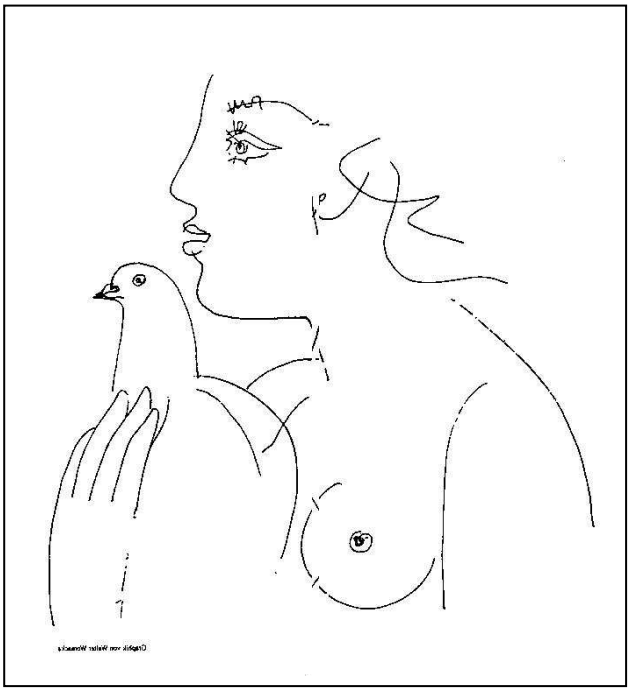
Europäisches Friedensforum epf Deutsche Sektion
Zentraler Arbeitskreis Frieden der
Gesellschaft zum Schutz von Bürgerrecht und Menschenwürde e.V.

Nr. 121



Achtung! Freund hört mit

Zur Geschichte der amerikanisch-deutschen Beziehungen im elektronischen Krieg

von

Klaus Eichner

Redaktionsschluss: 30. August 2013

c/o **Gesellschaft zum Schutz von Bürgerrecht und Menschenwürde e. V.**
Weitlingstrasse 89, 10317 Berlin
Tel.: 030/ 557 83 97 Fax: 030/ 555 63 55 E-mail: gbmev@t-online.de Homepage: www.gbmev.de/

Seit Wochen beschäftigen die Aktivitäten der Geheimdienste wieder einmal die deutsche Öffentlichkeit. Medien und Politiker reagieren so, als ob diese Praktiken für sie absolut neu und einzigartig sind und als ob es sich nur um ein bisschen „Schnüffelei“ handele.

Die Reaktionen der deutschen Öffentlichkeit weisen u. a. auch auf einige Defizite im Politgeschehen Deutschlands hin.
Zum einen sind das gravierende Mängel des so hochgelobten Systems der parlamentarischen Kontrolle der Geheimdienste. Selbst die ausgesuchten und handverlesenen Parlamentarier in den Kontrollgremien sind nicht in der Lage, wesentliche Fragen zu stellen, die die Verantwortlichen in der Regierung zwingen könnten, Hintergründe der Geheimdienstzusammenarbeit zwischen den USA und der BRD zu offenbaren.
Zum anderen versagte bisher die vielgerühmte „vierte Macht“ in ihrer Mehrheit bei der Informierung der Öffentlichkeit. Regierungspositionen werden meist nur nachgebetet, kaum einmal hinterfragt. Haben die investigativen Journalisten vergessen (oder verzichtet), in ihre eigenen Archive zu sehen oder evtl. im Internet zu recherchieren?

Hier einige Anregungen und Erinnerungen:

Elektronische Kriegführung (Cyber Warfare)

Aktionen der technischen Aufklärung waren seit Ende des II. Weltkrieges Bestandteil der Aktivitäten der US-Geheimdienste in Deutschland. Während es zu Beginn vorwiegend die Erfassung von Funkverkehren und die Versuche ihrer Dechiffrierung sowie grenznahe Aufklärungsflüge zur Bildaufklärung waren, spielten später geheime Angriffe gegen die Nachrichtenverbindungen über Kabel, die Erfassung der Satellitenfunkverkehre sowie andere Methoden unter Einsatz von Hochleistungstechnik eine größere Rolle. Ausgehend von den ersten Erfahrungen der technischen Aufklärung im II. Weltkrieg entwickelten alle Geheimdienste ganze Komplexe von technischen Maßnahmen zur Aufklärung und Bekämpfung potentieller Gegner, die im deutschen Sprachgebrauch unter dem Begriff Elektronische Kampfführung (ELOKA) zusammengefasst wurden.

In den letzten Jahrzehnten wuchs die Bedeutung der Elektronischen Kriegführung (Electronic Warfare - EW) ständig weiter an. Das entsprach der z. T. sprunghaften Entwicklung der technischen Möglichkeiten für die Peilung, Erfassung, Auswertung sowie Analyse der dabei anfallenden Daten. Parallel dazu wuchsen die Schwierigkeiten eines effektiven Umgangs mit dem Informationsaufkommen in völlig neuen Größenordnungen.
Die ELOKA wurde zunehmend zu einem bestimmenden Faktor der modernen Kriegführung. Der Bereich der Fernmelde/Elektronischen Aufklärung, zusammengefasst unter dem Begriff "Signal Intelligence - SIGINT", gewann damit bei allen Aufklärungseinheiten der Teilstreitkräfte der westlichen und östlichen Militärbündnisse und bei ihren Nachrichtendiensten zunehmend an Bedeutung und wurde entsprechend forciert.
In den modernen Kriegsführungsstrategien spielen komplexe Zusammenfassungen von Elemente der elektronischen Kriegführung zu einem eigenständigen Waffensystem (Cyber Warfare) gemeinsam mit dem Einsatz von Aufklärungs- und Kriegsdrohnen und von nachrichtendienstlichen Spezialeinheiten eine eigenständige Rolle. Gegenwärtig sind alle Bereiche einer modernen Gesellschaft durch eine Vernetzung von IT-Technologien fast durchgängig von computergestützten Systemen abhängig, so dass eine Störung oder gar Ausschaltung dieser Systeme zum Zusammenbruch des jeweiligen Gegners führen würde.
Auch die Geheimdienste werden immer deutlicher von der IT-Technologie abhängig. Experten gehen z.B. davon aus, dass nur ca. 25 Prozent des Informationsaufkommens der Geheimdienste von geheimen Quellen erbracht werden, von diesen Informationen stammen wiederum drei Viertel aus der Fernmelde/Elektronischen Aufklärung. Das daraus entstehende Informationsaufkommen ist (wenn überhaupt) nur noch durch den Einsatz von Hochleistungscomputern beherrschbar. Mit den elektronischen Informationen wachsen aber auch die Möglichkeiten der Täuschung und Desinformation sowie die Anfälligkeiten für elektronische Störmaßnahmen.

