihnen übertragenen Kontrollbefugnisse dem Schutz der Privatsphäre großes Gewicht beizumessen, unabhängig davon, ob es um die Überwachung eigener Bürger, anderer EU-Bürger oder Drittstaatler geht;

13. appelliert an Deutschland und England, die weitere Gestattung von Abhören von Kommunikation durch Nachrichtendienste der USA auf ihrem Gebiet davon abhängig zu machen, dass diese im Einklang mit der EMRK stehen, dh dass sie dem Verhältnismäßigkeitsgrundsatz genügen, ihre Rechtsgrundlage zugänglich und die Wirkung für den einzelnen absehbar ist, sowie eine entsprechend effiziente Kontrolle besteht, da sie für die Menschenrechtskonformität genehmigter oder auch nur geduldeter nachrichtendienstlicher Tätigkeit auf ihrem Territorium verantwortlich sind;

betreffend Maßnahmen zur Förderung des Selbstschutzes von Bürgern und Unternehmen

14. fordert die Kommission und die Mitgliedstaaten auf, Programme zu entwickeln, die das Bewusstsein von Bürgern und Unternehmen für die Sicherheitsproblematik fördern, und gleichzeitig praktische Hilfe für Entwurf und Umsetzung von umfassenden Schutzkonzepten anbieten;

15. ersucht die Kommission und die Mitgliedstaaten, geeignete Maßnahmen für die Förderung, Entwicklung und Herstellung von europäischer Verschlüsselungstechnologie und -software auszuarbeiten und vor allem Projekte zu unterstützen, die darauf abzielen, benutzerfreundliche Kryptosoftware, deren Quelltext offengelegt ist, zu entwickeln;

16. fordert die Kommission und die Mitgliedstaaten auf, Softwareprojekte zu fördern, deren Quelltext offengelegt wird, da nur so garantiert werden kann, dass keine "backdoors" eingebaut sind (sog. "open-source Software");

17. appelliert and die europäischen Institutionen sowie an die öffentlichen Verwaltungen der Mitgliedstaaten, Verschlüsselung von e-mails systematisch einzusetzen, um so langfristig Verschlüsselung zum Normalfall werden zu lassen;

betreffend anderer Maßnahmen

18. appelliert an die Unternehmen, mit den Spionageabwehreinrichtungen stärker zusammenzuarbeiten, ihnen insbesondere Attacken von Außen zum Zwecke der

Wirtschaftsspionage bekannt zu geben, um so die Effizienz der Einrichtungen zu erhöhen;

19. fordert Kommission auf, einen Vorschlag zur Einsetzung einer europäischen Beratungsstelle für Fragen der Sicherheit von Unternehmensinformation vorzulegen, die neben der Steigerung des Problembewußtseins auch praktische Hilfestellungen zur Aufgabe hat;

20. hält es für sinnvoll, einen übereuropäischen Kongress zum Schutz der Privatsphäre vor Telekommunikationsüberwachung zu organisieren, um für NGOs aus Europa, den USA und anderen Staaten eine Plattform zu schaffen, wo grenzüberschreitende und internationale Aspekte diskutiert und Tätigkeitsfelder und Vorgehen koordiniert werden können;

21. beauftragt seine Präsidentin, diese Entschließung dem Rat, der Kommission, den Regierungen und Parlamenten der Mitgliedstaaten sowie den beitrittswilligen Staaten und dem Europarat zu übermitteln.

BEGRÜNDUNG

1. Einleitung:

1.1. Anlass der Einsetzung des Ausschusses

Am 5. Juli 2000 beschloss das Europäische Parlament, einen nichtständigen Ausschuss über das ECHELON-System einzusetzen. Der Auslöser dafür war die Debatte um die von STOA[1] in Auftrag gegebene Studie über das so genannte ECHELON-System[2] gewesen, die der Autor Duncan Campbell anlässlich einer Anhörung des Ausschusses für Freiheiten und Rechte der Bürger, Justiz und innere Angelegenheiten zum Thema "Europäische Union und Datenschutz" vorgestellt hatte.

1.2. Die Behauptungen in den beiden STOA-Studien über ein globales Abhörsystem mit dem Decknamen ECHELON

1.2.1. Der erste STOA-Bericht aus dem Jahr 1997

In einem Bericht, den STOA[3] 1997 für das Europäische Parlament zum Thema "Bewertung von Technologien zur politischen Kontrolle" bei der Omega Foundation in Auftrag gegeben hatte, wurde im Kapitel "nationale und internationale Netzwerke der Kommunikationsüberwachung" auch ECHELON beschrieben. Der Verfasser der Studie stellte darin die Behauptung auf, dass innerhalb Europas sämtliche Kommunikation via E-Mail, Telefon und Fax von der NSA (dem amerikanischen Auslandsnachrichtendienst) routinemäßig abgehört wird[4]. Durch diesen Bericht wurde ECHELON als angeblich allumfassendes globales Abhörsystem europaweit bekannt.

1.2.2. Die STOA-Berichte aus dem Jahr 1999

Um mehr zu diesem Themenkreis zu erfahren, wurde 1999 von STOA eine fünfteilige Studie in Auftrag gegeben, die sich mit der "Entwicklung der Überwachungstechnologie und den Risiken des Missbrauchs von Wirtschaftsinformationen" befasst. Band 2/5, von Duncan Campbell verfasst, widmete sich der Untersuchung der derzeit bestehenden nachrichtendienstlichen Kapazitäten und insbesondere der Arbeitsweise von ECHELON.[5]

---

[1] STOA (Scientific and Technological Options Assesment) ist eine Dienststelle in der Generaldirektion Wissenschaft des Europäischen Parlaments, die Forschungsaufträge vergibt.

[2] Der Stand der Dinge der Fernmeldeaufklärung (COMINT) in der automatisierten Verarbeitung zu nachrichtendienstlichen Zwecken von überwachten mehrsprachigen Breitbandmietleitungssystemen und den öffentlichen Leitungsnetzen und die Anwendbarkeit auf die Zielbestimmung und -auswahl von COMINT einschließlich der Spracherkennung (Oktober 1999).

[3] Scientific and Technological Options Assesment

[4] Steve Wright, An appraisal of technologies for political control (1998), 20

[5] Der Stand der Dinge der Fernmeldeaufklärung (COMINT) in der automatisierten Verarbeitung zu nachrichtendienstlichen Zwecken von überwachten mehrsprachigen Breitbandmietleitungssystemen und den öffentlichen Leitungsnetzen und die Anwendbarkeit auf die Zielbestimmung und -auswahl von COMINT einschließlich der Spracherkennung (Oktober 1999), PE 168.184.

Besondere Aufregung hat die im Bericht enthaltene Aussage erregt, ECHELON sei von seinem ursprünglichen Zweck der Verteidigung gegenüber dem Osten abgekommen und werde heutzutage für Wirtschaftspionage verwendet. Die These wird im Bericht durch Beispiele für angebliche Wirtschaftsspionage untermauert, insbesondere sollen Airbus und Thomsom CFS dadurch Schaden erlitten haben.

Als Folge der STOA-Studie wurde ECHELON in fast allen Parlamenten der Mitgliedstaaten diskutiert, in Frankreich und in Belgien wurden dazu sogar Berichte verfasst.

1.3. Das Mandat des Ausschusses

Gleichzeitig mit dem Beschluss über die Einsetzung eines zeitlich befristeten Ausschusses beschloss das Europäische Parlament dessen Mandat. Demzufolge ist der nichtständige Ausschuss beauftragt,

"- das Bestehen des Kommunikationsabhörsystems mit der Bezeichnung ECHELON zu prüfen, dessen Tätigkeit in dem STOA-Bericht über die Entwicklung der Überwachungstechnologie und Gefahren des Missbrauchs von Wirtschaftsinformationen beschrieben wird,

- die Vereinbarkeit eines solchen Systems mit Gemeinschaftsrecht zu bewerten, insbesondere mit Artikel 286 des EG-Vertrags sowie den Richtlinien 95/46/EG und 97/66/EG, und mit Artikel 6 Absatz 2 des EU-Vertrags, unter Berücksichtigung folgender Fragen:
  - Sind die Rechte der Unionsbürger gegen Tätigkeiten von Nachrichtendiensten geschützt?
  - Bietet Verschlüsselung einen angemessenen und ausreichenden Schutz zur Gewährleistung der Privatsphäre der Bürger, oder sollten zusätzliche Maßnahmen ergriffen werden, und, falls ja, welche Art von Maßnahmen?
  - Wie können die EU-Organe besser auf die Gefahren infolge dieser Vorgänge aufmerksam gemacht werden, und welche Maßnahmen können ergriffen werden?
- festzustellen, ob die europäische Industrie durch die globale Abhörung von Informationen gefährdet ist,
- gegebenenfalls Vorschläge für politische und legislative Initiativen zu machen."

1.4. Warum kein Untersuchungsausschuss?

Das Europäische Parlament entschied sich deshalb für die Einsetzung eines nichtständigen Ausschusses, weil die Einrichtung eines Untersuchungsausschusses nur zur Überprüfung von Verstößen gegen das Gemeinschaftsrecht im Rahmen des EG-Vertrages (Art. 193 EGV) vorgesehen ist, sich dieser folgerichtig lediglich mit den dort geregelten Materien befassen kann. Angelegenheiten, die unter die Titel V (GASP) und VI EUV (Polizeiliche und justitielle Zusammenarbeit in Strafsachen) fallen, sind ausgeschlossen. Überdies bestehen die besonderen Befugnisse eines Untersuchungsausschusses betreffend Vorladung und Akteneinsicht nach dem interinstitutionellen Beschluss[6] nur dann, wenn dem nicht Gründe der Geheimhaltung oder der öffentlichen oder nationalen Sicherheit entgegenstehen, was die Vorladung von Geheimdiensten jedenfalls ausschließt. Auch kann ein Untersuchungsausschuss seine Arbeiten nicht auf Drittstaaten ausdehnen, weil diese definitionsgemäß EU-Recht nicht verletzen können. Die Einsetzung eines Untersuchungsausschusses hätte somit nur eine inhaltliche Beschränkung ohne

[6] Beschluss des Europäischen Parlaments, des Rates und der Kommission vom 19. April 1995 über die Einzelheiten der Ausübung des Untersuchungsrechts des Europäischen Parlaments (95/167/EG), Art. 3 Abs. 3-5

zusätzliche Rechte bedeutet und wurde deshalb von der Mehrheit der Abgeordneten des Europäischen Parlaments abgelehnt.

1.5. Die Arbeitsmethode und der Arbeitsplan

Um sein Mandat voll und ganz ausfüllen zu können, hat der Ausschuss folgende Vorgangsweise gewählt. In einem Arbeitsprogramm, das vom Berichterstatter vorgeschlagen und vom Ausschuss angenommen worden war, fanden sich folgende relevanten Themenkreise aufgelistet: 1. Gesichertes Wissen über ECHELON, 2. Diskussion auf nationaler Parlaments- und Regierungsebene, 3. Nachrichtendienste und ihre Aktivitäten, 4. Kommunikationssysteme und die Möglichkeit, sie abzufangen, 5. Verschlüsselung, 6. Wirtschaftsspionage, 7. Spionageziele und Schutzmaßnahmen und 8. Rechtliche Rahmenbedingungen und Schutz der Privatsphäre. Die Themen wurden konsekutiv in den einzelnen Sitzungen abgehandelt, wobei die Reihenfolge sich an praktischen Gesichtspunkten orientierte und somit keine Aussage über die Wertigkeit der einzelnen Themenschwerpunkte beinhaltete. In Vorbereitung der einzelnen Sitzungen wurde vom Berichterstatter vorhandenes Material systematisch gesichtet und ausgewertet. Zu den Sitzungen wurden dann den Anforderungen des jeweiligen Schwerpunkts entsprechend Vertreter der nationalen Verwaltungen (insbesondere der Geheimdienste) und Parlamente in ihrer Funktion als Kontrollorgane der Geheimdienste eingeladen, ebenso Rechtsexperten und Experten in den Bereichen Kommunikations- und Abhörtechnik, Unternehmenssicherheit und Verschlüsselungstechnik aus Wissenschaft und Praxis. Angehört wurden ebenfalls Journalisten, die zu diesem Thema recherchiert hatten. Die Sitzungen waren im Allgemeinen öffentlich, wurden zuweilen aber auch unter Ausschluss der Öffentlichkeit abgehalten, sofern dies zur Informationsfindung ratsam erschien. Darüber hinaus haben sich der Vorsitzende des Ausschusses und der Berichterstatter gemeinsam nach London und Paris begeben, um dort Personen zu treffen, denen aus verschiedensten Gründen die Teilnahme an Ausschusssitzungen unmöglich war, deren Einbeziehung in die Ausschussarbeit jedoch ratsam erschien. Aus den gleichen Gründen sind der Vorstand des Ausschusses, die Koordinatoren und der Berichterstatter in die USA gereist. Außerdem hat der Berichterstatter zahlreiche, teilweise vertrauliche Einzelgespräche geführt

1.6. Die dem ECHELON-System zugeschriebenen Eigenschaften

Das mit "ECHELON" bezeichnete Abhörsystem unterscheidet sich von anderen nachrichtendienstlichen Systemen dadurch, dass es aufgrund zweier Eigenschaften eine ganz besondere Qualität aufweist:
Als Erstes wurde ihm zugeschrieben, dass es die Fähigkeit zur gleichsam totalen Überwachung habe. Vor allem durch Satellitenempfangsstationen und Spionagesatelliten solle jede durch Telefon, Telefax, Internet oder E-Mail von gleich welcher Person übermittelte Nachricht abgefangen werden können, um so von ihrem Inhalt Kenntnis zu erlangen.

Als zweites Merkmal von ECHELON wird angeführt, dass das System durch das anteilige Zusammenwirken mehrerer Staaten (dem Vereinigten Königreich, der USA, Kanada, Australien und Neuseeland) weltweit funktioniert, was gegenüber nationalen Systemen einen Mehrwert bedeutet: Die am ECHELON-System teilnehmenden Staaten (ECHELON-Staaten) können sich ihre Abhöreinrichtungen gegenseitig zur Verfügung stellen, für den daraus erwachsenden Aufwand gemeinsam aufkommen und gewonnene Erkenntnisse gemeinsam nutzen. Dieses internationale Zusammenwirken ist gerade für eine weltweite Überwachung von Satellitenkommunikation unerlässlich, weil nur so gesichert werden kann, dass bei

internationaler Kommunikation beide Teile eines Gesprächs abgefangen werden können. Es ist offensichtlich, dass Satellitenempfangsstationen wegen ihrer Größe nicht auf dem Territorium eines Staates ohne dessen Zustimmung errichtet werden können. Das gegenseitige Einverständnis und das anteilige Zusammenwirken mehrerer über die Erde verteilter Staaten ist hier unerlässlich.

Mögliche Gefährdungen für Privatsphäre und Wirtschaft durch ein System vom Typ ECHELON gehen aber nicht nur davon aus, dass es ein besonders starkes Überwachungssystem ist. Vielmehr kommt hinzu, dass es im weitgehend rechtsfreien Raum agiert. Ein Abhörsystem für internationale Kommunikation zielt meistens nicht auf die Bewohner des eigenen Landes. Der Abgehörte verfügt dann als Ausländer über keinerlei innerstaatlichen Rechtsschutz. Das Individuum ist diesem System daher völlig ausgeliefert. Die parlamentarische Kontrolle ist in diesem Bereich ebenfalls unzulänglich, da die Wähler, die davon ausgehen, dass es nicht sie, sondern "nur" Personen im Ausland trifft, kein besonderes Interesse daran haben, und die Gewählten in erster Linie die Interessen ihrer Wähler verfolgen. So ist es auch nicht verwunderlich, dass die im amerikanischen Congress stattgefundenen Anhörungen zur Tätigkeit der NSA sich lediglich um die Frage drehen, ob auch amerikanische Bürger davon betroffen seien, die Existenz eines solchen Systems an sich aber nicht weiter Anstoß erregt. Umso wichtiger erscheint es, sich auf europäischer Ebene damit auseinander zu setzen.

2. Die Tätigkeit von Auslandsnachrichtendiensten

2.1. Einleitung

Die meisten Regierungen unterhalten zur Gewährleistung der Sicherheit des Landes neben der Polizei auch Nachrichtendienste. Da ihre Tätigkeit meist geheim ist, heißen sie auch Geheimdienste. Diese Dienste dienen

- der Gewinnung von Informationen zur Abwehr von Gefahren für die Staatssicherheit
- der Gegenspionage im Allgemeinen
- der Abwehr von Gefahren, die Streitkräfte bedrohen könnten
- der Gewinnung von Informationen über Sachverhalte im Ausland

2.2. Was ist Spionage?

Regierungen haben einen Bedarf an systematischer Sammlung und Auswertung von Informationen über bestimmte Sachverhalte in anderen Staaten. Es handelt sich dabei um Grundlagen für Entscheidungen im Bereich der Streitkräfte, der Außenpolitik etc. Sie unterhalten deshalb Auslandsnachrichtendienste. Von diesen Diensten werden zunächst systematisch Informationsquellen ausgewertet, die öffentlich zugänglich sind. Dem Berichterstatter liegen Aussagen vor, dass dies im Schnitt mindestens 80% der nachrichtendienstlichen Tätigkeit ausmacht.[7] Besonders bedeutsame Informationen in den genannten Bereichen werden aber von Regierungen oder Firmen geheim gehalten und sind deshalb nicht öffentlich zugänglich. Wer dennoch in ihren Besitz gelangen will, muss sie stehlen. Spionage ist nichts anderes als der organisierte Diebstahl von Informationen.

2.3. Ziele von Spionage

Die klassischen Ziele von Spionage sind militärische Geheimnisse, andere Regierungsgeheimnisse oder Informationen über die Stabilität oder die Gefährdung von Regierungen. Das betrifft z.B. neue Waffensysteme, militärische Strategien oder Informationen über die Stationierung von Truppen. Nicht weniger wichtig sind Informationen über bevorstehende Entscheidungen in der Außenpolitik, Währungsentscheidungen oder Insiderinformationen über Spannungen innerhalb einer Regierung. Daneben gibt es auch ein Interesse an wirtschaftlich bedeutsamen Informationen. Dazu können neben Brancheninformationen auch Details über neue Technologien oder Auslandsgeschäfte gehören.

2.4. Die Methoden von Spionage

Spionage bedeutet, den Zugang zu Informationen herzustellen, die der Besitzer der Informationen vor dem Zugang durch Fremde eigentlich schützen will. Der Schutz muss also überwunden und gebrochen werden. Das ist bei politischer Spionage genauso wie bei Wirtschaftsspionage der Fall. Deshalb stellen sich für Spionage in beiden Bereichen die gleichen Probleme und deshalb werden in beiden Bereichen die gleichen Spionagetechniken eingesetzt. Logisch gibt es keinen Unterschied, lediglich das Schutzniveau ist in der Wirtschaft meist geringer und deshalb ist Wirtschaftsspionage manchmal einfacher auszuführen. Insbesondere ist

[7] Die "Commission on the Roles and Capabilities of the US Intelligence Community" stellte in ihrem Bericht "Preparing for the 21st Century: An Appraisal of U.S. Intelligence" fest, dass 95 % aller economic intelligence aus offenen Quellen stammen (Kapitel 2 "The Role of intelligence").

das Risikobewusstsein bei der Verwendung abhörbarer Kommunikation in der Wirtschaft weniger ausgeprägt als dies beim Staat in Sicherheitsbereichen der Fall ist.

2.4.1. Der Einsatz von Menschen bei der Spionage

Der Schutz von geheimen Informationen ist stets auf die gleiche Weise organisiert:
- nur wenige überprüfte Personen haben Zugang zu den geheimen Informationen
- für den Umgang mit diesen Informationen gibt es feste Regeln
- die Informationen verlassen normalerweise nicht den Schutzbereich und wenn doch, dann nur auf sichere oder verschlüsselte Weise. Deshalb zielt organisierte Spionage zunächst darauf ab, über **Personen** (so genannte human intelligence) direkt und ohne Umwege Zugang zu der gewünschten Information zu bekommen. Dabei kann es sich handeln um
    - eingeschleuste Personen (Agenten) des eigenen Dienstes/Unternehmens
    - um angeworbene Personen aus dem Zielbereich

Die angeworbenen Personen arbeiten für fremde Dienste/Unternehmen meistens aus folgenden Gründen:
- sexuelle Verführung
- Bestechung mit Geld oder geldwerten Leitungen
- Erpressung
- Appell an Ideologien
- Verleihung einer besonderen Bedeutung oder Ehre (Appell an Unzufriedenheit oder Minderwertigkeitsgefühle)

Ein Grenzfall ist die unfreiwillige Mitarbeit durch „Abschöpfen“. Dabei werden unter vorgeblich harmlosen Randbedingungen (Gespräche am Rande von Konferenzen, bei Fachkongressen, an Hotelbars) Mitarbeiter von Behörden oder Firmen durch Appell an Eitelkeit etc. zum Plaudern verführt.

Der Einsatz von Personen hat den Vorteil des direkten Zugangs zu den gewünschten Informationen. Es gibt aber auch Nachteile:
- die Gegenspionage konzentriert sich immer auf Personen oder Führungsagenten
- bei angeworbenen Personen können sich die Schwächen, die der Ansatzpunkt für die Anwerbung waren, als Bumerang erweisen
- Menschen machen stets Fehler und landen deshalb irgendwann im Netz der Spionageabwehr

Dort, wo es möglich ist, versucht man daher den Einsatz von Agenten oder angeworbenen Personen durch eine anonyme und von Personen unabhängige Spionage zu ersetzen. Am einfachsten geht das bei Auswertung von Funksignalen militärisch bedeutsamer Einrichtungen oder Fahrzeuge.

2.4.2. Die Auswertung elektromagnetischer Signale

Die in der Öffentlichkeit am besten bekannte Form der Spionage mit technischen Mitteln ist der Einsatz von Satellitenfotografie. Daneben werden aber elektromagnetische Signale jedweder Art aufgefangen und ausgewertet (so genannte signal intelligence, SIGINT).

2.4.2.1. Nicht der Kommunikation dienende elektromagnetische Signale

Bestimmte elektromagnetische Signale, z.B. die Ausstrahlungen von Radarstationen, können im militärischen Bereich wertvolle Informationen über die Organisation der Luftabwehr des Gegners liefern (so genannte electronic intelligence, ELINT). Darüber hinaus sind elektromagnetische Ausstrahlungen, die Auskunft über die Position von Truppen, Flugzeugen, Schiffen oder U-Booten geben können, eine wertvolle Informationsquelle für einen Nachrichtendienst. Auch die Verfolgung von bildaufnehmenden Spionagesatelliten anderer Staaten und das Aufzeichnen und Decodieren der Signale solcher Satelliten hat Bedeutung.

Die Signale werden von Feststationen, von niedrig umlaufenden Satelliten oder von quasigeostationären SIGINT-Satelliten aufgenommen. Dieser Teil der elektromagnetisch gebundenen nachrichtendienstlichen Tätigkeit belegt einen quantitativ bedeutsamen Teil der Abhörkapazitäten der Dienste. Der Einsatz von Technik ist aber damit nicht erschöpft.

2.4.2.2. Die Auswertung abgefangener Kommunikation

Die Auslandsnachrichtendienste vieler Staaten hören die militärische und diplomatische Kommunikation anderer Staaten ab. Manche dieser Dienste überwachen auch, soweit sie dazu Zugang haben, die zivile Kommunikation anderer Staaten. In einigen Staaten haben die Dienste das Recht, auch die in das eigene Land kommende oder das Land verlassende Kommunikation zu überwachen. In Demokratien unterliegt die Überwachung der Kommunikation der **eigenen** Bürger durch Nachrichtendienste bestimmten Eingriffsvoraussetzungen und Kontrollen. Die nationalen Rechtsordnungen schützen aber nur Bürger, die sich im eigenen Staatsgebiet aufhalten (siehe Kapitel 8).

2.5. Die Tätigkeit bestimmter Nachrichtendienste

Die öffentliche Debatte hat sich vor allem an der Abhörtätigkeit von amerikanischen und britischen Nachrichtendiensten entzündet. In der Kritik ist das Mitschneiden und Auswerten von Kommunikation (Sprache, Fax, E-Mail). Eine **politische** Bewertung braucht eine Messlatte, mit der diese Tätigkeit beurteilt werden kann. Als Vergleichsmaßstab bietet sich die Abhörtätigkeit der Auslandsnachrichtendienste in der EU an. Die folgende Tabelle 1 gibt eine Übersicht. Daraus ergibt sich, dass das Abhören von privater Kommunikation durch Auslandsnachrichtendienste keine Besonderheit amerikanischer oder britischer Auslandsnachrichtendienste ist.

Land	Auslands-kommunikation	Staatliche Kommunikation	Zivile Kommunikation
Belgien	+	+	-
Dänemark	+	+	+
Finnland	+	+	+
Frankreich	+	+	+
Deutschland	+	+	+
Griechenland	+	+	-
Irland	-	-	-
Italien	+	+	+

Luxemburg	-	-	-
Niederlande	+	+	+
Österreich	+	+	-
Portugal	+	+	-
Schweden	+	+	+
Spanien	+	+	+
UK	+	+	+
USA	+	+	+
Kanada	+	+	+
Australien	+	+	+
Neuseeland	+	+	+

Tabelle1: Abhörtätigkeiten von Nachrichtendiensten in der EU und in den ECHELON-Staaten

Dabei bedeuten die einzelnen Spalten:
Spalte 1: das entsprechende Land
Spalte 2: Auslandskommunikation wird abgehört
Spalte 3: Staatliche Kommunikation (Militär, Botschaften etc.) wird abgehört
Spalte 4: Zivile Kommunikation wird abgehört

3. Technische Randbedingungen für das Abhören von Telekommunikation

3.1. Die Abhörbarkeit verschiedener Kommunikationsträger

Wenn Menschen über eine bestimmte Entfernung miteinander kommunizieren wollen, dann ist dazu ein Träger der Kommunikation notwendig. Das kann:

- Luft sein (Schall)
- Licht sein (Morseblinker, optische Glasfaserkabel)
- elektrischer Strom sein (Telegraf, Telefon)
- eine elektromagnetische Welle sein (Funk in den verschiedensten Formen)

Wer sich als Dritter Zugang zum Träger der Kommunikation schafft, kann sie abhören. Der Zugang kann leicht oder schwer, von überall aus oder nur von bestimmten Positionen aus möglich sein. Im Folgenden werden zwei Extremfälle diskutiert: die technischen Möglichkeiten eines Spions vor Ort einerseits und die Möglichkeiten eines weltweit arbeitenden Abhörsystems andererseits.

3.2. Die Möglichkeiten des Abhörens vor Ort[8]

Vor Ort kann jede Kommunikation abgehört werden, wenn der Lauscher zum Rechtsbruch entschlossen ist und der Abgehörte sich nicht schützt.

- **Gespräche** in Räumen können mit eingebrachten Mikrofonen (so genannte Wanzen) oder durch Abtasten der Schwingungen der Fensterscheibe mit Laser abgehört werden.

- **Bildschirme** senden Strahlung aus, die auf bis zu 30m Entfernung aufgefangen werden kann; der Inhalt des Bildschirms wird damit sichtbar.

- **Telefon, Telefax und E-Mail** können abgehört werden, wenn der Lauscher die aus dem Gebäude kommenden Kabel anzapft.

- ein **Handy** kann aus einer Entfernung von bis zu ..... Kilometern abgehört werden.

- der **Betriebsfunk** kann innerhalb der Reichweite des UKW-Funks abgehört werden.

Die Bedingungen für den Einsatz technischer Mittel zur Spionage sind vor Ort ideal, weil sich die Abhörmaßnahmen auf eine Zielperson oder ein Zielobjekt eingrenzen lassen und praktisch fast jede Kommunikation erfasst werden kann. Nachteilig ist nur im Falle des Einbaus von „Wanzen“ oder des Anzapfens der Kabel ein gewisses Entdeckungsrisiko.

[8] Manfred Fink, Lauschziel Wirtschaft – Abhörgefahren und –techniken, Vorbeugung und Abwehr, Richard Boorberg Verlag, Stuttgart 1996

3.3. Die Möglichkeiten eines weltweit arbeitenden Abhörsystems

Heutzutage gibt es für interkontinentale Kommunikation verschiedene Kommunikationsträger für alle Kommunikationsarten (Sprache, Fax und Daten). Die Möglichkeiten eines weltweit arbeitenden Abhörsystems sind durch zwei Faktoren begrenzt:

- die begrenzte Zugänglichkeit zum Träger der Kommunikation
- die Notwendigkeit der Ausfilterung der interessierenden Kommunikation aus einer Riesenfülle von stattfindenden Kommunikationen

3.3.1. Der Zugang zu den Kommunikationsträgern

3.3.1.1. Kabelgebundene Kommunikation

Über Kabel werden alle Arten von Kommunikation übertragen (Sprache, Fax, E-Mail, Daten). Kabelgebundene Kommunikation kann nur abgehört werden, wenn ein Zugang zum Kabel möglich ist. Ein Zugang ist in jedem Falle am Endpunkt einer Kabelverbindung möglich, wenn er auf dem Territorium des Staates liegt, der abhören lässt. Innerstaatlich lassen sich also **technisch gesehen** alle Kabel abhören, wenn das Abhören rechtlich erlaubt ist. Ausländische Nachrichtendienste haben aber meist keinen legalen Zugang zu Kabeln im Hoheitsgebiet anderer Staaten. Illegal können sie allenfalls einen punktuellen Zugang bei hohem Entdeckungsrisiko verwirklichen.

Interkontinentale Kabelverbindungen wurden vom Telegrafenzeitalter an mit Unterwasserkabeln realisiert. Ein Zugang zu diesen Kabeln ist stets dort gegeben, wo sie wieder aus dem Wasser kommen. Arbeiten mehrere Staaten in einem Abhörverbund zusammen, dann ergibt sich ein Zugang zu allen Endpunkten der Kabelverbindungen, die in diesen Staaten auflaufen. Dies war historisch von Bedeutung, weil sowohl die Unterwassertelegrafenkabel als die ersten Unterwassertelefonkoaxialkabel zwischen Europa und Amerika in Neufundland (kanadisches Staatsgebiet) aus dem Wasser kamen und die Verbindungen nach Asien über Australien liefen, weil Zwischenverstärker nötig waren. Heutzutage werden die optischen Glasfaserkabel ohne Rücksicht auf die Gebirgslandschaft unter Wasser und Zwischenverstärkernotwendigkeiten auf dem direkten Wege ohne Zwischenstopp in Australien oder Neuseeland verlegt.
Elektrische Kabel können auch zwischen den Endpunkten einer Verbindung induktiv (d.h. elektromagnetisch mit einer an das Kabel gelegten Spule) angezapft werden, ohne dass eine direkte elektrisch leitende Verbindung geschaffen wird. Dies ist mit hohem Aufwand von U-Booten aus auch bei elektrischen Unterwasserkabeln möglich. Diese Technik wurde von den USA benutzt, um ein bestimmtes Unterwasserkabel der UdSSR anzuzapfen, über das unverschlüsselt Befehle für die russischen Atomunterseeboote kommuniziert wurden. Eine flächendeckende Verwendung dieser Technik verbietet sich schon aus Kostengründen.

Bei den heute verwendeten optischen Glasfaserkabeln der älteren Generation ist ein induktives Anzapfen nur an den Zwischenverstärkern möglich. Bei diesen Zwischenverstärkern wird das optische Signal in ein elektrisches Signal umgewandet, das verstärkt und dann wieder in ein optisches Signal rückverwandelt wird. Allerdings stellt sich die Frage, wie die riesigen Datenmengen, die in solch einem Kabel transportiert werden, vom Ort des Abhörens zum Ort der Auswertung transportiert werden sollen, ohne dass ein eigenes Glasfaserkabel gezogen wird. Der Einsatz eines U-Bootes mit an Bord befindlicher Auswerttechnik kommt vom Aufwand her nur in ganz seltenen Fällen, etwa im Krieg zum Abgreifen strategischer militärischer Kommunikation des Gegners, in Frage. Für die Routineüberwachung von internationalem

Fernmeldeverkehr kommt aus Sicht des Berichterstatters ein U-Booteinsatz nicht in Frage. Die Glasfaserkabel der neueren Generation verwenden Erbiumlaser als Zwischenverstärker – eine elektromagnetische Ankopplung zum Abhören ist an diesen Verstärkern nicht mehr möglich! Solche Glasfaserkabel können also nur an den Endpunkten der Verbindung abgehört werden.

Praktisch angewandt bedeutet dies für den Abhörverbund der so genannten **ECHELON-Staaten,** dass sie mit vertretbarem Aufwand nur an den Endpunkten der Unterwasserkabel, die auf ihrem Staatsgebiet auflaufen, abhören können. Im Wesentlichen können sie also nur kabelgebundene Kommunikation abgreifen, die in ihr Land kommt oder ihr Land verlässt! Das heißt, ihr Zugriff auf die ins Land kommende und das Land verlassende Kabelkommunikation **in Europa** beschränkt sich auf **das Territorium des Vereinigten Königreichs!** Denn Inlandskommunikation wird bisher meist im inländischen Kabelnetz gehalten; mit der Privatisierung der Telekommunikation kann es Ausnahmen geben – aber sie sind partiell und nicht vorhersagbar!

Dies gilt zumindest für Telefon und Telefax. Bei Kommunikation über das Internet mit Kabel gelten andere Randbedingungen. Zusammenfassend lässt sich aber Folgendes einschränkend feststellen:

- Kommunikation im Internet wird über Datenpakete abgewickelt, wobei die an einen Empfänger adressierten Pakete verschiedene Wege im Netz nehmen können.
- Zu Beginn des Internetzeitalters wurden Auslastungslücken im öffentlichen Wissenschaftsnetz zur Übermittlung von E-Mail genutzt. Der Weg einer Nachricht war deshalb völlig unvorhersagbar, die Einzelpakete gingen chaotische, nicht vorhersagbare Wege. Die wichtigste internationale Verbindung zu dieser Zeit war das „Wissenschafts-Backbone“ zwischen Europa und Amerika.
- Mit der Kommerzialisierung des Internets und der Etablierung von Internetprovidern ergab sich in der Folge auch eine Kommerzialisierung des Netzes. Internetprovider betrieben oder mieteten eigene Netze. Sie versuchten deshalb zunehmend, Kommunikation innerhalb ihres eigenen Netzes zu halten, um die Zahlung von Nutzungsgebühren an andere Netzteilnehmer zu vermeiden. Der Weg eines Datenpakets im Netz ist heute deshalb nicht allein durch die Auslastung des Netzes bestimmt, sondern hängt auch von Kostenüberlegungen ab.
- Eine E-Mail , die vom Kunden eines Providers an den Kunden eines anderen Providers gesandt wird, bleibt in der Regel im Firmennetz, auch wenn dies nicht der schnellste Weg ist. Die über den Transport der Datenpakete entscheidenden, an den Knotenpunkten des Netze eingerichteten Computer (sogenannte „Router“) organisieren den Übergang in andere Netze an bestimmten Übergabepunkten (sogenannte „Switches“).
- Zu Zeiten des Wissenschafts-Backbones waren die „Switches“ der globalen Internetkommunikation in den USA beheimatet. Deshalb konnten Nachrichtendienste dort damals auf einen wesentlichen Teil der europäischen Internetkommunikation zugreifen. Heute wird innereuropäische Kommunikation im Internet nur zu einem sehr geringen Anteil über die USA abgewickelt.
- Die innereuropäische Kommunikation wird zu einem kleinen Teil über einen Switch in London abgewickelt, zu dem der britische Nachrichtendienst GCHQ Zugang hat. Der Hauptteil der Kommunikation verlässt den Kontinent nicht. So wird z.B. mehr als 95% der deutschen Internetkommunikation über einen Switch in Frankfurt abgewickelt.

Praktisch bedeutet dies, dass die ECHELON-Staaten nur auf einen **sehr beschränkten Teil** der kabelgebundenen Internetkommunikation Zugriff haben können.

3.3.1.2. Funkgebundene Kommunikation [9]

Die Abhörbarkeit von funkgebundener Kommunikation hängt von der Reichweite der verwendeten elektromagnetischen Wellen ab. Verlaufen die abgestrahlten Funkwellen längs der Erdoberfläche (so genannte **Bodenwelle**), so ist ihre Reichweite begrenzt und hängt von der Geländestruktur, der Bebauung und dem Bewuchs ab. Verlaufen die Funkwellen in Richtung des Weltraums (so genannte **Raumwelle),** so sind nach Reflexion an Schichten der Ionosphäre durch die Raumwelle erhebliche Entfernungen überbrückbar. Mehrfachreflexionen vergrößern die Reichweite erheblich.

Die Reichweite ist abhängig von der Wellenlänge:

- Längst- und Langwellen (3kHz – 300kHz) breiten sich nur über die Bodenwelle aus, weil die Raumwelle nicht reflektiert wird. Sie haben geringe Reichweiten
- Mittelwellen (300kHz-3 MHz) breiten sich über die Bodenwelle und nachts auch über die Raumwelle aus. Sie haben mittlere Reichweiten.
- Kurzwellen (3MHz-30 MHz) breiten sich vorrangig über die Raumwelle aus und erlauben aufgrund der Mehrfachreflexionen einen **erdumspannenden** Empfang.
- UKW-Wellen (30 MHz-300MHz) breiten sich nur als Bodenwelle aus, weil die Raumwelle nicht reflektiert wird. Sie breiten sich relativ geradlinig wie Licht aus , ihre Reichweite hängt deshalb wegen der Erdkrümmung von den Antennenhöhen beim Sender und Empfänger ab. Sie haben abhängig von der Leistung Reichweiten bis ca. 100km (bei Handy etwa 30 km).
- Dezimeter- und Zentimeterwellen (30MHz-30 GHz) breiten sich noch mehr als UKW-Wellen quasioptisch aus. Sie lassen sich leicht bündeln und erlauben so gerichtete Übertragungen mit geringer Leistung (erdgebundene Richtfunkstrecken). Sie können nur mit einer Antenne empfangen werden, die sehr nahe parallel zur Richtfunkstrecke oder in der Richtfunkstrecke oder ihrer Verlängerung steht.

Lang- und Mittelwellen werden nur für Rundfunksender, Funkbaken etc. verwandt. Militärische und zivile Funkkommunikation findet über Kurzwelle und vor allem über UKW und Dezimeter/Zentimeterwellen statt.

Aus den obigen Ausführungen ergibt sich, dass ein global arbeitendes Abhörsystem für Kommunikation nur auf Kurzwellenfunk zugreifen kann. Bei allen anderen Arten des Funks muss die Abhörstation 100 km oder näher sein (z.B. auf einem Schiff, in einer Botschaft).

Praktisch bedeutet das, dass die ECHELON-Staaten nur auf einen sehr begrenzten Teil der Funkkommunikation Zugriff haben.

3.3.1.3. Über geostationäre Fernmeldesatelliten vermittelte Kommunikation[10]

Dezimeter- und Zentimeterwellen lassen sich wie bereits erwähnt sehr gut bündeln zu Richtfunkstrecken. Baut man eine Richtfunkstrecke zu einem stationär in großer Höhe stehenden

[9] U. Freyer, Nachrichtenübertragungstechnik, Hanser Verlag 2000

[10] Hans Dodel, Satellitenkommunikation, Hüthig Verlag 1999

Kommunikationssatelliten auf, der die Richtfunksignale empfängt, umsetzt und wieder zur Erde zurücksendet, so kann man ohne den Einsatz von Kabeln große Entfernungen damit überbrücken. Die Reichweite einer solchen Verbindung ist eigentlich nur dadurch begrenzt, dass der Satellit nicht um die Erdkugel herum empfangen und senden kann. Deshalb setzt man für die weltweite Abdeckung mehrere Satelliten ein (Näheres dazu im Kapitel 4). Wenn ECHELON-Staaten in den notwendigen Regionen der Erde Abhörstationen betreiben, können sie im Prinzip den gesamten über solche Satelliten laufenden Telefon, Fax- und Datenverkehr abhören.

3.3.1.4. Die Abhörmöglichkeiten von Flugzeugen und von Schiffen aus

Es ist seit Langem bekannt, dass Spezialflugzeuge vom Typ AWACS zur weit reichenden Ortung anderer Luftfahrzeuge eingesetzt werden. Das Radar dieser Maschinen wird durch ein Erfassungssystem zur Identifizierung erkannter Ziele, das elektronische Ausstrahlungen orten, klassifizieren und mit Radarkontakten korrelieren kann. Eine separate SIGINT-Fähigkeit ist nicht vorhanden[11]. Dagegen besitzt das langsam fliegende Spionageflugzeug EP-3 der US-Navy Abhörmöglichkeiten für Mikro-, Ultrakurz- und Kurzwellen. Die Signale werden direkt an Bord ausgewertet, das Flugzeug dient rein militärischen Zwecken[12].