Historische Grundlagen: Der UKUSA-Vertrag von 1947

Elemente der Fernmelde/Elektronischen Aufklärung wurden durch die britischen und amerikanischen Geheimdienste bereits im Zweiten Weltkrieg u. a. durch die Entschlüsselung einiger deutscher und japanischer Codes erfolgreich eingesetzt (Operationen ULTRA bzw. MAGIC). Die britisch - amerikanischen Beziehungen auf diesem Gebiet beruhten auf dem "BRUSA Agreement" vom 17. Mai 1943.
Darauf aufbauend schufen die amerikanischen Geheimdienste sehr frühzeitig einen Informationsverbund von Partnerdiensten. Bereits 1947 wurde das "UK-USA Security Agreement" zwischen den USA und Vertretern des Commonwealth (UK = United Kingdom) abgeschlossen. Dieser sogenannte "UKUSA-Vertrag" teilt die regionalen Zuständigkeiten für die SIGINT-Informationsbeschaffung zwischen der Partei ersten Ranges (First Party) - den Vereinigten Staaten - und den Parteien zweiten Ranges (Second Parties) - Großbritannien, Australien, Kanada, Neuseeland auf.
Später kamen zu diesem Vertrag noch eine Vielzahl von Parteien dritten Ranges (Third Parties) hinzu, die häufig eine größere Bedeutung in den Partnerdienstbeziehungen auf SIGINT-Gebiet erlangten als die Geheimdienste der "Second Parties"; so z.B. die NATO-Partner Deutschland, Dänemark, Norwegen, Länder wie Malaysia und Singapore; Japan, Südkorea, Israel, Taiwan, Südafrika; auch die Volksrepublik China wurde durch die Nutzung einer Großanlage im Pamir-Gebirge in das System einbezogen..
Dieses Vertragssystem ermöglichte den US-Geheimdiensten damit die Errichtung eigener bzw. die Mitnutzung bestehender Peil-, Erfassungs- und Auswertungsstationen in allen bedeutsamen Regionen der Welt.
Der UKUSA-Vertrag enthält auch Regelungen zur Gestaltung des Informationsaustausches und zur innerstaatlichen Umsetzung der über diesen Austausch erhaltenen Partnerdienst-Informationen.
Damit sind die Grundsätze der zwischenstaatlichen Zusammenarbeit auf dem Gebiet der elektronischen Spionage allen beteiligten Regierungen seit Jahrzehnten bekannt.

Das UKUSA-System war Kind und Motor des Kalten Krieges. Mit ihm sollte ein immer dichterer Aufklärungsring um die UdSSR und ihre Verbündeten gezogen werden. Sein ständiger Ausbau war Be-

standteil des gigantischen Rüstungswettlaufes zwischen den Systemen; seine Ergebnisse wurden meist so analytisch verarbeitet, dass neue Impulse für den Rüstungswettlauf ausgelöst wurden. Das war insbesondere dann der Fall, wenn wieder einmal Entscheidungen über das Rüstungsbudget in den Parlamenten oder anderen Gremien der beteiligten Staaten anstanden.

Partner im UKUSA-Vertrag

Der zentrale Geheimdienst der USA für die Fernmelde / Elektronische Aufklärung wird korrekt bezeichnet als „National Security Agency/Central Security Service - NSA/CSS“ (umgangssprachlich nur als NSA bezeichnet). Die NSA wurde durch das Präsidenten-Memorandum: "Communications Intelligence Activities" vom 24. Oktober 1952 als ein Geheimdienst des Verteidigungsministeriums gebildet. Mit einer Direktive von 1972 wurde die zweite Grundrichtung des Einsatzes der NSA - die zentrale Verantwortung für die Sicherheit der Kommunikationslinien der Regierung durch die Errichtung des Central Security Service-CSS - festgelegt.
Das Hauptquartier der NSA ist in Fort George Meade/Maryland stationiert. Der Personalbestand wird mit rund 40.000 Mitarbeitern in der Zentrale und 150.000 Mitarbeitern im weltweiten Einsatz angegeben; das Jahresbudget auf rund 10 Milliarden US-Dollar geschätzt.
Seit 2010 leitet der Direktor der NSA außerdem das Cyber Command der US-Streitkräfte, in welchem die elektronische Kriegführung des US-Militärs konzipiert und geleitet wird.
Für die Zusammenfassung und Verarbeitung von Massendaten der US-Aufklärung soll noch im Jahr 2013 das sogenannte Utah Data Center (im Original: Comprehensive National Cybersecurity Initiative Data Center) im Camp Williams bei Bluffdale/Utah eingeweiht werden. Geschätzte Baukosten 1,7 Milliarden US-Dollar.
Seit der Bildung der NSA wurde es zur Regel, dass alle Neuentwicklungen auf dem Gebiet der Datenverarbeitung mit der NSA abgestimmt und meist auch dort erstmalig erprobt wurden. Damit waren alle Hochleistungscomputer vorerst in der NSA-Zentrale eingesetzt – und die NSA nahm auf die technische Entwicklung Einfluss, womit ihr jederzeit der Zugang zu allen Sicherheitssyste-

men der Hard- und Software gewährt wurde – entweder durch legale Vereinbarungen oder auf illegalem Wege.
Die NSA-Zentrale unterhält ein europäisches Hauptquartier (NSA/CSS Europe) mit seinem Stab im Europakommando der U.S.-Streikräfte (USEUCOM) in Stuttgart/Vaihingen. Außenstellen des NSA-Europakommandos operierten bisher in den Großstationen Augsburg und in Berlin (Teufelsberg).
Für die speziellen Kontakte der NSA-Zentrale zu Großbritannien im Rahmen des UKUSA-Vertrages existierte in London ein Büro für Sonderverbindungen (Special United States Liaison Office - SUSLO).

Die weltweiten Informationsinteressen der NSA wurden bereits Anfang der 80er Jahre durch ein umfangreiches Dokument mit der Bezeichnung National SIGINT Requirements List (NSRL) bekannt (1). In ihm wurden akribisch die Interessenlagen aller amerikanischen Geheimdienste sowie einzelner ihrer Strukturen, aber auch die Wünsche anderer Regierungsorgane, so des Weißen Hauses, des Außen- oder Energieministeriums an spezifischen Informationen zu bestimmten Regionen und Ländern weltweit festgehalten. Detailliert betraf das die Informationsinteressen über die Außen-, Innen-, Wirtschaftspolitik, Potenzen an strategischen Rohstoffen; Streitkräftelage, Besitz an Massenvernichtungswaffen, Grundlagenforschung (vor allem jene Bereiche, aus denen auch für die Vereinigten Staaten Überraschungseffekte durch potentielle Gegner oder Partner entstehen konnten), spezielle Rüstungsforschung, Energiepolitik, besonders Kernenergieforschung u. ä.; in der Regel auch Tätigkeit der Geheimdienste der Länder.
Aus diesem Dokument war deutlich zu ersehen, wie stark die Interessen der USA an der Aufklärung und Bearbeitung der Verbündeten der USA waren. Äußerst umfangreich wurden Informationswünsche zu Ländern wie Frankreich, Großbritannien, Kanada oder der BRD fixiert, insbesondere Umfang und Detailliertheit der Informationsinteressen zu Frankreich und der BRD waren hervorstechend.

1 vgl. Eichner/Dobbert: Headquarters Germany, edition ost, 1997, S. 240ff.

Sondereinsätze (Special Collection)

Am Anfang seiner Tätigkeit als Chef der zentralen Aufklärung (Director of Central Intelligence – DCI) und Direktor der CIA (9. März 1977 bis 20. Januar 1981) verfasste Admiral Stansfield Turner ein Memorandum der Geheimhaltungsstufe "DCI eyes only", das nur den Spitzenkräften der Intelligence Community und der CIA zugänglich war. Darin forderte er "...greater need for intelligence on allies and friends." Turner vertrat die Überzeugung, dass die unangenehmsten Überraschungen immer von den eigenen Freunden kommen.

Um diesem Anliegen konsequent nachzukommen, aktivierte Turner die Tätigkeit der "Division D" (2) der CIA, die sich – entweder durch legale Vereinbarungen oder auf illegalem Wege mit der Umsetzung operativ technischer Maßnahmen der Fernmelde/Elektronischen Aufklärung im Ausland befasste. Nach längeren Koordinierungsabsprachen kam es 1983 zur Bildung erster sogen. Special Collection Elements (SCE).

Dabei wurden die technischen Durchbrüche, die durch die NSA Ende der 70er und Anfang der 80er Jahre erzielt wurden, mit den operativen Erfahrungen und Anforderungen der Tätigkeit der Field-Officer der CIA vor Ort verbunden und somit in die unmittelbare Spionagetätigkeit integriert.

Die SCE waren Einsatzteams, die sich aus Kadern der "Division D" der CIA und den entsprechenden Partnern der NSA zusammensetzten. Diese geheimen Einsatzgruppen waren zu dieser Zeit in ca. einem Drittel aller USA-Auslandsvertretungen disloziert, nach einigen Angaben in rund 45 der Botschaften und Konsulate der USA. Schwerpunkt bildeten und bilden selbstverständlich die osteuropäischen Länder, aber nicht zuletzt akute und potentielle Krisenregio-

---

2 Der Stab D im CIA-Hauptquartier war mit den technischen und personellen Voraussetzungen zum Einsatz spezieller Technik der Fm/EloAufklärung der CIA befasst. Der britische Autor Peter Wright äußerte die Vermutung, dass er den amerikanischen Geheimdiensten auch dazu dienen sollte, die vertraglichen Pflichten aus dem UKUSA - Vertrag zum Informationsaustausch zu umgehen. Vgl. Peter Wright/Paul Greengrass: "Spy Catcher", Enthüllungen aus dem Secret Service; deutsche Ausgabe in: Ullstein Sachbuch Nr. 34486, Nov. 1989, S. 154ff.

nen gehörten und gehören zu den bevorzugten Einsatzzielen der SCE.
Die Leitung der US-Geheimdienste und der Nationale Sicherheitsrat definierten für die SCE zwei Richtungen von Spionageaktivitäten:
1. Spionage gegen alle kommunistischen oder in sonstiger Weise nicht- proamerikanischen Staaten;
2. sensitive Spionageoperationen gegen Freunde und Verbündete.

Sowohl Admiral Turner als auch der spätere CIA-Direktor Casey haben betont, dass Operationen gegen Freunde und Verbündete als notwendig betrachtet und soweit wie möglich und notwendig ausgebaut werden sollten. Zu Turners Zeiten waren das angeblich einige wenige pro Jahr. Als Casey 1981 zu seiner Amtsübernahme entsprechende Untersuchungen anstellen ließ, war er überrascht, dass es sich um mehr als drei Dutzend laufender Maßnahmen handelte. Zu diesem Zeitpunkt lieferten SCE in Europa (besonders auch aus osteuropäischen Hauptstädten), im Nahen Osten und in Asien regelmäßig wortwörtliche Mitschnitte von Beratungen hochrangiger Regierungsvertreter und von Telefongesprächen führender Politiker. Andere technische Anwendungen betrafen z.B. elektronische Raumüberwachungen ohne ein direktes Eindringen in die Räume, u. a. durch die Aufnahmen von Schwingungen der Fensterscheiben bei normalen Gesprächen mit Hilfe der Lasertechnik.

Selbstverständlich waren sich die Führungskräfte der Intelligence Community der Brisanz einer Tätigkeit gegen die eigenen Freunde und Verbündeten bewusst. Es konnten schwere Krisen in den zwischenstaatlichen und diplomatischen Beziehungen ausgelöst werden, wenn die globalen und tatsächlichen Ziele der USA in der Spionage gegen Freunde und Verbündete festgestellt und dokumentiert worden wären.
Die Risiken der Aufdeckung solcher Maßnahmen lagen jedoch nach Auffassung der Abwehrexperten fast ausschließlich in den eigenen Reihen. Sollten die eingesetzten technischen Hilfsmittel doch entdeckt werden, so würde jeder Verbündete oder Freund zuerst eine Spionageoperation des KGB oder seiner Verbündeten vermuten.