Darüber hinaus werden auch Überwasserschiffe und für den landnahen Einsatz U-Boote zum Abhören des militärischen Funkverkehrs eingesetzt[13].

3.3.1.5. Die Abhörmöglichkeiten von Spionagesatelliten aus

Funkwellen strahlen, solange sie nicht mit entsprechenden Antennen gebündelt werden, in alle Richtungen, also auch in den Weltraum. Niedrig umlaufende Signal Intelligence Satelliten können die aufzuklärenden Sender jeweils nur wenige Minuten erfassen. In dicht besiedelten, hoch industrialisierten Gebieten wird das Abhören durch die hohe Dichte von Sendern gleicher Frequenz so erschwert, dass einzelne Signale kaum herausgefiltert werden können.[14] Für die kontinuierliche Überwachung ziviler Funkkommunikation sind diese Satelliten nicht geeignet.
Daneben gibt es hoch (42000 km) positionierte so genannte quasistationäre SIGINT-Satelliten der USA.[15] Im Unterschied zu den geostationären Kommunikationssatelliten haben diese Satelliten eine Inklination von 3 bis 10 Grad, ein Apogee von 39000 bis 42000 km und ein Perigee von 30000 bis 33000 km. Die Satelliten stehen deshalb nicht unbeweglich im Orbit, sondern bewegen sich in einer komplexen eliptischen Bahn. Sie decken deshalb im Laufe eines Tages eine größere Region ab und erlauben das Einpeilen von Funkquellen. Dies und die ansonsten öffentlich zugänglichen Charakteristika der Satelliten weisen auf eine rein militärische Verwendung hin.
Die empfangenen Signale werden mit einer stark auf einen Punkt gebündelten Abwärtsverbindung mit 24 GHz zur Empfangsstation übertragen.

---

[11] Brief des Staatssekretärs im Bundesverteidigungsministerium Walter Kolbow vom 14.2.2001

[12] Süddeutsche Zeitung Nr.80, vom 5.4.2001,S.6

[13] Jeffrey T. Richelson, The U.S. Intelligence Community, Ballinger, New York 1989, S.188 , S.190

[14] Brief des Staatssekretärs im Bundesverteidigungsministerium Walter Kolbow vom 14.2.2001

[15] Major Andronov, Zarubezhnoye voyennoye obozreniye, Nr.12,1993,S.37-43

3.3.2. Möglichkeiten der automatischen Auswertung abgefangener Kommunikation: die Verwendung von Filtern

Beim Abhören von Auslandskommunikation wird nicht gezielt ein Telefonanschluss überwacht. Vielmehr wird sämtliche oder ein Teil der über den überwachten Satelliten oder das überwachte Kabel laufende Kommunikation mitgeschnitten und mit Computern unter Verwendung von Schlüsselbegriffen gefiltert. Denn die Auswertung sämtlicher erfasster Kommunikation ist völlig unmöglich.

Das Herausfiltern von Kommunikation entlang bestimmter Anschlüsse ist einfach. Mit Schlüsselbegriffen können auch Telefaxe und E-Mails spezifisch erfasst werden. Selbst eine bestimmte Stimme kann, wenn das System auf die Stimme trainiert wurde, erfasst werden[16]. Dagegen ist die automatische Erkennung von Wörtern, die von einer beliebigen Stimme gesprochen werden, nach den dem Berichterstatter vorliegenden Erkenntnissen derzeit jedenfalls noch nicht möglich. Die Möglichkeiten des Ausfilterns sind darüber hinaus auch durch andere Faktoren beschränkt: durch die endliche Kapazität der Computer, durch das Sprachenproblem und vor allem durch die begrenzte Zahl von Auswertern, die ausgefilterte Nachrichten lesen und bewerten können.

Bei der Bewertung der Möglichkeiten von Filtersystemen muss auch eingerechnet werden, dass sich die vollen technischen Möglichkeiten eines solchen nach dem „Staubsaugerprinzip“ arbeitenden Abhörsystems auf verschiedene Themen verteilen. Ein Teil der Schlüsselwörter hat mit militärischer Sicherheit zu tun, ein Teil mit Drogenhandel und anderen Formen der internationalen Kriminalität, ein Teil stammt aus der Begriffswelt des Handels mit dual-use Gütern und ein weiterer Teil hat mit dem Einhalten von Embargos zu tun. Ein Teil der Schlüsselbegriffe hat auch mit Wirtschaft zu tun. Das bedeutet, dass sich die Kapazitäten des Systems auf mehrere Bereiche aufspalten. Eine Verengung der Schlüsselwörter nur auf den wirtschaftlich interessanten Bereich widerspräche nicht nur den Anforderungen der politischen Führung an die Dienste, sie ist selbst nach dem Ende des kalten Krieg so nicht vorgenommen worden[17].

3.3.3. Das Beispiel des deutschen Bundesnachrichtendienstes

Die Abteilung 2 des deutschen Bundesnachrichtendienstes beschafft Informationen durch Abhören von Auslandskommunikation. Dies war Gegenstand einer Überprüfung durch das deutsche Verfassungsgericht. Die beim Prozess öffentlich gewordenen Details[18] geben zusammen mit den Ausführungen des Koordinators für die Geheimdienste im Bundeskanzleramt Ernst Uhrlau vor dem ECHELON-Ausschuss am 21.11.2000 einen Eindruck von den nachrichtendienstlichen Möglichkeiten beim Abhören von satellitengestützter Kommunikation.

Die Möglichkeiten anderer Nachrichtendienste mögen aufgrund ihres Rechts auf Zugang zur kabelgebundenen Kommunikation oder aufgrund von mehr Auswertpersonal im Detail da oder dort größer sein. Insbesondere erhöht sich bei der Einbeziehung der kabelgebundenen Verkehre die statistische Trefferwahrscheinlichkeit, nicht unbedingt aber die Zahl der auswertbaren Verkehre. Im Grunde wird am Beispiel des BND für den Berichterstatter exemplarisch sichtbar,

[16] Privatmitteilung an den Berichterstatter, Quelle geschützt

[17] Privatmitteilung an den Berichterstatter, Quelle geschützt

[18] BVerfG, 1 BvR 2226/94 vom 14.7.1999, Absatz 1

welche Möglichkeiten und Strategien Auslandsnachrichtendienste bei der Verfolgung von Auslandskommunikation haben, auch wenn sie dies nicht offen legen.

Der Bundesnachrichtendienst versucht mit **strategischer** Fernmeldekontrolle Informationen aus dem Ausland über das Ausland zu beschaffen. Dazu werden mit einer Reihe von Suchbegriffen (die in Deutschland von der so genannten G10-Kommission[19] vorher genehmigt werden müssen) Satellitenverkehre abgegriffen. Das Mengengerüst stellt sich so dar (Stand Jahr 2000): von den rund 10 Millionen internationalen Kommunikationsverbindungen/Tag, die von und nach Deutschland stattfinden, werden etwa 800.000 über Satellit abgewickelt. Davon werden knapp 10% (75.000) über eine Suchmaschine gefiltert. Diese Beschränkung ergibt sich nach Meinung des Berichterstatters nicht aus dem Gesetz (theoretisch wären zumindest vor dem Prozess vor dem Verfassungsgericht 100% erlaubt gewesen), sondern technisch aus anderen Beschränkungen, z.B. der limitierten Auswertungskapazität.

Auch die Zahl der handhabbaren Suchbegriffe ist technisch und durch den Genehmigungsvorbehalt begrenzt. In der Begründung zum Urteil des Bundesverfassungsgerichts ist neben den rein formalen Suchbegriffen (Anschlüsse von Ausländern oder ausländischen Firmen im Ausland) von 2.000 Suchbegriffen im Bereich der Proliferation, 1.000 Suchbegriffen im Bereich des Rüstungshandels, 500 Suchbegriffen im Bereich des Terrorismus und 400 Suchbegriffen im Bereich des Drogenhandels die Rede. Bei Terrorismus und Drogenhandel hat sich das Verfahren allerdings als nicht sehr erfolgreich erwiesen.

Die Suchmaschine prüft, ob bei Telefax und Telex genehmigte Suchbegriffe getroffen werden. Eine automatische Worterkennung bei Sprachverbindungen ist derzeit nicht möglich. Werden die Suchbegriffe nicht getroffen, fallen die Meldungen automatisch technisch in den Papierkorb; sie dürfen nicht ausgewertet werden, weil es dafür keine Rechtsgrundlage gibt. Täglich fallen etwa 5 Kommunikationen von Teilnehmern am Fernmeldeverkehr an, die unter den Schutz der deutschen Verfassung fallen. Die strategische Aufklärung des Bundesnachrichtendienstes ist darauf gerichtet, Mosaiksteine zu finden als Anhaltspunkte für eine weitere Aufklärung . Sie hat keine absolute Überwachung der Auslandskommunikation als Zielsetzung. Nach den dem Berichterstatter vorliegenden Erkenntnissen gilt dies auch für die SIGINT-Tätigkeit anderer Auslandsnachrichtendienste.

[19] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10 GG) vom 13.8.1968

4. Die Technik für satellitengestützte Kommunikation

4.1. Die Bedeutung von Kommunikationssatelliten

Kommunikationssatelliten bilden heute ein unverzichtbares Element des globalen Fernmeldenetzes und der Versorgung mit Fernseh- und Radioprogrammen sowie multimedialen Diensten. Trotzdem hat der Anteil der Satellitenverkehre an der internationalen Kommunikation in den vergangenen Jahren in Mitteleuropa stark abgenommen. In manchen Regionen liegt er heute sogar unter 10 % [20]. Dies hängt mit den Vorteilen der optischen Glasfaserkabel zusammen, die ungleich mehr an Verkehr bei höherer Verbindungsqualität aufnehmen können.

Kommunikation findet heutzutage auch im Sprachbereich digital statt. Die Kapazität von über Satelliten geführten digitalen Verbindungen beschränkt sich pro Transponder am Satelliten auf **1890** Sprachkanäle mit ISDN-Standard (64 kbits/sec). Demgegenüber können heute auf einer einzigen Glasfaser bereits **241920** Sprachkanäle mit dem gleichen Standard übertragen werden. Das entspricht einem Verhältnis von **1:128**!

Dazu kommt, dass die Qualität von Verbindungen über Satellit geringer ist als die über Glasfaser-Seekabel. Die Qualitätseinbußen aufgrund der langen Laufzeiten der Signale von mehreren hundert Millisekunden machen sich bei normaler Sprachübertragung kaum bemerkbar – obwohl man es hören kann. Bei Daten- und Telefaxverbindungen, die über ein kompliziertes „handshaking Verfahren" abgewickelt werden, hat das Kabel bei der Verbindungssicherheit klare Vorteile. Gleichzeitig sind allerdings an das globale Kabelnetz nur 15 % der Weltbevölkerung angeschlossen [21].

Bei bestimmten Anwendungen werden daher Satellitensysteme trotzdem auf Dauer vorteilhafter sein als Kabel. Einige Beispiele aus dem zivilen Bereich seien genannt:

- Nationale, regionale und internationale Telefon- und Datenverkehre in Gebieten mit geringem Kommunikationsaufkommen, d.h. dort, wo sich die Realisierung einer Kabelverbindung mangels Auslastung nicht lohnen würde.

- Zeitbegrenzte Kommunikation bei Katastropheneinsätzen, Veranstaltungen, Großbaustellen etc.

- UNO-Missionen in Regionen mit unterentwickelter Kommunikationsinfrastruktur

- Flexible/mobile Wirtschaftskommunikation mit Kleinsterdfunkstellen (V-SATs, s.u.)

Dieses Einsatzspektrum von Satelliten in der Kommunikation ergibt sich aus folgenden Eigenschaften: Die Abstrahlung eines einzigen geostationären Satelliten kann fast 50% der Erdoberfläche überdecken; auch unwegsames Gelände kann überbrückt werden. In diesem Gebiet werden dann 100% der Benutzer, egal ob zu Land, zur See oder in der Luft abgedeckt.

[20] Siehe Begründung zur Änderung des G10-Gesetzes in Deutschland

[21] Homepage der Deutschen Telekom: www.detesat.com/deutsch/

Satelliten sind in wenigen Monaten betriebsbereit unabhängig von der Infrastruktur vor Ort, sie sind zuverlässiger als Kabel und können müheloser abgelöst werden.

Negativ sind folgende Eigenschaften von satellitengestützter Kommunikation zu bewerten: die relativ langen Signallaufzeiten, die Ausbreitungsdegradation, die im Vergleich zum Kabel kürzere Lebensdauer von 12 bis 15 Jahren, die größere Verletzbarkeit sowie die leichte Abhörbarkeit.

4.2. Die Funktionsweise einer Satellitenverbindung

Mikrowellen lassen sich, wie bereits erwähnt (siehe Kapitel 3), mit entsprechenden Antennen gut eng bündeln. Deshalb kann man Kabel durch Richtfunkstrecken ersetzen. Stehen Sende- und Empfangsantenne nicht auf einer Ebene, sondern wie im Falle der Erde auf der Oberfläche einer Kugel, dann „verschwindet" die Empfangsantenne wegen der Krümmung ab einer bestimmten Entfernung unter dem Horizont. Die beiden Antennen „sehen" sich dann nicht mehr. Dies wäre zum Beispiel auch bei einer interkontinentalen Richtfunkstrecke zwischen Europa und den USA der Fall. Die Antennen müssten auf 1,8 km hohen Masten stehen, damit sie eine Verbindung herstellen könnten. Schon deshalb ist eine solche interkontinentale Richtfunkstrecke nicht realisierbar; von der Dämpfung des Signals durch Luft und Wasserdampf über die Strecke hinweg ganz abgesehen. Gelingt es hingegen, in großer Höhe im Weltraum an einer „festen Position" eine Art Spiegel für die Richtfunkstrecke einzurichten, dann können trotz der Erdkrümmung große Entfernungen überwunden werden, genauso wie man mit einem Verkehrsspiegel um die Ecke sehen kann. Das soeben beschriebene Prinzip wird mit dem Einsatz von so genannten geostationären Satelliten realisiert.

4.2.1. Geostationäre Satelliten

Lässt man einen Satelliten parallel zum Äquator in einer kreisförmigen Bahn in 24 Stunden einmal die Erde umkreisen, so folgt er exakt der Erdumdrehung. Von der Erdoberfläche aus gesehen steht er dann in 36000 km Höhe still – er hat eine **geostationäre** Position. Zu diesem Typ von Satelliten gehören die meisten der Kommunikations- und Fernsehsatelliten

4.2.2. Der Signalweg einer Satellitenkommunikationsverbindung

Die Übertragung von Signalen über Satelliten lässt sich so beschreiben:

Das von einer Leitung kommende Signal wird von einer Erdfunkstelle mit einer Parabolantenne über eine aufwärts gerichtete Richtfunkstreckenverbindung, den so genannten **uplink**, zum Satelliten gesendet. Der Satellit empfängt das Signal, verstärkt es und sendet es über eine abwärts gerichtete Richtfunkstreckenverbindung, den so genannten **downlink,** zurück zu einer anderen Erdfunkstelle. Von dort geht das Signal dann wieder zurück in ein Kabelnetz.

Bei der Mobilkommunikation wird das Signal direkt von der mobilen Kommunikationseinheit zum Satelliten übertragen und kann von dort aus über eine Erdfunkstelle wieder in eine Leitung eingespeist, oder aber direkt wieder auf eine weitere mobile Einheit übertragen werden.

4.2.3. Die wichtigsten existierenden Satellitenkommunikationssysteme

Die aus den **öffentlich zugänglichen Kabelnetzen** (nicht unbedingt staatlichen) stammende Kommunikation wird gegebenenfalls über Satellitensysteme unterschiedlicher Ausdehnung von

und zu ortsfesten Erdfunkstellen übertragen und dann wieder in Kabelnetze eingespeist. Man unterscheidet:

- globale (z.B. INTELSAT)

- regionale (kontinentale) (z.B. EUTELSAT)

- nationale (z.B. ITALSAT)

Satellitensysteme.

Die meisten dieser Satelliten befinden sich in einer geostationären Position; weltweit betreiben dort 120 private Gesellschaften ca. 1000 Satelliten[22].

Daneben gibt es für den hohen Norden umlaufende Satelliten mit einer hochexzentrischen Spezialumlaufbahn (russische Molnyiabahnen), bei der die Satelliten zur Hälfte ihrer Umlaufzeit für den Nutzer im hohen Norden sichtbar sind. Mit zwei Satelliten wird so eine regionale Bedeckung erreicht, die von einer geostationären Position über dem Äquator nicht zu realisieren ist.

Darüber hinaus gibt es mit dem global arbeitenden INMARSAT-System ein - ursprünglich für den Gebrauch auf See geschaffenes - **Mobilkommunikationssystem**, mit dem überall auf der Welt satellitengestützte Verbindungen hergestellt werden können. Es arbeitet ebenfalls mit geostationären Satelliten.

Das auf der Basis von mehreren zeitversetzt in niedrigen Bahnen umlaufenden Satelliten weltweit operierende Satellitenhandy-System namens IRIDIUM hat vor kurzem aus wirtschaftlichen Gründen mangels Auslastung seinen Betrieb eingestellt.

Außerdem existiert ein sich rasch entwickelnder Markt für so genannte VSAT-Verbindungen (VSAT = very small aperture terminal). Dabei geht es um Kleinsterdfunkstellen mit Antennen von Durchmessern zwischen 0,9 und 3,7 m, die von Firmen für ihren Bedarf (z.B. Videokonferenzen) oder von mobilen Dienstanbietern für zeitlich begrenzten Verbindungsbedarf (z.B. Tagungen) betrieben werden. 1996 waren 200.000 Kleinsterdfunkstellen weltweit in Betrieb. Die Volkswagen AG betreibt 3.000, Renault 4.000, General Motors 100.000 und der größte europäische Mineralölkonzern 12.000 VSAT-Einheiten. Die Kommunikation wird, wenn der Kunde nicht selbst für Verschlüsselung sorgt, offen abgewickelt[23].

4.2.3.1. Global arbeitende Satellitensysteme

Diese Satellitensysteme decken durch die Verteilung von mehreren Satelliten im atlantischen, indischen und pazifischen Bereich den gesamten Globus ab.

[22] G. Thaller, Satelliten im Erdorbit, Franzisverlag, München 1999

[23] H. Dodel, Privatmitteilung

INTELSAT[24]

INTELSAT (International Telecomunications Satellite Organisation) wurde 1964 als eine Behörde gegründet mit einer Organisationsstruktur ähnlich der UN und dem Geschäftszweck, internationale Kommunikation zu betreiben. Mitglieder waren nationale Postgesellschaften in Regierungsbesitz. Heute sind 144 Regierungen INTELSAT-Mitglieder. Im Jahr 2001 wird INTELSAT privatisiert.

Mittlerweile unterhält INTELSAT eine Flotte von 19 geostationären Satelliten, die mehr als 200 Länder verbinden, und deren Leistungen an die Mitglieder von INTELSAT vermietet werden. Die Mitglieder unterhalten ihre eigenen Bodenstationen. Durch INTELSAT Business Service (IBS) können seit 1984 auch Nichtmitglieder (z.B. Telefongesellschaften, große Firmen, internationale Konzerne) die Satelliten benützen. INTELSAT bietet global Dienstleistungen für verschiedene Dienste wie Kommunikation, Fernsehen etc. an. Die Telekommunikationsübertragung erfolgt im C- und Ku-Band (siehe unten).

INTELSAT-Satelliten sind die wichtigsten internationalen Kommunikationssatelliten. Über sie wird der größte Teil der satellitengetragenen internationalen Kommunikation abgewickelt.
Die Satelliten decken den atlantischen, indischen und pazifischen Bereich ab (siehe Tabelle, Kapitel 5, 5.3).

Über dem Atlantik stehen zwischen 304°E und 359°E 10 Satelliten, den indischen Bereich decken 6 Satelliten zwischen 62°E und 110,5°E ab, den pazifischen Raum 3 Satelliten zwischen 174°E und 180°E. Durch mehrere Einzelsatelliten im atlantischen Bereich wird das dortige hohe Verkehrsaufkommen abgedeckt.

INTERSPUTNIK[25]

1971 wurde die internationale Satellitenkommunikationsorganisation INTERSPUTNIK von 9 Ländern als Agentur der ehemaligen Sowjetunion mit einer Aufgabe ähnlich INTELSAT gegründet. Heute ist INTERSPUTNIK eine intergovernmentale Organisation, deren Mitglieder Regierungen eines jeden Staates sein können. Sie hat inzwischen 24 Mitgliedstaaten (u.a. Deutschland) und ca. 40 Nutzer (u.a. Frankreich und England), die durch ihre Postverwaltungen bzw. Telekoms vertreten sind. Ihr Sitz ist in Moskau.

Die Telekommunikationsübertragung erfolgt im C- und Ku-Band (siehe unten).

Durch die Satelliten (Gorizont, Express, Express A der russischen Föderation und LMI-1 aus dem Lockhead-Martin Joint venture), wird ebenfalls der gesamte Globus abgedeckt: im atlantischen Bereich steht 1 Satellit, ein zweiter ist geplant, im indischen Bereich stehen 3 Satelliten , im pazifischen Bereich 2 (siehe Tabelle, Kapitel 5, 5.3).

INMARSAT

INMARSAT (Interim International Maritime Satellite) stellt seit 1979 mit seinem Satellitensystem weltweit **mobile** Kommunikation zur See, in der Luft und zu Lande sowie ein Notfunksystem zur Verfügung. Entstanden ist INMARSAT aus einer Initiative der „International

[24] INTELSAT-Homepage http://www.intelsat.com

[25] Homepage von INTERSPUTNIK: http://www.intersputnik.com

Maritime Organisation“ als zwischenstaatliche Organisation. Inzwischen ist INMARSAT privatisiert und hat seinen Sitz in London.

Das INMARSAT-System besteht aus neun Satelliten in geostationären Umlaufbahnen. Vier der Satelliten – die INMARSAT-III Generation - decken bis auf die extremen Pol-Gebiete den gesamten Globus ab. Jeder Einzelne deckt etwa 1/3 der Erdoberfläche ab. Durch ihre Positionierung in den vier Ozean-Regionen (West-, Ost Atlantik, Pazifik, Indischer Ozean) kommt es zu der globalen Abdeckung. Gleichzeitig hat jeder INMARSAT auch eine Anzahl von „Spot-Beams“, was die Bündelung der Energie in Gebieten mit größerem Kommunikationsverkehr ermöglicht.

Die Telekommunikationsübertragung erfolgt im L- und Ku-Band (siehe unten 4.2.4).

4.2.3.2. Regionale Satellitensysteme

Durch die Ausleuchtzonen regionaler Satellitensysteme werden einzelne Regionen/Kontinente abgedeckt. Die durch sie übertragene Kommunikation kann folglich nur innerhalb dieser Regionen empfangen werden.

EUTELSAT[26]

EUTELSAT wurde 1977 von 17 Postverwaltungen Europas gegründet mit dem Ziel Europas spezifische Erfordernisse in der Satellitenkommunikation abzudecken und die europäische Raumfahrt-Industrie zu unterstützen. Es hat seinen Sitz in Paris und ca. 40 Mitgliedstaaten. Im Jahr 2001 soll EUTELSAT privatisiert werden.

EUTELSAT betreibt 18 geostationäre Satelliten, die Europa, Afrika und große Teile Asiens abdecken und eine Verbindung zu Amerika herstellen. Die Satelliten stehen zwischen 12,5°W und 48°E. EUTELSAT bietet hauptsächlich Fernsehen (850 digitale und analoge Kanäle) und Radio (520 Kanäle) an, dient aber darüber hinaus auch der Kommunikation – in erster Linie innerhalb Europas (einschließlich Russland): z.B. für Videokonferenzen, für private Netzwerke großer Unternehmen (u.a. General Motors, Fiat), für Presseagenturen (Reuters, AFP), für Anbieter von Finanzdaten sowie für mobile Dienste von Datenübertragung.
Die Telekommunikationsübertragung erfolgt im Ku-Band.

ARABSAT[27]

ARABSAT ist das Pendant zu EUTELSAT in der arabischen Region, gegründet 1976. Mitglieder sind 21 arabische Länder. ARABSAT-Satelliten werden sowohl zur Übertragung von Fernsehen als auch zur Kommunikation benützt.

Die Telekommunikationsübertragung erfolgt hauptsächlich im C-Band.

[26] Homepage von EUTELSAT: http://www.com

[27] Homepage von ARABSAT: http://www.arabsat.

PALAPA[28]

Das indonesische PALAPA-System ist seit 1995 in Betrieb und das südasiatische Pendant zu EUTELSAT. Es deckt durch seine Ausleuchtzone Malaysia, China, Japan, Indien, Pakistan und andere Länder der Region ab.

Die Telekommunikationsübertragung erfolgt im C- und Ku-Band.

4.2.3.3. Nationale Satellitensysteme[29]

Viele Staaten nutzen für die Abdeckung nationaler Anforderungen eigene Satellitensysteme mit begrenzten Ausleuchtzonen.

Der französische Fernmeldesatellit **TELECOM**, dient unter anderem dazu, die französischen Departments in Afrika und Südamerika mit dem Mutterland zu verbinden. Die Telekommunikationsübertragung erfolgt im C- und Ku-Band.

ITALSAT betreibt Fernmeldesatelliten, die mit nacheinander gelegten, eingegrenzten Ausleuchtzonen den gesamten italienischen Stiefel abdecken. Ein Empfang ist daher nur in Italien möglich. Die Telekommunikationsübertragung erfolgt im Ku-Band.

AMOS ist ein israelischer Satellit für hauptsächlich ortsfeste Kommunikation, dessen Footprint den Mittleren Osten abdenkt. Die Telekommunikationsübertragung erfolgt im Ku-Band.

Die spanischen Satelliten **HISPASAT** decken Spanien und Portugal ab (Ku-Spots) und transportieren spanische Fernsehprogramme nach Nord- und Südamerika.

4.2.4. Die Zuteilung von Frequenzen

Für die Verteilung von Frequenzen ist die International Telecommunication Union zuständig. Um gewisse Ordnung zu schaffen, wurde die Welt für Zwecke der Funkkommunikation in drei Regionen aufgeteilt:

1. Europa, Afrika, ehem. Sowjetunion, Mongolei

2. Nord- und Südamerika sowie Grönland

3. Asien außer Länder in Region 1, Australien und südlicher Pazifik

Diese historisch gewachsene Einteilung wurde für Zwecke der Satellitenkommunikation übernommen und führt zu einer Häufung von Satelliten in bestimmten geostationären Zonen.

Die wichtigsten Frequenzbänder für Satellitenkommunikation sind:

- das L-Band (0.4 - 1.6 GHz) für mobile Satellitenkommunikation, z.B. über INMARSAT.
- das C-Band (3,6 - 6,6 GHz) für Erdfunkstellen, z.B. über INTELSAT

[28] H.Dodel, Satellitenkommunikation, Hüthigverlag 1999

[29] H.Dodel und Internetrecherchen

- das Ku-Band (10 - 20GHz) für Erdfunkstellen, z.B. INTELSAT-Ku-Spot und EUTELSAT

- das Ka-Band (20 - 46 GHz) Erdfunkstellen, z.B. über nationale Satelliten wie ITALSAT

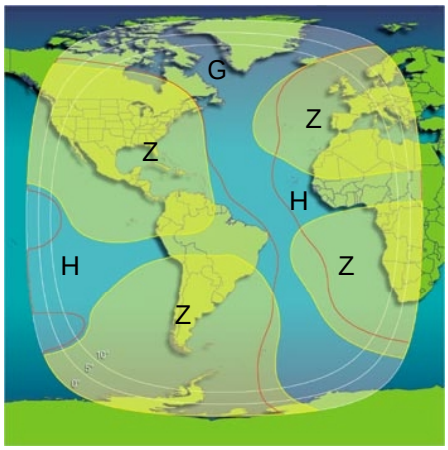
- das V-Band (46 – 56 GHz) für Kleinsterdfunkstellen (V-SATs)

4.2.5. Ausleuchtzonen der Satelliten (footprints)

Als Ausleuchtzone oder „Footprint“ bezeichnet man das Gebiet auf der Erde, das von der Satellitenantenne ausgeleuchtet wird. Sie kann sich auf bis zu 50 % der Erdoberfläche erstrecken oder durch Bündelung des Signals bis hin zu kleinen, regional begrenzten Spots begrenzt sein.

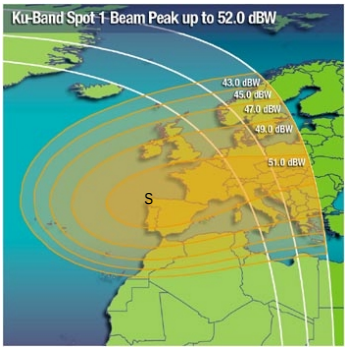
Je höher die Frequenz des abgestrahlten Signals ist, desto stärker lässt es sich bündeln, und desto kleiner wird demnach die Ausleuchtzone. Durch eine Bündelung des ausgestrahlten Satellitensignals auf kleinere Ausleuchtzonen kann die Energie des Signals erhöht werden. Je kleiner die Ausleuchtzone, desto stärker kann das Signal sein und desto kleiner können folglich die Empfangsantennen sein.

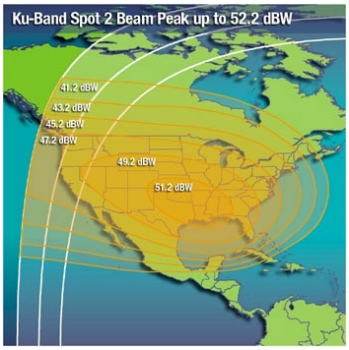
Für die INTELSAT-Satelliten sei dies kurz genauer dargestellt:

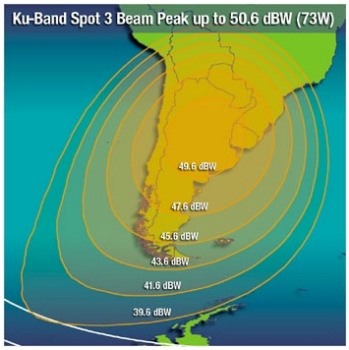


Die Ausleuchtzonen der INTELSAT-Satelliten sind in verschiedene Beams unterteilt:

Der Global-Beam (G) eines jeden Satelliten deckt etwa ein Drittel der Erdoberfläche ab, die Hemi-Beams (H) decken jeweils eine Fläche ab, die etwas kleiner ist als die Hälfte des Global-Beams. Zone-Beams (Z) sind Spots in bestimmte Zonen der Erde; sie sind kleiner als die Hemi-Beams. Darüber hinaus gibt es noch so genannte Spot-Beams; das sind präzise, kleine Footprints (s.u.).







Die Frequenzen des C-Band findet man in den Global-, Hemi- sowie Zone-Beams. In den Spot-Beams befinden sich die Frequenzen des Ku-Bands.

4.2.6. Die für eine Erdfunkstelle notwendigen Antennengrößen

Als Empfangsantennen auf der Erde werden Parabolantennen verwendet. Der Parabolspiegel reflektiert alle einfallenden Wellen und bündelt sie in seinem Brennpunkt. Im Brennpunkt befindet sich dann das eigentliche Empfangssystem. Je größer die Energie des Signals am Ort des Empfangs ist, desto kleiner kann der Durchmesser der Parabolantenne sein.

Für den Zweck der mit diesem Bericht durchgeführten Untersuchung ist entscheidend, dass ein Teil der interkontinentalen Kommunikation über das C-Band in den Global-Beams der INTELSAT-Satelliten und anderer Satelliten (z.B. INTERSPUTNIK) läuft, für dessen Empfang teilweise Satellitenschüsseln mit Durchmessern von ca. 30 m benötigt werden (siehe Kapitel 5). 30m-Antennen waren auch die für die ersten Abhörstationen von Kommunikationssatelliten notwendig, da die erste INTELSAT-Generation nur Global-Beams hatte und die Signalübertragung noch weit weniger ausgereift war, als sie das heute ist. Diese Schüsseln mit Durchmessern von zum Teil mehr als 30 m werden an den entsprechenden Stationen noch genutzt, auch wenn sie technisch nicht mehr notwendig sind.

Die typischen Antennen, die für INTELSAT-Kommunikation im C-Band heute benötigt werden, haben einen Durchmesser von 13 bis 18 m. Vereinzelt (z.B. bei INTELSAT 511) wird für den Global-Beam eine größere Antenne benötigt. Bei den neuesten INTELSAT-Satelliten reichen auch für das Zone-Beams des C-Bands Antennen mit einem Durchmesser bis 5m.
Für den Empfang der C-Band-Kommunikation von Intersputnik werden Antennen im Bereich von 2 bis 25 m Durchmesser benötigt.

Für die Ku-Spots der INTELSAT-Satelliten aber auch anderer Satelliten (EUTELSAT-KU-Band, AMOS Ku-Band etc.) werden Antennen im Bereich von 2 bis 10 m Durchmesser benötigt.

Für Kleinsterdfunkstellen, die im V-Band arbeiten und deren Signal aufgrund der hohen Frequenz noch stärker als im Ku-Band gebündelt werden kann, reichen Antennendurchmesser von 0,9-3,7 m (z.B. VSATs von EUTELSAT oder INMARSAT).

5. Der Indizienbeweis für die Existenz von mindest einem globalen Abhörsystem

5.1. Warum ein Indizienbeweis?

Geheimdienste legen naturgemäß Details ihrer Arbeit nicht offen. Es gibt deshalb jedenfalls keine offizielle Erklärung der Auslandsnachrichtendienste der ECHELON-Staaten, dass sie in Zusammenarbeit ein globales Abhörsystem betreiben. Ein Nachweis muss deshalb über das Sammeln möglichst vieler Indizien, die sich zu einem überzeugenden Indizienbeweis verdichten, gefunden werden.

Die Indizienkette für einen solchen Nachweis setzt sich aus drei Elementen zusammen:

- dem Nachweis, dass die Auslandsnachrichtendienste in den ECHELON-Staaten private und geschäftliche Kommunikation abhören.
- dem Nachweis, dass in den aufgrund der Funktionsweise des zivilen Kommunikationssatellitensystems notwendigen Teilen der Erde Abhörstationen auffindbar sind, die von einem der ECHELON-Staaten betrieben werden.
- dem Nachweis, dass es einen nachrichtendienstlichen Verbund zwischen diesen Staaten gibt, der über den Rahmen des Üblichen weit hinaus geht. Ob dies soweit geht, dass von Partnern Abhöraufträge angenommen und diesen dann das abgefangene Rohmaterial ohne eigene Auswertung direkt zugeleitet wird, ist für den Beweis der Existenz eines Verbunds unerheblich. Diese Frage spielt nur dann eine Rolle, wenn es um die Aufklärung von Hierarchien innerhalb eines solchen Abhörverbunds geht.

5.1.1. Der Nachweis der Abhörtätigkeit von Auslandsnachrichtendiensten

Zumindest in Demokratien arbeiten Nachrichtendienste auf der Grundlage von Gesetzen, die ihren Zweck und/oder ihre Vollmachten beschreiben. Es lässt sich deshalb einfach beweisen, dass es in vielen dieser Staaten Auslandsnachrichtendienste gibt, die zivile Kommunikation abhören. Dies gilt auch für die fünf sogenannten ECHELON-Staaten, die alle solche Dienste unterhalten. Bei jedem einzelnen dieser Staaten bedarf es keines besonderen zusätzlichen Beweises, dass sie ins Land und aus dem Land gehende Kommunikation abhören. Vom eigenen Territorium aus lassen sich bei Satellitenkommunikation auch ein Teil der Nachrichtenverkehre abgreifen, die für Empfänger im Ausland bestimmt sind. Es gibt in allen fünf ECHELON-Staaten für die Dienste keinerlei rechtliche Beschränkung, dies nicht zu tun. Die innere Logik der Methode der strategischen Kontrolle des Auslandsfernmeldeverkehrs und ihr zumindest zum Teil veröffentlichter Zweck lassen es als zwingend erscheinen, dass die Dienste dies auch so handhaben.[30]

[30] Der Berichterstatter hat Informationen, dass dies zutrifft. Quelle ist geschützt.

5.1.2. Der Nachweis der Existenz von Stationen in den geografisch notwendigen Bereichen

Die einzige Beschränkung für den Versuch, weltweit eine Überwachung der durch Satelliten gestützten Kommunikation aufzubauen, ergibt sich aus der Technik eben dieser Kommunikation. Es gibt keinen Ort, von dem aus sich **alle** Satellitenverkehre weltweit erfassen lassen (siehe Kapitel 4, 4.2.5).

Ein global arbeitendes Abhörsystem könnte unter drei Voraussetzungen aufgebaut werden:

- der Betreiber hat in allen dafür notwendigen Teilen der Welt eigenes Staatsterritorium
- der Betreiber hat in allen dafür notwendigen Teilen der Welt teilweise eigenes Territorium und ergänzend ein Gastrecht in den fehlenden Teilen der Welt und darf dort Stationen betreiben oder mitbenützen.
- der Betreiber ist ein nachrichtendienstlicher Verbund von Staaten und betreibt das System in den dafür notwendigen Teilen der Welt.

Keiner der ECHELON-Staaten könnte allein ein globales System betreiben. Die USA haben zumindest formal keine Kolonien. Kanada, Australien und Neuseeland haben ebenfalls kein Staatsterritorium außerhalb des Landes im engeren Sinne. Auch das Vereinigte Königreich könnte für sich alleine kein globales Abhörsystem betreiben (siehe Kapitel 6).

5.1.3. Der Nachweis eines engen nachrichtendienstlichen Verbundes

Nicht offengelegt ist dagegen, ob und wie die ECHELON-Staaten im Nachrichtendienstbereich miteinander zusammenarbeiten. Üblicherweise erfolgt eine Zusammenarbeit der Dienste bilateral und auf der Basis des Austausches von ausgewertetem Material. Ein multilateraler Verbund ist bereits etwas sehr Ungewöhnliches; wenn dann noch der regelmäßige Austausch von Rohmaterial hinzukommt, dann entsteht eine völlig neue Qualität. Ein Verbund dieser Art kann nur mit Indizien nachgewiesen werden.

5.2. Wie erkennt man eine Abhörstation für Satellitenkommunikation?

5.2.1. Kriterium 1: die Zugänglichkeit der Anlage

Mit großen Antennen ausgestattete Anlagen der Post, des Rundfunks oder von Forschungseinrichtungen sind zumindest nach Anmeldung für Besucher zugänglich, Abhörstationen dagegen nicht. Sie werden meist formal vom Militär betrieben, das dann auch technisch das Abhören vornimmt. So wickeln für die NSA z.B. die Naval Security Group (NAVSECGRU) oder die Air Intelligence Agency der US Airforce (AIA) den Stationsbetrieb ab. Bei britischen Stationen betreibt die britische Royal Airforce für den britischen Nachrichtendienst GCHQ die Anlagen. Dieses Arrangement erlaubt eine militärisch scharfe Bewachung der Anlage und dient gleichzeitig der Verschleierung.

5.2.2. Kriterium 2: die Art der Antenne

In Anlagen, die das Kriterium 1 erfüllen, kann man verschiedene Typen von Antennen finden, die sich charakteristisch in ihrer Gestalt unterscheiden. Ihre Form gibt Auskunft über den Zweck der Abhöranlage. So werden Anordnungen hoher Stabantennen zu einem Ring mit großem

Durchmesser (sog. Wullenweberantennen) zur Richtungspeilung von Funksignalen verwendet. Ebenfalls ringförmige Anordnungen von rhombisch geformten Antennen (sog. Pusherantennen) dienen dem gleichen Zweck. Antennen zum Empfang aus allen Richtungen oder Richtantennen, die wie riesige klassische Fernsehantennen aussehen, dienen dem Abhören von ungerichteten Funksignalen. **Zum Empfang von Satellitensignalen verwendet man dagegen ausschließlich Parabolantennen**. Wenn die Parabolantennen offen im Gelände stehen, dann kann man in Kenntnis ihres Standortes, ihres Neigungswinkels (Elevation) und ihres Kompasswinkels (Azimut) berechnen, welcher Satellit empfangen wird. Dies wäre z.B. in Morwenstow (UK) oder in Yakima (USA) und Sugar Grove (USA) möglich. Meist sind die Parabolantennen aber unter kugelförmigen weißen Hüllen, den sogenannten Radomen, verborgen. Sie dienen dem Schutz der Antennen, aber auch der Tarnung ihrer Ausrichtung.

Finden sich Parabolantennen oder Radome auf dem Gelände einer Abhörstation, so werden dort mit Sicherheit Signale von Satelliten empfangen. Allerdings ist damit noch nicht geklärt, um welche Art von Signalen es sich dabei handelt.