Ca. 1987 wandte sich die CIA an den BND mit Bitte um Unterstützung. Die USA - Geheimdienste wollten SCE auch in einigen Ländern einsetzen, in denen sie selbst nicht mit diplomatischen Vertre-

tungen oder Auslandsresidenturen präsent waren, vorrangig in Libyen (und in drei weiteren Ländern). Daraufhin beantragte die Leitung des BND beim Auswärtigen Amt in Bonn die Genehmigung zur Einrichtung einer Auslandsresidentur vorerst in Libyen, um für die CIA diese Maßnahmen zu realisieren und natürlich an dem Informationsaufkommen zu partizipieren.

All diese Entwicklungen blieben der östlichen Aufklärung nicht verborgen, der Informationsfluss aus den wesentlichen Komponenten der westlichen Spionagetätigkeit war fast durchgehend gewährleistet.

Dazu einige Beispiele aus dem Bereich der technischen Spionage:

Während des Koreakrieges kam der sowjetische Nachrichtendienst in Kontakt mit dem Mitarbeiter des britischen Secret Intelligence Service - SIS, **George Blake**. Dieser entwickelte sich zu einem Spezialisten für technische Aufklärungsoperationen gegen die Sowjetunion. In dieser Funktion war er u. a. an der Planung einer angloamerikanischen Operation gegen Kabelverbindungen des sowjetischen Oberkommandos in Berlin beteiligt – bekannt als „Spionagetunnel Altglienicke“. Während CIA und SIS diese Aktion als einen großen Erfolg feierten, hatte die sowjetische Seite durch George Blake von Anfang an Kenntnis über diese Aktion und bestimmte, welche Informationen der westlichen Seite gezielt zur Kenntnis gegeben wurden, und wann und wie die öffentlich wirksame Enttarnung des Spionagetunnels erfolgen sollte.

Von 1980 bis 1985 war der Kommunikations-Spezialist der National Security Agency, der US-Bürger **Ronald W. Pelton** als Quelle der sowjetischen Aufklärung tätig. Pelton informierte z.B. die sowjetische Seite über das streng geheime Projekt „Ivy Bells“. Im Rahmen von Sonderoperationen der US-Marine hatte die NSA technische Möglichkeiten zur berührungsfreien Erfassung von Informationen aus besonders gesicherten Kabelverbindungen entwickelt, die u. a. bei illegalen U-Boot-Einsätzen gegen Unterseekabel der Sowjetunion im Ochotskischen Meer vor Wladiwostok erprobt worden waren. Die Weiterentwicklung dieser Technik ermöglichte auch Einsätze gegen unterirdische und andere verkabelte Sonderverbindungen in verschiedenen Ländern.

Die Informationen von Ronald Pelton ermöglichten der sowjetischen Abwehr, rechtzeitig geeignete Gegenmaßnahmen einzuleiten. 1986 wurde Pelton von einem US-Gericht verurteilt.
Auf der Grundlage von Quelleninformationen und im Ergebnis der systematischen Überwachung der SCE-Aktivitäten in der UdSSR konnte die sowjetische Abwehr einige überraschende Ergebnisse vorweisen.

1986/87 wurde durch die sowjetische Abwehr eine Operation der US-Geheimdienste zum Abhören einer unterirdischen Kabelstrecke im Raum Moskau aufgedeckt (Operation PIPE der CIA). Das Telefonkabel verband ein bedeutsames Objekt der Verteidigungsindustrie mit zentralen Stellen in Moskau. Die technischen Einzelheiten wurden durch die sowjetische Abwehr im Detail dokumentiert und die beteiligten Spezialisten der in der US-Botschaft stationierten CIA-Residentur zugeordnet. Zu diesem Zeitpunkt erinnerte die Moskauer Botschaft der USA mit den dort eingebauten technischen Mitteln und Möglichkeiten mehr an einen Spionagesatelliten denn an eine diplomatische Auslandsvertretung.
Die Möglichkeiten zum Abhören des Telefonverkehrs (Autotelefone) und des Funkverkehrs z.B. des Außenministeriums, bestanden jedoch schon längere Zeit vor Bildung der SCE. Bekannt ist das Projekt GAMMA GUPY der CIA zum Abhören der Gespräche führender sowjetischer Politiker über ihre Autotelefone.

Westberlin war für die westlichen Geheimdienste insgesamt, besonders auch für die elektronische Spionage, ein Eldorado. Die amerikanischen Geheimdienste hatten mit der „Field Station Berlin“ auf dem Teufelsberg im Grunewald und mit der Luftwaffenstation in Berlin-Marienfelde, Diederdorfer Weg, zwei hocheffektive Einrichtungen zur Ausspähung des Ostens aufgebaut. Die britischen und französischen Geheimdienste wollten dem nicht nachstehen und bauten ihre Anlagen in Berlin-Gatow und -Reinickendorf auf. Insbesondere auf die amerikanischen Objekte konzentrierten sich die Abwehrmaßnamen der östlichen Seite, nicht zuletzt der Hauptverwaltung A der DDR.
Der Sergeant **James W. Hall** berichtete der HVA ab 1984 aus dem Objekt “Teufelsberg” und anderen Einrichtungen der elektronischen Spionage der USA-Geheimdienste in der BRD und weltweit.

Er hatte Zugang zu allen Grundsatzdokumenten der NSA und nachgeordneter Geheimdienststrukturen. Damit hatte die östliche Aufklärung einen tiefen Einblick in Arbeitsprinzipien, Strukturen und technische Ausrüstungen der bedeutendsten Elemente der elektronischen Spionage der USA. Das betraf auch alle Dienstanweisungen zur Arbeit des Objektes „Teufelsberg“, bis hin zur Modernisierungsplanung des Objektes bis zum Jahr 1995.

Ähnliche Ergebnisse erzielte die HVA zwischen 1983 und 1989 mit der Quelle **Jeffrey Carney**, der im Aufklärungsobjekt der US-Luftwaffe in Berlin-Marienfelde stationiert war. Carney lebte nach 1990 in Berlin-Friedrichshain. Am 22. April 1992 kidnappte ihn ein Einsatzkommando des Abwehrdienstes der US-Luftwaffe auf offener Straße und flog ihn illegal in die USA aus. Dort wurde er vor einem Militärgericht angeklagt und zu 38 Jahren Haft verurteilt. Nach 12 Jahren Gefängnisaufenthalt wurde Jeffrey Carney begnadigt.

Nach der Enttarnung der Quelle James W. Hall im Jahre 1988 erfolgten abwehrmäßige Überprüfungen des gesamten Personals der US-Geheimdienste in Berlin (West). Dabei wurde der Captain der US-Luftwaffe im Geheimdienst der elektronischen Aufklärung (Electronic Security Command) in Berlin-Tempelhof, **John Vladimir Hirsch**, verdächtigt, als Quelle der sowjetischen Aufklärung tätig gewesen zu sein.

„Regenbogenkonferenzen“

Die Fernmelde/Elektronische Aufklärung der amerikanischen Luftstreitkräfte organisierte in regelmäßigen Abständen sogenannte "Regenbogenkonferenzen". Unter Federführung der amerikanischen Dienste stellten dort Vertreter der entsprechenden Geheimdienst-Strukturen bzw. der Luftwaffe der einzelnen NATO-Länder neueste Entwicklungen in der Technik und in der Methodik der fernmeldeelektronischen Aufklärung vor, erläuterten aktuelle Strukturveränderungen, berieten Möglichkeiten des Informationsaustausches etc. Bei den "Regenbogenkonferenzen" gab es die politisch und völkerrechtlich so brisante Tatsache, dass Vertreter "neutraler" Staaten, in diesem Falle des schwedischen Geheimdienstes, an Tagungen von NATO-Einrichtungen teilnahmen. Die Organisatoren waren an-

gehalten, diese Tatsache selbst unter den Teilnehmern möglichst nicht publik zu machen.

Der östlichen Aufklärung lagen Informationen vor über ein spezielles Forschungsprogramm der NSA. Der Geheimdienst prüfte die Möglichkeiten, sich über Computersimulationen in den direkten Funkverkehr zwischen den Bodenleitstationen und den Einsatzflugzeugen bzw. U-Booten des potentiellen Gegners in Echtzeit so einzutakten, dass beide Gegenstellen das nicht bemerken konnten. Über diesen Weg sollten falsche Befehle an die Flugzeuge übermittelt werden. (3) Die Auswirkungen solcher Maßnahmen in einem realen Einsatz könnten katastrophal sein. Voraussetzungen dafür waren erst einmal umfangreiche Datenbanken, in denen die Stimmenprofile der Flugzeugbesatzungen und der Offiziere der Leitstellen erfasst und ständig aktualisiert wurden.

Zur Rolle der BRD

In der Bundesrepublik Deutschland war der Bundesnachrichtendienst – insbesondere seine Abteilung II – Technik – der Hauptpartner des UKUSA-Vertrages. Über Jahre hin waren aber auch spezielle Einheiten aller Teilstreitkräfte der Bundeswehr in das System eingebunden.
Bereits nach dem Ende des II. Weltkrieges begannen auf dem Territorium Deutschlands sehr früh abgestimmte Maßnahmen der elektronischen Ausforschung der potentiellen Gegner.
Der amerikanische militärische Nachrichtendienst Counter Intelligence Corps – CIC hatte 1946 Experten des Horchdienstes der faschistischen Wehrmacht in Bad Vilbel zusammengezogen, um über den Aufbau von Aufklärungsstationen zu beraten.
Bereits 1948 - im Zusammenhang mit der Berlin-Blockade - unterhielt die ORG Gehlen, der Vorläufer des BND, auf Schloss Kransberg eine Station zur Erfassung der Sprechfunk-Verbindungen sowjetischer Truppen und lieferte die Roh-Informationen an US-General LeMay in Wiesbaden und US-General Hall in Berlin.

---

3 Hinweise auf diese Realität sind z.B. zu finden in: „Der SPIEGEL“ Nr. 34/1995, S.132: „Schweiß schnuppern“. Der Autor verweist dort auf diverse Vorbereitungen des Pentagon auf „information warfare“, u.a. auch auf die Übermittlung gefälschter Befehle über Sprechfunk.

Die Auswertung dieser Informationslieferungen trug nicht wenig dazu bei, die Auffassungen über einen angeblich bevorstehenden Angriff sowjetischer Truppen beim amerikanischen Hochkommissar, General Lucius Clay, zu bestärken. (4)
1950 erarbeitete der Wehrmachtsgeneral Adolf Heusinger, zu diesem Zeitpunkt Leiter der Auswertung der Organisation Gehlen, ein Dokument unter dem Titel „Gedanken über eine zukünftige deutsche Funkaufklärung".
Die Frontstellung der BRD an der Ostgrenze des westlichen Paktsystems ermöglichte sowohl eine intensive Nahaufklärung der militärischen Komponenten des Warschauer Vertrages als auch strategische Aufklärung tief im Hinterland des potentiellen Gegners.
Das nutzten neben dem BND auch Geheimdienststrukturen der westlichen Alliierten auf dem Territorium der BRD und Westberlins. Ein Teil der Anlagen wurde erst nach 1990 Stück für Stück abgebaut.
In den 80er Jahren gaben die US-Geheimdienste für den Betrieb ihrer SIGINT-Stationen in Westberlin und entlang der Grenze zur DDR und CSSR jährlich rund eine Milliarde US-Dollar aus.