5.2.3. Kriterium 3: die Antennengröße

Satellitenempfangsantennen in einer Kriterium-1-Anlage können verschiedene Zwecke erfüllen:
- Empfangsstationen für militärische Kommunikation
- Empfangsstationen für Spionagesatelliten (Bilder, Radar)
- Empfangsstationen für militärische SIGINT-Satelliten
- Empfangsstationen zum Abhören ziviler Kommunikationssatelliten

Von außen sieht man den Antennen/Radomen nicht an, welcher Aufgabe sie dienen. Allerdings gibt es technisch bedingte Mindestgrößen für Antennen, die den sogenannten „global beam“ im C-Band der auf Satelliten gestützten zivilen internationalen Kommunikation empfangen wollen. Bei der ersten Generation dieser Satelliten waren Antennen eines Durchmessers von etwa 25 m bis 30 m erforderlich, heute reichen 15 m bis 18 m Durchmesser. Die automatische Filterung der abgefangenen Signale durch Computer erfordert eine möglichst gute Signalqualität, deshalb wählt man für nachrichtendienstliche Zwecke die Antennengröße am oberen Ende des Bereichs. Weil die Antennen auf Ständern montiert sind, sind die Durchmesser der Radome noch größer als die Durchmesser der Antennen.

5.2.4. Schlussfolgerung

Nach Kenntnis des Berichterstatters gibt es keinerlei militärische Anwendungen für Antennen dieser Größe. Werden sie deshalb auf einem Kriterium-1-Gelände festgestellt, dann wird dort zivile Satellitenkommunikation abgehört.

5.3. Öffentlich zugängliche Befunde über bekannte Abhörstationen

5.3.1. Methode

Um festzustellen, welche Stationen den in Kapitel 5.2. genannten Kriterien genügen und Teil des weltweiten Abhörsystems sind und welche Aufgaben sie haben, wurden die einschlägige, z.T. widersprüchliche Literatur (Hager[31], Richelson[32], Campbell[33]), deklassifizierte Dokumente[34], die

[31] Hager, Nicky: EXPOSING THE GLOBAL SURVEILLANCE SYSTEM http://www.ncoic.com/echelon1.htm
Hager, Nicky: Secret Power. New Zealands´s Role in the international Spy Network, New Zealand 1996

Homepage der Federation of American Scientists[35] sowie Homepages der Betreiber[36] (NSA, AIA, u.a.) und andere Internet-Veröffentlichungen ausgewertet. Darüber hinaus wurden die Ausleuchtzonen der Kommunikationssatelliten zusammengetragen, die notwendigen Antennengrößen berechnet, und zusammen mit den möglichen Stationen in Weltkarten eingetragen.

5.3.2. Genaue Analyse

Für die Auswertung gelten die folgenden mit der Physik der Satellitenkommunikation zusammenhängenden Prinzipien (siehe auch Kapitel 4):

- Eine Satellitenantenne kann immer nur das erfassen, was sich innerhalb derjenigen Ausleuchtzone befindet, in der sie steht. Um Kommunikation, die hauptsächlich im C- und Ku-Band läuft, empfangen zu können, muss eine Antenne innerhalb der Ausleuchtzonen liegen, die das C- bzw. Ku-Band enthalten.
- Für jeden Global-Beam ist eine Satellitenantenne notwendig, auch wenn sich die Beams zweier Satelliten überlappen.
- Hat ein Satellit mehr Ausleuchtzonen als nur den Global-Beam, was für die heutigen Satellitengenerationen charakteristisch ist, kann mit einer einzigen Satellitenantenne nicht mehr die gesamte über diesen Satelliten laufende Kommunikation erfasst werden, da eine einzige Satellitenantenne nicht in allen Ausleuchtzonen des Satelliten stehen kann. Für die Erfassung der Hemi-Beams und des Global-Beams eines Satelliten sind also zwei Satellitenantennen in verschiedenen Gebieten notwendig (siehe Darstellung der Ausleuchtzonen in Kapitel 4). Kommen weitere Beams (Zone- und Spotbeams) dazu, sind weitere Satellitenantennen notwendig. Verschiedene sich überlappende Beams eines Satelliten können allerdings von einer Satellitenantenne erfasst werden, da es technisch möglich ist, verschiedene Frequenzbänder beim Empfang zu trennen.

Darüber hinaus gelten die in Kapitel 5.2. genannten Voraussetzungen: die Nicht-Zugänglichkeit der Anlagen, da sie vom Militär betrieben werden[37], dass für den Empfang von Satellitensignalen Parabolantennen notwendig sind und dass die Größe der Satellitenantennen zur Erfassung des C-Bands im Global-Beam für die erste INTELSAT-Generation mehr als 25 m, für die weiteren Generationen mehr als 15 bis 18 m betragen muss.

---

[32] Richelson, Jeffrey, Desperately seeking Signals, 4 2000, The Bulletin of the Atomic Scientists, http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html
Richelson,T.Jeffrey, The U.S. Intelligence Community, Westview Press 1999

[33] Campbell, Duncan, Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5, 10 1999, STOA, http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf
Campbell, Duncan: Inside Echelon, 25.7.2000http://www.heise.de/tp/deutsch/special/ech/6928/1.html
Campbell, Duncan: Interception Capabilities n- Impact and Exploitation – Echelon and its role in COMINT, vorgelegt im Echelon-Ausschuß des Europäischen Parlaments am 22. Januar 2001
Federation of American Scientists, http://www.fas.org/irp/nsa/nsafacil.html

[34] Richelson, Jeffrey: Newly released documents on the restrictions NSA places on reporting the identities of US-persons: Declassified: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html

[35] Federation of American Scientists

[36] Military.com; *.mil-Homepages

[37] Verwendete Abkürzungen: NAVSECGRU: Naval Security Group, INSCOM: United States Army Intelligence And Security Command, AIA: Air Intelligence Agency, IG: Intelligence Group, IS: Intelligence Sqadron, IW: Intelligence Wing, IOG: Information Operation Group, MIG: Military Intelligence Group

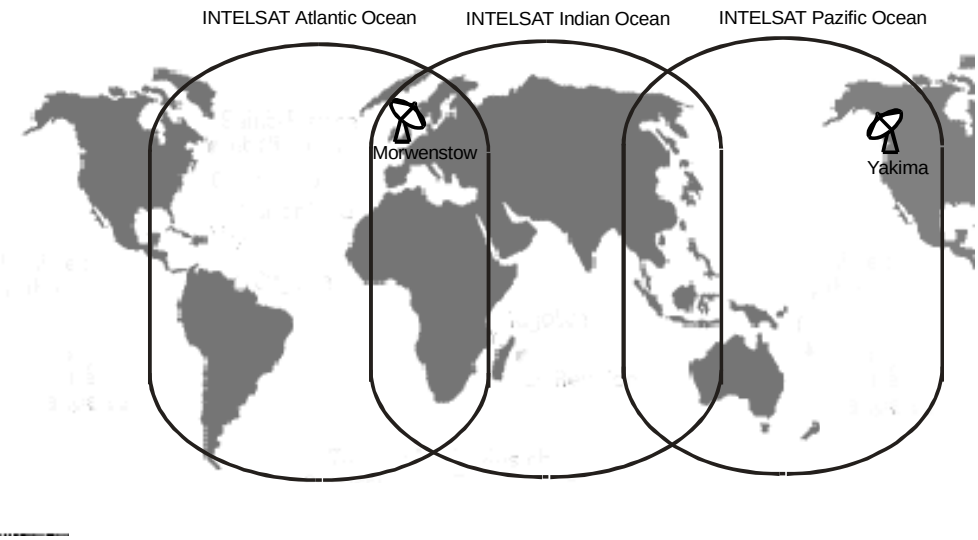
5.3.2.1. Die Parallelität der INTELSAT Entwicklung mit dem Bau von Stationen

Ein globales Abhörsystem muss mit dem Fortschritt der Kommunikation wachsen. Mit dem Beginn der Satelliten-Kommunikation muss folglich das Entstehen von Stationen einhergehen, und mit dem Einführen neuer Satellitengenerationen die Entstehung neuer Stationen sowie der Bau neuer Satellitenantennen, die den jeweiligen Anforderungen entsprechen. Die Zahl der Stationen und die Zahl der Satellitenantennen muss immer dann wachsen, wenn es zur Erfassung der Kommunikation notwendig ist.
Umgekehrt, wenn also dort, wo neue Ausleuchtzonen hinzukommen, neue Stationen entstehen und neue Satellitenantennen gebaut werden, ist das kein Zufall, sondern kann als Indiz für das Vorliegen einer Abhörstation für Kommunikation betrachtet werden.
Da die INTELSAT-Satelliten die ersten Kommunikationssatelliten waren, die darüber hinaus den gesamten Globus abgedeckt haben, ist es logisch, dass die Entstehung und Vergrößerung von Stationen mit den INTELSAT-Generationen einhergeht.

Die erste Generation

Bereits 1965 wurde der erste INTELSAT-Satellit (Early Bird) in die geostationäre Umlaufbahn gebracht. Seine Übertragungskapazität war noch gering und seine Ausleuchtzone erstreckte sich nur über die nörliche Hemisphäre.
Mit den INTELSAT-Generationen II und III, die 1967 bzw. 1968 in Betrieb gingen, wurde zum ersten Mal eine globale Abdeckung erreicht. Die Global-Beams der Satelliten deckten den atlantischen, den pazifischen und den indischen Bereich ab. Kleinere Ausleuchtzonen gab es noch nicht. Für die Erfassung der gesamten Kommunikation waren daher drei Satellitenantennen notwendig. Da sich zwei der Global-Beams über dem europäischen Raum überlappten, konnte in diesem Gebiet an einer Station mit zwei Satellitenantennen unterschiedlicher Ausrichtung die globalen Ausleuchtzonen zweier Satelliten erfasst werden.

Erste global arbeitende Satellitengeneration von INTELSAT



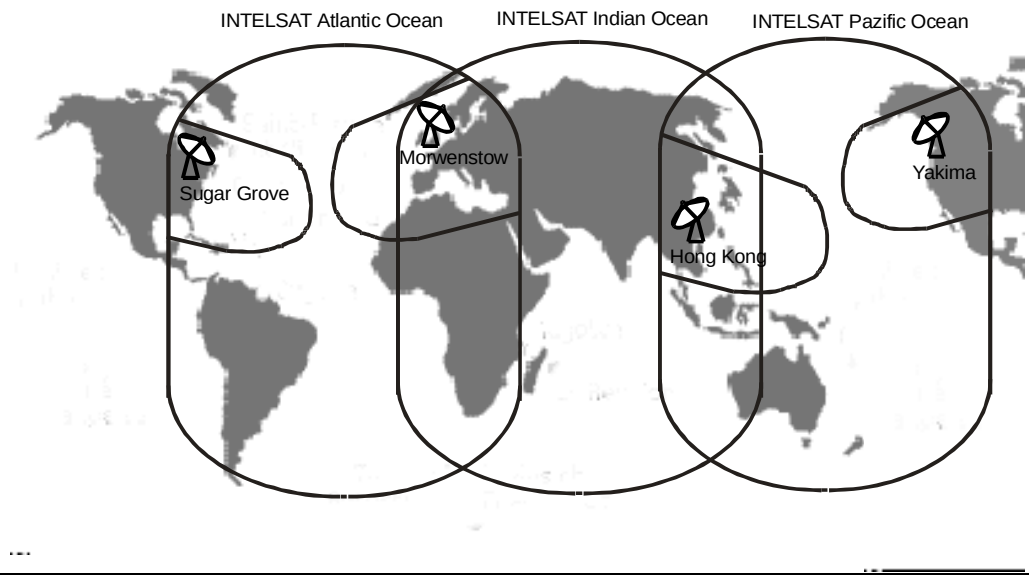
1970 wurde **Yakima** im Nordwesten der USA gegründet, 1972/73 **Morwenstow** in Südengland. Yakima hatte damals eine große Antenne (in Richtung Pazifik), Morwenstow hatte zwei große Antennen (eine in Richtung Atlantik, eine in Richtung Indischer Ozean). Durch die Lage der

beiden Stationen war das Erfassen der gesamten Kommunikation möglich. 1974 wurde darüber hinaus in Menwith Hill die erste große Satellitenantenne aufgebaut.

Die zweite globale Generation

Die zweite Generation der INTELSAT-Satelliten (IV und IVA) wurde in den 70ern entwickelt und in die geostationäre Umlaufbahn gebracht (1971 und 1975). Die neuen Satelliten, die ebenfalls eine globale Bedeckung sicherstellten und über wesentlich mehr Fernsprechkanäle (4000 – 6000) verfügten, hatten neben den Global-Beams auch Zone-Beams in der nördlichen Hemisphäre (siehe Kap. 4). Ein Zone-Beam deckte den Osten der USA ab, einer den Westen der USA, einer West-Europa und ein weiterer Ost-Asien. Durch zwei Stationen mit drei Satellitenantennen war so das Erfassen der gesamten Kommunikation nicht mehr möglich. Mit den existierenden Stationen in Yakima konnte der Zone-Beam im Westen der USA abgedeckt werden, mit Morwenstow der Zone-Beam über Europa. Zur Erfassung der zwei weiteren Zone-Beams wurden eine Station im Osten der USA und eine im ostasiatischen Raum notwendig.

Zweite global arbeitende Satellitengeneration von INTELSAT



In den späten 70er Jahren wurde **Sugar Grove** im Osten der USA aufgebaut (die Station existierte bereits zum Abhören russischer Kommunikation); sie trat 1980 in Funktion. Ebenfalls in den späten 70ern wurde eine Station in **Hongkong** gegründet.
Damit war mit den vier Stationen – Yakima, Morwenstow, Sugar Grove und HongKong - in den 80ern ein globales Abhören der INTELSAT-Kommunikation möglich.

Die späteren INTELSAT-Satelliten mit Zone-Beams und Spot-Beams zusätzlich zu den Global- und Hemi-Beams machten weitere Stationen in verschiedenen Teilen der Welt erforderlich. Hier lässt sich ein Zusammenhang zwischen der Entstehung weiterer Stationen bzw. dem Aufstellen von weiteren Satellitenantennen nur sehr schwer herstellen.

Da man darüber hinaus nur schwer Zugang zu Informationen über Stationen bekommt, lässt sich nicht genau ermitteln, welche Satelliten mit welchen Beams von welcher Station erfasst werden. Man kann allerdings feststellen, in welchen Beams bekannte Stationen liegen.

5.3.2.2. Die globale Abdeckung durch Stationen die eindeutig Kommunikationssatelliten abhören

Heute wird globale Satellitenkommunikation durch Satelliten von INTELSAT, von INMARSAT und INTERSPUTNIK gewährleistet. Die Aufteilung in drei Ausleuchtzonen (indischer, pazifischer und atlantischer Bereich) ist wie bei den ersten Satellitengenerationen beibehalten. In jeder der Ausleuchtzonen befinden sich Stationen, auf die die für Abhörstationen charakteristischen Kriterien zutreffen:

Satelliten über dem indischen Ozean:

INTELSAT 604 (60°E), 602 (62°E), 804 (64°E), 704 (66°E) EXPRESS 6A (80°E) INMARSAT indischer Bereich	Geraldton, Australien Pine Gap, Australien Morwenstow, England Menwith Hill, England
INTELSAT APR1 (83°), APR-2 (110,5°)	Geraldton, Australien Pine Gap, Australien Misawa, Japan

Satelliten über dem Pazifik:

INTELSAT 802 (174°), 702 (176°), 701 (180°) GORIZONT 41 (130°E), 42 (142°E), LM-1 (75°E) INMARSAT pazifischer Bereich	Waihopai, Neuseeland Geraldton, Australien Pine Gap, Australien Misawa, Japan Yakima, USA - nur Intelsat und Inmarsat

Satelliten über dem Atlantik:

INTELSAT 805 (304,5°), 706 (307°), 709 (310°) 601 (325,5°), 801 (328°), 511(330,5°), 605 (332,5°), 603 (335,5°), 705 (342°) EXPRESS 2 (14°W), 3A (11°W) INMARSAT atlantischer Bereich	Sugar Grove, USA Buckley Field, USA Sabana Seca, Puerto Rico Morwenstow, England Menwith Hill, England
INTELSAT 707 (359°)	Morwenstow, England Menwith Hill, England

Dadurch ist gezeigt, dass ein globales Abhören von Kommunikation möglich ist.

Darüber hinaus gibt es noch weitere Stationen, auf die zwar das Kriterium der Antennengröße nicht zutrifft, die aber dennoch Teil des globalen Abhörsystems sein können. Mit diesen Stationen könnten z.B. die Zone- oder Spot-Beams von Satelliten erfasst werden, deren Global-Beams von anderen Stationen abgehört werden, oder für deren Global-Beam keine großen Satellitenantennen notwendig sind.

5.3.2.3. Die Stationen im Detail

In der detaillierten Beschreibung von Stationen wird unterschieden zwischen Stationen, die eindeutig Kommunikationssatelliten abhören (Kriterien aus Kap. 5.2) und Stationen, deren Aufgabe nicht mit Hilfe der oben genannten Kriterien belegt werden kann.

5.3.2.3.1. Stationen für das Abhören von Kommunikationssatelliten

Die in Kapitel 5.2. beschriebenen Kriterien, die als Indizien für eine Abhörstation von Kommunikationssatelliten bewertet werden können, treffen auf folgende Stationen zu:

Yakima, USA (120°W, 46°N)

Die Station wurde 1970 zeitgleich mit der ersten Satellitengeneration gegründet. Seit 1995 ist die Air Intelligence Agency (AIA) mit der 544th Intelligence Group (Detachment 4) vor Ort. Ebenfalls dort stationiert ist die Naval Security Group (NAVSECGRU). Auf dem Gelände sind 6 Satellitenantennen installiert, über deren Größe aus den Quellen nichts zu entnehmen ist. Hager beschreibt die Satellitenantennen als groß und gibt ihre Ausrichtung auf Intelsat-Satelliten über dem Pazifik (2 Satellitenantennen) und Intelsat-Satelliten über dem Atlantk an, sowie die Ausrichtung auf den Inmarsat-Satelliten 2.
Das Gründungsdatum Yakimas gleichzeitig mit der ersten Intelsat-Satellitengeneration sowie die generelle Aufgabenbeschreibung der 544th Intelligence Group sprechen für eine Rolle Yakimas in der globalen Überwachung von Kommunikation. Ein weiteres Indiz dafür ist die Nähe Yakimas zu einer Satelliten-Empfangsstation, die 100 Meilen nördlich liegt.

Sugar Grove, USA (80°W, 39°N)

Gegründet wurde Sugar Grove gleichzeitig mit der Inbetriebnahme der zweiten Generation von Intelsat-Satelliten in den späten 70ern. Stationiert sind hier die NAVSECGRU sowie die AIA mit der 544th Intelligence Group (Detachment 3). Die Station hat nach Angaben verschiedener Autoren 10 Satellitenantennen, wovon drei größer sind als 18m (18,2 m, 32,3 m und 46 m) und damit eindeutig für das Abhören von Kommunikations-Satelliten zuständig sind. Eine Aufgabe des Detachment 3 der 544th IG an der Station ist es, „Intelligence Support“ zur Verfügung zu stellen für die Sammlung von Information von Kommunikationssatelliten durch die Navy-Feldstationen.[38]
Darüberhinaus liegt Sugar Grove in der Nähe (60 Meilen) der Satelliten-Empfangsstation in Etam.

Sabana Seca, Puerto Rico (66°W, 18°N)

1952 wurde die NAVSECGRU in Sabana Seca stationiert. Seit 1995 befindet sich dort auch die AIA mit der 544th IG (Detachment 2). Die Station hat mindestens eine Satellitenantenne von 32 m Durchmesser und 4 weitere kleine Satellitenantennen.
Aufgabe der Station ist nach offiziellen Angaben die Verarbeitung von Satellitenkommunikation („performing satellite communication processing“), „cryptologic and communications service“ sowie die Unterstützung von Navy und DoD Aufgaben (u.a. Sammeln von COMSAT Information (aus Beschreibung der 544th IG)). In der Zukunft soll Sabana Seca die erste Feldstation für die Analyse und Verarbeitung von Satellitenkommunikation werden.

[38] „It provides enhhanced intelligence support to Air Force operational commanders and other consumers of communications satellite information collected by Navy-commanded filed stations.“ aus der Homepage der (44th Intelligence Group http://www.aia.af.mil

Morwenstow, England (4°W, 51°N)
Morwenstow wurde wie Yakima zeitgleich mit der ersten Intelsat-Satellitengeneration Anfang der 70er gegründet. Betreiber von Morwenstow ist der britische Nachrichtendienst (GCHQ). In Morwenstow stehen ca. 30 Satellitenantennen, zwei davon mit einem Durchmesser von 30 m; über die Größe der anderen Antennen gibt es keine Angaben.
Über die Aufgabe der Station ist von offizieller Seite nichts bekannt, die Größe und die Anzahl der Satellitenantennen sowie ihre Lage nur 110 km entfernt von der Telekom-Station in Goonhilly lassen keinen Zweifel an ihrer Funktion als Abhörstation für Kommunikationssatelliten.

Menwith Hill, England (2°W, 53°N)
Die Gründung von Menwith Hill war 1956, 1974 waren bereits 8 Satellitenantennen vorhanden. Inzwischen stehen dort ca. 30 Satellitenantennen, von denen einige einen Durchmesser von mehr als 20 m haben. In Menwith Hill arbeiten Briten und Amerikaner zusammen. Von amerikanischer Seite sind dort die NAVSECGRU, die AIA (451st IOS) sowie das INSCOM, das das Kommando der Station inne hat. Der Grund, auf dem Menwith Hill steht, gehört dem Verteidigungsministerium Englands und ist an die US-Regierung vermietet. Nach offiziellen Angaben ist die Aufgabe von Menwith Hill „to provide rapid radio relay and to conduct communications research". Nach Aussagen von Richelson und der Federation of American Scientists ist Menwith Hill sowohl Bodenstation für Spionage-Satelliten als auch Bodenstation für russische Kommunikationssatelliten.

Geraldton, Australien (114°O, 28°S)
Die Station existiert seit Anfang der 90er. Die Leitung der Station obliegt dem australischen Geheimdienst (DSD), Briten, die ehemals in Hongkong stationiert waren (s.o.) gehören nun zu der Besatzung dieser Station. Sechs Satellitenantennen, von denen mindestens einer einen Durchmesser von ca. 20 m (Schätzung) hat, sind nach Aussage von Hager auf Satelliten über dem indischen Ozean und auf Satelliten über dem Pazifik ausgerichtet.
Nach Angaben eines unter Eid genommenen Experten im Australischen Parlament werden in Geraldton Kommunikationssatelliten abgehört.[39]

Pine Gap, Australien (133°O, 23°S)
Die Station in Pine Gap wurde 1966 gegründet. Die Leitung hat der australische Geheimdienst (DSD); etwa die Hälfte der dort stationierten ca. 900 Personen sind Amerikaner vom CIA und der NAVSECGRU.[40]
Pine Gap hat 18 Satellitenantennen, davon eine mit ca. 30 m und eine mit ca. 20 m Durchmesser. Nach offiziellen Angaben sowie Angaben verschiedener Autoren ist die Station seit Beginn Bodenstation für SIGINT-Satelliten. Von hier aus werden verschiedene Spionagesatelliten kontrolliert und gesteuert sowie ihre Signale empfangen, weiterverarbeitet und analysiert. Die großen Satellitenantennen sprechen aber auch für das Abhören von Kommunikationssatelliten, da für SIGINT-Satelliten die Notwendigkeit von großen Satellitenantennen nicht besteht. Bis

[39] Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra; http://www.aph.gov.au/hansard

[40] Proof Committee Hansard, Joint Standing Committee on Treaties, Reference: Pine Gap, 9 August 1999, Canberra; http://www.aph.gov.au/hansard

1980 waren Australier von der Signal-Analyse-Abteilung ausgeschlossen, seither haben sie freien Zugang zu allem außer dem nationalen Kryptographieraum der Amerikaner.

Misawa, Japan (141°O, 40°N)
Die Station in Misawa existiert seit 1948. Es sind Japaner und Amerikaner dort stationiert. Von amerikanischer Seite befinden sich dort die NAVSECGRU, INSCOM sowie einige Gruppen der AIA (544th IG, 301st IS,). Auf dem Gelände befinden sich ca. 14 Satellitenantennen, von denen einige einen Durchmesser von ca. 20 m (Schätzung) besitzen. Misawa dient offziell als „Cryptology Operations Center". Nach Angaben von Richelson werden mit Hilfe von Misawa die russischen Molnyia-Satelliten sowie weitere russische Kommunikationssatelliten abgehört.

Waihopai, Neuseeland (173°O, 41°S)
Waihopai existiert seit 1989. Seither gibt es eine große Antenne mit 18 m Durchmesser, eine zweite kleinere wurde später dazugebaut. Laut Hager ist die große Antenne auf Intelsat 701 über dem Pazifik ausgerichtet.

Buckley Field, USA, Denver Colorado (104°W, 40°N)
Die Station wurde 1972 gegründet. Stationiert ist dort die 544th IG (Det. 45). Auf dem Gelände stehen etwa 5 Satellitenantennen von denen 4 einen Durchmesser von ca. 20 m haben. Offizielle Aufgabe der Station ist es, Daten über nukleare Ereignisse gewonnen durch SIGINT-Satelliten zu sammeln, auszuwerten und zu analysieren. Die Größe der Satellitenantennen deutet auf eine Rolle beim Abfangen von ziviler Kommunikation hin.

Hong Kong (22°N, 114°O)
Die Station wurde in den späten 70ern zeitgleich mit der zweiten INTELSAT-Generation gegründet und war mit großen Satellitenantennen ausgestattet. Über die genauen Größen liegen keine Angaben vor. 1994 wurde mit dem Abbau der Station in Hongkong begonnen, die Antennen wurden nach Australien gebracht. Welche der Stationen die Aufgaben von Hong-Kong übernommen hat, ist nicht eindeutig: Geraldton, Pine Gap oder aber Misawa in Japan. Eventuell wurden die Aufgaben auf verschiedene Stationen aufgeteilt.

5.3.2.3.2. weitere Stationen

Bei folgenden Stationen kann mit Hilfe der oben genannten Kriterien die Funktion nicht eindeutig belegt werden:

Leitrim, Kanada (75°W, 45°N)
Leitrim ist Teil eines Austauschprogramms zwischen kanadischen und US amerikanischen militärischen Einheiten. Daher sind in Leitrim nach Angaben der Navy ca. 30 Personen stationiert. 1985 wurde die erste von 4 Satellitenantennen installiert, von denen die beiden größeren lediglich einen Durchmesser von ca. 12 m (Schätzung) haben.
Aufgabe der Station ist nach offiziellen Angaben „Cryptologic rating" und das Abhören von diplomatischem Verkehr.

Bad Aibling, Deutschland (12°O, 47°N)
Die Station in der Nähe Bad Aiblings, in der ca. 750 Amerikaner arbeiten wurde 1952 von der US-Armee übernommen (von 1972 bis 1994 war sie in den Händen des Department of Defense). Stationiert sind in Bad Aibling die NAVSECGRU, INSCOM (66th IG, die 718 IG) sowie

verschiedene Gruppen der AIA (402nd IG, 26th IOG). Es befinden sich dort 14 Satellitenantennen, von denen keine größer ist als 18 m. Nach offiziellen Angaben hat Bad Aibling folgende Aufgaben: “Rapid Radio Relay and Secure Commo, Support to DoD and Unified Commands, Medium and Longhand Commo HF& Satellite, Communication Physics Research, Test and Evaluate Commo Equipment”. Nach Richelson ist Bad Aibling Bodenstation für SIGINT-Satelliten und für russische Kommunikationssatelliten.

Ayios Nikolaos, Zypern (32°O, 35°N)
Ayios Nikolaos auf Zypern ist eine britische Station. Die Aufgaben der Station mit 9 Satellitenantennen, deren Größe unbekannt ist, sind auf zwei Einheiten verteilt, das „Signals Regiment Radio und die Signals Unit (RAF)“.
Die Lage von Agios Nikolaos in der Nähe zu den arabischen Staaten und die Tatsache, dass Ayios Nikolaos die einzige Station innerhalb einiger Ausleuchtzonen (v.a. Spot-Beams) in diesem Bereich ist, sprechen für eine wichtige Rolle dieser Station in der Nachrichten-Beschaffung.

Shoal Bay, Australien (134°O, 13°S)
Shoal Bay ist eine nur vom australischen Nachrichtendienst betriebene Station. Die Station soll 10 Satellitenantennen haben, deren Größe nicht näher beschrieben ist. Von den auf Photos zu sehenden Satellitenantennen haben die größeren 5 maximal einen Durchmesser von 8m, die sichtbare sechste ist noch kleiner. Nach Angaben von Richelson sind die Antennen auf die indonesischen PALAPA-Satelliten ausgerichtet. Ob die Station Teil des globalen Systems zum Abhören ziviler Kommunikation ist, bleibt unklar.

Guam, Pazifik (144°O, 13°S)
Guam ist seit 1898 existent. Heute befindet sich dort eine Naval Computer and Telecommunication Station, auf der die 544th IG der AIA sowie Navy-Soldaten stationiert sind. Es gibt an der Station mindestens zwei Satellitenantennen, über deren Größe nichts bekannt ist. Die Funktion von Guam bleibt daher unklar.

Kunia, Hawai (158°W, 21°N)
Diese Station ist seit 1993 Regional Security Operation Center (RSOC) in Funktion, betrieben von der NAVSECGRU und der AIA. Zu ihren Aufgaben gehört die Bereitstellung von Information und Kommunikation sowie kryptologische Unterstützung. Die Funktion von Kunia bleibt unklar.

Medina Annex, USA Texas (98°W, 29°N)
Medina ist wie Kunia ein Regional Security Operation Center – gegründet 1993 - , betrieben von NAVSECGRU und AIA-Einheiten mit Aufgaben in der Karibik.

Fort Gordon (81°W, 31°N)
Fort Gordon ist ebenso ein Regional Security Operation Center, betrieben von INSCOM und AIA (702nd IG, 721st IB, 202nd IB, 31st IS) mit unklaren Aufgaben.

Fort Mead, USA (76°W, 39°N)
Fort Mead ist Headquater der NSA.

5.3.3. Zusammenfassung der Ergebnisse

Folgende Schlussfolgerungen lassen sich aus den gesammelten Daten über die Stationen, die Satelliten und den oben beschriebenen Voraussetzungen ziehen:
1. Es existieren in jeder Ausleuchtzone Abhörstationen für mindestens einige der Global-Beams mit jeweils mindestens einer Antenne größer als einen Durchmesser von 18m, die von Amerikanern oder Briten betrieben werden, bzw. wo Amerikaner oder Briten nachrichtendienstliche Tätigkeiten ausüben. Das ist ein starkes Indiz für die Existenz eines globalen Abhörsystems.
2. Die Entwicklung der INTELSAT-Kommunikation und die gleichzeitige Entstehung von entsprechenden Abhörstationen belegen die globale Ausrichtung des Systems.
3. Aus Punkt 1 und 2 ist es möglich, bestimmte Stationen eindeutig als Stationen, die internationale Satellitenkommunikation abhören, zu identifizieren.
4. Die Angaben in den deklassifizierten Dokumenten und der Betreiber (AIA, NSA, Navy usw.) sind als Beleg für die dort genannten Stationen zu bewerten.

5. Einige Stationen stehen gleichzeitig in Beams bzw. Spots von verschiedenen Satelliten, so dass ein großer Teil der Kommunikation abgefangen werden kann.
6. Es gibt einige weitere Stationen, die über keine großen Antennen verfügen, trotzdem aber Teil des Systems sein können, da sie Kommunikation aus den Beams und Spots empfangen können. Hier muss man auf das Indiz der Antennengröße verzichten und andere Indizien heranziehen.
7. Einige der genannten Stationen liegen nachweislich in unmittelbarer Nähe von regulären Bodenstationen von Kommunikationssatelliten.

5.4. Das UKUSA-Agreement

Als UKUSA-Abkommen wird ein 1948 unterzeichnetes SIGINT-Abkommen zwischen Grossbritannien (United Kingdom, UK), den Vereinigten Staaten (USA) sowie Australien, Kanada und Neuseeland bezeichnet.

5.4.1. Die historische Entwicklung des UKUSA-Agreements[41]

Das UKUSA-Abkommen ist eine Fortsetzung der bereits während des zweiten Weltkriegs sehr engen Zusammenarbeit der Vereinigten Staaten und Großbritannien, die sich bereits im ersten Weltkrieg abgezeichnet hat.
Die Initiative für die Schaffung einer SIGINT-Allianz kam im August 1940 bei einem Treffen von Amerikanern und Briten in London von Seiten der Amerikaner.[42] Im Februar 1941 lieferten die amerikanischen Kryptoanalysten eine Cipher-Maschine (PURPLE) nach Großbritannien. Im

[41] Christopher Andrew, "The making of the Anglo-American SIGINT Alliance" in E. Hayden, h. Peake and S. Halpern eds, In the Name of Inteligence. Essays in honor of Washington Pforzheimer (Washington NIBC Press 1995) pp. 95 -109

[42] ibidem, p. 99: „At a metteing in London on 31 August 1940 between the British Chiefs of Staff and the American Military Observer Mission, the US Army representative, Brigadier General George V. Strong, reported that ´it had recently been arranged in principle between the British and the United States Governments that periodic exchange of information would be desirable,´ and said that ´the time had come or a free exchange of intelligence´. (COS (40)289, CAB 79/6, PRO. Smith, The Ultra Magic Deals, pp. 38, 43-4. Sir F.H. Hinsley, et al., British Intellgence in the Second Worls War, vol.I, pp.312-13)

Frühling 1941 begann die kryptoanalytische Zusammenarbeit.[43] Die nachrichtendienstliche Zusammenarbeit wurde verstärkt durch den gemeinsamen Einsatz der Flotten im nördlichen Atlantik im Sommer 1941. Im Juni 1941 konnten die Briten den deutschen Flottencode ENIGMA brechen.
Der Eintritt Amerikas in den Krieg hat die SIGINT-Zusammenarbeit weiter gestärkt. 1942 begannen amerikanische Kryptoanalytiker der „naval SIGINT agency" in Großbritannien zu arbeiten.[44] Die Kommunikation zwischen den U-Boot Tracking-Rooms in London, Washington und von Mai 1943 an auch Ottawa in Kanada, wurde so eng, dass sie nach Aussage eines damaligen Beteiligten, wie eine einzige Organisation arbeiteten.[45]
Im Frühjahr 1943 wurde das BRUSA-SIGINT Abkommen unterzeichnet, sowie ein Austausch von Personal vorgenommen. Der Inhalt des Übereinkommens betrifft v.a. die Aufteilung der Arbeit und ist in seinen ersten drei Absätzen zusammengefasst: Es beinhalten den Austausch von jeglicher Informationen aus dem Entdecken, Identifizieren und Abhören von Signalen sowie die Lösungen von Codes und Verschlüsselungen. Die Amerikaner waren hauptverantwortlich für Japan, die Briten für Deutschland und Italien[46]

Nach dem Krieg ging die Initiative für die Beibehaltung einer SIGINT-Allianz hauptsächlich von Großbritannien aus. Die Grundlage dafür wurde vereinbart auf einer Welttour britischer Nachrichtendienstler (u.a. Sir Harry Hinsley, dessen Bücher Grundlage des zitierten Artikels sind) im Frühjahr 1945. Ein Ziel war, SIGINT-Personal von Europa Richtung Pazifik zu senden für den Krieg mit Japan. In diesem Zusammenhang wurde mit Australien vereinbart, den australischen Diensten Ressourcen und Personal (Briten) zur Verfügung zu stellen. Auf der Rückreise in die USA führte der Weg über Neuseeland und Kanada.
Im September 1945 unterzeichnete Truman ein strenggeheimes Memorandum, das den Eckstein einer SIGINT-Allianz in Friedenszeiten bildet.[47] Daran anschließend wurden Verhandlungen zwischen den Briten und den Amerikanern über ein Abkommen aufgenommen. Eine britische Delegation nahm darüber hinaus Kontakt zu den Kanadiern und Australiern auf, um eine mögliche Beteiligung zu diskutieren. Im Februar und März 1946 fand eine strenggeheime angloamerikanische SIGINT Konferenz statt, um Details zu diskutieren. Die Briten waren von den Kanadiern und Australiern autorisiert. Produkt der Konferenz war ein immer noch klassifiziertes Abkommen von ca. 25 Seiten, das die Details eines SIGINT-Abkommens zwischen den Vereinigten Staaten und dem Britischen Commonwealth besiegelte. Weitere

[43] Ibidem, p. 100: „ In the spring of 1941, Steward Menzies, the Chief of SIS, appointed an SIS liason officer to the British Joint Services Missin in Washington, Tim O´Connor, …, to advice him on cryptologic collaboration" (

[44] Ibidem, p. 100 (Sir F.H. Hinsley, et al., British Intellgence in the Second Worls War, vol II, p.56)

[45] Ibidem, p. 101 (Sir F.H. Hinsley, et al., British Intellgence in the Second Worls War, vol. II, p 48)

[46] Ibidem, p.101-2: Interivews mit Sir F.H. Hinsley, „Operations of the Military Intelligence Service War Department London (MIS WD London)," 11 June 1945, Tab A, RG 457 SRH-110, NAW

[47] Truman, Memorandum for the Secretaries of the State, War and the Navy, 12 Sept. 1945: „The Secretary of War and the Secretary of the Navy are hereby authorised ti direct the Chief of Staff, U.S. Army and the Commander in Chief, U.S. Fleet; and Chief of Naval Oerations to continue collaboration in the field of communication intelligence between the United States Army and Navy and the British, and to extend, modify or discontinue this collaboration, as determined to be in the best interests of the United States." (from Bradley F. Smith, The Ultra-Magic Deals and the Most Secret Special Relationship (Novato, Ca: Presidio 1993))

Verhandlungen folgten in den darauffolgenden zwei Jahren, so dass der endgültige Text des sogenannten UKUSA Abkommens im Juni 1948 unterzeichnet wurde.[48]

5.4.2. Belege für die Existenz des Abkommens

Bisher gibt es keine offizielle Anerkennung des UKUSA-Abkommens durch die Unterzeichnerstaaten. Dennoch gibt es mehrere klare Belege für seine Existenz.

5.4.2.1. Das Akronym-Verzeichnis der Navy

UKUSA steht laut US-Navy[49] für „United Kingdom – USA" und bezeichnet ein „5-nation SIGINT agreement".

5.4.2.2. Aussage des DSD Direktors

Der Direktor des australischen Nachrichtendienstes (DSD) bestätigte die Existenz dieses Abkommens in einem Interview: Nach seiner Auskunft arbeitet der australische Geheimdienst mit anderen überseeischen Nachrichtendiensten unter dem UKUSA-Abkommen zusammen.[50]

5.4.2.3. Bericht des Canadian Parliamentary Security and Intelligence Committee

In diesem Bericht wird beschrieben, daß Kanda mit einigen seiner engsten und längsten Verbündeten in Nachrichtendienstlichen Fragen zusammenarbeitet. Der Bericht nennt diese Verbündete: Die Vereinigten Staaten (NSA), Grobritannien (GCHQ), Australien (DSD) und Neuseeland (GCSB). Der Namen des Abkommens wird in dem Bericht nicht genannt.

5.4.2.4. Aussage des ehemaligen stellvertretenden Direktors der NSA, Dr. Louis Torella

In einem Interview mit Christopher Andrew, Professor an der Cambridge University, im November 1987 und April 1992 bestätigt der ehemaligen stellvertretenden Direktors der NSA, Dr. Louis Torella, der bei der Unterzeichnung anwesend war, die Existenz des Abkommens.[51]

5.4.2.5. Brief des ehemaligen GCHQ Direktors Joe Hooper

Der ehemaligen GCHQ Direktor Joe Hooper nennt in einem Brief vom an den ehemaligen NSA-Direktor Marshall S.Carter das UKUSA-Abkommen.

---

[48] Christopher Andrew, "The making of the Anglo-American SIGINT Alliance" in E. Hayden, h. Peake and S. Halpern eds, In the Name of Inteligence. Essays in honor of Washington Pforzheimer (Washington NIBC Press 1995) pp. 95 –109: Interviews with Sir Harry Hinsley, March/April 1994, who did a part of the negotiations; Interviews with Dr. Louis Tordella, Deputy Director of NSA from 1958 to 1974, who was present at the signing

[49] „Terms/Abbreviations/Acronyms" veröffentlicht durch das US Nave and Marine Corps Intelligence Training Centre (NMITC) bei http://www.cnet.navy.mil/nmitc/training/u.html

[50] Martin Brady, Direktor des DSD, Canberra 16. März 2000

[51] Andrew, Christopher „The growth of the Australian Intelligence Community and the Anglo-American Connection", pp. 223-4

5.4.2.6. Gesprächspartner des Berichterstatters

Der Berichterstatter hat mit mehreren Personen, die von ihren Funktionen her das UKUSA-Agreement und seinen Inhalt kennen müssen, über das Abkommen gesprochen. Dabei ist seine Existenz in allen Fällen durch die Art der Antworten indirekt bestätigt worden.