Unter den sozialdemokratischen Regierungen von Willy Brandt und Helmut Schmidt nahm die nationale und internationale Kooperation des BND auf dem Gebiet der elektronischen Aufklärung, insbesondere unter BND-Präsident Gerhard Wessel (1968 bis 1979), einen großen Aufschwung.
Am 18. Oktober 1969 wurden die „Richtlinien für die Zusammenarbeit zwischen Bundeswehr und Bundesnachrichtendienst auf dem Gebiet der Fernmeldeaufklärung und Elektronischen Aufklärung" (intern als ZUGVOGEL-Vereinbarung bezeichnet) in Kraft gesetzt. Nach diesen Richtlinien war der BND-Präsident im nationalen Maßstab für die Gesamtplanung, die Aufgabenverteilung und die Koordinierung der Fm/Elo-Aufklärung zuständig. Damit hatte der BND alle entscheidenden Fäden in der Hand.
Das wurde in einer Vereinbarung vom August 1992 noch einmal bestätigt. Neben der Koordinierung aller Aktivitäten war dem BND

---

4 aus einem Vortrag des ersten CIA-Verbindungsoffiziers zur ORG Gehlen, James H. Critchfield, auf der Jahrestagung des Arbeitskreises Geschichte der Nachrichtendienste e.V., 2.-4. Mai 1997 in Strausberg

die alleinige Verantwortung für die strategische Aufklärung zugeschrieben worden, die Bundeswehr musste sich auf den operativen und taktischen Bereich beschränken.
Am 23. September 1993 kam es zu einer erneuten Vereinbarung, diesmal unter offizieller Beteiligung des Bundeskanzleramtes. Danach erhielt der BND das ausschließliche Recht zum Informationsaustausch mit den Partnerdiensten.

Partnerdienstbeziehungen mit den USA
Combined Group Germany

Als eine Kombination zwischen den Erfordernissen des UKUSA-Vertrages für "Third Parties" und der Tätigkeit des Verbindungsstabes der CIA zum BND operierte in der „McGraw-Kaserne“ in München über Jahre hin eine spezielle Verbindungsgruppe unter der Bezeichnung "Combined Group Germany - CGG". Dort waren Vertreter der amerikanischen und britischen Partnerdienste des BND auf dem Gebiet der Fernmelde/Elektronischen Aufklärung tätig (5). Die CGG residierte ursprünglich in einer Villa in München-Krailling, und nahm später im obersten Stockwerk des Stabsgebäudes der „McGraw-Kaserne“ in München eine ganze Etage in Anspruch.
Über diese Gruppe erfolgte der ständige Informationsaustausch zwischen dem BND und den Geheimdiensten der USA/Großbritanniens auf dem Gebiet der Fernmelde/Elektronischen Aufklärung. Die CGG war mit Standleitungen für Datenverbindungen mit der BND-Zentrale in Pullach verbunden und unterhielt entsprechende Kommunikationskanäle mit den Zentralen der NSA und des britischen Geheimdienstes GCHQ.
In den 80er Jahren wurde die CGG in den Komplex der NSA-Field Station Augsburg verlegt. Ihr Pendant auf Seiten des BND erhielt die nicht sonderlich originelle Tarnbezeichnung: "Bundeswehr-Austauschgruppe".

---

5 Langjähriger Leiter der CGG war der Deutsch-Amerikaner Mr. Keller. Dieser Mr. Keller war nach Kriegsende für kurze Zeit der erste Bürgermeister der Stadt Bad Neuenahr-Ahrweiler.

Drehpunkt-Vertrag

Im Frühsommer 1973 richtete der BND eine Anfrage an den CIA-Residenten in München, Arthur Stimson. Der BND äußerte den Wunsch, in der Field-Station Augsburg-Gablingen der NSA mehr als 70 Empfangsplätze und mehrere Peilplätze mitnutzen zu können. Die Field-Station hatte im BND den Decknamen DREHPUNKT. Im Februar 1974 erfolgte im Hauptquartier der NSA die feierliche Unterzeichnung des sogen. Drehpunkt-Vertrages. Der Vertrag beinhaltete mehrere Bauvorhaben der „Fernmeldestelle Süd“ der Bundeswehr und des BND im Objekt.
Da es vor allem um die „Mitnutzung“ der US-amerikanischen Anlagen zur Erfassung und Auswertung ging, wurden die Anforderungen der deutschen Seite sehr häufig am Ende einer langen Warteschlange geparkt.

Field Station Bad Aibling

In Mietraching bei Bad Aibling, südlich von München, war bis vor wenigen Jahren eines der größten europäischen Zentren des SIGINT-Systems der NSA - das Regional SIGINT Operation Center – RSOC oder auch Field Station F-81, angesiedelt. Das Gelände eines früheren faschistischen Fliegerhorstes war seit 1952 unter amerikanischer Nutzung.
1988 baute der BND in der wenige hundert Meter entfernten Mangfall-Kaserne eine als „Fernmeldeweitverkehrsstelle der Bundeswehr“ getarnte SIGINT-Station (BND-interner Deckname: Objekt „SEELAND“) auf.
Diese dient neben der Realisierung eigener SIGINT-Aufgaben (z.B. der Satellitenaufklärung) dem ständigen Informationsaustausch mit der US-Station bis zu deren endgültiger Auflösung.
Ab 2004 erfolgte der Rückbau der SIGINT-Anlagen der Field Station und ihre Verlagerung – teilweise in die größte europäische Anlage im britischen Menwith Hill und vor allem in das neue NSA-Abhörzentrum bei Wiesbaden (mit Zwischenstation in Griesheim bei Darmstadt). Der Personalbestand betrug zwischen 750 und 1000 Mitarbeitern.

Der ständige Einsatz modernster Technik und der verstärkte Ausbau der größten SIGINT-Station in Europa im britischen Menwith Hill ermöglichten den Rückbau der Anlagen in Bad Aibling. Von Menwith Hill aus werden alle deutschen Fernmeldeverbindungen überwacht und ausgewertet.
Bestandteil der Field Station in Bad Aibling war u. a. das im Jahr 2001 eingerichtete automatische Dokument-Auswertungssystem DOCEX (Document Exploitation System), womit Texte aus Dokumenten und anderen Medien in 31 verschiedenen Sprachen übersetzt und ausgewertet werden können.

Aufschlussreich, aber auch etwas makaber, mutet unter diesen Bedingungen die Antwort der Bundesregierung vom 25. 04. 2000 (BT-DS 14/3224) auf eine Kleine Anfrage der FDP bezüglich Echelon und der US-Station in Bad Aibling an:

Frage 5: Sieht die Bundesregierung eine Verletzung von Souveränitätsrechten, zumal Abhörgeräte auch von Deutschland aus betrieben werden?

„Mit dieser Frage ist offenbar die amerikanische Station Bad Aibling angesprochen. Diese Station wird zur Erfassung militärischer Hochfrequenz- und Satellitenverkehre betrieben, die für die außen- und sicherheitspolitische Lage der Vereinigten Staaten von Amerika sowie ihrer europäischen Partner von Relevanz sind. Die dabei gewonnen Erkenntnisse werden im Übrigen auch dem Bundesnachrichtendienst zu Verfügung gestellt. Die von Bad Aibling ausgehende Aufklärung ist demnach grundsätzlich nicht auf private Telekommunikationsverkehre ausgerichtet. Die Arbeit der Station erfolgt auf der Grundlage des NATO-Truppenstatuts. Darin ist berücksichtigt, dass ein missbräuchliches Vorgehen gegen die Bundesrepublik Deutschland nicht stattfindet. Ein solcher Einsatz wäre daher unzulässig. Von amerikanischer Seite ist mehrfach versichert worden, dass von Bad Aibling keine gegen die Interessen der BRD gerichteten Aktivitäten ausgehen. Die Bundesregierung hat keinen Anlass, an diesen Versicherungen zu zweifeln.“

Consolidated Intelligence Center – CIC bei Wiesbaden

In den letzten Jahren kam es mehrfach zu Veränderungen in der Struktur und den Standorten des Geheimdienstes der US-Landstreitkräfte (Intelligence and Security Command – INSCOM)

im Einsatzraum Europa. INSCOM wurde per 1.1.1977 aus dem Zusammenschluss der bisherigen Strukturen der Militäraufklärung, der elektronischen Spionage und der Spionageabwehr in den Landstreitkräften der USA gebildet.
1999 konzentrierte der Geheimdienst INSCOM rund 50 Einheiten und Dienststellen im Raum Griesheim bei Darmstadt (im sogen. Dagger Complex). Mit einem Aufwand von 18 Millionen US-Dollar wurde dort das deutsche Hauptquartier von INSCOM aufgebaut.
Auf den benachbarten August-Euler-Flugplatz verlegte INSCOM im Jahr 2003 unter der Projektbezeichnung „ICEBOX" Antennenanlagen aus Bad Aibling. Die Anlagen wurden zwischen 2006 und 2008 von Wiesbaden aus fernbedient betrieben und anschließend wieder zurückgebaut.
Gegenwärtig soll dort noch das „European Cryptologic Center" mit rund 1.100 Mitarbeitern tätig sein.
Im Augenblick bereitet INSCOM eine erneute Verlegung vor. Im Bereich des Europa-Hauptquartiers der US-Landstreitkräfte (US-Army Europe – USAREUR) in der Lucius D. Clay-Kaserne in Wiesbaden-Erbenheim baut INSCOM bis 2015 für 124 Millionen Euro ein sogenanntes „Consolidated Intelligence Center - CIC" auf.
Nach den bisher bekannten Dimensionen entsteht hier ein neues Abhörzentrum für Europa, ausgerüstet mit den modernsten Anlagen für die Erfassung von elektronischen Abstrahlungen aller Art und entsprechenden Kommunikationsanlagen.
Vordergründig soll das Consolidated Intelligence Center Aufklärungsdaten für die Einsätze der dem Europakommando der US-Army unterstellten Einheiten beschaffen und auswerten – das betrifft Spionageinformationen aus über 50 Ländern – von Russland bis Israel.
Die Bundesregierung ist über dieses Projekt ausreichend informiert, wie der BND-Präsident in einer Sondersitzung des Innenausschusses des Bundestages im Juli 2013 bestätigte. Im CIC wird die jahrzehntelange enge Zusammenarbeit der deutschen und amerikanischen Geheimdienste fortgesetzt.

Partnerdienstbeziehungen

Es gab aber auch viele Anzeichen, dass diese Partnerdienstbeziehungen für den BND oft zur Einbahnstraße wurden. Das führte

wiederum zu typischen geheimdienstlichen Reaktionen. In mehreren hochrangigen Delegationsgesprächen hatte z.B. der BND immer wieder gefordert, direkt an dem Informationsaufkommen der US-Geheimdienste aus ihren Stationen in Westberlin, speziell zur DDR, im direkten Zugriff zu den Rohinformationen beteiligt zu werden. Freundlich, aber bestimmt, lehnten die Amerikaner immer wieder ab und bestanden darauf, dem BND nur ausgewählte und aufbereitete Informationen zu übergeben. Daraufhin hatte sich die Leitung des BND entschieden, ein eigenes, streng geheimes Aufklärungsobjekt mit Hilfe des französischen Geheimdienstes im Bereich der französischen Garnison "Cité Fochè" in Berlin-Reinickendorf zu errichten. Die strengste Geheimhaltung galt in erster Linie gegenüber dem amerikanischen Partner, der es nicht gern sah, wenn seine "Juniorpartner" eigene Wege gingen.

Und der BND war nicht zimperlich bei der Suche nach eigenen Wegen.
Seit 1975 nutzte der BND in Zusammenarbeit mit dem spanischen Geheimdienst „Oberste Zentrale für Verteidigungsinformationen – CESID“ ein Objekt im Ort Conil de la Frontera an der spanischen Mittelmeerküste zur elektronischen Spionage.
In diesem Ort ist der Knotenpunkt mehrerer transatlantischer Unterseekabel, die Europa mit Afrika und dem amerikanischen Kontinent verbinden. Gleichzeitig unterhält dort die spanischen Gesellschaft Telefónica eine Satelliten-Bodenstation.
Der Standort Conil war zugleich als ein Ausweichquartier des BND im Spannungs- bzw. Kriegsfall vorgesehen. Jedoch bestand die Hauptfunktion der Station „Eismeer“ – so die Tarnbezeichnung im BND - in einer massenhaften illegalen Erfassung von Informationen, die über die transatlantischen Unterseekabel hin und zurück geflossen sind.
Delikaterweise hatte das Projekt im BND die Deckbezeichnung „Delikatesse“. Offiziell hat der BND die Verfügung über das Objekt 1992 an den spanischen Geheimdienst übergeben, dürfte sich aber die Nutzungsrechte am weiteren Informationsaufkommen nachhaltig gesichert haben. In den fast zwanzig Jahren der direkten Nutzung der Station „Eismeer“ durch den BND werden Milliarden von Daten über die europäischen und atlantischen Kommunikations-

partner und über den Inhalt ihrer Informationen beim BND gespeichert worden sein.
Übrigens war und ist die Iberische Halbinsel in mehrfacher Hinsicht ein begehrter Ausgangspunkt für weltweite Spionageaktivitäten. Seit 1953 besteht ein spanisch-amerikanisches Abkommen, das den USA die Errichtung eigener Stützpunkte auf dem Territorium Spaniens gestattet. In der US-amerikanischen Luftwaffenbasis Rota bei Cadiz unterhält der Spionagedienst der US-Marine seit 1960 einen eigenen Stützpunkt mit einer Antennenanlage, die funkelektronische Abstrahlungen im Umkreis von 5.000 km erfasst. Eine weitere US-Anlage arbeitet in Moron de la Frontera.
Die Geheimdienste Großbritanniens nutzen ihre Zugangsrechte in Gibraltar für Aktivitäten von zwei Geheimdienst-Stationen an den Endpunkten der Straße von Gibraltar.