5.5. Auswertung amerikanischer deklassifizierter Dokumente

5.5.1. Die Art der Dokumente

Im Rahmen des „Freedom of Information Acts“ von 1966 (5 U.S.C. § 552) und der Regelung des Departments of Defense (DoD FOIA Regulation 5400.7-R von 1997) wurden ehemals klassifizierte Dokumente deklassifiziert und damit der Öffentlichkeit zugänglich gemacht.
Über das 1985 gegründete National Security Archive an der George Washington University in Washington D.C. sind die Dokumente der Öffentlichkeit zugänglich. Der Autor Jeffrey Richelson, ehemaliges Mitglied des National Security Archives, hat per Internet 16 Dokumente zugänglich gemacht, die einen Einblick geben in die Entstehung, die Entwicklung, das Management und das Mandat der NSA (National Security Agency).[52] Darüber hinaus wird in zwei der Dokumente „ECHELON“ erwähnt. Diese Dokumente werden von verschiedenen Autoren, die über ECHELON geschrieben haben, immer wieder zitiert und als Beweis für die Existenz des globalen Spionagesystems ECHELON herangezogen. Darüber hinaus findet man in den von Richelson zur Verfügung gestellten Dokumenten solche, die die Existenz der NRO (National Reconnaissance Office) bestätigen und ihre Funktion als Manager und Betreiber von SIGINT-Satelliten beschreiben.[53]

5.5.2. Inhalt der Dokumente

Die Dokumente enthalten fragmentarisch Beschreibungen oder Erwähnungen der folgenden Themen:

5.5.2.1 Auftrag und Konzeption der NSA (Dokumente 1, 4, 10, 11, 16)

In der National Security Council Intelligence Directive 9 (NSCID 9) vom 10. März 1950 wird für die Zwecke von COMINT der Begriff Auslandskommunikation definiert; demnach beinhaltet **Auslandskommunikation jedwede Regierungskommunikation im umfassenden Sinne (nicht nur militärisch) sowie alle andere Kommunikation, die Information von militärischem, politischem, wissenschaftlichem oder wirtschaftlichem Wert enthalten könnte**.

Die Direktive (NSCID 9 rev, 29. 12. 52) stellt ausdrücklich klar, dass für Innere Sicherheit nur das FBI verantwortlich ist.

Die Department of Defense (DoD) Directive vom 23. Dezember 1991 über die NSA und den Central Security Service (CSS) definiert das Konzept für die NSA folgendermaßen:

- Die NSA ist eine getrennt organisierte Dienststelle innerhalb des Department of Defense unter der Leitung, des „Secretary of Defense".

[52] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html
[53] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/index.html

- Die NSA sorgt zum einen für die Erfüllung der SIGINT-Mission der USA, zum anderen stellt sie sichere Kommunikationssysteme für alle Departments und Dienststellen zur Verfügung.
- Die SIGINT-Tätigkeit der NSA beinhaltet nicht die Produktion und Verteilung fertiger Nachrichten. Dies fällt in den Aufgabenbereich anderer Departments und Dienststellen.

Darüber hinaus skizziert die DoD-Direktive von 1991 die Struktur in der NSA bzw. dem CSS.

In seinem Statement vor dem „House Permanent Select Committee on Intelligence“ am 12. April 2000 definiert NSA-Direktor Hayden die Aufgaben der NSA wie folgt:
- über elektronische Überwachung wird Auslandskommunikation für Militär und Politiker (policymaker) gesammelt;
- die NSA liefert Intelligence für „U.S. Government consumers“ über internationalen Terrorismus, Drogen, Waffenproliferation;
- es gehört nicht in den Aufgabenbereich der NSA, alle elektronische Kommunikation zu sammeln;
- die NSA darf Informationen nur an von der Regierung autorisierte Empfänger weitergeben, nicht aber direkt an U.S. Firmen.

In einem Memorandum des Vizeadmirals der U.S. Navy W.O. Studeman im Namen der Regierung vom 8. April 1992 wird auf die zunehmend globale Aufgabe (access) der NSA hingewiesen, neben dem „Support of military operations“.

5.5.2.2. Befugnisse der Intelligence Agencies (Dokument 7)

Aus der United States Signals Intelligence Directive 18 (USSID 18) geht hervor, dass sowohl Kabel als auch Radio-Signale abgehört werden.

5.5.2.3. Zusammenarbeit mit anderen Diensten (Dokumente 2a, 2b)

Zu den Aufgaben des U.S. Communications Intelligence Board gehört u.a., alle „arrangements“ mit ausländischen Regierungen im Bereich COMINT zu überwachen. Zu den Aufgaben des Direktors der NSA gehört es, alle Verbindungen mit ausländischen COMINT-Diensten abzuwickeln.

5.5.2.4. Nennung von in „ECHELON-Sites“ aktiven Einheiten (Dokumente 9, 12)

In den NAVSECGRU INSTRUCTIONs C5450.48A wird der Auftrag, die Funktion und das Ziel der Naval Security Group Activity (NAVSECGRUACT), 544th Intelligence Group in Sugar Grove, West Virginia beschrieben. Hier wird aufgeführt, dass eine spezielle Aufgabe ist: „Maintain and operate an ECHELON-Site“; darüber hinaus wird die Verarbeitung von nachrichtendienstlicher Informationen als Aufgabe genannt.

Im Dokument „History of the Air Intelligence Agency – 1 January to 31 December 1994 (RCS: HAF-HO(A&SA)7101 Volume 1) wird unter dem Punkt “Activation of Echelon Units“ die Air Intelligence Agency (AIA), Detachment 2 und 3, genannt:

Die Dokumente geben keine Auskunft darüber, was ein „ECHELON-site“ ist, was an einem „ECHELON-site“ gemacht wird, wofür der Deckname ECHELON steht. Aus den Dokumenten geht nichts über das UKUSA-Agreement hervor.

5.5.2.5. Nennung von Stationen (Dokumente 6, 9, 12)

- Sugar Grove, West Virginia in den NAVSECGRU INSTRUCTIONs C5450.48A
- Misawa Air Base, Japan in History of the Air Intelligence Agency - January to 31 December 1994 (RCS: HAF-HO(A&SA)7101 Volume 1)
- Puerto Rico (i.e. Sabana Seca), ibidem
- Guam, ibidem
- Yakima, Washington, ibidem
- Fort Meade, Maryland, ein COMINT Report der NSA aus Fort George G. Meade, Maryland vom 31. August 1972 belegt die COMINT-Aktivitäten dort.

5.5.2.6. Schutz der Privatheit von US-Bürgern (Dokumente 7, 7a bis f, 11,16)

In den NAVSECGRU INSTRUCTIONs C5450.48A heißt es, dass die Privatheit der Bürger sichergestellt sein muss.

In verschiedenen Dokumenten wird ausgeführt, dass und wie die Privatheit von amerikanischen Bürgern zu schützen ist (Baker, General Counsel, NSA, Brief vom 9. September 1992, United States Signals Intelligence Directive (USSID) 18, 20. Oktober 1980, und verschiedene Ergänzungen[54].

5.5.2.7. Definitionen (Dokumente 4, 5a,7)

Die Department of Defense Directive vom 23. Dezember 1991 liefert genaue Definitionen für SIGINT, COMINT, ELINT und TELINT, ebenso die National Security Council Intelligence Directive No.6 vom 17. Februar 1972.

Danach bedeutet COMINT das Erfassen und Verarbeiten von Auslandskommunikation (passed by electromagnetic means) bis auf Abhören und Verarbeiten von unverschlüsselter geschriebener Kommunikation, Presse, Propaganda, es sei denn sie ist verschlüsselt.

5.5.3. Zusammenfassung

1. Schon vor 50 Jahren galt das Interesse nicht nur Informationen aus den Bereichen Politik und Sicherheit, sondern ebenso aus der Wissenschaft und der Wirtschaft.
2. Die Dokumente beweisen, dass die NSA mit anderen Diensten bei COMINT zusammenarbeitet.
3. Die Dokumente, die Aufschluss darüber geben, wie die NSA organisiert ist, welche Aufgaben sie hat und dass sie dem Department of Defense untersteht, gehen im Wesentlichen nicht über das hinaus, was man öffentlich zugänglichen Quellen auf der Homepage der NSA entnehmen kann.
4. Kabel dürfen abgehört werden.

[54] Dissemination of U.S. Government Organizations and Officials, Memorandum 5 February 1993; Reporting Guidance on References to the First Lady, 8 July 1993; Reporting Guidance on Former President Carter's Involvement in the Bosnian Peace Process, 15 December 1994; Understanding USSID 18, 30 September 1997; USSID 18 Guide 14 February 1998;
NSA/US IDENTITIES IN SIGINT, March 1994; Statement for the record of NSA Director Lt Gen. Michael V. Hayden, USAF, 12. April 2000)

5. Die 544th Intelligence group und Detachment 2 und 3 der Air Intelligence Agency sind an der Sammlung von nachrichtendienstlichen Informationen beteiligt.
6. Der Begriff „ECHELON“ taucht in verschiedenen Zusammenhängen auf.
7. Sugar Grove in West Virginia, Misawa Air Base in Japan, Puerto Rico (i.e. Sabana Seca), Guam, Yakima im Saat Washington werden als SIGINT-Stationen genannt
8. Die Dokumente geben Auskunft darüber, wie die Privatheit amerikanischer Bürger geschützt werden muss.

Die Dokumente liefern keinen Beweis, aber starke Indizien, die zusammen mit anderen Indizien Rückschlüsse erlauben.

5.6. Angaben von Fachautoren und Journalisten

5.6.1. Das Buch von Nicky Hager

In dem 1996 erschienenen Buch von Nicky Hager "Secret Powers – New Zealand's role in the international spy network" wird erstmals das System ECHELON ausführlich beschrieben. Ihm zufolge gehen seine Anfänge auf das Jahr 1947 zurück, als das Vereinigte Königreich mit den Vereinigten Staaten im Anschluss an die Zusammenarbeit im Krieg das Übereinkommen traf, weltweit gemeinsam die bisherigen COMINT-Aktivitäten fortzusetzen. Die Staaten sollten zur Errichtung eines möglichst globalen Abhörsystems zusammenwirken, indem sie sich die dafür erforderlichen spezifischen Einrichtungen sowie die dabei entstehenden notwendigen Ausgaben teilen und gemeinsam Zugriff auf die Ergebnisse bekommen. In der Folge schlossen sich Kanada, Australien und Neuseeland dem UKUSA-Abkommen an.

Nach den Angaben von Hager bildet dabei das Abhören von Satellitenkommunikation den Kernpunkt des heutigen Systems. Bereits in den 70er Jahren wurde angefangen, durch Bodenstationen die via Intel Satelliten – dem ersten globalen Satelliten-Kommunikations-System[55] - gesendeten Nachrichten abzuhören. Diese Nachrichten werden dann mittels Computer nach festgelegten Schlüsselwörtern bzw. Adressen durchsucht, um so die relevanten Nachrichten herauszufiltern. In der Folge wurde die Überwachung auf weitere Satelliten, wie z.B. die von Inmarsat[56], das sich auf maritime Kommunikation konzentrierte, ausgeweitet.

Hager weist in seinem Buch darauf hin, dass das Abhören der Satellitenkommunikation nur eine - wenngleich wichtige - Komponente des Abhörsystems bildet. Daneben gebe es noch zahlreiche Einrichtungen zur Überwachung von Richtfunk und Kabeln, die allerdings weniger dokumentiert und schwieriger nachzuweisen sind, da sie im Gegensatz zu Bodenstationen kaum auffallen. "ECHELON" wird damit zum Synonym für ein globales Abhörsystem.

5.6.2. Angaben von Duncan Campbell

Duncan Campbell legte in der STOA-Studie 2/5 von 1999, die sich eingehend mit der technischen Seite befasst, ausführlich dar, dass und wie jedes Medium, das zur Kommunikationsübertragung verwendet wird, abgehört werden kann. In einem seiner letzten Aufsätze stellt er aber klar, dass auch ECHELON seine Grenzen habe, die ursprüngliche

[55] Vgl. dazu http://www.intelsat.int/index.htm

[56] Vgl. dazu http://www.inmarsat.org/index3.html

Auffassung, dass eine lückenlose Überwachung möglich sei, habe sich als falsch herausgestellt, "Weder ECHELON noch das elektronische Spionagesystem, von dem es ein Teil ist, sind dazu in der Lage. Das Equipment ist auch gar nicht vorhanden, das die Kapazität hätte, den Inhalt jeder Sprachnachricht oder jedes Telefonanrufs zu verarbeiten und zu erkennen." [57]

5.6.3. Angaben von Jeff Richelson

Der Autor Jeffrey Richelson, ehemaliges Mitglied des National Security Archives, hat per Internet 16 ehemals klassifizierte Dokumente zugänglich gemacht, die einen Einblick geben in die Entstehung, die Entwicklung, das Management und das Mandat der NSA (National Security Agency)[58].
Darüber hinaus ist er Autor verschiedener Bücher und Artikel nachrichtendienstlicher Tätigkeiten der U.S.A. In seinem 1985 erschienenen Buch „The Ties That Bind“[59] beschreibt er ausführlich das Zustandekommen des UKUSA-Abkommens und die Tätigkeiten der an diesem Abkommen beteiligten Geheimdienste der USA, Großbritanniens, Kanadas, Australiens und Neuseelands.
In seinem sehr umfangreichen Buch „ The U.S. Intelligence Community“[60] von 1999 gibt er einen Überblick über die nachrichtendienstlichen Tätigkeiten der USA, es beschreibt die Organisationsstrukturen der Dienste, ihre Methoden der Sammlung und Analyse von Information. In Kapitel 8 des Buches geht er detailliert auf die SIGINT-Kapazitäten der Nachrichtendienste ein und beschreibt einige Bodenstationen. In Kapitel 13 beschreibt er die Beziehungen der USA zu anderen Nachrichtendiensten, u.a. das UKUSA-Übereinkommen. Den Namen ECHELON erwähnt er an einer Stelle als Codewort für ein computerbasiertes Austauschsystem.
In seinem im 2000 erschienenen Artikel „Desperately seeking Signals“[61] beschreibt er in kurzer Form das UKUSA-Abkommen, nennt Satellitenabhöranlagen für Kommunikationssatelliten und beschreibt Möglichkeiten und Grenzen des Abhörens von ziviler Kommunikation.

5.6.4. Angaben von James Bamford

wird nachgereicht

5.6.5. Angaben von Bo Elkjaer und Kenan Seeberg,

Die beiden dänischen Journalisten Bo Elkjaer und Kenan Seeberg gaben am 22. Januar 2001 vor dem Ausschuss an, dass ECHELON bereits in den 80er Jahren sehr weit vorangeschritten war, und dass Dänemark seit 1984 mit den USA zusammenarbeite.

---

[57] Duncan Campbell, Inside Echelon. Zur Geschichte, Technik und Funktion des unter dem Namen Echelon bekannten globalen Abhör- und Filtersystems, 1

[58] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html

[59] Jeffrey T. Richelson, Desmond Ball 1985: The Ties That Bind, Boston UNWIN HYMAN, Sydney Wellington London

[60] Jeffrey T. Richelson 1999 (4th ed.): „The U.S. Intelligence Community“, Westview Press

[61] Jeffrey T. Richelson 2000: „Desperately seeking Signals“ The Bulletin of the Atomic Scientists, March/April 2000, Vol. 56, No. 2, pp. 47-51

5.7. Aussagen von ehemaligen Nachrichtendienstmitarbeitern

5.7.1. Margaret Newsham (ehemalige NSA-Mitarbeiterin)

Margaret Newsham[62] war von 1974 bis 1984 bei Ford und Lockheed angestellt und arbeitete während dieser Zeit ihren eigenen Aussagen zufolge für die NSA. Sie war im NSA Headquarter in Fort George Meade in Maryland, USA, für die Arbeit ausgebildet worden, und von 1977-1978 in Menwith Hill, der amerikanischen Bodenstation auf britischem Boden, eingesetzt. Dort habe sie festgestellt, dass eine Konversation von US-Senator Strohm Thurmond abgehört wurde. Bereits 1978 konnte ECHELON die Telekommunikation einer bestimmten Person abfangen, die über Satellit transportiert wurde.

Was ihre eigene Rolle bei der NSA betreffe, so sei sie dafür verantwortlich gewesen, Systeme und Programme zu erstellen, sie zu konfigurieren und auf großen Computern betriebsbereit zu machen. Die Softwareprogramme seien SILKWORTH und SIRE genannt worden, ECHELON sei hingegen der Name für das Netzwerk gewesen.

5.7.2. Wayne Madsen (ehemaliger NSA-Mitarbeiter)

Wayne Madsen[63], früherer Mitarbeiter der NSA, bestätigt ebenfalls die Existenz von ECHELON. Seiner Ansicht nach hat das Sammeln von Wirtschaftsdaten höchste Priorität und wird zum Vorteil von US-Betrieben genützt. Er äußert insbesondere Befürchtungen, dass ECHELON NGOs wie Amnesty International oder Greenpeace ausspionieren könnte. Dazu führt er aus, dass die NSA zugeben musste, dass sie mehr als 1,000 Seiten Informationen zu Prinzessin Diana hatte, die sich durch ihre Kampagne gegen Landminen konträr zur US-Politik verhielt.

5.7.3. Mike Frost (ehemaliger kanadischer Geheimdienstmitarbeiter)

Mike Frost war über 20 Jahre bei dem kanadischen Geheimdienst CSE[64] beschäftigt. Die Abhörstation in Ottawa sei nur ein Teil eines weltweiten Netzwerkes von Spionagestationen.[65] In einem Interview mit CBS erklärte er, dass "überall auf der Welt, jeden Tag, die Telefongespräche, e-mails und Faxe von ECHELON überwacht werden, einem geheimen Überwachungsnetzwerk der Regierung".[66] Dies betreffe auch zivile Kommunikation. Als Beispiel führt er in einem Interview mit einem australischen Sender an, dass vom CSE tatsächlich Name und Telefonnummer einer Frau in eine Datenbank möglicher Terroristen aufgenommen wurden, die einen zweideutigen Begriff in einem harmlosen Telefongespräch mit einem Freund verwendet hatte. Der Computer hatte beim Durchsuchen von Kommunikation das Stichwort gefunden und die Kommunikation wiedergegeben, der für die Analyse Zuständige war sich nicht sicher und hat deshalb ihre Personaldaten aufgenommen.[67]

---

[62] Vgl. zum Folgenden Bo Elkjaer, Kenan Seeberg, Echelon was my baby – Interview with Margaret Newsham, Ekstra Bladet, 17.1.1999

[63] Fernsehinterview von NBC "60 Minutes" vom 27.2.2000; http://cryptome.org/echelon-60min.htm

[64] Communication Security Establishment, untersteht kanadischem Verteidigungministerium, betreibt SIGINT

[65] Fernsehinterview von NBC "60 Minutes" vom 27.2.2000; http://cryptome.org/echelon-60min.htm

[66] Rötzer, Die NSA geht wegen Echelon an die Öffentlichkeit;
http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special

[67] Fernsehinterview von NBC "60 Minutes" vom 27.2.2000; http://cryptome.org/echelon-60min.htm

Die Nachrichtendienste der ECHELON-Staaten würden sich auch dadurch gegenseitig helfen, dass einer für den anderen spioniere, so dass man zumindest dem heimischen Nachrichtendienst nichts vorwerfen könne. So habe der GCHQ den kanadischen CSE gebeten, für ihn zwei englische Minister auszuspionieren, als Premierministerin Thatcher wissen wollte, ob diese sich auf ihrer Seite befinden.[68]

5.7.4. Fred Stock (ehemaliger kanadischer Geheimdienstmitarbeiter)

Fred Stock ist nach eigenen Angaben 1993 aus dem kanadischen Geheimdienst CSE ausgeschlossen worden, weil er sich gegen das neue Schwergewicht des Dienstes auf Wirtschaftsinformationen und zivile Ziele ausgesprochen hatte. Abgefangene Kommunikation habe Informationen über Geschäfte mit anderen Ländern, u.a. auch Verhandlungen über die NAFTA, chinesischen Getreideankauf und französischen Waffenverkauf beinhaltet. Laut Stock habe der Dienst auch routinemäßig Nachrichten über Umweltprotestaktionen von Greenpeace-Schiffen auf hoher See bekommen.[69]

5.8. Regierungsinformationen

5.8.1. Aussagen von amerikanischer Seite

Der ehemalige CIA-Direktor James Woolsey erklärte in einer Pressekonferenz,[70] die er auf Ersuchen des US-State Departments gab, dass die USA in Kontinentaleuropa Spionage betreibe. "Economic Intelligence" werde aber zu 95% durch die Auswertung öffentlich zugänglicher Informationsquellen gewonnen, nur 5% seien gestohlene Geheimnisse. Wirtschaftsdaten anderer Länder werden in den Fällen ausspioniert, in denen es um die Einhaltung von Sanktionen und um Dual-use-Güter gehe, sowie um Bestechung bei der Auftragsvergabe zu bekämpfen. Diese Informationen werden aber nicht an amerikanische Betriebe weitergegeben. Woolsey betont, dass selbst wenn man durch das Ausspionieren von Wirtschaftsdaten auf wirtschaftlich verwendbare Informationen stieße, es sehr zeitaufwendig für einen Analysten wäre, die große Menge vorhandener Daten diesbezüglich zu analysieren, und es ein Missbrauch wäre, ihre Zeit für die Spionage gegen befreundete Handelspartner zu verwenden. Darüber hinaus weist er darauf hin, dass selbst wenn man dies täte, es aufgrund der internationalen Verflechtung schwierig wäre zu entscheiden, welche Unternehmen als US-Unternehmen gelten und man damit die Information zukommen lassen solle.

In einem späteren Artikel für The Wall Street Journal Europe[71] wiederholte Woolsey, dass die USA Europa ausspioniere, dass dies aber nur geschehe, um Bestechungen aufzudecken. Er erklärt darin auch dezidiert, dass die USA Computer verwende, um Daten nach Schlüsselwörtern zu durchsuchen.

---

[68] Interview des australischen Senders Channel 9 vom 23..3.1999; http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm

[69] Bronskill, Canada a key snooper in huge spy network, Ottawa citizen, 24.10.2000, http://www.ottawacitizen.com/national/990522/2630510.html

[70] Transcript, 7.3.2000, http://cryptome.org/echelon-cia.htm

[71] James Woolsey, Why America Spies on its Allies, The Wall Street Journal, 22.3.2000, 31

5.8.2. Aussagen von englischer Seite

Aus den diversen Anfragen im House of Commons[72] ergibt sich, dass die Station RAF Menwith Hill dem englischen Verteidigungsministerium gehört, aber dem US-Verteidigungsministerium, insbesondere der NSA[73], die den Stationsleiter stellt,[74] als Kommunikationseinrichtung zur Verfügung gestellt wird.[75] Mitte 2000 waren in RAF Menwith Hill 415 Personen aus dem US-Militär, 5 aus dem UK-Militär, 989 US-Zivilisten und 392 UK-Zivilisten beschäftigt, wobei anwesende GCHQ-Mitarbeiter nicht einberechnet sind.[76] Die Anwesenheit der US-Truppen wird durch den Nordatlantischen Vertrag und spezielle geheime[77] Verwaltungsabkommen geregelt, die als angemessen für die bestehenden Beziehungen zwischen den Regierungen des UK und der USA für eine gemeinsame Verteidigung bezeichnet werden.[78] Die Station ist integraler Bestandteil des weltweiten Netzwerkes des US-Verteidigungsministerium, das die UK-, die USA- und die NATO-Interessen unterstützt.[79]

Im Jahresbericht 1999/2000 wird ausdrücklich der Wert betont, den die enge Zusammenarbeit unter dem UKUSA-Agreement bringt und sich in der Qualität der nachrichtendienstlichen Ergebnisse wiederspiegle. Insbesondere wird darauf verwiesen, dass, als über drei Tage die Anlagen des NSA ausfielen, der GCHQ direkt neben der UK-Klientel auch die US-Klientel bediente.[80]

5.8.3. Aussage von australischer Seite[81]

Martin Brady, Direktor des australischen Nachrichtendienstes DSD[82], bestätigte in einem Brief an das Programm "Sunday" des australischen Senders "Channel 9", dass es eine Zusammenarbeit des DSD mit andern Nachrichtendiensten unter der UKUSA-Beziehung gibt. Im gleichen Brief wird betont, dass sämtliche nachrichtendienstliche Einrichtungen Australiens von australischen Diensten alleine oder gemeinsam mit amerikanischen Diensten betrieben werden. In den Fällen, in denen Einrichtungen gemeinsam genutzt werden, hat die australische Regierung volle Kenntnis von allen Aktivitäten und ist australisches Personal auf allen Ebenen beteiligt.[83]

---

[72] Commons Written Answers, House of Commons Hansard Debares

[73] 12.7.1995.

[74] 25.10.1994

[75] 3.12.1997

[76] 12.5.2000

[77] 12.7.1995

[78] 8.3.1999, 6.7.1999

[79] 3.12.1997

[80] Intelligence and Security Committee, Annual Report 1999-2000, Z. 14, der dem Parlament vom Premierminister im November 2000 vorgelegt wurde.

[81] http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp

[82] Defence Signals Directorate, Australischer Nachrichtendienst der SIGINT betreibt

[83] Brief von Martin Brady, Direktor der DSD vom 16.März 1999 an Ross Coulthart, Sunday Program; Vgl. dazu auch: http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp

5.8.4. Aussagen von niederländischer Seite

Am 19 Januar 2001 präsentiert der niederländische Verteidigungsminister dem niederländischen Parlament einen Bericht über technische und rechtliche Aspekte globaler Abhörung moderner Telekommunikationssysteme.[84] Die niederländische Regierung vertritt darin die Ansicht, dass, obwohl sie dazu keine eigenen Erkenntnisse habe, es aufgrund der verfügbaren Information von dritter Seite höchst wahrscheinlich sei, dass das ECHELON-Netzwerk bestehe, dass es aber auch andere Systeme mit den gleichen Möglichkeiten gebe. Die niederländische Regierung sei zu dem Schluss gelangt, dass globales Abfangen von Kommunikationssystemen nicht auf die am ECHELON-System beteiligten Staaten beschränkt sei, sondern auch von Regierungsbehörden anderer Länder durchgeführt werde.

5.8.5. Aussagen von italienischer Seite

Luigi Ramponi, ehemaliger Direktor des italienischen Nachrichtendienstes SISMI, lässt in seinem Interview für "il mondo" keinen Zweifel daran bestehen, dass "ECHELON" existiert.[85] Ramponi erklärt ausdrücklich, dass er in seiner Funktion als Chef von SISMI über die Existenz von ECHELON Bescheid wusste. Seit 1992 sei er auf dem Laufenden gewesen über eine starke Aktivität des Abhörens von Wellen niederer, mittlerer und hoher Frequenz. Als er 1991 bei SISMI angefangen habe, musste man sich am meisten mit dem Vereinigten Königreich und den Vereinigten Staaten beschäftigen.

5.9. Parlamentsberichte

5.9.1. Berichte des belgischen Kontrollausschusses Comité Permanent R

Der belgische Kontrollausschuss Comité Permanent R äußerte sich bereits in zwei Berichten zum Thema ECHELON.

Im Bericht "Rapport d'activités 1999" widmete sich das 3. Kapitel der Frage, auf welche Weise die belgischen Nachrichtendienste auf die Möglichkeit eines ECHELON-Systems der Kommunikationsüberwachung reagieren. Der gut 15 Seiten starke Bericht kommt zum Schluss, dass die beiden belgischen Nachrichtendienste Sûreté de l'Etat und Service général du Renseignement (SGR) Information über ECHELON nur durch öffentliche Dokumente bekamen.

Der zweite Bericht "Rapport complémentaire d'activités 1999“ befasst sich wesentlich ausführlicher mit dem ECHELON-System. Er nimmt zu den STOA-Studien Stellung und widmet einen Teil der Erläuterungen der Beschreibung der technischen und gesetzlichen Rahmenbedingungen des Abhörens von Telekommunikation. Seine Schlussfolgerungen lauten dahingehend, dass ECHELON tatsächlich besteht und auch in der Lage ist, alle durch Satellit übertragene Information abzuhören (ca. 1% der gesamten internationalen Telefonate), sofern über Schlüsselwörter gesucht werde, und dass seine Kapazitäten bezüglich Entschlüsselung ungleich größer seien als von amerikanischer Seite dargestellt. Über die Aussagen, dass in Menwith Hill keine Industriespionage betrieben werde, bleibe Zweifel bestehen. Es wird

[84] Brief aan de Tweede Kamer betreffende "Het grootschalig afluisteren van moderne telecommunicatiesystemen" vom 19.01.01

[85] Francesco Sorti, Dossier. exclusivo. caso Echelon. parla Luigi Ramponi. Anche I politici sapevano, il mondo, 17.4.1998

ausdrücklich betont, dass es unmöglich sei, mit Sicherheit festzustellen, was ECHELON mache oder nicht mache.

5.9.2. Bericht des Ausschusses für nationale Verteidigung der französischen Assemblée Nationale

In Frankreich wurde vom Ausschuss für nationale Verteidigung der Assemblée Nationale ein Bericht zum Thema Abhörsysteme vorgelegt.[86]

Nach ausführlicher Erörterung der unterschiedlichsten Aspekte kommt der Berichterstatter Arthur Paecht zum Schluss, dass ECHELON existiert und es sich bei ihm um das einzige bekannte multinationale Überwachungssystem handle. Die Kapazitäten des Systems seien reell, sie haben jedoch ihre Grenzen erreicht, nicht nur weil der getätigte Aufwand nicht mehr verhältnismäßig zur Kommunikationsexplosion sei, sondern auch weil bestimmte Ziele sich zu schützen gelernt haben.

Das ECHELON System sei von seinen ursprünglichen Zielen abgekommnen, welche an den Kontext des Kalten Krieges gebunden waren, sodass es nicht unmöglich sei, dass die gesammelten Information zu politischen und wirtschaftlichen Zwecken gegen andere NATO Staaten eingesetzt werden.

ECHELON könne sehr wohl eine Gefahr für Grundfreiheiten darstellen, es werfe diesbezüglich zahlreiche Probleme auf, die passender Antworten bedürfen. Es sei falsch sich vorzustellen, dass die Mitgliedstaaten von ECHELON ihre Aktivitäten aufgeben. Vielmehr scheinen mehrere Indizien darauf hinzuweisen, dass ein neues System mit neuen Partnern erschaffen wurde, um die Grenzen von ECHELON mit Hilfe neuer Mittel zu überwinden.

[86] Rapport d'information déposé en application de l'article 145 du règlement par la commission de la défense nationale et des forces armées, sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurit´nationale, N° 2623 Assemblée nationale , enregisté à la Présidence de l'Assemblée nationale le 11 octobre 2000.

6. Kann es weitere globale Abhörsysteme geben?

6.1. Voraussetzungen für ein solches System

6.1.1. Technisch-geographische Voraussetzungen

Zum Abhören von internationaler und über Satelliten der ersten Generation vermittelter Kommunikation sind Empfangsstationen im Bereich des Atlantik, im Bereich des Indischen Ozeans und im pazifischen Raum Voraussetzung. Bei der neueren Satellitengeneration, die Abstrahlung in Unterbereiche ermöglicht, müssen weitere Bedingungen bezüglich der geographischen Position von Abhörstationen eingehalten werden, wenn die gesamte über Satellit vermittelte Kommunikation erfasst werden soll.

Ein weiteres global arbeitendes Abhörsystem ist gezwungen seine Stationen außerhalb der Hoheitsgebiete der ECHELON-Staaten zu errichten.

6.1.2. Politisch-ökonomische Voraussetzungen

Die Einrichtung eines solchen weltweit arbeitendend Abhörsystems muss aber auch für den/die Betreiber wirtschaftlich und politisch sinnvoll sein. Der oder die Nutznießer eines solchen Systems müssen globale wirtschaftliche, militärische oder sonstige Sicherheitsinteressen haben oder zumindest glauben, dass sie zu den so genannten Weltmächten gehören. Damit begrenzt sich der Kreis im Wesentlichen auf China und die G8-Staaten ohne die USA und das UK.

6.2. Frankreich

Frankreich verfügt in allen der drei oben genannten Bereichen über eigene Territorien, Départments und Gebietskörperschaften.

Im Bereich des Atlantik liegen östlich von Kanada Saint Pierre et Miquelon (65° W / 47° N), nordöstlich von Südamerika Guadeloupe (61° W / 16° N) und Martinique (60° W / 14° N) sowie an der Nordostküste Südamerikas Französisch Guyana (52° W / 5° N).

Im Bereich des Indischen Ozeans befinden sich östlich des südlichen Afrikas Mayotte (45° O / 12° S) und La Réunion (55° O / 20° S) sowie ganz im Süden die Terres Australes et Antarticques Francaises. Im Bereich des Pazifik liegen Nouvelle Calédonie (165° O / 20° S), Wallis et Futana (176° W / 12° S) sowie Polynésie Francaise (150° W / 16° S).

Über mögliche Stationen des französischen Nachrichtendienstes DGSE (Direction générale de la sécurité extérieur) in diesen überseeischen Gebieten liegen nur wenige Erkenntnisse vor. Nach Angaben französischer Journalisten[87] existieren Stationen in Kourou in Französisch Guyana sowie in Mayotte. Über die Größe der Stationen, die Anzahl der Satellitenantennen und deren Größe liegen im einzelnen keine Angaben vor. Weitere Stationen sollen in Frankreich in Domme in der Nähe von Bordeaux sowie in Alluetts-le-Roi in der Nähe von Paris angesiedelt sein. Die Anzahl der Satellitenschüsseln schätzt Jauvert auf insgesamt 30. Der Buchautor Schmidt-Enboom[88] behauptet, dass auch in Neukaledonien eine Station betrieben wird.

Theoretisch könnte Frankreich ebenfalls ein global arbeitendes Abhörsystem betreiben. Für eine seriöse Behauptung liegen dem Berichterstatter aber nicht genügend öffentlich zugängliche Informationen vor.

6.3. Russland

Der für Kommunikationssicherheit und SIGINT verantwortliche russische Nachrichtendienst FAPSI betreibt angeblich zusammen mit der russischen militärischen Nachrichtendienst GRU Bodenstationen in Lettland, Vietnam und Kuba.

Im Bereich des Atlantik liegt nach Angaben der Federation of American Scientists die Station in Lourdes auf Kuba (82°W, 23°N), die zusammen mit dem kubanischen Nachrichtendienst betrieben wird. Im Bereich des indischen Ozeans liegen Stationen in Russland, über die keine näheren Informationen vorliegen sowie eine Station in Skrunda in Lettland. Im Bereich des Pazifik soll es eine Station in Cam Rank Bay in Nord Vietnam geben. Einzelheiten über die Stationen, was die Anzahl von Antennen und deren Größe betrifft sind nicht bekannt.

Zusammen mit in Russland selbst vorhandenen Stationen ist theoretisch eine globale Abdeckung möglich. Auch hier reichen die vorliegenden Informationen für eine seriöse Behauptung nicht aus.

[87] Jean Guisnel, L'éspionage n'ést plus un secret, The Tocqueville Connection, 10.7.1998

Vincent Jauvert, Espionnage comment la France, Le Nouvel Observateur, 5.4.2001, Nr. 1900, S. 14 ff.

[88] E.Schmidt-Eenboom, in: Streng Geheim, Museumsstiftung Post und Telekommunikation, Heidelberg 1999, S.180

6.4. Die übrigen G-8 Staaten und China

Weder die übrigen G8-Staaten noch China haben eigenes Territorium oder enge Verbündete in den dafür notwendigen Teilen der Welt, um ein globales Abhörsystem zu betreiben.

7. Die Vereinbarkeit eines Kommunikationsabhörsystems des Typs "ECHELON" mit Unionsrecht

7.1. Erläuterungen zur Fragestellung

Das Mandat des Ausschusses beinhaltet u.a. den ausdrücklichen Auftrag, die Vereinbarkeit eines Kommunikationsabhörsystems des Typs "ECHELON" mit Gemeinschaftsrecht zu prüfen.[89] Es soll insbesondere bewertet werden, ob ein solches System mit den beiden Datenschutzrichtlinien 95/46/EG und 97/66/EG, mit Art. 286 EGV und Art. 8 Abs. 2 EUV vereinbar ist.

Es erscheint notwendig, die Überprüfung unter zwei verschiedenen Gesichtspunkten vorzunehmen. Der erste Aspekt ergibt sich aus dem in Kapitel 5 aufgezeigten Indizienbeweis, aus dem hervorgeht, dass das mit "ECHELON" bezeichnete System als Kommunikationsabfangsystem konzipiert wurde, das durch das Sammeln und Auswerten von Kommunikationsdaten den amerikanischen, kanadischen, australischen, neuseeländischen und britischen Geheimdiensten Informationen über Vorgänge im Ausland liefern soll. Es handelt sich somit um ein klassisches Spionageinstrument von Auslandsnachrichtendiensten.[90] In einem ersten Schritte soll somit die Vereinbarkeit eines derartigen nachrichtendienstlichen Systems mit Unionsrecht überprüft werden.

Daneben wurde im vom Campbell vorgelegten STOA Bericht der Vorwurf erhoben, dass dieses System zur Konkurrenzspionage missbraucht werde, und die Wirtschaft europäischer Länder infolgedessen gravierende Verlust hinnehmen musste. Zudem gibt es Aussagen des ehemaligen CIA-Direktors R. James Woolsey, dass die USA zwar europäische Unternehmen auszuspionieren, dies allerdings nur, um Marktgerechtigkeit herzustellen, da die Aufträge nur aufgrund von Bestechung erlangt würden.[91] Trifft es zu, dass die Systeme zur Konkurrenzspionage verwendet werden, so stellt sich die Frage der Vereinbarkeit mit Gemeinschaftsrecht neu. Dieser zweite Aspekt soll deshalb getrennt in einem weiteren Schritt untersucht werden.

7.2. Die Vereinbarkeit eines nachrichtendienstlichen Systems mit Unionsrecht

7.2.1. Vereinbarkeit mit EG-Recht

Tätigkeiten und Maßnahmen im Dienste der Staatssicherheit bzw. der Strafverfolgung fallen grundsätzlich nicht in den Regelungsbereich des EG-Vertrages. Da die Europäische Gemeinschaft aufgrund des Prinzips der beschränkten Einzelermächtigung nur dort tätig werden kann, wo ihr eine entsprechende Kompetenz zusteht, hat sie folgerichtig in den Datenschutzrichtlinien, die auf den EG-Vertrag, insbesondere dessen Art. 95 (ex-Artikel 100a) gestützt sind, diese Gebiete vom Anwendungsbereich ausgenommen. Richtlinie 59/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien

[89] Vgl. dazu oben Kapitel 1, 1.3

[90] Vgl. dazu Kapitel 2

[91] *Vgl. dazu Kapitel 5, 5.6. und 5.8.*

Datenverkehr[92] und Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation[93] gelten "auf keinen Fall für Verarbeitungen[94]/Tätigkeiten[95] betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung/Tätigkeit die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich". Die gleiche Formulierung wurde in den derzeit dem Parlament vorliegenden Richtlinienvorschlag über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation[96] übernommen. Die Beteiligung eines Mitgliedstaates an einem Abhörsystem im Dienste der Staatssicherheit kann somit nicht im Widerspruch zu Datenschutzrichtlinien stehen.

Ebenso wenig kann eine Verletzung des Art. 286 EGV bestehen, der den Anwendungsbereich der Datenschutzrichtlinien auf die Datenverarbeitung durch Organe und Einrichtungen der Gemeinschaft ausdehnt. Das gleiche gilt für die Verordnung 45/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr.[97] Auch diese Verordnung ist nur insofern anwendbar, als die Organe im Rahmen des EG-Vertrages tätig werden.[98] Um Missverständnisse zu vermeiden, sei an dieser Stelle aber ausdrücklich betont, dass eine Beteiligung der Gemeinschaftsorgane und -einrichtungen an einem Abhörsystem von keiner Seite jemals behauptet wurde und dem Berichterstatter dafür auch keinerlei Anhaltspunkt vorliegen.

7.2.2. Vereinbarkeit mit sonstigem EU-Recht

Für die Bereich des Titel V (Gemeinsame Außen- und Sicherheitspolitik) und VI (Polizeiliche und justitielle Zusammenarbeit in Strafsachen) gibt es keine den EG-Richtlinien vergleichbaren Datenschutzbestimmungen. Von Seiten des Europäischen Parlaments wurde bereits mehrfach darauf hingewiesen, dass hier größter Handlungsbedarf besteht.[99]

Der Schutz der Grundrechte und Grundfreiheiten von Personen wird in diesen Bereichen nur durch Art. 6 und 7, insbesondere durch Art. 6 Abs. 2 EUV gewährleistet, in dem sich die Union zur Achtung der Grundrechte verpflichtet, wie sie in der EMRK gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben. Zusätzlich zur Verbindlichkeit der Grundrechte und insbesondere der EMRK für die Mitgliedstaaten (vgl. dazu unten Kapitel 8) entsteht damit eine Verbindlichkeit der Grundrechte für die Union bei

---

[92] ABl. 1995 L 281/31

[93] ABl. 1998 L 24/1

[94] Art. 3 Abs. 2 RL 95/46

[95] Art. 1 Abs. 3 RL 97/66

[96] KOM (2000) 385 endg., ABl. C 365 E/223

[97] Verordnung (EG) Nr. 45/2001, ABl. 2001 L 8/1

[98] Art. 3 Abs. 1; Vgl. auch Erwägungsgrund 15 "Wird diese Verarbeitung von den Organen und Einrichtungen der Gemeinschaft in Ausübung von Tätigkeiten außerhalb des Anwendungsbereichs der vorliegenden Verordnung, insbesondere für die Tätigkeiten gemäß den Titel V und VI des Vertrags über die Europäische Union, durchgeführt, so wird der Schutz der Grundrechte und Grundfreiheiten der Personen unter Beachtung des Artikels 6 des Vertrags über die Europäische Union gewährleistet."

[99] Vgl. z.B. P 25 der Entschließung zu dem Aktionsplan des Rates und der Kommission zur bestmöglichen Umsetzung der Bestimmungen des Amsterdamer Vertrags über den Aufbau eines Raums der Freiheit, der Sicherheit und des Rechts (13844/98 - C4-0692/98 - 98/0923(CNS)), ABl. C 219 vom 30.7.1999, 61 ff

ihrer Tätigkeit in Gesetzgebung und Verwaltung. Da es jedoch auf EU-Ebene bislang keine Regelung über die Zulässigkeit der Überwachung von Telekommunikation zu sicherheits- oder nachrichtendienstlichen Zwecken gibt,[100] stellt sich die Frage der Verletzung des Art. 6 Abs. 2 EUV vorerst nicht.

7.3. Die Frage der Vereinbarkeit im Falle des Missbrauchs des Systems zur Wirtschaftsspionage

Würde ein Mitgliedstaat einem Abhörsystem, das u.a. auch Konkurrenzspionage betreibt, Vorschub leisten, indem er die eigenen Nachrichtendienste dafür instrumentalisieren lässt bzw. fremden Nachrichtendiensten eigenes Territorium für diesen Zweck zur Verfügung stellt, läge sehr wohl ein Verstoß gegen EG-Recht vor. Die Mitgliedstaaten sind nämlich nach Art. 10 EGV zur umfassenden Loyalität verpflichtet, insbesondere zur Unterlassung aller Maßnahmen, die die Verwirklichung der Ziele des Vertrages gefährden würden. Selbst wenn das Abfangen von Telekommunikation nicht zugunsten der heimischen Wirtschaft erfolgt (was übrigens in der Wirkung einer Staatsbeihilfe gleichkäme, und damit gegen Artikel 87 EGV verstieße), sondern zugunsten von Drittstaaten, würde eines solche Tätigkeit in fundamentalem Widerspruch zu dem EG Vertrag zugrunde liegenden Konzept eines Gemeinsamen Marktes stehen, da sie eine Verzerrung des Wettbewerbs bedeuten würde.

Ein solches Verhalten würde nach Ansicht der Berichterstatters überdies eine Verletzung der Datenschutzrichtlinie für den Bereich der Telekommunikation[101] bedeuten, da die Frage der Anwendbarkeit der Richtlinien nach funktionellen Gesichtspunkten und nicht nach organisatorischen gelöst werden muss. Dies ergibt sich nicht nur aus dem Wortlaut der Regelung des Anwendungsbereichs, sondern auch aus dem Sinn des Gesetzes. Benützen Nachrichtendienste ihre Kapazitäten zur Wirtschaftsspionage, so erfolgt ihre Tätigkeit nicht im Dienste der Sicherheit oder Strafverfolgung, sondern ist zweckentfremdet und fällt folglich voll in den Anwendungsbereich der Richtlinie. Diese verpflichtet aber die Mitgliedstaaten in ihrem Art. 5, die Vertraulichkeit de Kommunikation zu sichern, insbesondere "das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Kommunikation durch andere Personen als die Benutzer" zu untersagen. Ausnahmen dürfen nach Art. 14 nur dort gemacht werden, wo sie zur Staatssicherheit, Landesverteidigung und Strafverfolgung notwendig sind. Da Wirtschaftsspionage nicht zu Ausnahmen legitimiert, würde in diesem Fall eine Verletzung von Gemeinschaftsrecht vorliegen.

---

[100] Im Bereich der Telekommunikationsüberwachung gibt es derzeit im Rahmen der EU nur zwei Rechtsakte, die beide nicht die Frage der Zulässigkeit regeln:

- die Entschließung des Rates vom 17. Januar 1995 über die rechtmäßige Überwachung des Fernmeldeverkehrs (ABl. Nr. C 329 v 4.11.1996), in deren Anhang technische Anforderungen zur Realisierung rechtmäßiger Überwachungsmaßnahmen in modernen Telekommunikationssystemen enthalten sind, und

- der Rechtsakt des Rates vom 29. Mai 2000 über die Erstellung des Übereinkommens – gemäß Artikel 34 des Vertrags über die Europäische Union – über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union (ABl. 2000 C 197/1, Art. 17 f), in dem geregelt wird, unter welchen Voraussetzungen Rechtshilfe in Strafsachen hinsichtlich der Telekommunikationsüberwachung möglich sein soll. Die Rechte der Abgehörten werden dadurch in keiner Weise beschnitten, da der Mitgliedstaat, in dem sich der Abgehörte befindet, die Rechtshilfe immer dann verweigern kann, wenn sie nach dessen innerstaatlichem Recht nicht zulässig ist.

[101] RL 97/66 EG, ABl. 1998 L 24/1

7.4. Ergebnis

Zusammenfassend lässt sich sagen, dass bei der derzeitigen Rechtslage ein nachrichtendienstliches System des Typs ECHELON deshalb nicht in Widerspruch zu Unionsrecht stehen kann, weil es nicht die Berührungspunkte mit Unionsrecht aufweist, die für eine Unvereinbarkeit erforderlich wären. Dies gilt allerdings nur, solange das System wirklich ausschließlich im Dienste der Staatssicherheit verwendet wird. Wird es hingegen zweckentfremdet und zur Konkurrenzspionage gegen ausländische Unternehmen eingesetzt, so ergibt sich ein Widerspruch zum EG-Recht. Beteiligte sich ein Mitgliedstaat daran, würde er gegen Gemeinschaftsrecht verstoßen.

8. Die Vereinbarkeit nachrichtendienstlicher Kommunikationsüberwachung mit dem Grundrecht auf Privatsphäre

8.1. Kommunikationsüberwachung als Eingriff in das Grundrecht auf Privatsphäre

Jedes Abhören von Kommunikation, ja schon die Erfassung von Daten durch Nachrichtendienste zu diesem Zweck[102] stellt einen tiefgreifenden Eingriff in die Privatsphäre des Einzelnen dar. Nur in einem 'Polizeistaat' ist ein schrankenloses Abhören von staatlicher Seite zulässig. In den Mitgliedstaaten der EU als gewachsenen Demokratien hingegen ist die Notwendigkeit der Achtung des Privatlebens durch staatliche Organe, und somit auch durch Nachrichtendienste, unbestritten und findet in der Regel in den Verfassungen der Mitgliedstaaten ihren Niederschlag. Die Privatsphäre genießt somit besonderen Schutz, Eingriffsmöglichkeiten werden nur nach Rechtsgüterabwägung und unter Beachtung des Verhältnismäßigkeitsgrundsatzes gewährt.

Auch in den ECHELON-Staaten ist man sich der Problematik bewusst. Die vorgesehenen Schutzbestimmungen zielen hier allerdings auf die Achtung der Privatsphäre der eigenen Einwohner ab, sodass der europäische Bürger in der Regel daraus keinen Nutzen zieht. So werden in den US-Vorschriften, die die Bedingungen der elektronischen Überwachung regeln, den Staatsinteressen an einem funktionierenden Nachrichtendienst nicht die Interessen eines effektiven allgemeinen Grundrechtsschutzes gegenübergestellt, sondern der erforderliche Schutz der Privatsphäre von "US-Persons".[103]

8.2. Der Schutz der Privatsphäre durch internationale Übereinkommen

Die Achtung der Privatsphäre als grundlegendes Recht wurde in zahlreichen völkerrechtlichen Übereinkommen berücksichtigt.[104] Auf weltweiter Ebene ist insbesondere der "Internationale Pakt über bürgerliche und politische Rechte"[105] zu nennen, der 1966 im Rahmen der UNO

[102] Deutsches Bundesverfassungsgericht (BVerfG), 1 BvR 2226/94vom 14.7.1999, Rz 187 "Eingriff ist [...] schon die Erfassung selbst, insofern sie die Kommunikation für den Bundesnachrichtendienst verfügbar macht und die Basis des nachfolgenden Abgleichs mit den Suchbegriffen bildet."

[103] Vgl. dazu den Bericht an den amerikanischen Congress Ende Februar 2000 "Legal Standards for the Intelligence Community in Conducting Electronic Surveillance", http://www.fas.org/irp/nsa/standards.html, der auf den Foreign Intelligence Surveillance Act (FISA), abgedruckt in Titel 50 Kapitel 36 U.S.C. § 1801 ff und die Exec. Order No. 12333, 3 C.F.R. 200 (1982), abgedruckt in Titel 50, Kapitel 15 U.S.C. § 401 ff verweist, http://www4.law.cornell.edu/uscode/50/index.html.

[104] Art. 12 Allgemeine Erklärung der Menschenrechte; Art. 17 UN Internationaler Pakt über bürgerliche und politische Rechte; Art. 7 der Charta der EU, Art. 8 EMRK; Empfehlung des OECD Rates über Leitlinien für die Sicherheit von Informationssystemen, angenommen am 26./27.11.1993 C(92) 188/Final; Art. 7 Europaratskonvention über den Schutz von Personen betreffend die automatische Verarbeitung personenbezogener Daten; Vgl. dazu die von STOA in Auftrag gegebene Studie „Development of surveillance tehnology and risk of abuse of economic information; Vol 4/5: The legality of the interception of electronic communications: A concise survey of the principal legal issues and instruments under international, European and national law“ (Chris Elliot), Oktober 1999, 2

[105] Internationaler Pakt über bürgerliche und politische Rechte, angenommen von der Generalversammlung der Vereinten Nationen am 96. 12. 1966

abgeschlossen wurde, und in seinem Art. 17 den Schutz der Privatsphäre garantiert. Den Entscheidungen des gemäß Art. 41 errichteten konventionellen Menschenrechtsausschusses, der über die Frage völkerrechtlicher Verletzungen des Paktes befindet, haben sich sämtliche ECHELON-Staaten unterworfen, soweit es um Klagen anderer Staaten geht. Das Zusatzprotokoll[106], das die Kompetenz des Menschenrechtsausschusses auf Individualbeschwerde ausdehnt, wurde aber von den USA nicht unterzeichnet, sodass es für Privatpersonen keine Möglichkeit gibt, im Falle der Verletzung des Paktes durch die USA den Menschenrechtsausschuss anzurufen.

Auf EU-Ebene wurde versucht, einen besonderen europäischen Grundrechtsschutz durch die Erstellung einer "Charta der Grundrechte der EU" zu verwirklichen. Artikel 7 der Charta, der mit "Achtung des Privat- und Familienlebens" betitelt ist, normiert sogar ausdrücklich das Recht auf Achtung der Kommunikation.[107] Überdies wird in Artikel 8 wird das Grundrecht auf "Schutz personenbezogener Daten" normiert. Dies hätte den Einzelnen in den Fällen geschützt, in denen seine Daten (automatisiert oder nicht-automatisiert) verarbeitet werden, was beim Abhören in der Regel, beim sonstigen Abfangen sogar stets der Fall ist.

Die Charta ist bislang nicht in den Vertrag aufgenommen worden. Bindungswirkung entfaltet sie daher nur für die drei Organe, die sich ihr in der "Feierlichen Erklärung" am Rande des Europäischen Rates von Nizza unterworfen haben: Rat, Kommission und Europäisches Parlament. Diese sind nach Kenntnis des Berichterstatters in keinerlei geheimdienstliche Aktivitäten verwickelt. Auch wenn die Charta ihre volle Geltungskraft nach Aufnahme in den Vertrag erreichen wird, muss ihr eingeschränkter Anwendungsbereich berücksichtigt werden. Gemäß Art. 51 gilt die Charta "... für die Organe und Einrichtungen der Union ... und für die Mitgliedstaaten ausschließlich bei der Durchführung des Rechts der Union." Die Charta käme daher allenfalls über das Instrument des Verbots wettbewerbswidriger staatlicher Beihilfen zum Tragen (s. Kapitel 7, 7.3).

Das einzige wirksame Instrument auf internationaler Ebene zum umfassenden Schutz der Privatsphäre stellt die Europäische Menschenrechtskonvention dar.

8.3. Die Regelung der Europäischen Menschenrechtskonvention (EMRK)

8.3.1. Die Bedeutung der EMRK in der EU

Der Grundrechtsschutz, der durch die EMRK eingeräumt wird, hat insofern besondere Bedeutung, als die Konvention von sämtlichen Mitgliedstaaten der EU ratifiziert wurde und damit ein einheitliches europäisches Schutzniveau bildet. Die Vertragsstaaten haben sich völkerrechtlich verpflichtet, die in der EMRK verbrieften Rechte zu garantieren und haben sich der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte (EGMR) in Straßburg unterworfen. Die jeweiligen nationalen Regelungen können daher vom EGMR auf ihre Konformität mit der EMRK überprüft und die Vertragsstaaten im Falle eines Verstoßes gegen

[106] Fakultativprotokoll zu dem internationalen Pakt über bürgerliche und politische Rechte, angenommen von der Generalversammlung von den Vereinten Nationen am 19.12.1966

[107] "Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation."

die Menschenrechte verurteilt und zu Ausgleichszahlungen verpflichtet werden. Darüber hinaus gewann die EMRK dadurch an Bedeutung, dass sie wiederholt vom EuGH im Rahmen von Gesetzesüberprüfungen gemeinsam mit den allgemeinen Rechtsgrundsätzen der Mitgliedstaaten zur Entscheidungsfindung herangezogen wurde. Mit dem Vertrag von Amsterdam wurde überdies in Art. 6 Abs. 2 EUV die Verpflichtung der EU zur Achtung der Grundrechte, wie sie in der EMRK gewährleistet sind, festgeschrieben.

8.3.2. Der räumliche und personelle Schutzumfang der EMRK

Die in der EMRK verbürgten Rechte stellen allgemeine Menschenrechte dar und sind somit nicht an eine Staatsangehörigkeit gebunden. Sie müssen allen Personen, die der Jurisdiktion der Vertragsstaaten unterworfen sind, gewährt werden. Die bedeutet, dass die Menschenrechte jedenfalls auf dem gesamten Staatsgebiet gewährt werden müssen und örtliche Ausnahmen eine Vertragsverletzung bedeuten würden. Darüber hinaus haben sie aber auch außerhalb des Staatsgebietes der Vertragsstaaten Geltung, sofern dort Staatsgewalt ausgeübt wird. Die von der EMRK garantierten Rechte gegenüber einem Vertragsstaat stehen somit auch Personen außerhalb des Staatsgebietes zu, wenn ein Vertragsstaat außerhalb seines Staatsgebietes in deren Privatsphäre eingreift[108].

Letzteres ist hier deshalb besonders wichtig, weil die Grundrechtsproblematik auf dem Gebiet der Telekommunikationsüberwachung die Besonderheit aufweist, dass der für die Überwachung verantwortliche Staat, der Überwachte und der tatsächliche Abhörvorgang räumlich auseinander fallen können. Dies gilt insbesondere für internationale Kommunikation, unter Umständen aber auch für nationale Kommunikation, wenn der Informationstransport über Leitungen im Ausland führt. Für das Vorgehen von Auslandsnachrichtendiensten ist dies sogar der typische Fall. Auch kann nicht ausgeschlossen werden, dass Information aus Überwachung, die ein Nachrichtendienst erlangt hat, an andere Staaten weitergegeben wird.

8.3.3. Die Zulässigkeit der Telekommunikationsüberwachung nach Artikel 8 EMRK

Gemäß Art. 8 Abs. 1 MRK hat "jedermann […] einen Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs." Der Schutz von Telefonie oder Telekommunikation ist zwar nicht ausdrücklich genannt, nach der Rechtsprechung des EGMR sind aber auch sie durch die Begriffe "Privatleben" und "Briefverkehr" vom Schutzumfang des Art. 8 MRK umfasst.[109] Der Schutzumfang des Grundrechts erstreckt sich dabei nicht nur auf den Kommunikationsinhalt, sondern auch auf die Aufzeichnung äußerer Gesprächsdaten. Das bedeutet, dass selbst wenn der Nachrichtendienst nur Daten wie Zeit und Dauer der Verbindungen so wie die angewählten Nummern aufzeichnet, dies einen Eingriff in die Privatsphäre darstellt.[110]

---

[108] Vgl. dazu EGMR Loizidou/Türkei, 23.3.1995, Z 62 mit weiteren Nachweisen "...the concept of 'jurisdiction' under this provision is not restricted to the national territory of the High Contracting Parties.[...] responsibility can be involved because of acts of their authorities, whether performed within or outside national boundaries, which produce effects outside their own territory" mit Verweis auf EGMR, Drozd und Janousek, 26.6.1992, Z 91. Vgl. dazu ausführlich Jacobs, The European Convention on Human Rights (1996), 21 ff

[109] Vgl. dazu EGMR, Klass u.a., 6.9.1978, Z 41.

[110] Vgl. dazu EGMR, Malone, 2.8.1984, Z 83 ff; so auch Davy, B/Davy/U, Aspekte staatlicher Informationssammlung und Art. 8 MRK, JBl 1985, 656.

Das Grundrecht wird gemäß Art. 8 Abs. 2 MRK nicht unbeschränkt gewährt. Eingriffe in das Grundrecht auf Achtung der Privatsphäre können zulässig sein, sofern sie eine Rechtsgrundlage im innerstaatlichen Recht haben.[111] Das Recht muss allgemein zugänglich und seine Konsequenzen vorhersehbar sein.[112]

Die Mitgliedstaaten sind dabei in der Gestaltung dieser Eingriffe nicht frei. Art. 8 EMRK gestattet sie nur zur Verwirklichung der in Absatz 2 aufgelisteten Zwecke, das sind insbesondere die nationale Sicherheit, die öffentliche Ruhe und Ordnung, die Verhinderung von strafbaren Handlungen, aber auch das wirtschaftliche Wohl des Landes[113], das allerdings Wirtschaftsspionage nicht rechtfertigt, da nur "in einer demokratischen Gesellschaft notwendige" Eingriffe darunter fallen. Für jeden Eingriff muss das gelindeste zur Zielerreichung geeignete Mittel gewählt werden, darüber hinaus müssen ausreichende Garantien gegen Missbrauch bestehen.

8.3.4. Die Bedeutung von Artikel 8 EMRK für die Tätigkeit der Nachrichtendienste

Diese allgemeinen Grundsätze bedeuten für die grundrechtskonforme Ausgestaltung der Tätigkeit der Nachrichtendienste Folgendes: Scheint es zur Gewährleistung nationaler Sicherheit notwendig¸ Nachrichtendienste zum Abfangen von Telekommunikationsinhalt oder zumindest Verbindungsdaten zu berechtigen, so muss dies im innerstaatlichen Recht niedergelegt und die Regelung allgemein zugänglich gemacht werden. Die Konsequenzen daraus müssen für den Einzelnen vorhersehbar sein, die besonderen Erfordernisse im Geheimbereich werden aber wohl zu berücksichtigen sein. So hat der Gerichtshof in einer Entscheidung über die Art. 8-Konformität von geheimen Kontrollen von Bediensteten in Bereichen, die die nationale Sicherheit betreffen, festgestellt, dass der Anspruch an Vorhersehbarkeit in diesem speziellen Fall nicht der Gleiche sein kann wie auf anderen Gebieten.[114] Er hat aber auch hier verlangt, dass das Recht jedenfalls darüber Auskunft geben müsse, unter welchen Umständen und Bedingungen die Staatsgewalt einen geheimen und damit potenziell gefährlichen Eingriff in die Privatsphäre vornehmen darf.[115]

Für die menschenrechtskonforme Ausgestaltung der nachrichtendienstlichen Tätigkeit ist dabei zu beachten, dass die nationale Sicherheit zwar einen Rechtfertigungsgrund dafür darstellt, dass dieser aber nach Art. 8 Abs. 2 EMRK dem Verhältnismäßigkeitsgrundsatz unterliegt: Auch die nationale Sicherheit kann Eingriffe nur dort rechtfertigen, wo sie in einer demokratischen Gesellschaft notwendig sind. Der EGMR hat dazu eindeutig erklärt, dass das Interesse des

---

[111] Nach der Rspr. des EGMR (insbesondere Sunday Times, 26.4.1979, Z 46 ff, Silver u.a., 25.3.1983, Z 85 ff) umfasst der Begriff "law" in Art. 8 Abs. 2 nicht nur Gesetze im formellen Sinn, sondern auch Rechtsvorschriften unter der Gesetzesstufe, u.U. sogar ungeschriebenes Recht. Voraussetzung ist jedoch jedenfalls, dass es dem Rechtsunterworfenen erkennbar ist, unter welchen Umständen ein solcher Eingriff möglich ist. Vgl. dazu Wessley, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht? ÖJZ 1999, 491 ff, 495

[112] Silver u.a., 25.3.1983, Z 87 f

[113] Der Rechtfertigungsgrund des "wirtschaftlichen Wohles" wurde vom EGMR angenommen in einem Fall, in dem es um Weitergabe von für die Zuweisung öffentlicher Ausgleichszahlungen bedeutsamen medizinischen Daten ging M.S./Schweden, 27.8.1997, Z 38, sowie in einem Fall, in dem es um die Ausweisung einer Person aus den Niederlanden ging, die von der sozialen Wohlfahrt lebte, nachdem der Grund für ihre Aufenthaltsberechtigung weggefallen war. Ciliz/Niederlande, 11.7.2000, Z 65.

[114] EGMR, Leander, 26.3.1987, Z 51

[115] EGMR, Malone, 2.8.1984, Z 67

Staates, seine nationale Sicherheit zu schützen, gegen die Schwere des Eingriffes mit den Interessen des Einzelnen an der Achtung seiner Privatsphäre abgewogen werden muss.[116] Eingriffe sind zwar nicht auf das unerlässliche Maß beschränkt, aber ein bloßes nützlich oder wünschenswert sein genügt nicht[117]. Die Auffassung, dass ein Abhören jedweder Telekommunikation der beste Schutz vor organisierter Kriminalität wäre, würde selbst wenn dies vom innerstaatlichen Recht vorgesehen wäre, gegen Art. 8 EMRK verstoßen.

Zudem müssen aufgrund des besonderen Charakters nachrichtendienstlicher Tätigkeit, welcher Geheimhaltung und damit eine besondere Interessenabwägung verlangt, umso stärkere Kontrollmöglichkeiten vorgesehen werden. Der Gerichtshof hat ausdrücklich darauf hingewiesen, dass ein geheimes Überwachungssystem zur Sicherung nationaler Sicherheit das Risiko in sich trägt, dass es unter dem Vorwand, die Demokratie zu verteidigen, diese unterminiert oder gar zerstört, und es deshalb adäquater und effektiver Garantien gegen solchen Missbrauch bedürfe.[118] Die gesetzlich legitimierte Tätigkeit von Nachrichtendiensten ist somit nur dann grundrechtskonform, wenn der Vertragsstaat der EMRK ausreichende Kontrollsysteme und andere Garantien gegen Missbrauch geschaffen hat. Der Gerichtshof hob dabei im Zusammenhang mit der nachrichtendienstlichen Tätigkeit Schwedens hervor, dass er dem Beisein von Abgeordneten im polizeilichen Kontrollorgan sowie der Überwachung durch den Justizminister, den parlamentarischen Ombudsmann und den parlamentarischen Rechtsausschuss besondere Bedeutung beimesse. Unter diesem Aspekt erscheint bedenklich, dass Frankreich, Griechenland, Irland, Luxemburg und Spanien keine eigenen parlamentarischen Kontrollausschüsse für Geheimdienste haben[119] und auch ein dem parlamentarischen Ombudsmann der nordischen Staaten vergleichbares Kontrollsystem nicht kennen.[120] Der Berichterstatter begrüßt daher die Bestrebungen des Verteidigungsausschusses der französischen Assemblée Nationale, einen Kontrollausschuss zu gründen,[121] umsomehr als Frankreich technisch und geographisch über bemerkenswerte nachrichtendienstliche Kapazitäten verfügt.

8.4. Die Verpflichtung zur Wachsamkeit gegenüber der Tätigkeit fremder Nachrichtendienste

8.4.1. Unzulässigkeit der Umgehung von Artikel 8 EMRK durch Einschalten fremder Nachrichtendienste

Wie oben ausführlich dargelegt müssen die Vertragsstaaten eine Summe von Voraussetzungen erfüllen, damit die Tätigkeit ihrer Nachrichtendienste mit Art. 8 MRK vereinbar ist. Es liegt auf der Hand, dass sich die Nachrichtendienste dieser Verpflichtungen nicht dadurch entledigen können, dass sie auf die Tätigkeit anderer Nachrichtendienste zurückgreifen, die weniger strengen Bestimmungen unterliegen. Anderenfalls wäre das Legalitätsprinzip mit seinen beiden

[116] EGMR, Leander, 26.3.1987, Z 59, Sunday Times, 26.4.1979, Z 46 ff

[117] EGMR, Silver u.a., 24.10.1983, Z 97

[118] EGMR, Leander, 26.3.1987, Z 60.

[119] Dem Berichterstatter ist bekannt, dass weder Luxemburg noch Irland über einen Auslandsnachrichtendienst verfügen und auch kein SIGINT betreiben. Das Erfordernis einer besonderen Kontrollinstanz bezieht sich hier nur auf die nachrichtendienstlichen Tätigkeiten im Inland.

[120] Zur Situation der Kontrolle der Nachrichtendienste in den Mitgliedstaaten siehe Kapitel 9.

[121] Vgl. dazu den Gesetzesentwurf "Proposition de loi tendant à la création de délégations parlementaires pour le renseignement", und den diesbezüglichen Bericht von Abgeordnetem Arthur Paecht, N° 1951 Assemblée nationale, 11. Legislaturperiode, registriert am 23. November 1999

Komponenten der Zugänglichkeit und Voraussehbarkeit seiner Wirkung beraubt und die Rechtsprechung des EGMR in ihrem Inhalt ausgehöhlt.

Dies bedeutet zum einen, dass Datenaustausch zwischen Nachrichtendiensten nur eingeschränkt zulässig ist. Ein Nachrichtendienst darf von einem anderen Daten nur dann erlangen, wenn diese unter Voraussetzungen ermittelt werden konnten, die das eigene nationale Recht vorsieht. Der vom Gesetz vorgesehene Aktionsradius darf nicht durch Absprachen mit anderen Diensten erweitert werden. In gleicher Weise darf er Tätigkeiten für einen fremden Nachrichtendienst entsprechend dessen Anweisungen nur dann durchführen, wenn er sich von deren Konformität mit dem eigenen nationalen Recht überzeugt hat. Auch wenn die Informationen für einen anderen Staat bestimmt sind, ändert dies nichts an der Grundrechtswidrigkeit eines für den Rechtsunterworfenen unvorhersehbaren Eingriffs.

Zum anderen dürfen Vertragsstaaten der EMRK fremde Nachrichtendienste nicht auf ihrem Gebiet tätig werden lassen, wenn es Anlass zur Vermutung gibt, dass deren Tätigkeit nicht den Voraussetzungen der EMRK entspricht.[122]

8.4.2. Konsequenzen für die geduldete Tätigkeit außereuropäischer Nachrichtendienste auf dem Territorium von Mitgliedstaaten der EMRK

8.4.2.1. Die einschlägige Rechtssprechung des Europäischen Gerichtshofs für Menschenrechte

Mit Ratifizierung der EMRK haben sich die Vertragsstaaten verpflichtet, die Ausübung ihrer Souveränität der Grundrechtsüberprüfung zu unterwerfen. Sie können sich dieser Verpflichtung nicht dadurch begeben, dass sie auf ihre Souveränität verzichten. Diese Staaten bleiben für ihr Staatsgebiet verantwortlich und damit den europäischen Rechtsunterworfenen auch dann verpflichtet, wenn die Ausübung der Hoheitsgewalt durch nachrichtendienstliche Tätigkeit von einem anderen Staat vorgenommen wird. Vom EGMR wird mittlerweile in ständiger Judikatur eine Pflicht der Vertragsstaaten bejaht, positive Maßnahmen zum Schutz der Privatsphäre zu setzen, damit keine Verletzung des Art. 8 EMRK durch Private (!) eintritt, also selbst auf horizontaler Ebene, wo der Einzelne nicht der Staatsgewalt, sondern einer anderen Person gegenüber steht.[123] Lässt ein Staat einen fremden Nachrichtendienst auf seinem Territorium arbeiten, so ist das Schutzbedürfnis wesentlich größer, weil hier eine andere Obrigkeit ihre Hoheitsgewalt ausübt. Es scheint hier nur logisch davon auszugehen, dass der Staat über die Menschenrechtskonformität nachrichtendienstlicher Tätigkeit auf seinem Territorium wachen muss.

8.4.2.2. Konsequenzen für Stationen

In Deutschland wird den Vereinigten Staaten von Amerika in Bad Aibling eigenes Territorium zur ausschließlichen Nutzung für Satellitenempfang zur Verfügung gestellt. In Menwith Hill in Großbritannien wird eine Mitnutzung von Gelände zum gleichen Zweck erlaubt. Falls in diesen Stationen von einem amerikanischen Nachrichtendienst nichtmilitärische Kommunikation von Privaten oder von Unternehmen abgehört würde, die aus einem Vertragsstaat der EMRK stammt,

[122] Vgl. dazu auch Yernault, "Echelon" et l'Europe. La protection de la vie privée face à l'espionnage des communications, Journal des tribunaux, Droit Européen 2000, 187 ff.

[123] EGMR, Abdulaziz, Cabales und Balkandali, 28.5.1985, Z 67; X u Y/Niederlande, 26.3.1985, Z 23; Gaskin vs Vereinigtes Königreich 7.7.1989, Z 38; Powell und Rayner, 21.2.1990, Z 41

so löst die EMRK Aufsichtspflichten aus. Das bedeutet praktisch, dass Deutschland und das Vereinigte Königreich als Vertragsstaaten der EMRK verpflichtet sind, sich der Grundrechtskonformität der Tätigkeit der amerikanischen Nachrichtendienste zu vergewissern. Dies gilt umso mehr, als sich Vertreter von NRO und Presse bereits mehrfach über das Vorgehen der NSA besorgt gezeigt haben.

8.4.2.3. Konsequenzen für in fremdem Auftrag durchgeführtes Abhören

In Morwenstow in Großbritannien wird nach den vorliegenden Informationen von GCHQ in Zusammenarbeit mit der NSA zivile Kommunikation strikt nach deren Anweisung abgefangen und als Rohmaterial an die USA weitergegeben. Auch bei Auftragsarbeiten für Dritte gilt die Pflicht, die Grundrechtskonformität des Auftrags zu prüfen.

8.4.2.4. Besondere Sorgfaltspflicht bei Drittstaaten

Bei Vertragsstaaten der EMRK kann bis zu einem gewissen Grad wechselseitig davon ausgegangen werden, dass der andere Staat die EMRK auch einhält. Dies gilt jedenfalls solange, bis einem EMRK-Vertragsstaat nachgewiesen wird, dass er systematisch und chronisch die EMRK verletzt. Bei den USA handelt es sich um einen Staat, der nicht Vertragsstaat der EMRK ist, und der sich auch nicht einem vergleichbaren Kontrollsystem unterworfen hat. Die Tätigkeit seiner Nachrichtendienste ist sehr präzise geregelt, sofern sie US-Bürger bzw. Personen, die sich rechtmäßig in den USA aufhalten, betrifft. Auf die Tätigkeit der NSA im Ausland finden aber andere Regelungen Anwendung, von denen augenscheinlich viele klassifiziert und damit unzugänglich sind. Zusätzlich besorgniserregend erscheint dabei, dass der amerikanische Nachrichtendienst zwar der Kontrolle durch die Ausschüsse in Abgeordnetenhaus und Senat unterliegt, diese parlamentarischen Ausschüsse an der Tätigkeit der NSA im Ausland aber nur geringes Interesse zeigen.

Es scheint daher angebracht, an Deutschland und England zu appellieren, die aus der EMRK erwachsenden Verpflichtungen ernst zu nehmen und die Gestattung weiterer nachrichtendienstlicher Tätigkeiten durch die NSA auf ihrem Territorium davon abhängig zu machen, dass diese im Einklang mit der EMRK stehen. Dabei sind drei Hauptaspekte zu beachten.

1. Nach der EMRK dürfen Eingriffe in die Privatsphäre nur aufgrund rechtlicher Regelungen erfolgen, die allgemein zugänglich und deren Konsequenzen für den Einzelnen absehbar sind. Diese Anforderung ist nur dann erfüllt, wenn die USA der europäischen Bevölkerung offen legen, auf welche Weise und unter welchen Umständen Aufklärung betrieben wird. Sofern Unvereinbarkeiten mit der EMRK bestehen, müssen die Regelungen an das europäische Schutzniveau angepasst werden.

2. Eingriffe dürfen nach der EMRK nicht unverhältnismäßig sein, zudem muss das gelindeste Mittel gewählt werden. Für den europäischen Bürger ist ein Eingriff, der von europäischer Seite vorgenommen wird, als weniger tiefgreifend zu werten als einer von amerikanischer Seite, da ihm nur im ersten Fall der Rechtszug an nationale Instanzen offen steht.[124] Eingriffe müssen daher so weit wie möglich von deutscher bzw. englische Seite vorgenommen werden, folgerichtig jedenfalls die im Dienste der Strafverfolgung. Von amerikanischer Seite wurde

[124] Dadurch wird auch Konformität zu Art. 13 EMRK hergestellt, der den Verletzten ein Recht auf Beschwerde vor den nationalen Instanzen zuerkennt.

wiederholt versucht, das Abhören von Telekommunikation mit dem Vorwurf der Korruption und Bestechung von europäischer Seite zu rechtfertigen.[125] Die USA seien darauf verwiesen, dass alle EU-Staaten über funktionierende Strafrechtssysteme verfügen. Liegen Verdachtsmomente vor, so hat die USA die Strafverfolgung den Gastländern zu überlassen. Liegen keine Verdachtsmomente vor, so ist eine Überwachung als unverhältnismäßig einzustufen, folglich menschenrechtswidrig und daher unzulässig. Vereinbarkeit mit der EMRK ist daher nur dann gegeben, wenn sich die USA auf Überwachungsmaßnahmen beschränken, die ihrer nationalen Sicherheit dienen, von solchen zum Zwecke der Strafverfolgung aber absehen.

3. Wie oben bereits dargestellt, hat der EGMR im seiner Rechtsprechung für die Grundrechtskonformität verlangt, dass es ausreichende Kontrollsysteme und Garantien gegen Missbrauch gibt. Dies bedeutet, dass amerikanische Telekommunikationsüberwachung von europäischem Boden aus nur dann menschenrechtskonform ist, wenn die USA für die Fälle, in denen sie von dort aus Kommunikation zum Zwecke ihrer nationalen Sicherheit abfangen, entsprechend effektive Kontrollen schaffen bzw. wenn sich die NSA in ihrer Tätigkeit auf europäischem Boden den Kontrolleinrichtungen des Aufnahmestaates (also denen Deutschlands bzw. Großbritanniens) unterwirft.

Nur wenn den in diesen drei Punkten niedergelegten Anforderungen entsprochen wird, kann die Konformität des Vorgehens der USA beim Abfangen von Telekommunikation mit der EMRK sichergestellt werden und das durch die EMRK einheitlich garantierte Schutzniveau in Europa aufrechterhalten bleiben.

[125] Woolsey (ehemaliger Direktor der CIA), Why America Spies on its Allies, The Wall Street Journal Europe, 22.3.2000, 31

9. Sind EU-Bürger gegenüber der Tätigkeit der Nachrichtendienste ausreichend geschützt?

9.1. Schutz vor nachrichtendienstlicher Tätigkeit: eine Aufgabe der nationalen Parlamente

Da die Tätigkeit der Nachrichtendienste zwar künftig einen Aspekt der GASP darstellen kann, derzeit aber auf EU-Ebene noch keine diesbezüglichen Regelungen bestehen,[126] ist die Gestaltung des Schutzes gegenüber der Tätigkeit der Nachrichtendienste allein von den nationalen Rechtsordnungen abhängig.

Die nationalen Parlamente üben hierbei eine doppelte Funktion aus: Als Gesetzgeber entscheiden sie über den Bestand und die Befugnisse der Nachrichtendienste sowie über die Ausgestaltung der Kontrolle nachrichtendienstlicher Tätigkeit. Wie im vorigen Kapitel ausführlich dargelegt, müssen sich die Parlamente bei der Regelung der Frage der Zulässigkeit von Telekommunikationsüberwachung an die durch Art. 8 EMRK festgelegten Schranken halten, d.h. die Regelungen müssen notwendig, verhältnismäßig und ihre Konsequenzen für den Einzelnen absehbar sein, überdies müssen den Befugnissen der Überwachungsbehörden entsprechend adäquate und effektive Kontrollmechanismen geschaffen werden.

Darüber hinaus haben die nationalen Parlamente in den meisten Staaten eine aktive Rolle als Kontrollbehörden, da die Kontrolle der Exekutive (und damit auch der Nachrichtendienste) neben der Gesetzgebung die zweite "klassische" Funktion eines Parlaments ist. Die Ausgestaltung erfolgt in den Mitgliedstaaten der EU aber auf sehr unterschiedliche Weise, häufig bestehen parlamentarische und nichtparlamentarische Organe nebeneinander.

9.2. Die Befugnis nationaler Behörden zur Durchführung von Überwachungsmaßnahmen

Überwachungsmaßnahmen von staatlicher Seite dürfen in der Regel zur strafrechtlichen Verfolgung, zur Gewährung der inneren Ruhe und Ordnung und zur Staatssicherheit[127] (gegenüber dem Ausland) vorgenommen werden.

Zum Zwecke der Strafrechtsverfolgung darf in allen Mitgliedstaaten das Fernmeldegeheimnis gebrochen werden, sofern der hinlängliche Verdacht der Begehung einer (zuweilen besonders qualifizierten, also mit einem höheren Unwertsgrad ausgestatteten) Straftat durch eine konkrete Person besteht. Aufgrund der Schwere des Eingriffs ist hierfür in der Regel eine richterliche Genehmigung erforderlich,[128] es gibt präzise Angaben über zulässige Dauer der Überwachung, ihre Kontrolle und die Löschung der Daten.

---

[126] Vgl. dazu auch Kapitel 7

[127] Diese Zwecke werden auch von Art. 8 Abs. 2 EMRK als Rechtfertigungsgründe für Eingriffe in die Privatsphäre anerkannt. Vgl. dazu oben 8.3.2.

[128] Anders allerdings das britische Recht, das die Entscheidung über die Genehmigung dem Secretary of State überträgt (Regulation of Investigatory Powers Act 2000, Section 5 (1) und (3) (b)

Zur Gewährleistung der inneren Sicherheit und Ordnung wird die staatliche Informationsbeschaffung über individuelle Untersuchungen im Falle von konkretem Straftatverdacht hinaus ausgeweitet. Zur Früherkennung von extremistischen oder subversiven Bewegungen, von Terrorismus und organisierter Kriminalität gestattet der nationale Gesetzgeber zusätzliche Informationsgewinnung über bestimmte Personen oder Gruppierungen. Das Sammeln relevanter Daten sowie deren Analyse erfolgen dabei durch besondere Inlandsnachrichtendienste.

Schlussendlich bilden einen wichtigen Teil der Überwachungsmaßnahmen jene im Dienste der Staatssicherheit. Die Bearbeitung, Auswertung und Darstellung relevanter Informationen über das Ausland obliegt in der Regel einem eigenen Auslandsnachrichtendienst.[129] Das Ziel der Überwachung sind im Regelfall keine konkreten Einzelpersonen, erfasst werden vielmehr bestimmte Gebiete bzw. Frequenzen. Abhängig von den dem Auslandsnachrichtendienst zur Verfügung stehenden Mitteln und rechtlichen Befugnissen gibt es ein weites Spektrum, das von rein militärischer Funkaufklärung im Kurzwellenbereich bis zur Überwachung sämtlicher Arten von Telekommunikationsverbindungen zum Ausland reicht. In manchen Mitgliedstaaten ist die Überwachung von Telekommunikation zu rein nachrichtendienstlichen Zwecken überhaupt verboten,[130] in anderen Mitgliedstaaten ist sie - teilweise unter Vorbehalt der Genehmigung durch eine unabhängige Kommission[131] - bei Anordnung durch Minister gestattet,[132], für manche Kommunikationswege sogar ohne jede Beschränkung.[133] Die verhältnismäßig großen Befugnisse mancher Auslandsnachrichtendienste sind darauf zurückzuführen, dass sie auf die Überwachung von Auslandskommunikation abzielen und daher nur einen geringen Anteil der eigenen Rechtsunterworfenen treffen, die Sorge darum daher wesentlich geringer ist.

9.3. Die Kontrolle der Nachrichtendienste

Eine effiziente und umfassende Kontrolle ist deshalb besonders wichtig, weil zum einen Nachrichtendienste im Geheimen arbeiten, ihr Arbeit langfristig ausgerichtet ist, die betroffenen Personen also oft lange Zeit oder (abhängig von der Rechtslage) auch gar nicht von der vollzogenen Überwachung erfahren, und zum anderen Überwachungsmaßnahmen oft größere, unscharf definierte Gruppen von Personen betreffen, sodass der Staat sehr schnell eine sehr große Menge persönlicher Daten erlangen kann.

Es stellt sich natürlich allen Kontrollegremien - völlig unabhängig von ihrer Ausgestaltung - das Problem, dass aufgrund des besonderen Charakters von Geheimdiensten oft kaum feststellbar ist, ob tatsächlich alle Informationen zur Verfügung gestellt werden oder ein Teil zurückgehalten wird. Umso sorgfältiger muss die Reglementierung erfolgen. Grundsätzlich wird man davon ausgehen können, dass eine hohe Wirksamkeit der Kontrolle und damit eine weitgehende

[129] Zu der Tätigkeit von Auslandsnachrichtendiensten Vgl. die ausführliche Darstellung in Kapitel 2

[130] So in Österreich und Belgien

[131] So in Deutschland, Gesetz zur Beschränkung des Brief-, Post-, und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz). Gemäß § 9 ist die Kommission (außer bei Gefahr im Verzug) vor dem Vollzug zu benachrichtigen.

[132] So in Großbritannien (Regulation of Investigatory Powers Act, Section 1) und in Frankreich für leitungsgebundene Kommunikation (Art. 3 une 4 Loi 91-646 du 10 Juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications)

[133] So für leitungsungebundene Kommunikation in Frankreich (Art. 20 Loi 91-646 du 10 Juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications)

Garantie der Gesetzmäßigkeit der Eingriffe dann gegeben ist, wenn die Anordnung der Telekommunikationsüberwachung der höchsten Verwaltungsebene vorbehalten ist, sie für die Durchführung einer vorherigen richterlichen Genehmigung bedarf und ein unabhängiges Organ auch den Vollzug der Maßnahmen überwacht. Darüber hinaus ist es unter demokratiepolitischen und rechtsstaatlichen Überlegungen wünschenswert, dass die Arbeit der Nachrichtendienstes als Ganzes in Übereinstimmung mit dem Prinzip der Gewaltenteilung der Kontrolle eines parlamentarischen Organs unterliegt.

Dies ist weitgehend in Deutschland verwirklicht. Dort werden Maßnahmen zur Telekommunikationsüberwachung vom zuständigen Bundesminister angeordnet. Außer bei Gefahr im Verzug ist vor der Durchführung eine eigene unabhängige, weisungsungebundene Kommission ("G-10-Kommission"[134]) darüber zu unterrichten, die über die Notwendigkeit und Zulässigkeit der Maßnahme entscheidet. In den Fällen, in denen der deutsche Auslandsnachrichtendienst BND zur Überwachung des nicht leitungsgebundenen Telekommunikationsverkehr mithilfe der Filterung durch Suchbegriffe berechtigt werden kann, entscheidet die Kommission auch über die Zulassung der Suchbegriffe. Der G-10-Kommission obliegt überdies die Kontrolle über die gesetzlich vorgeschriebene Mitteilung an die Betroffenen sowie über die Vernichtung der gewonnenen Daten durch den BND.

Daneben gibt es ein parlamentarisches Kontrollgremium (PKGr)[135], das sich aus 9 Abgeordneten des nationalen Parlamentes zusammensetzt und die Tätigkeit aller drei deutschen Nachrichtendienste überwacht. Das PKGr hat Recht auf Akteneinsicht, auf Anhörung von Mitarbeitern der Nachrichtendienste sowie auf Besuch bei den Diensten und auf Unterrichtung, wobei Letzteres nur verweigert werden kann, wann dies aus zwingenden Gründen des Nachrichtenzugangs oder aus Gründen des Schutzes von Persönlichkeitsrechten Dritter notwendig ist oder wenn der Kernbereich der exekutiven Eigenverantwortung betroffen ist. Die Beratungen des PKGr sind geheim, die Mitglieder sind – auch nach ihrem Ausscheiden - zur Geheimhaltung verpflichtet. In der Mitte und am Ende der Wahlperiode erstattet das PKGr dem Deutschen Bundestag einen Bericht über die Kontrolltätigkeit.

Eine derartig umfassende, praktisch lückenlose Kontrolle der Nachrichtendiensten bildet allerdings in den Mitgliedstaaten die Ausnahme.

In Frankreich[136] beispielsweise bedürfen nur Überwachungsmaßnahmen, die das Anzapfen von Kabel verlangen, der Genehmigung des Premierministers. Nur sie unterliegen der Überwachung durch die eigens eingerichtete Kommission (Commission nationale de contrôle des interceptions de sécurité), der ein Abgeordneter und ein Senator angehören. Die Genehmigung einer von einem Minister oder dessen Delegierten beantragten Abhörmaßnahme wird dem Vorsitzenden der Kommission zugestellt, der bei Zweifel an der Gesetzmäßigkeit die Kommission damit befassen kann, welche dann Empfehlungen abgibt und im Falle der Vermutung einer strafrechtlich relevanten Gesetzesverletzung die Staatsanwaltschaft verständigt.

---

[134] Vgl. dazu ausführlich: Die Parlamentarische Kontrolle der Nachrichtendienste in Deutschland, Stand 9.9.2000, herausgegeben vom Deutschen Bundestag, Sekretariat des PKGr

[135] Gesetz über die Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG)vom 17. Juni 1999 BGBl I 1334 idgF.

[136] Loi 91-646 du 10 Juillet 1991, loi relative au secret des correspondances émises par la voie des telécommunications

Abhörmaßnahmen zum Zwecke der Verteidigung nationaler Interessen, die das Abhören von Funkverkehr beinhalten, also auch Kommunikation via Satellit, unterliegen keinerlei Beschränkung und damit auch nicht der Kontrolle einer Kommission.

Die Arbeiten der französischen Nachrichtendienste unterliegen im Übrigen auch nicht der Kontrolle eines eigenen parlamentarischen Kontrollausschusses, es sind jedoch diesbezügliche Arbeiten im Gange. Vom Verteidigungsausschuss der Assemblée Nationale wurde bereits eine diesbezüglicher Vorschlag angenommen,[137] eine Diskussion darüber im Plenum hat derzeit aber noch nicht statt gefunden.

Im Vereinigten Königreich bedarf jede Kommunikationsüberwachung auf britischem Boden der Genehmigung auf Ministerebene (Secretary of State). Die Formulierung des Gesetzes lässt jedoch Unklarheit darüber bestehen, ob das nicht zielgerichtete, breite Abfangen von Kommunikation, die auf Schlüsselwörter überprüft wird, auch unter den von der "Regulation of Investigatory Powers Act 2000" (RIP) verwendeten Begriff "interception" fallen würde, wenn die Auswertung nicht auf britischen Boden erfolgt, sondern das "Rohmaterial" ohne Auswertung ins Ausland übermittelt wird. Die Kontrolle der Einhaltung der Bestimmungen des RIP 2000 erfolgt (ex-post) durch Commissioners, vom Premierminister ernannte amtierende oder ehemalige höhere Richter. Der für Abhörmaßnahmen zuständige Commissioner (Interception Commissioner) überwacht die Erteilung von Abhörgenehmigungen und unterstützt die Untersuchung von Beschwerden über Abhörmaßnahmen. Der Intelligence Service Commissioner überwacht die Genehmigungen für die Aktivitäten der Nachrichten- und Sicherheitsdienste und unterstützt die Untersuchungen von Beschwerden über diese Dienste. Das Investigatory Powers Tribunal, dem ein höherer Richter vorsitzt, untersucht alle Beschwerden über Abhörmaßnahmen und die Tätigkeiten der Dienste.

Die parlamentarische Kontrolle erfolgt durch das Intelligence and Security Committee (ISC),[138] das die Tätigkeit aller drei zivilen Nachrichtendienste (MI5, MI6 und GCHQ) überwacht. Ihm obliegt insbesondere die Prüfung der Ausgaben und der Verwaltung sowie die Kontrolle des Vorgehens des Sicherheitsdienstes, des Nachrichtendienstes und des GCHQ. Der Ausschuss besteht aus 9 Mitgliedern aus Unterhaus und Oberhaus, unter denen kein Minister sein darf. Im Unterschied zu den Kontrollausschüssen anderer Staaten, die in der Regel vom Parlament bzw. Parlamentspräsidenten gewählt oder ernannt sind, werden sie vom Premierminister nach Konsultation des Oppositionsführers ernannt.

Schon anhand dieser Beispiele zeigt sich, dass das Schutzniveau sehr unterschiedlich ist. Was die parlamentarische Kontrolle anbelangt, so möchte der Berichterstatter darauf hinweisen, dass das Bestehen eigener Kontrollausschüsse für die Überwachung von Nachrichtendiensten sehr wichtig ist. Sie haben nämlich gegenüber den Hauptausschüssen den Vorteil, dass sie höheres Vertrauen bei den Nachrichtendiensten genießen, da ihre Mitglieder der Verschwiegenheit unterliegen und die Sitzungen unter Ausschluss der Öffentlichkeit stattfinden. Zudem sind sie zur Erfüllung ihrer besonderen Aufgabe mit besonderen Rechten ausgestattet, was zur Überwachung von Tätigkeiten im Geheimbereich unerlässlich ist.

[137] Vgl. dazu den Gesetzesentwurf "Proposition de loi tendant à la création de délégations parlementaires pour le renseignement", und den diesbezüglichen Bericht von Abgeordnetem Arthur Paecht, N° 1951 Assemblée nationale, 11. Legislaturperiode, registriert am 23. November 1999

[138] Intelligence services act 1994, Section 10

Erfreulicherweise hat die Mehrzahl der Mitgliedstaaten der EU zur Kontrolle der Nachrichtendienste eigene parlamentarische Kontrollausschüsse eingesetzt. In Belgien[139], Dänemark[140], Deutschland[141], Italien[142], den Niederlanden[143] und Portugal[144] gibt es einen parlamentarischen Kontrollausschuss, der sowohl für die Kontrolle des militärischen als auch für die des zivilen Nachrichtendienstes zuständig ist. Im Vereinigten Königreich[145] überwacht der besondere Kontrollausschuss nur die (allerdings wesentlich bedeutsameren) zivilen Nachrichtendienste, der militärische wird vom normalen Verteidigungsausschuss überwacht. In Österreich[146] werden die beiden Zweige des Nachrichtendienstes von zwei verschiedenen Kontrollausschüssen abgedeckt, die allerdings gleich organisiert und mit den gleichen Rechten ausgestattet sind. In den nordischen Staaten Finnland[147] und Schweden[148] nehmen Ombudsmänner die Aufgaben der parlamentarischen Kontrolle wahr, die unabhängig sind und vom Parlament gewählt werden. In Frankreich, Griechenland, Irland, Luxemburg und Spanien gibt es keine eigenen parlamentarischen Ausschüsse, die Kontrollaufgaben werden hier nur von den Hauptausschüssen im Rahmen der allgemeinen parlamentarischen Tätigkeit ausgeübt.

9.4. Beurteilung der Situation für den europäischen Bürger

Die Situation in Europa erscheint für den europäischen Bürger wenig zufriedenstellend. Die Befugnisse der Nachrichtendiensten im Bereich der Telekommunikationsüberwachung sind in ihrer Reichweite sehr unterschiedlich, das Gleiche gilt für die Kontrollausschüsse. Nicht alle Mitgliedstaaten, die einen Nachrichtendienst betreiben, verfügen auch über unabhängige

---

[139] Comité permanent de contrôle des services de renseignements et de sécurité, Comité permanent R, Loi du 18 juillet 1991 /IV, organique du contrôle des services de police et de renseignements.

[140] Udvalget vedrørende efterretningstjenesterne, Lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester, lov 378 af 6/7/88.

[141] Das parlamentarische Kontrollgremium (PKGr), Gesetz über die Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG)vom 17. Juni 1999 BGBl I 1334 idgF.

[142] Comitato parlamentare, L. 24 ottobre 1977, n. 801, Art. 11, Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato.

[143] Tweede-Kamercommissie voor de Inlichtingen- en Veiligheidsdiensten, 17. Reglement van orde van de Tweede Kamer der Staten-General, Art. 22.

[144] Conselho de Fiscalização dos Serviços de Informações (CFSI), Gesetz 30/84 vom 5. September 1984, geändert durch das Gesetz 4/95 vom 21. Februar 1995, das Gesetz 15/96 vom 30. April 1996 und das Gesetz 75-A/97 vom 22. Juli 1997.

[145] Intelligence and Security Committee (ISC), intelligence services act 1994, Section 10.

[146] Ständiger Unterausschuss des Landesverteidigungsausschusses zur Überprüfung von nachrichtendienstlichen Maßnahmen zur Sicherung der militärischen Landesverteidigung und Ständiger Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit, Art. 52a B-VG, §§ 32b ff Geschäftsordnungsgesetz 1975.

[147] Ombudsmann, gesetzliche Grundlage für die Kontrolle für die Polizei (SUPO): Poliisilaki 493/1995 §33 und Laki pakkokeinolain 5 a luvun muuttamisesta 366/1999 §15, für das Militär: Poliisilaki 493/1995 §33 und Laki poliisin tehtävien suorittamisesta puolustusvoimissa 1251/1995 §5.

[148] Rikspolisstyrelsens ledning, Förordning (1989:773) med instruktion för Rikspolisstyrelsen (Verordnung (1989:773) über die nationale Polizeibehörde).

parlamentarische Kontrollgremien, die mit den entsprechenden Kontrollbefugnissen ausgestattet sind. Von einem einheitlichen Schutzniveau ist man weit entfernt.

Aus europäischer Sicht ist dies umso bedauerlicher, als dieser Zustand nicht sosehr die eigenen Bürger dieser Staaten trifft, die durch ein entsprechendes Wahlverhalten auf das Schutzniveau Einfluss nehmen können. Die nachteiligen Auswirkungen treffen vor allem die Staatsangehörigen anderer Staaten, da der Tätigkeitsbereich von Auslandsnachrichtendiensten naturgemäß auf das Ausland gerichtet ist. Ausländischen Systemen ist der Einzelne relativ wehrlos ausgeliefert, das Schutzbedürfnis ist hier noch größer. Es darf auch nicht vergessen werden, dass aufgrund des besonderen Charakters von Nachrichtendiensten EU-Bürger von der Tätigkeit mehrerer Nachrichtendienste gleichzeitig betroffen sein können. Ein einheitliches Schutzniveau, das den demokratischen Grundsätzen gerecht wird, wäre hier wünschenswert. Es sollten in diesem Zusammenhang auch Überlegungen angestellt werden, inwieweit auf diesem Gebiet Datenschutzbestimmungen auf EU-Ebene realisierbar erscheinen.

Darüber hinaus wird sich die Frage des Schutzes des europäischen Bürgers ganz neu stellen, wenn im Rahmen einer gemeinsamen Sicherheitspolitik eine Zusammenarbeit der Nachrichtendienste der Mitgliedstaaten in Angriff genommen wird. Hier sind dann die europäischen Institutionen gefordert, ausreichende Schutzbestimmungen zu erlassen. Es wird Aufgabe des Europäischen Parlaments als Verfechter rechtsstaatlicher Prinzipien sein, darauf zu dringen, dass dann von seiner Seite als demokratisch legitimiertem Organ eine entsprechende Kontrolle erfolgt. Das Europäische Parlament ist hier aber auch berufen, die Voraussetzungen dafür zu schaffen, damit die vertrauliche Behandlung derart sensibler Daten sowie anderer geheimer Dokumente durch einen besonders ausgestalteten Ausschuss, dessen Mitglieder zur Verschwiegenheit verpflichtet sind, garantiert werden kann. Nur bei Vorliegen dieser Bedingungen wird es realistisch und im Hinblick auf eine - für eine ernst zu nehmende gemeinsame Sicherheitspolitik absolut notwendige - funktionierende Zusammenarbeit der Nachrichtendienste verantwortbar sein, diese Kontrollrechte einzufordern.

10. Der Schutz gegen Wirtschaftsspionage

*)

10.1. Das Spionageziel Wirtschaft

In einem Wirtschaftsunternehmen gibt es hinsichtlich von Geheimhaltung drei Arten von Informationen. Das sind zum einen Informationen, die absichtlich **möglichst weit verbreitet** werden. Dazu gehören Sachinformationen über die Produkte des Unternehmens (z.B. Produkteigenschaften, Preise etc.) und werbewirksame Informationen, die das Image des Unternehmens beeinflussen.

Dann gibt es Informationen die **weder geschützt noch aktiv verbreitet** werden, weil sie mit der Wettbewerbsposition des Unternehmens nicht zu tun haben. Als Beispiele seien das Datum des Betriebsausfluges, die Speisekarte in der Kantine oder die Marke der verwendeten Faxgeräte angeführt.

Und schließlich gibt es Informationen, die **vor der Kenntnisnahme durch andere geschützt** werden. Die Information werden vor der Konkurrenz aber auch, wenn ein Unternehmen die Gesetze nicht einhalten will, vor dem Staat (Steuer, Embargoregeln etc.) geschützt. Dabei gibt es verschiedene Grade des Schutzes bis hin zur strengen Geheimhaltung, z.B. bei Forschungsergebnissen vor der Patentanmeldung oder bei der Produktion von Rüstungsgütern[149].

Spionage hat in dem jetzt diskutierten Fall mit der Beschaffung der von einem Unternehmen geheimgehaltenen Informationen zu tun. Ist der Angreifer ein Konkurrenzunternehmen, so spricht man von **Konkurrenzspionage** (auch Werkspionage, Industriespionage). Handelt es sich beim Angreifer um einen staatlichen Nachrichtendienst, spricht man von **Wirtschaftsspionage.**

10.1.1. Die Spionageziele im Detail

Strategische Daten, die für auf Wirtschaft gerichtete Spionage von Bedeutung sind, lassen sich nach Branchen oder nach Unternehmensbereichen klassifizieren.

10.1.1.1. Branchen

Es ist selbsterklärend klar, dass Informationen aus den folgenden Bereichen von hohem Interesse sind: Biotechnologie, Gentechnologie, Medizintechnik, Umwelttechnik, Hochleistungscomputer, Software, Optoelektronik, Bild-Sensor- und Signaltechnik, Datenspeicher, technische Keramik, Hochleistungslegierungen, Nanotechnologie. Die Liste ist nicht komplett und ändert sich im Übrigen auch laufend entsprechend der technologischen Entwicklung. In diesen Bereichen geht es bei Spionage vor allem um das Stehlen von Forschungsergebnissen oder speziellen Produktionstechniken.

10.1.1.2. Unternehmensbereiche

Die Angriffsziele für Spionage liegen logischerweise in den Bereichen Forschung und Entwicklung, Einkauf, Personal, Produktion, Distribution, Verkauf, Marketing, Produktlinien

[149] Informationen für geheimschutzbetreute Unternehmen, BMWI 1997

und Finanzen. Oft werden die Bedeutung und der Wert dieser Daten unterschätzt (siehe unten 10.1.4)

10.1.2. Konkurrenzspionage

Die strategische Position eines Unternehmens am Markt hängt von seiner Verfassung in den Bereichen Forschung und Entwicklung, Produktionsverfahren, Produktlinien, Finanzierung, Marketing, Verkauf, Distribution, Einkauf und Arbeitskräfte ab[150]. Informationen darüber sind für jeden Mitwettbewerber am Markt von hohem Interesse, weil sie Auskunft über Pläne und Schwächen geben und so das Einleiten strategischer Gegenmaßnahmen erlauben.

Ein Teil dieser Informationen ist öffentlich zugänglich. Es gibt hoch spezialisierte Beratungsfirmen, die im völlig legalen Rahmen eine Konkurrenzanalyse erstellen, darunter so renommierte Firmen wie z.B. Roland & Berger in Deutschland. „Competitive Intelligence" gehört in den USA inzwischen zum Standardwerkzeug des Managements [151]. Aus einer Vielzahl von Einzelinformationen wird bei professioneller Ausführung eine klares Situationsbild erstellt.

Der Übergang von der Legalität zur strafbewehrten Konkurrenzspionage ergibt sich durch die Wahl der Mittel, mit denen Informationen beschafft werden. Erst wenn die eingesetzten Mittel in der jeweiligen Rechtsordnung illegal sind, beginnt der kriminelle Bereich – das Anfertigen von Analysen an sich ist nicht strafbar. Die für einen Konkurrenten besonders interessanten Informationen werden natürlich vor einem Zugriff geschützt und können nur unter Rechtsbruch beschafft werden. Die dabei verwendeten Techniken unterscheiden sich in nichts von den im Kapitel 2 beschrieben allgemeinen Methoden von Spionage.

Präzise Angaben über das Ausmaß von Konkurrenzspionage gibt es nicht. Die Dunkelziffer ist, wie bei klassischer Spionage auch, sehr hoch. Die beiden beteiligten Parteien (Täter und Opfer) haben kein Interesse an Publizität. Für betroffene Unternehmen bedeutet dies immer einen Imageverlust., und die Angreifer haben natürlich auch kein Interesse an der Veröffentlichung ihrer Aktivitäten. Deshalb werden nur wenige Fälle vor Gericht anhängig.

Trotzdem gibt es immer wieder Berichte in der Presse über Konkurrenzspionage. Der Berichterstatter hat darüber hinaus über diese Frage mit einigen Sicherheitschefs großer deutscher Unternehmen[152] und mit Managern amerikanischer und europäischer Firmen gesprochen. Zusammenfassend lässt sich feststellen, dass Konkurrenzspionage immer wieder entdeckt wird, dass sie aber nicht das tägliche Geschehen bestimmt.

10.2. Der Schaden durch Wirtschaftsspionage

Aufgrund der hohen Dunkelziffer lässt sich das Ausmaß des Schadens durch Konkurrenzspionage/Wirtschaftsspionage nicht exakt beziffern. Dazu kommt, dass ein Teil der genannten Zahlen interessengeleitet hoch sind. Sicherheitsfirmen und Abwehrdienste haben ein verständliches Interesse, den Schaden am oberen Ende der realistisch möglichen Skala anzusiedeln. Trotzdem geben die Zahlen einen gewissen Eindruck.

---

[150] M.F.Porter, Competitive Strategy

[151] Hummelt, Roman, Wirtschaftsspionage auf dem Datenhighway, Hanserverlag, München 1997

[152] Details und Namen sind geschützt.

Bereits 1988 schätzte das Max Planck Institut den Schaden durch Wirtschaftspionage in Deutschland auf mindestens 8 Milliarden DM[153]. Der Vorsitzende des Verbandes der Sicherheitsberatungsunternehmen in Deutschland nennt unter Berufung auf Experten einen Betrag von 15 Milliarden DM/Jahr. Der Präsident der europäischen Polizeigewerkschaften Hermann Lutz schätzt den Schaden auf 20 Mrd. DM jährlich. Das FBI[154] nennt für die Jahre 1992/1993 einen Schaden von 1,7 Mrd. US-Dollar, den die amerikanische Wirtschaft durch Konkurrenz- und Wirtschaftsspionage erleidet. Der ehemalige Vorsitzende des Geheimdienstkontrollausschusses des House of Representatives in den USA spricht von 100 Milliarden US-Dollar an Verlusten, bedingt durch entgangene Aufträge und zusätzliche Forschungs- und Entwicklungskosten. Zwischen 1990 und 1996 habe dies einen Verlust von 6 Millionen Arbeitsplätzen zur Folge gehabt.[155]

Im Grunde ist es nicht notwendig, den Schaden genau zu kennen. Eine Verpflichtung des Staates mit Polizei und Abwehrbehörden gegen Konkurrenz- und Wirtschaftsspionage vorzugehen besteht unabhängig von der Höhe des volkswirtschaftlichen Schadens. Auch für die Entscheidungen in den Unternehmen über den Schutz von Informationen und eigene Spionageabwehrmaßnahmen sind Gesamtschadenszahlen keine brauchbare Grundlage. Jedes Unternehmen muss für sich den maximal möglichen Schaden durch Informationsdiebstahl berechnen, die Eintrittswahrscheinlichkeit abschätzen und die so zustande gekommen Beträge mit den Kosten für Sicherheit vergleichen. Das eigentliche Problem besteht nicht im Fehlen genauer Gesamtschadenszahlen. Vielmehr ist es so, dass außer in den Großunternehmen solche Kosten/Nutzenrechnungen kaum angestellt werden und deshalb Sicherheit vernachlässigt wird.

10.3. Wer spioniert?

Die wesentlichen Auftraggeber bei Spionage gegen Unternehmen sind laut einer Studie der Wirtschaftsprüfergesellschaft Ernest Young LLP[156] mit 39% Konkurrenten, mit 19% Kunden, mit 9% Zulieferer und mit 7% Geheimdienste. Spioniert wird von eigenen Mitarbeitern, privaten Spionagefirmen, bezahlten Hackern und Profis der Geheimdienste.[157]

10.3.1. Eigene Mitarbeiter (Insiderdelikte)

Die ausgewertete Literatur, die diesbezüglichen Angaben von Experten im Ausschuss und die Gespräche des Berichterstatters mit Sicherheitschefs und Spionageabwehrbehörden zeigen übereinstimmend: Die größte Spionagegefahr geht von enttäuschten und unzufriedenen Mitarbeitern aus. Sie haben als Beschäftigte des Betriebes direkt Zugang zu Informationen, lassen sich durch Geld anwerben und spähen für ihre Auftraggeber Betriebsgeheimnisse aus.

Große Risiken gibt es auch beim Jobwechsel. Heutzutage müssen nicht Berge von Papier kopiert werden, damit wichtige Informationen aus dem Unternehmen getragen werden können. Sie lassen sich unbemerkt auf Disketten speichern und beim Arbeitsplatzwechsel zum neuen Arbeitgeber mitnehmen.

---

[153] IMPULSE,3/97,S.13 ff.

[154] Congressional Statement, L.J.Freech, Director FBI, 9.5.1996

[155] Robert Lyle, Radio Liberty/Radio fre Europe, 10.Februar 1999

[156] Computerzeitung, 30.11.1995, S.2

[157] R.Hummelt, Spionage auf dem Datenhighway, München 1997, S.49ff

10.3.2. Private Spionagefirmen

Die Zahl der Firmen, die sich auf das Ausspähen von Daten spezialisiert haben, wächst ständig. Teilweise arbeiten ehemalige Mitarbeiter von Nachrichtendiensten in solchen Firmen. Diese Firmen arbeiten häufig sowohl als Sicherheitsberatungsunternehmen als auch als Detekteien, die im Auftrag Informationen beschaffen. In der Regel werden legale Methoden eingesetzt, aber es gibt auch Firmen, die sich illegaler Methoden bedienen.

10.3.3. Hacker

Hacker sind Computerspezialisten, die sich mit ihren Kenntnissen von außen Zugang zu Computernetzen verschaffen können. In den Gründerjahren der Hackerszene waren es Computerfreaks, die ihren Spaß daran hatten, die Sicherheitsvorkehrungen von Rechnersystemen zu überwinden. Heute gibt es Auftragshacker, sowohl bei den Diensten als auch auf dem Markt.

10.3.4. Nachrichtendienste

Nach dem Ende des kalten Krieges haben sich die Aufgaben der Nachrichtendienste verschoben. Internationale Organisierte Kriminalität und wirtschaftliche Sachverhalte sind neue Aufgabenfelder (Näheres in Kapitel 10, 10.5).

10.4. Wie wird spioniert?

Nach Angaben von Abwehrbehörden und von Sicherheitschefs großer Unternehmen werden bei der Wirtschaftsspionage alle erprobten nachrichtendienstlichen Methoden und Instrumente eingesetzt (siehe Kapitel 2, 2.4). Unternehmen haben aber offenere Strukturen als militärische und nachrichtendienstliche Einrichtungen oder Regierungsstellen. Bei Wirtschaftsspionage kommen deshalb zusätzliche Risiken hinzu:

- das Anwerben von Mitarbeitern ist einfacher, weil die Möglichkeiten der Konzernsicherheit mit denen der Abwehrbehörden nicht vergleichbar sind;
- die Mobilität des Arbeitsplatzes führt dazu, dass wichtige Informationen auf dem Laptop mitgeführt werden. Der Diebstahl von Laptops oder das heimliche Kopieren der Festplatte nach Einbruch ins Hotelzimmer gehört deshalb zur Standardtechnik der Wirtschaftsspionage;
- der Einbruch in Computernetze gelingt leichter als bei sicherheitsempfindlichen staatlichen Einrichtungen, weil gerade bei kleinen und mittleren Unternehmen Sicherheitsbewusstsein und Sicherheitsvorkehrungen viel weniger ausgeprägt sind;
- Das Abhören vor Ort (siehe Kapitel 3, 3.2) ist aus den gleichen Gründen einfacher.

Die Auswertung der dazu gesammelten Informationen ergibt, dass die Wirtschaftsspionage hauptsächlich vor Ort oder am mobilen Arbeitsplatz ansetzt, weil sich mit wenigen Ausnahmen (siehe unten 10.6) die gesuchten Informationen nicht durch Abhören der internationalen Telekommunikationsnetze finden lassen.

10.5. Wirtschaftsspionage durch Staaten

10.5.1. Strategische Wirtschaftsspionage durch Nachrichtendienste

Nach dem Ende des kalten Krieges sind nachrichtendienstliche Kapazitäten freigeworden, die jetzt auf anderen Gebieten eingesetzt werden. Die USA erklären offen, dass ein Teil ihrer nachrichtendienstlichen Tätigkeiten auch die Wirtschaft berührt. Darunter fällt z.B. die Überwachung der Einhaltung von Wirtschaftssanktionen, die Überwachung der Einhaltung der Regeln für Lieferung von Waffen und sogenannten Dual-use-Gütern, die Entwicklungen auf Rohstoffmärkten und das Geschehen auf den internationalen Finanzmärkten. Nach Erkenntnissen des Berichterstatters kümmern sich nicht nur die US-Dienste um diesen Bereich und daran gibt es auch keine massive Kritik.

10.5.2. Nachrichtendienste als Agenten von Konkurrenzspionage

Kritik wird dann formuliert, wenn staatliche Nachrichtendienste dafür missbraucht werden, Unternehmen auf ihrem Staatsgebiet durch Spionage Vorteile im internationalen Wettbewerb zu verschaffen. Dabei sind zwei Fälle zu unterscheiden[158].

10.5.2.1. Hightech-Staaten

Hochentwickelte Industriestaaten können durchaus von Industriespionage profitieren. Durch Ausspähung des Entwicklungsstandes einer Branche können eigene außenwirtschaftliche und subventionspolitische Maßnahmen veranlasst werden, die entweder die eigene Industrie konkurrenzfähiger machen oder Subventionen einsparen. Ein weiterer Schwerpunkt kann in der Beschaffung von Details bei Aufträgen mit hohem Auftragswert bestehen (siehe unten 10.6).

10.5.2.2. Technisch weniger fortgeschrittene Staaten

Bei einem Teil dieser Staaten geht es um die Beschaffung von technischen Know-how, um den Rückstand der eigenen Industrie ohne Entwicklungskosten und Lizenzgebühren aufholen zu können .Darüber hinaus geht es um die Beschaffung von Produktvorlagen und Fertigungstechniken, um mit kostengünstiger (Löhne!) gefertigten Nachbauten auf dem Weltmarkt wettbewerbsfähig zu sein. Es ist bewiesen, dass die russischen Dienste diese Aufgabe zugewiesen bekommen haben. Das Bundesgesetz Nr.5 der Russischen Föderation über die Auslandsaufklärung benennt ausdrücklich die Beschaffung wirtschaftlicher und wissenschaftlich-technischer Informationen als Aufgabe der Nachrichtendienste.
Bei einem anderen Teil von Staaten (z.B. Iran, Irak, Syrien, Libyen, Nordkorea, Indien und Pakistan) geht es um die Beschaffung von Informationen für ihre nationalen Rüstungsprogramme vor allem im Nuklearbereich und im Bereich der biologischen und chemischen Waffen. Ein anderer Teil der Tätigkeit der Dienste dieser Staaten besteht im Betreiben von Tarnfirmen zum unverdächtigen Einkauf von Dual-use-Gütern.

10.6. Eignet sich ECHELON für Industriespionage?

Mit der strategischen Kontrolle internationaler Fernmeldeverkehre lassen sich für Konkurrenzspionage bedeutsame Informationen nur als Zufallsfunde gewinnen. Tatsächlich befinden sich sensible Unternehmensdaten vor allem in den Unternehmen selbst, **sodass Konkurrenzspionage in erster Linie dadurch erfolgt, dass versucht wird, über Mitarbeiter**

[158] Privatmitteilung eines Abwehrdienstes an den Berichterstatter, Quelle geschützt

oder eingeschleuste Personen Informationen zu bekommen oder in die internen Computernetzwerke einzudringen. Nur wenn sensible Daten über Leitungen oder via Funk (Satellit) nach außen gelangen, kann ein Kommunikationsüberwachungssystem zur Konkurrenzspionage eingesetzt werden. Dies trifft systematisch in folgenden drei Fällen zu:

- bei Unternehmen, die in 3 Zeitzonen arbeiten, so dass die Zwischenergebnisse von Europa nach Amerika und weiter nach Asien gesendet werden;

- im Falle von Videokonferenzen in multinationalen Konzernen, die über V-Sat oder Kabel laufen;

- wenn wichtige Aufträge vor Ort verhandelt werden (wie beim Anlagenbau, beim Aufbau von Telekommunikationsinfrastruktur, Neuerrichtung von Transportsystemen etc.), und von dort aus Rücksprachen mit der Firmenzentrale gehalten werden müssen**.**

Wenn Unternehmen in diesen Fällen ihre Kommunikation nicht schützen, dann liefert ein Abgreifen dieser Kommunikation wertvolle Daten für Konkurrenzspionage.

10.7. Veröffentlichte Fälle

Es gibt einige Fälle von Wirtschafts- bzw. Konkurrenzspionage, die in der öffentlichen Presse bzw. in einschlägiger Literatur beschrieben sind. Ein Teil dieser Quellen wurde ausgewertet und ist in der folgenden Tabelle zusammengefasst. Es wird kurz genannt, wer daran beteilig war, wann der Fall aufgetreten ist, worum es im Detail gegangen ist, was das Ziel und die Folgen waren.
Auffällig ist, dass teilweise über ein und denselben Fall sehr unterschiedlich berichtet wird. Als Beispiel sei der Fall Enercon genannt, bei dem als „Täter“ die NSA oder das US-Wirtschaftsministerium oder der fotografierenden Konkurrenten beschrieben wird.

Fall	Wer	Wann	Was	Wie	Ziel	Folgen	Quelle
Air France	DGSE	Bis 1994	Gespräche reisender Geschäftsleute	In den 1.Klasse Kabinen der Air France wurden Wanzen entdeckt – Fluggesellschaft entschuldigte sich öffentlich	Informationsbeschaffung	Nicht genannt	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/
Airbus	NSA	1994	Informationen über Flugzeuggeschäft zwischen Airbus und saudi-arabischer Fluglinie	Abhören der Faxe und Telefonate zwischen den Verhandlungspartnern	Informationsweitergabe an die amerikanischen Konkurrenten Boeing und Mc-Donnell-Douglas	Amerikaner schließen das 6-Milliarden-Doller-Geschäft ab	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9. November 2000
Airbus	NSA	1994	Vertrag über 6 Milliarden $ mit Saudi Arabien Aufdeckung von Bestechung des europäischen Airbus-Konsortiums.	Abhören von Faxen und Telephonaten zw: europäischem Airbus-Konsortium und saudischer Fluggesellschaft/Regierung über Kommunikationssatelliten	Aufdeckung von Bestechung	McDonnel-Douglas, der amerikanische Konkurrent zu Airbus schließt das Geschäft ab	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, von Duncan Campbell
BASF	Vertriebsmann	Nicht genannt	Verfahrensbeschreibung für Produktion von Hautcremerohstoff der Firma BASF (Kosmetiksparte)	nicht genannt	nicht genannt	keine, weil aufgeflogen	„Nicht gerade zimperlich“, Wirtschaftswoche Nr.43 / 16. Oktober 1992
Bundeswirtschaftsministerium DE	CIA	1997	Informationen über High-Tech-Produkte im Bundeswirtschaftsministerium	Einsatz von Agent	Informationsbeschaffung	Agent wird bei Versuch enttarnt und ausgewiesen	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Bundeswirtschaftsministerium DE	CIA	1997	Hintergründe des Berliner Mykonos-Prozesses, Hermeskredite bzgl. Iran-Exporten, Aufstellung deutscher Unternehmen, die High-Tech-Produkte an Iran liefern	CIA-Agent getarnt als US-Botschafter führt freundschaftliches Gespräche mit Leiter des für den arabischen Raum (Schwerpunkt Iran) zuständigen Referates im Bundeswirtschafts-Ministerium	Informationsbeschaffung	Nicht genannt Beamter wendet sich an deutsche Sicherheitsbehörden, die den amerik. Stellen signalisieren, CIA-Operation sei unerwünscht. CIA-Agent wird daraufhin „abgezogen“.	„Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste“, Landesamt für Verfassungsschutz Baden-Württemberg, Stuttgart, Stand: 1998
Dasa	Russischer NDs	1996 – 1999	Verkauf und Weitergabe rüstungstechnologischer Unterlagen eines Münchner Wehrtechnik-Unternehmens (nach SZ / 30.05.2000: Rüstungskonzern Dasa in Ottobrunn)	2 Deutsche im Auftrag	Informationsbeschaffung über Lenkflugkörper, Waffensysteme (Panzer- und Flugabwehr)	SZ / 30.05.2000: „(...) Verrat unter militärischen Gesichtspunkten „nicht besonders schwer“. Dies gelte auch für den wirtschaftlichen Schaden, stellte das Gericht fest.“	„Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Bonn, April 2001 „Haftstrafe wegen Spionage für Russland“, SDZ / 30. Mai 2000
Embargo	BND	um 1990	Erneuter Export embargo-geschützter Technologie nach	Abhören des Fernmeldeverkehrs	Aufdeckung illegalen Waffen- u. Technologietransfers	keine besonderen Konsequenzen, Lieferungen	"Maulwürfe in Nadelstreifen", Andreas Förster, S. 110

			Libyen (u.a. durch Siemens)			werden nicht verhindert	

Fall	Wer	Wann	Was	Wie	Ziel	Folgen	Quelle
Enercon	Windkraftexperte aus Oldenburg und Mitarbeiterin von Kenetech	Nicht genannt	Windkraftanlage der Auricher Firma Enercon	nicht genannt	nicht genannt	nicht genannt	„Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Bonn, April 2001
Enercon	NSA	Nicht genannt	Windrad zur Stromgewinnung, entwickelt von ostfriesischem Ingenieur Aloys Wobben	Nicht genannt	Weitergabe technischer Vorgaben Wobbens an US-Firma	US-Firma meldet Windrad vor Wobben zum Patent an; Wobben wird von US-Anwaltskanzlei angeklagt (Patentrechtverletzung)	„Aktenkrieger“, SZ, 29. März 2001
Enercon	US-Firma Kenetech Windpower Corp	1994	Wichtige Details einer High-Tech-Windanlage (Schaltanlagen bis Platinen)	Fotographien	erfolgreiches Patentverfahren in den USA	Enercon GmbH legt Pläne zur Erschließung des amerikanischen Marktes auf Eis	„Sicherheit muss künftig zur Chefsache werden“, HB / 29. August 1996
Enercon	Oldenburger Ingenieur W. und US-Firma Kenetech	März 1994	Windgenerator Typ E-40 von Enercon	Ingenieur W. gibt Erkenntnisse weiter, Mitarbeiterin von Kenetech fotografiert Anlage + elek. Details	Kenetech: recherchiert Beweise für spätere (1995) Patentverletzungsklage gegenüber Enercon Enercon: illegale Informationsbeschaffung von Betriebsgeheimnissen Fernsehjournalist soll von ehemaligem NSA-Mitarbeiter erfahren haben, dass Detailwissen von Enercon über Echelon von den Amerikanern an Kenetech weitergeleitet wurde.	nicht genannt	„Klettern für die Konkurrenz“, SZ 13. Oktober 2000
Enercon	Kenetech Windpower	Vor 1996	Daten für Windenergie-Anlage von Enercon	Kenetech-Ingenieure fotografieren Anlage	Nachbau der Anlage bei Kenetech	Enercon bekommt recht; gegen Spione wird Strafantrag gestellt; Geschätzter Verlust: mehrere hundert Mio DM	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Handelsministerium Japan	CIA	1996	Verhandlungen über Importquoten für US-Wagen auf dem japanischen Markt	Hacking im Computersystem des japanischen Handelsministeriums	US-Unterhändler Mickey Kantor soll bei niedrigstem Angebot einwilligen	Kantor nimmt niedrigstes Angebot an	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98

Japanische Autos	US Regierungr	Nicht genannt	Verhandlungen über den Import von japanischen Luxuswagen Information zu Emissionsstandards von japanischen Wagen.	COMINT, nicht genauer beschrieben	Informationsbeschaffung	Keine Angaben	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, von Duncan Campbell

Fall	Wer	Wann	Was	Wie	Ziel	Folgen	Quelle
López	NSA	Nicht genannt	Videokonferenz von VW und López	Abhören von Bad Aibling aus	Infoweitergabe an General Motors und Opel	Durch Abhörmaßnahme hätte Staatsanwaltschaft „sehr genaue Hinweise“ für Ermittlung erhalten	Bundeswehrhauptmann Erich Schmidt-Eenboom, zitiert in „Wenn Freunde spionieren“ www.zdf.msnbc.de/news/54637.asp?cp1=1
López	López u. drei seiner Mitarbeiter	1992 - 1993	Papiere u. Daten aus den Bereichen Forschung, Planung, Fertigung u. Einkauf (Unterlagen f. Werk in Spanien, Kostendaten versch. Modellreihen, Projektstudien, Einkaufs- und Sparstrategien)	Material sammeln	Verwendung der General-Motors-Unterlagen durch VW	Nach strafrechtlicher Auseinandersetzung einigen sich die Konzerne außergerichtlich. López tritt 1996 als VW-Manager zurück, VW trennt sich 1997 von drei weiteren Mitarbeitern des López-Teams, zahlt 100 Millionen Dollar an GM/Opel (angeblich Anwaltskosten) und erwirbt 7 Jahre lang Ersatzteile für insgesamt 1 Milliarde Dollar von GM/Opel	„Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste“, Landesamt für Verfassungsschutz Baden-Württemberg, Stuttgart, Stand: 1998
López	NSA	1993	Videokonferenz zwischen José Ignacio López und VW-Chef Ferdinand Piëch	Mitschnitt der Videokonferenz und deren Weitergabe an General Motors (GM)	Schutz der amerikanischen GM-Betriebsgeheimnisse, die López an VW weitergeben wollte (Preislisten, geheime Pläne über neue Autofabrik und neuen Kleinwagen)	López fliegt auf, Strafverfahren wird 1998 gegen Zahlung von Geldbussen eingestellt, Bezüglich NSA nichts	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9. November 2000 „Abgehört“, Berliner Zeitung, 22. Januar 1996 „Die Affäre López ist beendet“, Wirtschaftsspiegel, 28. Juli 1998 „Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
Los Alamos	Israel	1988	Zwei Mitarbeiter des israel. Atomforschungsprogramms knacken den Zentralcomputer des Atomwaffenlabors Los Alamos	Hacking	Informationsbeschaffung über neuen US-Atomwaffenzünder	keine besonderen Konsequenzen, da Hacker nach Israel fliehen, einer wird dort vorübergehend festgenommen, von Verbindung mit israel. Geheimdienst ist offiziell keine Rede	"Maulwürfe in Nadelstreifen", Andreas Förster, S. 137

Schmuggel	BND	70er Jahre	Schmuggel von Computeranlagen in die DDR	nicht genannt	Aufdeckung von Technologietransfer in den Ostblock	keine besonderen Konsequenzen, Lieferungen werden nicht verhindert	"Maulwürfe in Nadelstreifen", Andreas Förster, S. 113

Fall	Wer	Wann	Was	Wie	Ziel	Folgen	Quelle
TGV	DGSE	1993	Kostenkalkulation von Siemens Auftrag für Lieferung von Hochgeschwindigkeitszügen nach Südkorea	Nicht genannt	Preisunterbietung	Der ICE-Hersteller verliert den Auftrag zugunsten Alcatel-Alsthom	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ von Arno Schütze, 1/98
TGV	Unbekannt	1993	Kostenkalkulation von AEG u. Siemens bzgl. Staatsauftrag in Südkorea zur Lieferung von Hochgeschwindigkeitszügen	Siemens erhebt Vorwurf, seine Telefon- und Faxverbindungen bei der Firmenniederlassung in Seoul seinen abgehört worden	Verhandlungsvorteil für den britisch-französischen Mitbewerber GEC Alsthom	Auftraggeber entscheiden sich für GEC Alsthom, obwohl deutsches Angebot erst besser war	„Abgehört“, Berliner Zeitung, 22. Januar1996
Thomson-Alcatel vs. Raytheon	CIA/ NSA	1994	Vergabe eines brasilianischen Milliardenauftrags zur Satellitenüberwachung des Amazonas an frz Thomson-Alcatel (1,4 Mia $)	Abhören des Kommunikationsverkehrs des Gewinners der Ausschreibung (Thomson-Alcatel, FR)	Aufdeckung von Korruption (Auszahlung von Bestechungsgeldern)	Clinton beschwert sich bi brasilianischer Regierung; auf Drängen der US-Regierung Neuvergabe des Auftrags an US-Firma "Raytheon"	"Maulwürfe in Nadelstreifen", Andreas Förster, S. 91
Thomson-Alcatel vs. Raytheon	US-Wirtschaftsministerium „habe sich bemüht“	1994	Verhandlungen über Milliardenprojekt zur Radarüberwachung des brasilianischen Regenwaldes	Nicht genannt	Auftrag übernehmen	Die franz. Konzerne Thomson CSF und Alcatel verlieren zugunsten der US-Firma Raytheon den Auftrag	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9. November 2000
Thomson-Alcatel vs. Raytheon	NSA Department of Commerce	Department of Commerce	Verhandlungen über Milliardenprojekt (1.4 Mia $) zur Überwachung des Amazonas (SIVA) Aufdeckung von Bestechung des brasilisanischen Selection Panels. Anmerkung von Campbell: Rayethon rüstet Abhörstation in Sugar Grove aus	Abhören der Verhandlung zwischen Thomson-CSF und Brasilien und Weitergabe der Ergebnisse an Raytheon Corp.	Aufdeckung von Bestechung Auftragsübernahme	Raytheon bekommt den Vertrag	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, von Duncan Campbell http://www:rayethon:com/sivam/contract:html
Thyssen	BP	1990	Millionenauftrag zur Gas- und Ölförderung in der Nordsee	Abhören von Faxen des Gewinners der Ausschreibung (Thyssen)	Aufdeckung von Korruption	BP verklagt Thyssen auf Schadensersatz	"Maulwürfe in Nadelstreifen", Andreas Förster, S. 92
VW	Unbekannt	„vergangene Jahre“	nicht genannt	u. a. in Erdhügel eingegrabene Infrarotkamera, die per Funk Bilder übermittelt	Informationsbeschaffung über Neuentwicklungen	V W gibt Gewinnverluste in dreistelliger Höhe an	„Sicherheit muss künftig zur Chefsache werden“, HB / 29. August 1996
VW	Unbekannt	1996	Teststrecke in Ehra-Lessien von VW	Versteckte Kamera	Informationen über neue Modelle von VW	Nicht genannt	„Auf Schritt und Tritt“ Wirtschaftswoche Nr. 25, 11. Juni 1998

10.8. Schutz vor Wirtschaftsspionage

10.8.1. Rechtlicher Schutz

In den Rechtsordnungen aller Industriestaaten ist der Diebstahl von Betriebsgeheimnissen strafbewehrt. Wie in allen anderen Fällen des Strafrechts auch ist das nationale Schutzniveau verschieden dicht ausgestaltet. In der Regel gilt aber, dass das Strafmaß deutlich hinter dem für Fälle von Spionage im Zusammenhang mit militärischer Sicherheit zurückbleibt. In vielen Fällen ist die Konkurrenzspionage aber nur gegen Unternehmen im Inland verboten, aber nicht gegen Unternehmen im Ausland. Dies ist auch bei den Vereinigten Staaten von Amerika der Fall.

Die einschlägigen Gesetze verbieten im Kern nur die Spionagetätigkeit von Industrieunternehmen gegeneinander. Ob sie auch die Tätigkeit staatlicher Nachrichtendienste einschränken ist zweifelhaft. Denn diese haben aufgrund der sie etablierenden Gesetze die Erlaubnis zum Diebstahl von Informationen.

Ein Grenzfall ergibt sich, wenn Nachrichtendienste durch Spionage gewonnene Informationen einzelnen Unternehmen zur Verfügung stellen würden. Normalerweise wäre dies durch die Gesetze, die Nachrichtendiensten besondere Befugnisse geben, nicht mehr abgedeckt. Insbesondere innerhalb der EU wäre dies eine Verletzung des EWG-Vertrages (siehe Kapitel...).

Unabhängig davon wäre aber in der Praxis die Inspruchnahme rechtlichen Schutzes durch Anrufung von Gerichten für ein Unternehmen sehr schwer zu verwirklichen. Abhören hinterläßt keine Spuren und führt zu keinen gerichtsverwertbaren Beweisen.

10.8.2. Sonstige Hindernisse für Wirtschaftsspionage

Die Tatsache, dass Nachrichtendienste im Sinne der Gewinnung allgemeiner strategischer Informationen auch im Bereich der Wirtschaft tätig sind, ist zwischen Staaten akzeptiert. Das "gentlemen agreement" wird aber bei Konkurrenzspionage zugunsten der eigenen Industrie massiv verletzt. Wird ein Staat dabei beweisbar dingfest gemacht, bekommt er massiv politische Probleme. Dies gilt auch und gerade für eine Weltmacht wie die USA, deren Anspruch auf globale politische Führung damit dramatisch beschädigt würde. Mittelmächte könnten es sich an der Stelle eher leisten, vorgeführt zu werden, eine Weltmacht nicht.

Neben den politischen Problemen stellt sich auch die praktische Frage, welchem einzelnen Unternehmen denn die Ergebnisse von Konkurrenzspionage zur Verfügung gestellt werden sollen. Im Bereich Flugzeugbau läßt sich das einfach beantworten, weil es hier global nur zwei große Anbieter gibt. In allen anderen Fällen ist dort, wo es mehrere Anbieter gibt die außerdem nicht im Staatsbesitz sind, äußerst schwierig einen Einzelnen zu bevorzugen. Bei der Übermittlung von Detailinformation über die Angebote von Mitwettbewerbern an einzelne Unternehmen im Zusammenhang mit internationalen öffentlichen Ausschreibungen könnte eine Weitergabe von Spionageinformationen an alle Mitbewerber des eigenen Landes noch denkbar sein. Dies gilt insbesondere dann, wenn es eine für alle nationalen Wettbewerber gleichermaßen zugängliche Unterstützungsstruktur der Regierung gibt, wie dies in den USA beim beim sogenannten Adcocacy Center der Fall ist. Im Falle von Technologiediebstahl, der zwangsläufig in einer Patentanmeldung münden müßte, wäre eine Gleichbehandlung von Firmen logisch nicht mehr möglich.

Dies wäre allerdings insbesondere im amerikanischen politischen System ein großes Problem. Amerikanische Politiker hängen bei der Finanzierung ihrer Wahlkämpfe massiv von Spenden der Industrie in ihren Wahlkreisen ab. Würde die Bevorzugung einzelner Firmen durch Nachrichtendienste auch nur in einem Falle exemplarisch offenkundig, gäbe es riesige Verwerfungen im politischen System. Wie es der ehemalige Direktor der CIA Woolsey in einem Gespräch mit Vertretern des Ausschusses formuliert hat: "In this case the hill (i..e the US-Congress) would go mad!". Wo er Recht hat, hat er Recht!

10.9. USA und Wirtschaftsspionage

10.9.1. Die offizielle Position der amerikanischen Seite zu Wirtschaftsspionage

Der ehemalige Direktor der CIA Woolsey und der Vorsitzende des Geheimdienstkontrollausschusses im House of Reprersentatives Porter Goss haben bei Gesprächen kurz zusammengefasst die folgende Position vertreten:

1. Die USA überwachen internationalen Fernmeldeverkehr um allgemeine Informationen über wirtschaftliche Entwicklungen, über Lieferungen von dual-use Gütern und das Einhalten von Embargos zu erhalten.

2. Die USA überwachen gezielt Komminikation von Einzelunternehmen im Zusammenhang mit Auschreibungen von Aufträgen um Marktverzerrungen durch Bestechung zu Ungunsten von US-Firmen zu verhindern.

Bestechung sei amerikanischen Firmen gesetzlich verboten und Wirtschaftsprüfer seien zur Meldung verpflichtet, wenn sie auf das Zahlen von Bestechungsgeldern stoßen. Würde duch Kommunikationsüberwachung Bestechung bei öffentlichen Aufträgen festgestellt, dann würde der amerikanische Botschafter bei der Regierung des entsprechenden Landes intervenieren. Die mitbietenden US-Firmen würden hingegen nicht direkt informiert.

10.9.2. Die Rolle des Advocacy Centers bei der US-Exportförderung

10.9.2.1. Die Aufgabe des Advocacy Centers

Das beim US- Handelsministerium angesiedelte Adcocacy Center ist das Herzstück der von Präsident Clinton betriebenen und von Bush fortgeführten nationalen Exportstrategie. Das 1993 gegründete Zentrum hat seitdem hunderten von US-Firmen geholfen öffentliche Aufträge imAusland zu erhalten. Das Zentrum bündelt die einschlägigen Ressourcen der US- Regierung von Expertin in Einzelbereichen über die Wirtschaftsattaches der Botschaften bis hin zum Weißen Haus.

10.9.2.2. Die Arbeitsweise des Zentrums

Im Zentrum selbst arbeitet nur ein kleiner Stab von 12 Personen(Stand 6.2.2001). Das Zentrum dient den Firmen als zentrale Anlaufstelle für die verschiedenen Behörden der US-Administration, die mit Exportförderung zu tun haben. Es arbeitet für die Firmen nichtdiskriminierend, unterstützt aber nach klaren Regeln nur Projekte im nationalen Interesse

der USA. So müssen die gelieferten Produkte dem Wert nach zu mindestens 50 Prozent aus den USA stammen.

10.9.2.3. Offene Fragen in Zusammenhang mit dem Zentrum

Die amerikanische Regierung hat das geplante Gespräch zwischen Mitgliedern des Ausschusses und dem Zentrum nicht erlaubt. Deshalb konnten zwei Fragen, an die sich Zweifel knüpfen, nicht ausdisktutiert werden:

a, dem Ausschuss liegen Dokumente vor, die eine Beteiligung der CIA an Arbeiten des Zentrums zu belegen scheinen.

b, das Zentrum gibt im Rahmen der ins Internet gestellten Informationen an, dass es die Ressourcen von 19 "U.S. government agencies" bündelt. An anderer Stelle werden namentlich aber nur 14 agencies genannt. Es stellt sich die Frage, warum die Namen von 5 agencies nicht öffentlich genannt werden.

10.10.Die Sicherheit von Computernetzen

wird nachgereicht

10.11.Die Unterschätzung der Risiken

wird nachgereicht

10.11.1. Großunternehmen

10.11.2. Kleine und mittlere Unternehmen

10.11.3. Europäische Institutionen

10.11.4. Forschungseinrichtungen

11. Selbstschutz durch Kryptografie

11.1. Zweck und Wirkungsweise einer Verschlüsselung

11.1.1. Zweck der Verschlüsselung

Bei jeder Nachrichtenübermittlung besteht das Risiko, dass die Nachricht einem Unbefugten in die Hände gelangt. Möchte man in so einem Fall verhindern, dass Außenstehende von ihrem Inhalt Kenntnis erlangen, muss die Botschaft für sie unlesbar oder unabhörbar gemacht, also verschlüsselt werden. Im militärischen und diplomatischen Bereich wurden deshalb schon seit jeher Verschlüsselungstechniken eingesetzt.[159]

In den letzten 20 Jahren nahm die Bedeutung der Verschlüsselung zu, da ein immer größerer Anteil der Kommunikation ins Ausland ging und der eigene Staat dort das Brief- und Fernmeldegeheimnis nicht mehr schützen konnte. Darüber hinaus haben die erweiterten technischen Möglichkeiten des eigenen Staates, Kommunikation legal abzuhören/mitzuschneiden, zu einem erhöhten Schutzbedürfnis von besorgten Bürgern geführt. Und schließlich hat das gestiegene Interesse von Straftätern an illegalem Zugang zu Informationen sowie an ihrer Verfälschung Schutzmaßnahmen ausgelöst (z.B. im Bankensektor).

Durch die Erfindung der elektrischen und elektronischen Kommunikation (Telegraf, Telefon, Funk, Fernschreiber, Fax und Internet) wurde die Übermittlung von Nachrichten stark vereinfacht und unvergleichlich schneller. Der Nachteil war, dass es keinerlei **technischen** Schutz gegen Abhören/Mitschneiden gab, und jeder mit einem entsprechenden Gerät die Kommunikation abgreifen konnte, wenn er Zugang zum Kommunikationsträger bekam. Abhören hinterlässt, wenn es professionell ausgeführt wird, kaum oder gar keine Spuren. Damit kam der Verschlüsselung eine ganz neue Bedeutung zu. Es war der Bankensektor, der zuerst mit dem Aufkommen des elektronischen Geldverkehrs die damit zusammenhängende Kommunikation regelmäßig mit Verschlüsselung geschützt hat. Mit zunehmender Internationalisierung der Wirtschaft wurde auch dort zumindest teilweise mit Kryptografie die Kommunikation geschützt. Mit der breiten Einführung der völlig ungeschützten Kommunikation im Internet wuchs auch das Bedürfnis von Privatleuten, ihre Kommunikation gegen Abhören zu schützen.

Im Zusammenhang mit diesem Bericht stellt sich also die Frage, ob es kostengünstige, rechtlich erlaubte, hinreichend sichere und einfach zu handhabende Methoden der Verschlüsselung von Kommunikation gibt, die einen Selbstschutz gegen Abhören erlauben.

11.1.2. Die Wirkungsweise einer Verschlüsselung

Das Prinzip der Verschlüsselung besteht darin, dass ein Klartext so in einen Geheimtext umgewandelt wird, dass er keinen oder einen anderen Sinn ergibt. Von Eingeweihten kann er aber wieder in das Original rückverwandelt werden. Aus einer sinnvollen Anordnung von

[159] Diesbezügliche Nachweise gehen bis auf die Antike zurück, so z.B. der Gebrauch der Skytale durch die Spartaner im 5. Jh. n. C.

Buchstaben wird bei Verschlüsselung z.B. eine sinnfremde gemacht, die niemand außerhalb versteht.

Dies geschieht nach einer bestimmten Methode (Algorithmus der Verschlüsselung), die auf dem Vertauschen von Buchstaben (Transposition) und/oder dem Ersatz von Buchstaben (Substitution) beruht. **Die Methode der Verschlüsselung** (Algorithmus) wird heutzutage nicht geheim gehalten. Im Gegenteil: es gab vor kurzem eine öffentliche weltweite Ausschreibung für den neuen globalen Standard der Verschlüsselung zur Anwendung in der Wirtschaft. Dies gilt auch für die Realisierung eines bestimmten Verschlüsselalgorithmus als Hardware in einem Gerät, z.B. in einem Kryptofaxgerät.

Das **wirklich Geheime** ist der so genannte **Schlüssel.** Am besten lässt sich der Sachverhalt mit einem Beispiel aus einem verwandten Bereich erklären. Die Funktionsweise von Türschlössern ist in der Regel öffentlich bekannt, schon deshalb weil sie Gegenstand eines Patents sind. Der individuelle Schutz einer Tür ergibt sich daraus, dass für einen bestimmten Schlosstyp viele verschiedene Schlüssel existieren können. Genauso verhält es sich bei der Verschlüsselung von Informationen: Mit **einer öffentlich bekannten Methode** der Verschlüsselung (Algorithmus) lassen sich mit verschiedenen, von den Beteiligten **geheim gehaltenen** individuellen Schlüsseln **viele** verschiedene Nachrichten geheim halten.

Zur Erläuterung der vorher verwendeten Begriffe sei das Beispiel der so genannten „Cäsarverschlüsselung“ angeführt. Der römische Feldherr Cäsar verschlüsselte Nachrichten, indem er einfach jeden Buchstaben durch den Buchstaben ersetzte, der drei Stellen weiter im Alphabet folgte, also A durch D, B durch E usw. Aus dem Wort **ECHELON** wird dann das Wort **HFKHORQ.** Der **Verschlüsselungsalgorithmus** besteht also hier im **Verschieben von Buchstabe**n innerhalb des Alphabets, der konkrete **Schlüssel** ist die Anweisung zur Verschiebung um **drei Stellen im Alphabet!** Sowohl das Ver- als auch das Entschlüsseln erfolgt auf dieselbe Weise: durch die Verschiebung der Buchstaben um 3 Stellen. Es handelt sich somit um ein symmetrisches Verfahren. Heutzutage schützt ein solches Verfahren nicht einmal eine Sekunde lang!

Bei einer guten Verschlüsselung kann die Methode durchaus öffentlich bekannt sein, und trotzdem kann die Verschlüsselung als sicher bezeichnet werden. Erforderlich ist dafür aber, dass die Schlüsselvielfalt so groß ist, dass ein Durchprobieren aller Schlüssel (so genannte **brute force attack**) auch unter Einsatz von Computern in angemessener Zeit nicht möglich ist. Andererseits ist Schlüsselvielfalt allein kein Hinweis auf kryptologische Sicherheit, wenn die Methode der Verschlüsselung einen Geheimtext liefert, der Anhaltspunkte für eine Dechiffrierung (z.B. Häufung bestimmter Buchstaben) enthält [160] Die Cäsarverschlüsselung ist unter beiden Aspekten keine sichere Verschlüsselung. Durch die einfache Substitution kann schon wegen der unterschiedlichen Häufigkeit der Buchstaben in einer Sprache das Verfahren schnell geknackt werden, zudem gibt es nur 25 Verschiebemöglichkeiten, also nur 25 Schlüssel, da das Alphabet ja nur aus 26 Buchstaben besteht. Der Gegner kann hier sehr schnell durch einfaches Probieren den passenden Schlüssel erhalten und den Text dechiffrieren.

Im Folgenden soll die Frage erläutert werden, wie ein sicheres System aussehen müsste.

[160] Vgl. dazu auch Leiberich, Vom diplomatischen Code zur Falltürfunktion - Hundert Jahre Kryptographie in Deutschland, Spektrum der Wissenschaft, Juni 1999, 26 ff.

11.2. Die Sicherheit von Verschlüsselungssystemen

11.2.1. Allgemeines zum Begriff Sicherheit beim Verschlüsseln

Verlangt man von einem Verschlüsselungssystem, dass es "sicher " sein muss, so können damit zwei verschiedene Sachverhalte gemeint sein. Zum einen kann verlangt sein, dass es absolut sicher ist, dass also das Dechiffrieren der Botschaft ohne Kenntnis des Schlüssels unmöglich und diese Unmöglichkeit mathematisch beweisbar ist. Zum anderen kann man sich damit begnügen, dass der Code nach Stand der Technik nicht gebrochen werden kann und damit Sicherheit für einen Zeitraum gegeben erscheint, der die "kritische" Zeit, innerhalb der eine Nachricht geheim gehalten werden muss, weit übersteigt.

11.2.2. Absolute Sicherheit: das one-time pad

Ein absolut sicheres Verfahren stellt bislang nur das one-time pad dar. Dieses System wurde gegen Ende des Ersten Weltkriegs entwickelt[161], aber später auch für den Krisenfernschreiber zwischen Moskau und Washington verwendet. Das Konzept besteht in einem Schlüssel, der aus völlig zufällig aneinander gereihten Buchstaben besteht, wobei sich die Reihung nicht wiederholt. Sender und Empfänger verschlüsseln anhand dieser Buchstabenreihen und vernichten den Schlüssel, sobald er das erste Mal verwendet wurde. Da es keine innere Ordnung innerhalb des Schlüssels gibt, ist es für einen Kryptoanalytiker unmöglich, den Code zu brechen. Dies kann sogar mathematisch bewiesen werden.[162]

Der Nachteil des Verfahrens besteht darin, dass es nicht leicht ist, große Mengen solcher Zufallsschlüssel zu erzeugen,[163] und dass die Verteilung der Schlüssel auf sicherem Wege schwierig und unpraktisch ist. Diese Methode wird daher im allgemeinen Geschäftsverkehr nicht verwendet.

11.2.3. Relative Sicherheit entsprechend dem Stand der Technik

11.2.3.1. Der Einsatz von Maschinen zur Ent- und Verschlüsselung

Schon vor der Erfindung des one-time pad wurden wurden Kryptoverfahren entwickelt, die eine hohe Zahl von Schlüsseln zur Verfügung stellten und Geheimtexte erzeugten, die möglichst wenig Regelmäßigkeiten im Text enthielten und so kaum Angriffspunkte für eine Kryptoanalyse boten. Um diese Methoden für den praktischen Einsatz hinreichend schnell zu gestalten, wurden zur Ver- und Entschlüsselung Maschinen entwickelt. Die spektakulärste ihrer Art war wohl die ENIGMA[164], die im zweiten Weltkrieg von Deutschland eingesetzt wurde. Dem in Bletchley Park in England eingesetzten Heer von Entschlüsselexperten gelang es, die Verschlüsselung der ENIGMA mithilfe spezieller Maschinen, den so genannten "Bomben", zu knacken. Sowohl die ENIGMA als auch die „Bombe“ waren mechanische Maschinen.

---

[161] Eingeführt wurde es von Major Joseph Mauborgne, Leiter der kryptographischen Forschungsabteilung der amerikanischen Armee. Vgl. dazu Singh, Geheime Botschaften (1999), 151

[162] Vgl. dazu Singh, Geheime Botschaften (1999), 151 ff.

[163] Vgl. dazu Wobst, Abenteuer Kryptologie^2 (1998), 60.

[164] Die Enigma wurde von Arthur Scherbius entwickelt und 1928 patentiert. Sie glich in gewisser Weise einer Schreibmaschine, da sie mit einer Tastatur versehen war, auf der der Klartext eingegeben wurde. Durch ein Steckerbrett und rotierende Walzen wurde der Text einer gegebenen Vorschrift entsprechend verschlüsselt und mit der gleichen Maschine anhand von Codebüchern entschlüsselt.

11.2.3.2. Der Einsatz des Computers in der Kryptologie

Die Erfindung des Computers war bahnbrechend für die Kryptowissenschaft, da seine Leistungsfähigkeit die Verwendung von zunehmend komplexeren Systemen erlaubt. Auch wenn die Grundprinzipien der Verschlüsselung dadurch nicht verändert wurden, so ergaben sich doch bestimmte Neuerungen. Erstens wurde der Grad der möglichen Komplexität von Verschlüsselungssystemen um ein Vielfaches erhöht, da sie nicht mehr durch das mechanisch Realisierbare limitiert war, zweitens wurde die Geschwindigkeit des Verschlüsselungsprozesses drastisch gesteigert.

Die Information wird von Computern digital mit Binärzahlen verarbeitet. Letzteres bedeutet, dass die Information in der Reihenfolge von zwei Signalen ausgedrückt wird, nämlich 0 und 1. 1 entspricht im physikalischen einer elektrischen Spannung bzw. einer Magnetisierung ("Licht ein"), 0 Wegfall der Spannung bzw. der Magnetisierung ("Licht aus"). Dabei hat sich die Normierung nach ASCII[165] durchgesetzt, der jeden Buchstaben durch eine siebenstellige Kombination von 0 und 1 darstellt[166]. Ein Text nimmt daher die Gestalt einer Zahlenreiche von 0 und 1 an, anstelle von Buchstaben werden Zahlen verschlüsselt.

Dabei können sowohl die Formen der Transposition (Vertauschung) als auch die der Substitution (Ersetzung) Verwendung finden. Substitution kann beispielsweise durch hinzuaddieren eines Schlüssels in Form einer beliebigen Zahlenreihe erfolgen. Nach den Regeln der binären Mathematik addieren sich gleiche Zahlen zu Null (also 0 +0=0 und 1 +1=0), zwei verschiedene Zahlen zu Eins (0+1=1). Die durch Addition entstehende neue verschlüsselte Zahlenreihe ist somit eine binäre Folge, die entweder digital weiterverarbeitet oder durch das Abziehen des hinzuaddierten Schlüssels wieder lesbar gemacht werden kann.

Mit der Verwendung von Computern ist bei Einsatz starker Verschlüsselalgorithmen die Erzeugung von Geheimtexten realisierbar, die für eine Kryptoanalyse praktisch keine Angriffspunkte mehr bieten. Ein Entschlüsselangriff lässt sich dann nur mehr mit einem Durchprobieren sämtlicher möglicher Schlüssel ausführen. Je länger der Schlüssel ist, umso mehr scheitert dieses Vorhaben selbst beim Einsatz von Hochleistungscomputern an der dafür notwendigen Zeit. Es gibt also handhabbare Verfahren, die nach dem Stand der Technik als sicher gelten können

11.2.4. Standardisierung und vorsätzliche Beschränkung der Sicherheit

Aufgrund der Verbreitung der Computer in den 70er-Jahren wurde die Standardisierung von Verschlüsselungssystemen immer dringlicher, da nur so für Unternehmen die sichere Kommunikation mit Geschäftspartnern ohne unverhältnismäßigen Aufwand möglich war. Die ersten Bestrebungen dazu gab es in den USA.
Eine starke Verschlüsselung kann auch zu unlauteren Zwecken oder vom potenziellen militärischen Gegner verwendet werden; sie kann auch elektronische Spionage erschweren oder unmöglich machen. Deshalb drang die NSA darauf, dass ein für die Wirtschaft hinreichend sicherer Verschlüsselungsstandard gewählt wurde, bei dem ihr selbst aufgrund ihrer besonderen technischen Ausstattung eine Entschlüsselung aber möglich blieb. Dazu wurde die Länge des Schlüssels auf 56-Bit begrenzt. Das vermindert die Zahl der möglichen Schlüssel auf 100 000

[165] American Standard Code for Information Interchange

[166] A = 1000001, B= 1000010, C= 1000011, D= 1000100, E = 1000101, etc

000 000 000 000 Stück[167]. Tatsächlich wurde am 23. November 1976 die so genannte Lucifer-Chiffre von Horst Feistel in der **56-bit Version** offiziell unter dem Namen Data Encryption Standard (DES) übernommen und stellte für ein Vierteljahrhundert den offiziellen amerikanischen Verschlüsselungsstandard dar.[168] Auch in Europa und Japan wurde dieser Standard insbesondere im Bankenbereich übernommen. Der Algorithmus von DES wurde entgegen Behauptung in diversen Medien bislang nicht geknackt, es gibt jedoch inzwischen Hardware, die stark genug ist, um sämtliche Schlüssel durchzuprobieren ("brute force attack"). Triple-DES, das einen 112 bit Schlüssel hat, gilt dagegen weiterhin als sicher. Der Nachfolger von DES, der AES (Advanced Encryption Standard), ist ein europäisches Verfahren[169], das unter dem Namen Rijndael in Leuven, Belgien, entworfen wurde. **Es ist schnell und gilt als sicher, da hier von einer Schlüssellängenbeschränkung Abstand genommen wurde.** Dies ist auf eine veränderte amerikanische Kryptopolitik zurückzuführen (siehe oben 11.1.4).

Die Standardisierung bedeutete für die Unternehmen eine wesentliche Vereinfachung der Verschlüsselung. Bestehen blieb jedoch das Problem der Schlüsselverteilung.

11.3. Das Problem der sicheren Schlüsselverteilung/-übergabe

11.3.1. Asymmetrische Verschlüsselung: das public-key-Verfahren

Solange ein System mit einem Schlüssel arbeitet, mit dem sowohl ver- als auch entschlüsselt wird (symmetrische Verschlüsselung), ist es mit **vielen** Kommunikationspartnern nur schwierig handhabbar. Der Schlüssel muss nämlich jedem neuen Kommunikationspartner **vorher** so übergeben werden, dass kein Dritter davon Kenntnis erlangt hat. Das ist für die Wirtschaft praktisch schwierig, für Privatpersonen nur in Einzelfällen möglich.

Eine Lösung dieses Problems bietet die asymmetrischen Verschlüsselung: zur Ver- und Entschlüsselung wird nicht derselbe Schlüssel verwendet. Mit einem Schlüssel, der durchaus jedermann bekannt sein darf, dem so genannten **öffentlichen Schlüssel,** wird die Nachricht verschlüsselt. Das Verfahren arbeitet aber wie eine Einbahnstraße nur in einer Richtung, eine Rückverwandlung in Klartext ist mit dem öffentlichen Schlüssel nicht mehr möglich. Deshalb kann jeder, der eine verschlüsselte Nachricht erhalten will, seinem Kommunikationspartner seinen öffentlichen Schlüssel auch auf einem unsicheren Weg zum Verschlüsseln der Nachricht schicken. Zum Entschlüsseln der dann erhaltenen Nachricht dient ein anderer Schlüssel, der **private Schlüssel**, der geheim gehalten und nicht versandt wird.[170] Der einleuchtendste Vergleich für das Verständnis des Verfahrens ist der mit einem Vorhängeschloss: jeder kann ein solches Schloss einschnappen lassen und damit eine Truhe sicher verschließen, öffnen kann sie jedoch nur der, der den richtigen Schlüssel besitzt.[171] Der öffentliche und der private Schlüssel hängen miteinander zusammen; aus dem öffentlichen Schlüssel lässt sich der private Schlüssel aber nicht berechnen.

---

[167] Diese Zahl, binär dargestellt, besteht aus 56 Nullen und 'Einsen. Vgl. dazu Singh, Geheime Botschaften (1999), 03

[168] Vgl. dazu Singh, Geheime Botschaften (1999), 302 ff

[169] Es wurde kreiert von zwei belgischen Kryptographen and der Katholischen Universität Leuven, Joan Daemen und Vincent Rijmen.

[170] Die Idee der asymmetrischen Verschlüsselung in Form des public-key-Verfahrens stammt von Whitfield Diffie und Martin Hellmann.

[171] Singh, Geheime Botschaften (1999), 327

Ron Rivest, Adi Shamir und Leonard Adleman haben eine asmetrische Verschlüsselung mit dem nach ihnen benannte RSA-Verfahren erfunden. In eine Einwegfunktion (eine so genannte Falltürfunktion) wird als ein Bestandteil des öffentlichen Schlüssels das Ergebnis der Multiplikation zweier sehr großer Primzahlen eingesetzt. Damit wird der Klartext verschlüsselt. Die Entschlüsselung ist nur dem möglich, der die Werte der beiden verwendeten Primzahlen kennt. Es gibt aber kein mathematisches Verfahren, mit dem sich die Multiplikation zweier Primzahlen so umkehren lässt, dass sich aus dem Ergebnis der Multiplikation die Ausgangsprimzahlen errechnen lassen. Bislang ist dies nur durch systematisches Probieren möglich.. Deshalb ist das Verfahren nach derzeitigem Wissensstand sicher, sofern ausreichend hohe Primzahlen gewählt werden. Das einzige Risiko besteht darin, dass irgendwann ein brillanter Mathematiker einen schnelleren Weg für die Faktorzerlegung finden könnte. Bislang ist dies jedoch trotz größter Bemühungen noch niemandem gelungen.[172] Vielfach wird sogar die Auffassung vertreten, dass das Problem unlösbar ist, ein exakter Beweis dafür wurde bislang jedoch noch nicht erbracht.[173]

Die public-key-Verschlüsselung verlangt allerdings verglichen mit symmetrischen Verfahren (z.B. DES) auf dem PC weit mehr Rechenzeit oder den Einsatz von schnellen Großrechnern.

11.3.2. Public-key-Verschlüsselung für Privatpersonen

Um das public-key-Verfahren allgemein zugänglich zum machen, kam Phil Zimmerman auf die Idee, das rechnerisch aufwendige public-key-Verfahren mit einem schnelleren symmetrischen Verfahren zu verbinden. Die Nachricht selbst sollte mit einem symmetrischen Verfahren, dem in Zürich entwickelten IDEA-Verfahren verschlüsselt werden, der Schlüssel für die symmetrische Verschlüsselung hingegen gleichzeitig nach dem public-key-Verfahren übermittelt werden. Zimmermann schuf ein benutzerfreundliches Programm, Pretty Good Privacy genannt, das auf Knopfdruck (bzw. Mausklick) die notwendigen Schlüssel kreierte und die Verschlüsselung vornahm. Das Programm wurde ins Internet gestellt, wo es jeder herunterladen konnte. PGP wurde schließlich vom amerikanischen Unternehmen NAI gekauft, wird aber Privatpersonen immer noch gratis zur Verfügung gestellt.[174] Von den früheren Versionen wurde der Quelltext veröffentlicht, sodass davon ausgegangen werden kann, dass keine Hintertüren eingebaut sind. Die Quelltexte von der neuesten Version PGP 7, die sich durch eine ausgesprochen benutzerfreundliche graphische Oberfläche auszeichnet, sind leider nicht mehr veröffentlicht.
Es existiert allerdings noch eine andere Implementierung des Open PGP Standards: GnuPG. GnuPG bietet die selben Verschlüsselungsmethoden wie PGP an, und ist auch mit PGP kompatibel. Es handelt sich dabei aber um freie Software, ihr Quellcode ist bekannt und jeder kann sie verwenden und weitergeben. Das deutsche Bundesministerium für Wirtschaft und Technologie hat die Portierung von GnuPG auf Windows und die Entwicklung einer grafischen Oberfläche gefördert, leider sind sie derzeit noch nicht völlig ausgereift. Nach Informationsstand des Berichterstatters wird allerdings daran gearbeitet.

Daneben gibt es noch konkurrierende Standards zu OpenPGP, wie S/MIME, welches von vielen E-Mail-Programmen unterstützt wird. Dem Berichterstatter liegen hier allerdings keine Informationen über freie Implementierungen vor.

---

[172] Vgl. dazu Buchmann, Faktorisierung großer Zahlen, Spektrum der Wissenschaft 2 1999, 6 ff

[173] Vgl. dazu Singh, Geheime Botschaften (1999), 335 f

[174] Informationen zur Software finden sich unter www.pgpi.com

11.3.3. Künftige Verfahren

Ganz neue Aspekte für die sichere Schlüsselübergabe könnten sich in der Zukunft durch die Quantenkryptographie ergeben. Sie stellt sicher, dass ein Abhörvorgang bei einer Schlüsselübergabe bemerkt würde. Werden polarisierte Photonen verschickt, so kann ihre Polarisierung nicht festgestellt werden, ohne sie zu verändern. Lauscher an der Datenleitung könnten somit mit Sicherheit festgestellt werden. Nur ein Schlüssel, der nicht abgehört wurde, würde dann verwendet werden. Bei Versuchen ist bereits eine Übertragung über 48 km Glasfaserkabel und über 500 m in der Luft gelungen.[175]

11.4. Sicherheit von Verschlüsselprodukten

In der Diskussion um die tatsächliche Sicherheit von Verschlüsselungen ist auch immer wieder der Vorwurf aufgetaucht, dass amerikanische Produkte Hintertüren enthalten. Schlagzeilen in den Medien hat hier z.B. Excel gemacht, von dem behauptet wird, dass in der europäischen Version die Hälfte des Schlüssels im Header der Datei offen abgelegt ist. Aufmerksamkeit in der Presse hat auch Microsoft dadurch erregt, dass ein Hacker einen "NSA-key" im Programm versteckt gefunden hat, was von Microsoft natürlich heftigst dementiert wurde. Da Microsoft seinen Quellcode nicht offengelget hat, ist jedes Urteil darüber Spekulation. Für die früheren Versionen von PGP und GnuPG kann ein solches backdoor jedenfalls mit großer Sicherheit ausgeschlossen werden, da ihr Quelltext offen gelegt wurde.

11.5. Verschlüsselung im Konflikt mit Staatsinteressen

11.5.1. Versuche der Beschränkung der Verschlüsselung

Etliche Staaten verbieten zunächst den Gebrauch von Verschlüsselsoftware oder von Kryptogeräten und machen Ausnahmen von einer Erlaubnis abhängig. Dabei handelt es sich nicht nur um Diktaturen wie z.B. China, Iran oder Irak. Auch demokratische Staaten haben den Gebrauch oder Verkauf von Verschlüsselprogrammen oder Maschinen gesetzlich eingeschränkt. Die Kommunikation sollte zwar gegen das Mitlesen durch unbefugte Privatpersonen geschützt werden, der Staat sollte aber nach wie vor die Möglichkeit behalten, gegebenenfalls rechtmäßig abzuhören. Der Verlust der technischen Überlegenheit der Behörden sollte durch rechtliche Verbote wettgemacht werden. So hat Frankreich bis vor kurzem den Gebrauch von Kryptografie allgemein untersagt und von einer Einzelgenehmigung abhängig gemacht. In Deutschland gab es vor einigen Jahren ebenfalls eine Debatte über Beschränkungen der Verschlüsselung und den Zwang einer Schlüsselhinterlegung. Die USA haben stattdessen in der Vergangenheit die Schlüssellänge begrenzt.

11.5.2. Die Bedeutung sicherer Verschlüsselung für den E-Commerce

Inzwischen dürften diese Versuche ein für alle Mal gescheitert sein. Dem Staatinteresse, Zugang zur Entschlüsselung und damit zu den Klartexten zu haben, stehen nämlich nicht nur das Recht auf Wahrung der Privatsphäre entgegen, sondern auch handfeste wirtschaftliche Interessen. Denn E-Commerce und electronic banking sind von einer sicheren Kommunikation im Internet abhängig. Kann diese nicht gewährleistet werden, sind diese Techniken zum Scheitern verurteilt, weil das Kundenvertrauen dann nicht mehr gegeben wäre. Dieser Zusammenhang erklärt den Wandel in der amerikanischen oder französischen Kryptopolitik.

[175] Zur Quantenkryptographie Vgl. Wobst, Abenteuer Kryptographie[2] (1998), 234 ff.

An dieser Stelle sei angemerkt, dass der E-Commerce in zweifacher Hinsicht sicherer Verschlüsselungsverfahren bedarf: Nicht nur um Nachrichten zu verschlüsseln, sondern auch um die Identität des Geschäftspartners zweifelsfrei belegen zu können. Die elektronische Unterschrift kann nämlich durch eine umgekehrte Anwendung des public-key-Verfahrens geleistet werden: Der private Schlüssel wird zur Verschlüsselung verwendet, der öffentliche zur Entschlüsselung. Diese Form der Verschlüsselung bestätigt die Urheberschaft der Unterschrift. Jeder kann sich durch Gebrauch des öffentlichen Schlüssels einer Person von ihrer Echtheit überzeugen, die Unterschrift selbst aber nicht nachahmen. Auch diese Funktion ist in PGP benutzerfreundlich eingearbeitet.

11.5.3. Probleme für Geschäftsreisende

In manchen Staaten ist für Geschäftsreisende der Gebrauch von Verschlüsselprogrammen auf mitgeführten Laptops untersagt. Dies verhindert jedweden Schutz der Kommunikation mit dem eigenen Unternehmen oder die Sicherung mitgeführter Daten gegen Zugriffe.

11.6. Praktische Fragen bei der Verschlüsselung

Möchte man die Frage beantworten, wem unter welchen Umständen zur Verschlüsselung geraten werden soll, so scheint es richtig, zwischen Privatleuten und Unternehmen zu differenzieren. Was Privatleute betrifft, so muss offen gesagt werden, dass das Verschlüsseln von Fax und Telefongesprächen durch Kryptotelefon bzw. Cypherfax nicht wirklich realisierbar ist. Dies nicht nur deshalb, weil die Anschaffungskosten dieser Geräte relativ hoch sind, sondern auch weil ihre Anwendbarkeit voraussetzt, dass der Gesprächspartner ebenfalls über derartige Geräte verfügt, und dies wohl nur in den seltensten Fällen zutrifft.

E-Mails können und sollen hingegen von jedermann verschlüsselt werden. Der oft vorgebrachten Behauptung, man habe kein Geheimnis, und brauche deshalb nicht verschlüsseln, muss entgegengehalten werden, dass man ja auch schriftliche Nachrichten üblicherweise nicht auf Postkarten verschickt. Ein unverschlüsseltes Mail ist aber nichts anderes als ein Brief ohne Umschlag. Die Verschlüsselung von E-Mails ist sicher und relativ problemlos, im Internet finden sich bereits benutzerfreundliche Systeme, wie z.B. PGP/GnuPG, die Privatpersonen sogar gratis zur Verfügung gestellt werden. Es fehlt aber bedauerlicherweise noch an der notwendigen Verbreitung. Hier wäre wünschenswert, dass die öffentliche Hand mit gutem Beispiel vorangeht und selbst zur standardmäßigen Verschlüsselung schreitet, um Verschlüsselung zu entmystifizieren.

Was Unternehmen anbelangt, so sollte streng darauf geachtet werden, dass sensible Informationen nur auf gesicherten Kommunikationswegen übermittelt werden. Dies erscheint selbstverständlich, ist es für Großunternehmen wohl auch, aber gerade bei kleinen und mittleren Unternehmen werden via E-Mail firmeninterne Informationen oft unverschlüsselt weitergegeben, weil das Problembewusstsein nicht hinlänglich ausgebildet ist. Hier ist zu hoffen, dass sich Industrieverbände und Wirtschaftskammern verstärkt um Aufklärung bemühen. Freilich ist Verschlüsselung von E-Mails nur ein Sicherheitsaspekt unter vielen, und nützt vor allem dann nichts, wenn die Information bereits vor der Verschlüsselung anderen zugänglich gemacht wird. Dies bedeutet, dass das gesamte Arbeitsumfeld gesichert werden muss, somit die Sicherheit der verwendeten Räumlichkeiten gewährleistet und der physische Zugang zu Büros und Computern überprüft werden muss. Es muss aber auch der unautorisierte Zugang zu Informationen über das

Netz mittels entsprechende fire-walls verhindert werden. Besondere Gefahren stelle hier die Verknüpfung von internem Netz und Internet dar. Nimmt man Sicherheit ernst, sollte man auch nur Betriebssysteme verwenden, deren Quellencode offen gelegt und überprüft ist, da man nur dort mit Sicherheit sagen kann, was mit den Daten geschieht. Für Unternehmen stellen sich also im Sicherheitsbereich eine Vielzahl von Aufgaben. Es gibt auf dem Markt bereits zahlreiche Firmen, die Sicherheitsberatung und -umsetzung zu verträglichen Preisen anbieten, entsprechend der Nachfrage steigt das Angebot ständig. Darüber hinaus ist aber zu hoffen, dass sich Industrieverbände und Wirtschaftskammern dieser Probleme annehmen, um besonders Kleinunternehmen auf die Sicherheitsproblematik aufmerksam zu machen und bei Entwurf sowie Umsetzung eines umfassenden Schutzkonzeptes zu unterstützen.

12. Die Außenbeziehungen der EU und die Sammlung nachrichtendienstlicher Informationen

12.1. Einleitung

Mit der Annahme des Vertrags von Maastricht im Jahr 1991 wurde die Gemeinsame Außen- und Sicherheitspolitik (GASP) in ihrer elementarsten Form als neues politisches Instrument der Europäischen Union geschaffen. Der Vertrag von Amsterdam gab der GASP sechs Jahre später eine stärkere Struktur und schaffte die Möglichkeit für Gemeinsame Verteidigungsinitiativen innerhalb der Europäischen Union, unter Beibehaltung der bestehenden Allianzen. Auf der Grundlage des Vertrags von Amsterdam und vor dem Hintergrund der Kosovo-Erfahrungen brachte der Europäische Rat von Helsinki im Dezember 1999 die Europäische Sicherheits- und Verteidigungsinitiative auf den Weg. Diese Initiative zielt auf die Schaffung einer multinationalen Truppe mit einer Stärke von 50 – 60.000 Soldaten bis Mitte 2003 ab. Das Bestehen einer solchen multinationalen Streitmacht wird die Entwicklung einer eigenständigen Aufklärungskapazität unverzichtbar machen. Einfach die bestehende WEU-Aufklärungskapazität zu integrieren wird für diesen Zweck nicht ausreichen. Eine Ausweitung der Zusammenarbeit zwischen den Aufklärungseinrichtungen der Mitgliedstaaten weit über die bestehenden Formen der Zusammenarbeit hinaus lässt sich nicht vermeiden.

Die weitere Entwicklung der GASP jedoch ist nicht das einzige Element, das zu einer stärkeren Zusammenarbeit zwischen den Aufklärungsdienststellen in der Union führt. Auch die stärkere wirtschaftliche Integration innerhalb der Europäischen Union wird eine intensivere Zusammenarbeit auf dem Gebiet der Sammlung nachrichtendienstlicher Informationen erforderlich machen. Eine einheitliche europäische Wirtschaftspolitik macht einheitliche Erkenntnisse über die wirtschaftlichen Realitäten in der Welt außerhalb der Europäischen Union notwendig. Eine einheitliche Position bei handelspolitischen Verhandlungen im Rahmen der WTO oder mit Drittländern erfordert einen gemeinsamen Schutz der Verhandlungsposition. Starke europäische Unternehmen brauchen einen gemeinsamen Schutz gegen Wirtschaftsspionage von außerhalb der Europäischen Union.

Es muss schließlich betont werden, dass die weitere Entwicklung des zweiten Pfeilers der Union und der Aktivitäten der Union im Bereich Inneres und Justiz auch zur stärkeren Zusammenarbeit zwischen den Nachrichtendiensten führen muss. Insbesondere der gemeinsame Kampf gegen Terrorismus, den illegalen Waffenhandel, den Menschenhandel und die Geldwäsche können nicht ohne intensive Zusammenarbeit zwischen den Aufklärungsdiensten erfolgen.

12.2. Möglichkeiten für die Zusammenarbeit innerhalb der EU

12.2.1 Bestehende Zusammenarbeit

Obwohl es eine lange Tradition bei den Aufklärungsdiensten gibt, nur solchen Informationen zu trauen, die sie selbst gesammelt haben, möglicherweise auch eine Tradition des Misstrauens zwischen den einzelnen Aufklärungsdiensten innerhalb der Europäischen Union nimmt die Zusammenarbeit zwischen solchen Dienststellen bereits zu. Häufige Kontakte bestehen im Rahmen der NATO, der WEU und innerhalb der Europäischen Union. Während die

Aufklärungsdienste im Rahmen der NATO nach wie vor stark von den weitaus fundierteren Beiträgen der Vereinigten Staaten abhängig sind, haben die Einrichtung des WEU-Satellitenzentrums in Torrejon (Spanien) und die Schaffung einer Aufklärungseinheit auf Ebene des WEU-Hauptquartiers zu stärker eigenständigem europäischen Handeln in diesem Bereich beigetragen.

12.2.2. Vorteile einer Gemeinsamen Europäischen Aufklärungspolitik

Es muss zusätzlich zu den bereits laufenden Entwicklungen betont werden, dass es objektive Vorteile einer Gemeinsamen Europäischen Aufklärungspolitik gibt. Diese Vorteile lassen sich wie folgt beschreiben.

12.2.2.1. Praktische Vorteile

Zunächst einmal gibt es einfach zu viel klassifiziertes und nicht klassifiziertes Material, als dass es von einer einzigen Agentur oder durch bilaterale Vereinbarungen in Westeuropa gesammelt analysiert und bewertet werden könnte. Die Anforderungen an die Aufklärungsdienste reichen von der Aufklärung im Verteidigungsbereich durch nachrichtendienstliche Tätigkeit über die interne und internationale Wirtschaftspolitik von Drittstaaten bis hin zur Aufklärung zur Unterstützung des Kampfes gegen das organisierte Verbrechen und den Drogenhandel. Selbst wenn die Zusammenarbeit nur auf der untersten Ebene erfolgen würde, d.h. bei der Sammlung offen zugänglicher Informationen (OSINT), wären die Ergebnisse dieser Zusammenarbeit bereits für die Politik der Europäischen Union von großer Bedeutung.

12.2.2.2. Finanzielle Vorteile

In jüngster Vergangenheit sind die Mittel für die Sammlung nachrichtendienstlicher Informationen gekürzt worden, in einigen Fällen setzt sich diese Entwicklung fort. Gleichzeitig hat der Bedarf an Informationen und deshalb an Aufklärung zugenommen. Diese gekürzten Mittel machen diese Zusammenarbeit nicht nur möglich, sondern langfristig gesehen auch finanziell lohnend. Insbesondere im Fall der Einrichtung und Betreibung technischer Einrichtungen sind gemeinsame Operationen angesichts knapper Mittel interessant, aber auch im Bereich der Auswertung der gesammelten Informationen. Stärkere Zusammenarbeit wird die Wirksamkeit der Sammlung nachrichtendienstlicher Informationen weiter erhöhen.

12.2.2.3. Politische Vorteile

Grundsätzlich dienen nachrichtendienstliche Erkenntnisse dazu, den Regierungen eine bessere und besser fundierte Entscheidungsfindung zu ermöglichen. Eine stärkere politische und wirtschaftliche Integration auf Ebene der Europäischen Union macht es erforderlich, dass Informationen auf europäischer Ebene verfügbar sind und dass sie sich auf mehr als nur eine einzige Quelle stützen.

12.2.3. Schlussbemerkungen

Diese objektiven Vorteile sind nur Beispiele für die wachsende Bedeutung der Zusammenarbeit innerhalb der Europäischen Union. In der Vergangenheit gewährleisteten die Nationalstaaten jeder für sich die externe Sicherheit, die innere Ordnung, den nationalen Wohlstand und die kulturelle Identität. Heute ist die Europäische Union in zahlreichen Bereichen dabei, eine Rolle zu übernehmen, die die Rolle des Nationalstaates zumindest ergänzt. Es ist unmöglich, dass die Aufklärungsdienste der letzte und einzige Bereich sind, der nicht vom Prozess der europäischen Integration erfasst ist.

12.3. Zusammenarbeit über die Ebene der Europäischen Union hinaus

Seit dem Zweiten Weltkrieg vollzog sich die Zusammenarbeit im Bereich der Sammlung nachrichtendienstlicher Informationen nicht in erster Linie auf europäischer Ebene, sondern sehr viel mehr auf transatlantischer Ebene. Es ist bereits erwähnt worden, dass im Bereich der Sammlung nachrichtendienstlicher Informationen enge Beziehungen zwischen dem Vereinigten Königreich und den Vereinigten Staaten hergestellt wurden. Aber auch im Bereich der militärischen Aufklärung im Rahmen der NATO und darüber hinaus waren und sind die Vereinigten Staaten der absolut dominierende Partner. Es stellt sich deshalb die wichtige Frage, ob eine stärkere europäische Zusammenarbeit im Bereich der Sammlung nachrichtendienstlicher Informationen die Beziehungen zu den Vereinigten Staaten schwerwiegend beeinträchtigen könnte oder möglicherweise zu einer Stärkung dieser Beziehungen führt. Wie werden sich die Beziehungen zwischen der EU und den USA unter der neuen Bush-Regierung entwickeln? Wie wird insbesondere die besondere Beziehung zwischen den Vereinigten Staaten und dem Vereinigten Königreich in diesem Rahmen sich entwickeln? Von verschiedener Seite wird die Auffassung vertreten, dass es keinen Widerspruch zwischen den besonderen Beziehungen zwischen dem Vereinigten Königreich und den USA und der weiteren Entwicklung der GASP geben muss. Andere sind der Auffassung, dass insbesondere der Bereich der Sammlung nachrichtendienstlicher Informationen eine Frage sein kann, die das Vereinigte Königreich zu der Entscheidung zwingt, ob sein Schicksal europäisch oder transatlantisch ist. Die engen Verbindungen des Vereinigten Königreichs zu den USA (und zu den anderen Partnern in dem UKUSA-Abkommen) machen es für die anderen EU-Staaten möglicherweise schwieriger, nachrichtendienstliche Informationen untereinander gemeinsam zu nutzen – weil Großbritannien an einer solchen innereuropäischen Nutzung weniger interessiert ist und weil die EU-Partner dem Vereinigten Königreich möglicherweise weniger trauen. Falls die USA der Ansicht sind, dass Großbritannien besondere Verbindungen mit seinen EU-Partnern entwickelt hat und dies Teil eines besonderen europäischen Abkommens ist, könnten die USA möglicherweise zurückhaltender werden, weiterhin ihre nachrichtendienstlichen Informationen mit dem Vereinigten Königreich zu teilen. Eine stärkere EU-Zusammenarbeit auf dem Gebiet der nachrichtendienstlichen Kooperation könnte deshalb einen ernsten Test für die europäischen Ambitionen des Vereinigten Königreichs wie auch für die Integrationskapazität der EU sein.

Unter den gegebenen Bedingungen ist es jedoch höchst unwahrscheinlich, dass selbst extrem rasche Fortschritte bei der Zusammenarbeit zwischen den europäischen Partnern kurzfristig und sogar langfristig den technologischen Vorsprung der Vereinigten Staaten ersetzen können. Die Europäische Union wird nicht in dieser Lage sein, ein fortschrittliches Netz von SIGINT-Satelliten, bilddarstellerischen Satelliten und Bodenstationen aufzubauen. Die Europäische Union wird kurzfristig nicht in der Lage sein, ein hoch entwickeltes Netz von Computern zu schaffen, das für die Sammlung und Auswertung des gesammelten Materials benötigt wird. Die Europäische Union wird nicht bereit sein, die notwendigen finanziellen Mittel bereitzustellen, um eine wirkliche Alternative zu den nachrichtendienstlichen Tätigkeiten der Vereinigten Staaten zu schaffen. Deshalb wird es schon aus technologischen und finanziellen Aspekten im Interesse der Europäischen Union liegen, eine enge Beziehung auf dem Gebiet der nachrichtendienstlichen Aufklärung mit den Vereinigten Staaten aufrecht zu erhalten. Aber auch unter politischen Aspekten wird es wichtig sein, die Beziehungen zu den Vereinigten Staaten aufrecht zu erhalten und sie ggf. zu verstärken, insbesondere mit Blick auf den gemeinsamen Kampf gegen das organisierte Verbrechen, den Terrorismus, den Drogen- und Waffenhandel und

die Geldwäsche. Gemeinsame nachrichtendienstliche Operationen sind notwendig, um gemeinsame Anstrengungen zu unterstützen. Gemeinsame friedenserhaltende Aktionen wie im früheren Jugoslawien erfordern einen größeren europäischen Beitrag in allen Handlungsbereichen.

Auf der anderen Seite sollte ein wachsendes europäisches Bewusstsein auch von größerer europäischer Verantwortung begleitet sein. Die Europäische Union sollte ein stärker gleichberechtigter Partner werden, nicht nur auf wirtschaftlichen Gebiet, sondern auch im Verteidigungssektor und folglich im Bereich der Sammlung nachrichtendienstlicher Informationen. Eine stärker eigenständige europäische Aufklärungskapazität sollte deshalb nicht als Schwächung der transatlantischen Beziehungen betrachtet werden, sondern sollte auch ein Beitrag dazu sein, dass die Europäische Union ein stärker gleichberechtigter und kompetenterer Partner werden. Gleichzeitig muss die Europäische Union eigenständige Anstrengungen unternehmen, um ihre Wirtschaft und ihre Industrie gegen illegale und unerwünschte Bedrohungen wie Wirtschaftsspionage, Cyber-Kriminalität und terroristische Angriffe zu schützen. Es bedarf zudem auch eines transatlantischen Einvernehmens auf dem Gebiet der Industriespionage. Die Europäische Union und die Vereinigten Staaten sollten sich auf Regeln darüber einigen, was auf diesem Gebiet erlaubt ist und was nicht. Zur Stärkung der transatlantischen Zusammenarbeit auf diesem Gebiet sollte eine gemeinsame Initiative auf Ebene der WTO eingeleitet werden, um die Verfahren dieser Organisation zum Schutz einer weltweiten fairen wirtschaftlichen Entwicklung zu nutzen.

12.4. Abschließende Bemerkungen

Der grundlegende Punkt, nämlich der Schutz der Privatsphäre der europäischen Bürger, behält unverändert Gültigkeit, die stärkere Entwicklung einer gemeinsamen Aufklärungskapazität der Europäischen Union sollte jedoch als notwendig und unausweichlich angesehen werden. Die Zusammenarbeit mit Drittländern und insbesondere den Vereinigten Staaten sollte beibehalten und, was sehr gut möglich ist, gestärkt werden. Dies bedeutet nicht notwendigerweise, dass die europäischen SIGINT-Tätigkeiten automatisch in ein unabhängiges ECHELON-System der Europäischen Union integriert wird oder dass die Europäische Union zu einem vollständigen Partner im bestehenden UKUSA-Abkommen werden. Die Schaffung einer wirklichen europäischen Verantwortung im Bereich der Sammlung nachrichtendienstlicher Informationen jedoch muss aktiv geprüft werden. Eine integrierte europäische Aufklärungskapazität erfordert gleichzeitig ein System der politischen Kontrolle in Europa über die Tätigkeiten dieser Einrichtungen. Es müssen Beschlüsse gefasst werden über die Mittel für die Bewertung der Informationen und für das Treffen politischer Entscheidungen, die das Ergebnis einer Analyse der nachrichtendienstlichen Berichte sind. Ohne ein solches System der politischen Kontrolle und deshalb des politischen Bewusstseins und der politischen Verantwortung, was das Verfahren der Sammlung nachrichtendienstlicher Informationen angeht, würden sich Nachteile für den europäischen Integrationsprozess ergeben.

13. Schlussfolgerungen und Empfehlungen

13.1. Vorbemerkung

Dieses Kapitel fasst Erkenntnisse und mögliche Schlussfolgerungen zusammen. Es darf nicht als endgültig verstanden werden. Vielmehr möchte der Berichterstatter eine Arbeitsgrundlage für die jetzt zu führende politische Debatte im Ausschuss schaffen. Der Text wird sich danach nochmals ändern müssen, damit Elemente dieser Diskussion aufgenommen werden können.

13.2. Schlussfolgerungen

Zur Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON)

An der Existenz eines weltweit arbeitenden Kommunikationsabhörsystems, das durch anteiliges Zusammenwirken der USA, des Vereinigten Königreichs, Kanadas, Australiens und Neuseelands im Rahmen des UKUSA agreements funktioniert, kann nicht mehr gezweifelt werden. Dass sein Name tatsächlich "ECHELON" ist, scheint aufgrund vorliegender Indizien wahrscheinlich, ist allerdings von nachrangiger Bedeutung. Wichtig ist, dass das System nicht zum Abhören militärischer, sondern privater und wirtschaftlicher Kommunikation dient.
Die Analyse hat gezeigt, dass die Mächtigkeit dieses System bei Weitem nicht so umfangreich sein kann, wie von den Medien teilweise angenommen.

Zu den Grenzen des Abhörsystems

Das Überwachungssystem baut auf dem globalen Abhören von Satellitenkommunikation auf. Kommunikation wird jedoch in Gebieten mit hoher Kommunikationsdichte nur zu einem sehr geringen Teil über Satelliten vermittelt. Dies bedeutet, dass der überwiegende Teil der Kommunikation nicht durch Bodenstationen abgehört werden kann, sondern nur durch Anzapfen von Kabeln und Abfangen von Funk. Die Untersuchungen haben aber gezeigt, dass die ECHELON-Staaten nur auf einen sehr beschränkten Teil der kabel- und funkgebundenen Kommunikation Zugriff haben, und aufgrund des Personalaufwands auch nur einen beschränkten Teil der Kommunikation auswerten können.

Zur möglichen Existenz anderer Abhörsysteme

Da das Abhören von Kommunikation ein unter Nachrichtendiensten übliches Spionagemittel ist, könnte ein solches System auch von anderen Staaten betrieben werden, sofern sie über die entsprechenden finanziellen Mittel und die geographischen Voraussetzungen verfügen. Frankreich wäre - zumindest was die geographischen Voraussetzungen betrifft - aufgrund seiner Territorien in Übersee als einziger EU-Mitgliedstaat sogar in der Lage, alleine ein globales Abhörsystem zu errichten. Es gibt Hinweise, dass auch Russland ein solches System betreiben könnte.

Zur Vereinbarkeit mit EU-Recht

Was die Frage der Vereinbarkeit eines Systems des Typs ECHELON mit EU-Recht betrifft, so ist zu unterscheiden: Wird das System nur zu nachrichtendienstlichen Zwecken verwendet, so ergibt sich kein Widerspruch zu EU-Recht, da Tätigkeiten im Dienste der Staatssicherheit vom EGV nicht erfasst sind, sondern unter Titel V EUV (GASP) fallen würden, es derzeit dort aber noch keine einschlägigen Regelungen gibt, und es somit an Berührungspunkten fehlt. Wird das System hingegen zur Konkurrenzspionage missbraucht, so steht das System im Widerspruch zur

Loyalitätspflicht der Mitgliedstaaten und zum Konzept eines gemeinsamen Marktes mit freiem Wettbewerb. Beteiligt sich ein Mitgliedstaat daran, so verletzt er EG-Recht.

Zur Vereinbarkeit mit dem Grundrecht auf Privatsphäre (Art 8 EMRK)

Jedes Abhören von Kommunikation stellt einen tiefgreifenden Eingriff in die Privatsphäre des Einzelnen dar. Art 8 EMRK, der die Privatsphäre schützt, lässt Eingriffe nur zur Gewährleistung der nationalen Sicherheit zu, sofern die Regelungen im innerstaatlichen Recht niedergelegt und allgemein zugänglich sind, und festlegen, unter welchen Umständen und Bedingungen die Staatsgewalt sie vornehmen darf. Eingriffe müssen verhältnismäßig sein, es muss daher eine Interessenabwägung vorgenommen werden, dass er rein nützlich oder wünschenswert ist, genügt nicht.

Ein nachrichtendienstliches System, das ohne Gewährleistung der Einhaltung des Verhältnismäßigkeitsprinzips jedwede Kommunikation abfangen würde, wäre mit der EMRK nicht vereinbar. In gleicher Weise läge ein Verstoß gegen die EMRK vor, wenn die Regelung, nach der Kommunikationsüberwachung erfolgt, keine Rechtsgrundlage hat, wenn diese nicht allgemein zugänglich ist oder wenn sie so formuliert ist, dass ihre Konsequenzen für den einzelnen nicht vorhersehbar sind. Da die Regelungen, nach denen amerikanische Nachrichtendienste im Ausland tätig werden, großteils klassifiziert sind, ist die Wahrung des Verhältnismäßigkeitsprinzips zumindest fraglich. Ein Verstoß gegen die die vom EGMR aufgestellten Prinzipien der Zugänglichkeit der Rechts und die Voraussehbarkeit seiner Wirkung liegt aber wohl vor.Auch wenn die USA selbst nicht Vertragsstaat der EMRK ist, so müssen sich doch die Mitgliedstaaten konform zur EMRK verhalten. Sie können sich ihrer aus der EMRK erwachsenden Verpflichtungen nicht dadurch entziehen können, dass sie die Nachrichtendienste anderer Staaten auf ihrem Territorium tätig werden lassen, die weniger strengen Bestimmungen unterliegen. Anderenfalls würde das Legalitätsprinzip mit seinen beiden Komponenten der Zugänglichkeit und Voraussehbarkeit seiner Wirkung beraubt und die Rechtssprechung des EGMR in ihrem Inhalt ausgehöhlt.

Die Grundrechtskonformität gesetzlich legitimierter Tätigkeit von Nachrichtendiensten verlangt zudem, dass ausreichende Kontrollsysteme vorhanden sind, um einen Ausgleich zur Gefahr zu schaffen, die das geheime Agieren eines Teiles des Verwaltungsapparates mit sich bringt. In Anbetracht der Tatsache, dass der Europäische Gerichtshof für Menschenrechte ausdrücklich die Bedeutung eines effizienten Kontrollsystems im Bereich nachrichtendienstlicher Tätigkeit hervorhob, erscheint bedenklich, dass einige Mitgliedstaaten über keine eigenen parlamentarischen Kontrollorgane für Geheimdienste verfügen.

Zur Frage, ob EU-Bürger ausreichend vor Nachrichtendienste geschützt sind

Da der Schutz der EU-Bürger von der Rechtslage in den einzelnen Mitgliedstaaten abhängt, und diese sehr unterschiedlich gestaltet sind, teilweise gar keine parlamentarischen Kontrollorgane bestehen, kann kaum von einem ausreichenden Schutz gesprochen werden. Die europäischen Bürger haben ein fundamentales Interesse daran, dass ihre nationalen Parlamente mit einem formell strukturierten speziellen Kontrollausschuss ausgestattet sind, der die Aktivitäten der Nachrichtendienste überwacht und kontrolliert. Aber selbst wo es Kontrollorgane gibt, ist für diese der Anreiz groß, sich mehr um die Tätigkeit von Inlandsnachrichtendiensten als von Auslandsnachrichtendiensten zu kümmern, da in der Regel nur im ersten Fall die eigenen Bürger betroffen sind.

Im Falle einer Zusammenarbeit der Nachrichtendienste im Rahmen der GASP sind die Institutionen gefordert, ausreichende Schutzbestimmungen zugunsten der europäischen Bürger zu schaffen.

Zur Wirtschaftsspionage

Es ist Bestandteil des Aufgabengebiets von Auslandsnachrichtendiensten, sich für wirtschaftliche Daten, wie Branchenentwicklungen, Entwicklung von Rohstoffmärkten, Einhaltung von Wirtschaftsembargos, Einhaltung der Lieferregeln für Dual-use-Güter etc zu interessieren. Aus diesen Gründen werden einschlägige Unternehmen oftmals überwacht. Nicht tolerierbar wird die Situation, wenn sich Nachrichtendienste für Konkurrenzspionage instrumentalisieren lassen, indem sie ausländische Unternehmen ausspionieren, um inländischen einen Wettbewerbsvorteil zu verschaffen. Dass das globale Abhörsystem dafür eingesetzt wurde, wird zwar vielfach behauptet, es gibt aber keinen belegten Fall.
Tatsächlich befinden sich sensible Unternehmensdaten vor allem in den Unternehmen selbst, sodass Konkurrenzspionage in erster Linie dadurch erfolgt, dass versucht wird, über Mitarbeiter oder eingeschleuste Personen Informationen zu bekommen oder in die internen Computernetzwerke einzudringen. Nur wenn sensible Daten über Leitungen oder via Funk (Satellit) nach außen gelangen, kann ein Kommunikationsüberwachungssystem zur Konkurrenzspionage eingesetzt werden. Dies trifft systematisch in folgenden drei Fällen zu:
- bei Unternehmen, die in 3 Zeitzonen arbeiten, so dass die Zwischenergebnisse von Europa nach Amerika und weiter nach Asien gesendet werden.
- im Falle von Videokonferenzen in multinationalen Konzernen, die über V-Sat oder Kabel laufen.
- wenn wichtige Aufträge vor Ort verhandelt werden (wie im Anlagenbau, Telekommunikationsinfrastruktur, Neuerrichtung von Transportsystemen, etc), und von dort aus Rücksprachen mit der Firmenzentrale gehalten werden müssen.

Zu den Möglichkeiten, sich selbst zu schützen
Unternehmen müssen das gesamte Arbeitsumfeld absichern sowie alle Kommunikationswege schützen, auf denen sensible Informationen übermittelt werden. Es gibt ausreichend sichere Verschlüsselungssysteme zu erschwinglichen Preisen auf dem europäischen Markt. Auch Privaten muss dringend zur Verschlüsselung von e-mails geraten werden, ein unverschlüsseltes Mail ist wie ein Brief ohne Umschlag. Im Internet finden sich relativ benutzerfreundliche Systeme, die sogar für den Privatgebrauch unentgeltlich zur Verfügung gestellt werden.

Zu einer Zusammenarbeit der Nachrichtendienste innerhalb der EU
Die EU hat sich darauf verständigt, nachrichtendienstliche Informationssammlung im Rahmen der Entwicklung einer eigenen Sicherheits- und Verteidigungspolitik zu koordinieren, dabei aber die Zusammenarbeit mit anderen Partnern in diesen fortzusetzen. Eine Zusammenarbeit der Nachrichtendienste innerhalb der EU erscheint insoweit wünschenswert, als einerseits eine Gemeinsame Sicherheitspolitik ohne Einbeziehung der Geheimdienste sinnwidrig wäre, andererseits damit zahlreiche Vorteile in professioneller, finanzieller und politischer Hinsicht verbunden wären. Auch würde es eher der Idee eines gleichberechtigten Partner der USA gegenüber entsprechen, und könnte sämtliche Mitgliedstaaten in ein System einbinden, das in voller Konformität zur EMRK erstellt wird. Eine entsprechende Kontrolle durch das Europäische Parlament muss dann natürlich gesichert sein. Das Europäische Parlament ist im Begriff, eigene Regelungen betreffend den Zugriff auf vertrauliche und sensible Informationen und Dokumente aufzustellen.

13.3. Empfehlungen

betreffend Abschluss und Änderung internationaler Verträge zum Schutz der Bürger und Unternehmen

1. Der Generalsekretär des Europarats wird aufgefordert, dem Ministerkommittee eine Untersuchung zu unterbreiten, ob die Anpassung des in Art 8 EMRK garantierten Schutzes

der Privatsphäre an die modernen Kommunikationsmethoden und Abhörmöglichkeiten in einem Zusatzprotokoll oder gemeinsam mit der Regelung des Datenschutzes im Rahmen einer Revision der Datenschutzkonvention sinnvoll wäre, unter der Voraussetzung, dass dadurch weder eine Minderung des durch den Gerichtshof entwickelten Rechtsschutzniveaus noch eine Minderung der für die Anpassung an weitere Entwicklungen notwendigen Flexibilität bewirkt wird;

2. Die Mitgliedstaaten werden aufgefordert, eine europäische Plattform zu schaffen, um die gesetzlichen Regelungen zur Gewährleistung von Brief- und Fernmeldegeheimnis zu überprüfen, sich überdies auf einen gemeinsamen Text zu verständigen, der den Schutz der Privatsphäre, so wie er in Art 7 der Europäischen Charta der Grundrechte definiert ist, allen europäischen Bürgern auf dem Staatsterritorium der Mitgliedstaaten in seiner Gesamtheit gewährleistet und darüberhinaus garantiert, dass die Tätigkeit der Nachrichtendienste grundrechtskonform erfolgt, somit den in Kapitel 8 des Berichts, insbesondere in 8.3.4 aus Art 8 EMRK abgeleiteten Bedingungen entspricht;

3. Die Mitgliedstaaten des Europarats werden ersucht, ein Zusatzprotokoll zu beschließen, das den Europäischen Gemeinschaften den Beitritt zur EMRK ermöglicht, oder über andere Maßnahmen nachzudenken, die Konflikte in der Rechtsprechung zwischen dem Straßburger und dem Luxemburger Gerichtshof ausschließen;

4. Der Generalsekretär der UNO wird aufgefordert, den verantwortlichen Ausschuss mit der Vorlage von Vorschlägen zu beauftragen, die auf eine Anpassung des Art 17 des Internationalen Paktes über bürgerliche und politische Rechte, der den Schutz der Privatsphäre garantiert, an die technischen Neuerungen abzielen;

5. Die USA werden aufgefordert, das Zusatzprotokoll zum Internationalen Pakt über bürgerliche und politische Rechte zu unterzeichnen, damit Individualbeschwerden gegen die USA wegen seiner Verletzung vor dem konventionellen Menschenrechtsausschuss zulässig werden; die einschlägigen amerikanischen NGOs, insbesondere ACLU (American Civil Liberties Union) und EPIC (Electronic Privacy Information Center) werden ersucht, auf die amerikanische Regierung entsprechenden Druck auzuüben;

betreffend nationale gesetzgeberische Maßnahmen zum Schutze von Bürgern und Unternehmen

6. An alle Mitgliedstaaten wird appelliert, ihre eigene Gesetzgebung betreffend die Tätigkeit von Nachrichtendiensten auf ihre Grundrechtskonformität zu überprüfen;

7. Die Mitgliedstaaten werden aufgefordert, ein gemeinsames Schutzniveau gegenüber nachrichtendienstlicher Tätigkeit anzustreben, das sich am höchsten mitgliedstaatlichen Schutz orientiert, da die von der Tätigkeit eines Auslandsnachrichtendienstes betroffenen Bürger in der Regel die anderer Staaten und daher auch die anderer Mitgliedstaaten sind;

8. Die EU-Institutionen werden aufgefordert, im Falle einer Zusammenarbeit der Nachrichtendienste im Rahmen der GASP ausreichende Schutzbestimmungen zugunsten der europäischen Bürger zu schaffen. Das Europäische Parlament als logisches Kontrollorgan muss seinerseits die für die Überwachung dieses hoch sensiblen Bereichs notwendigen Voraussetzungen schaffen, damit es realistisch, aber auch verantwortbar ist, die notwendigen Kontrollrechte einzufordern;

betreffend besondere rechtliche Maßnahmen zur Bekämpfung der Wirktschaftsspionage

9. Die Mitgliedstaaten werden aufgefordert, Überlegungen anzustellen, inwieweit durch Regelungen im europäischen und internationalen Recht Wirtschaftsspionage und Bestechung

zum Zweck der Auftragsbeschaffung bekämpft werden können, insbesondere ob eine Regelung im Rahmen der WTO möglich wäre, die der wettbewerbsverzerrenden Wirkung eines derartigen Vorgehens Rechnung trägt, z.B. indem sie die Nichtigkeit solcher Verträge festlegt.;

10. Die Mitgliedstaaten werden aufgefordert, sich in einer gemeinsamen eindeutigen Erklärung selbst zu verpflichten, keine Wirtschaftsspionage gegeneinander zu betreiben, und damit ihren Einklang mit dem Geiste und den Bestimmungen des EG-Vertrags zu signalisieren;

betreffend Maßnahmen in der Rechtsanwendung und ihrer Kontrolle

11. appelliert an die nationalen Parlamente, die über keine eigenen paralementarischen Kontrollorgane zur Überwachung der Nachrichtendienste verfügen, solche einzurichten;

12. Die nationalen Kontrollausschüsse der Geheimdienstewerden ersucht, bei der Ausübung der ihnen übertragenen Kontrollbefugnisse dem Schutz der Privatsphäre großes Gewicht beizumessen, unabhängig davon, ob es um die Überwachung eigener Bürger, anderer EU-Bürger oder Drittstaatler geht;

13. Die Nachrichtendienste der Mitgliedstaaten werden aufgefordert, Daten von anderen Nachrichtendiensten nur dort entgegenzunehmen, wo diese unter Voraussetzungen ermittelt werden konnten, die das eigene nationale Recht vorsieht, da sich die Mitgliedstaaten nicht den aus der EMRK erwachsenen Verpflichtungen dadurch entledigen können, dass sie andere Nachrichtendienste einschalten;

14. An Deutschland und England wird appelliert, die weitere Gestattung von Abhören von Kommunikation durch Nachrichtendienste der USA auf ihrem Gebiet davon abhängig zu machen, dass diese im Einklang mit der EMRK stehen, dh dass sie dem Verhältnismäßigkeitsgrundsatz genügen, ihre Rechtsgrundlage zugänglich und die Wirkung für den einzelnen absehbar ist, sowie eine entsprechend effiziente Kontrolle besteht, da sie für die Menschenrechtskonformität genehmigter oder auch nur geduldeter nachrichtendienstlicher Tätigkeit auf ihrem Territorium verantwortlich sind.

betreffend Maßnahmen zur Förderung des Selbstschutzes von Bürgern und Unternehmen

15. Die Kommission und die Mitgliedstaaten werden aufgefordert, Programme zu entwickeln, die das Bewusstsein von Bürgern und Unternehmen für die Sicherheitsproblematik fördern, und gleichzeitig praktische Hilfe für Entwurf und Umsetzung von umfassenden Schutzkonzepten anbieten.

16. Die Kommission und die Mitgliedstaaten werden ersucht, geeignete Maßnahmen für die Förderung, Entwicklung und Herstellung von europäischer Verschlüsselungstechnologie und -software auszuarbeiten und vor allem Projekte zu unterstützen, die darauf abzielen, benutzerfreundliche Kryptosoftware, deren Quelltext offengelegt ist, zu entwickeln;

17. Die Kommission und die Mitgliedstaaten werden aufgefordert, Softwareprojekte zu fördern, deren Quelltext offengelegt wird, da nur so garantiert werden kann, dass keine "backdoors" eingebaut sind (sogenannte "open source software");

18. An die europäischen Institutionen sowie an die öffentlichen Verwaltungen der Mitgliedstaaten wird appelliert, Verschlüsselung von e-mails systematisch einzusetzen, um so langfristig Verschlüsselung zum Normalfall werden zu lassen;

betreffend anderer Maßnahmen

19. An die Unternehmen wird appelliert, mit den Spionageabwehreinrichtungen stärker zusammenzuarbeiten, ihnen insbesondere Attacken von Außen zum Zwecke der Wirtschaftsspionage bekannt zu geben, um so die Effizienz der Einrichtungen zu erhöhen;

20. Die Kommission wird aufgefordert, einen Vorschlag zur Einsetzung einer europäischen Beratungsstelle für Fragen der Sicherheit von Unternehmensinformation vorzulegen, die neben der Steigerung des Problembewußtseins auch praktische Hilfestellungen zur Aufgabe hat;

21. Das Europäische Parlament wird augefordert, einen übereuropäischen Kongress zum Schutz der Privatsphäre vor Telekommuhnikationsüberwachung zu organisieren, um für NGOs aus Europa, den USA und anderen Staaten eine Platform zu schaffen, wo grenzüberschreitende und internationale Aspekte diskutiert und Tätigkeitsfelder und Vorgehen koordiniert werden können;