Das Projekt ECHELON

Bereits 1998 entstand im Auftrag des Ausschusses für Bürgerrechte des Europaparlaments ein erster Bericht über ECHELON. Darin wurde es als weltweites Spionagesystem im Dienste der amerikanischen NSA vorgestellt, mit dem alle über Satelliten laufenden Telefongespräche, Faxe und E-Mails aufgefangen und ausgewertet werden können. Obwohl der damalige EU-Kommissar für Telekommunikation, Martin Bangemann, sagte, wenn es so etwas gäbe, wäre es „ein Skandal“ (6) erregte dieser Bericht kaum Aufsehen. Einige Zeit später erschien dann einer weitere Studie des Amtes zur Bewertung von Technologiefolgen bei der EU (STOA-Scientific and Technological Options Assessment) aus der Feder des britischen Sicherheitsexperten Duncan Cambell. Er konzentrierte die Aussagen zu Echelon insbesondere auf die Funktion in der Wirtschaftsspionage - und nun ging es an und um das Geld, und die Politik und die Medien reagierten.

Weitgehend verschwiegen wird in der Diskussion, dass Echelon ein Spionagesystem der NATO-Staaten unter strenger Führung durch die USA darstellt. Die beteiligten NATO-Partner werden von den USA relativ willkürlich und unter Beachtung ihres Nutzens für die

6 Vgl. SZ vom 6.7.2000; „Die Big-Brother-Hotline“

USA und ihrer „Zuverlässigkeit“ an den Ergebnissen der weltumspannenden elektronischen Spionage beteiligt.

Das System ECHELON erfasst Informationen auf mehreren Ebenen:
Es werden die internationalen und regionalen Telekommunikationssatelliten (z.B. INTELSAT) angezapft.
Dann stehen die Überseekabel unter Kontrolle, entweder durch Knoten an ihren landseitigen Schnittstellen oder durch elektronische Erfassungssysteme direkt an den Kabeln.
Alle Richtfunkstrecken, über die immer mehr Fernmeldeverkehre abgewickelt werden, werden überwacht.
Hochleistungsfähige Antennen- und Peilsysteme erfassen weiterhin die Funkverkehre, insbesondere Funk-Fernverbindungen.

SIGNIT-Aktivitäten waren ursprünglich mit Schwerpunkt auf die militärischen Aufklärungserfordernisse ausgerichtet (Beiträge zur Aufklärung der Stärken und Gliederungen der Streitkräfte, zum Einsatz neuer Waffensysteme etc.) und hatten als zweiten Schwerpunkt die verschlüsselten diplomatischen Funkverkehre.
Später verschoben sich die Prioritäten deutlich in Richtung der politischen und wissenschaftlich-technischen Aufklärung.
Mit Beginn der Entspannungsprozesse, insbesondere der Abrüstungsverhandlungen, der vertrauensbildenden Maßnahmen, erhielt SIGNIT eine Doppelfunktion: es blieb zum einen aktive Spionage, wurde aber auch zu einem unverzichtbaren Bestandteil der gegenseitigen Vertrauensbildung durch die Möglichkeiten der Verifizierung der Abrüstungsvereinbarungen.

Die politische Aufklärung richtet sich u. a. auch und nicht zuletzt gegen die politische Opposition oder andere politisch missliebige Personen oder Organisationen. So konnten sich vor einiger Zeit die Engländer darüber aufregen, dass ihre Prinzessin Diana ebenfalls Objekt der Echelon-Überwachung war und in den Speichern der NSA erfasst wurde. Das geschah vor dem Hintergrund der Überwachung solcher Organisationen wie Amnesty International, Christian Aid oder Greenpeace. Nach Aussagen des ehemaligen Mitar-

beiters der NSA, Wayne Madsen, wird „jeder, der politisch aktiv ist, früher oder später von Radarschirm der NSA erfasst werden.“ (7)

Nun stehen dem geheimdienstlichen Einsatz gegen die politische Opposition in einigen Staaten rechtliche Regelungen entgegen, die solche Aktivitäten verbieten oder bestimmten Einschränkungen unterwerfen. Gehen wir einmal positiv davon aus, dass die Geheimdienste ihr innerstaatliches Recht achten und angeblich auch einhalten. Dann bietet ihnen der Datenverbund in ECHOLON immer noch die Möglichkeit, dieses Recht scheinbar legal zu brechen. Dann erfassen die Stationen in Kanada Daten über USA-Bürger, die Amerikaner in Bad Aibling hören Gespräche britischer Bürger ab etc. – und im Informationsaustausch landen diese Daten dort, wo sie gebraucht werden.

Das erinnert sehr klar an die aktuellen Diskussionen in der deutschen Politik, die auf die strikte Einhaltung der deutschen Datenschutzrichtlinien bei den Aufklärungsoperationen der USA pochen.

Die öffentliche Diskussion war aufgrund des STOA-Berichts sehr stark auf das Problem der Wirtschaftsspionage focusiert. Man nutzt dazu auch gern Beispiele, wo Konkurrenten sich mit Hilfe der Geheimdienste gegenseitig lukrative Aufträge abgejagt haben.
Dazu ist anzumerken, dass die Orientierung auf die Geheimnisse von Firmen und Konzernen sehr eng ist. Wirtschaftsspionage umfasst auch die Überwachung finanzieller Transaktionen (nicht nur zur Bekämpfung der Geldwäsche!), die Erfassung wissenschaftlich-technischer Entwicklungen, die Lage auf den Rohstoffmärkten (auch Wasser und Getreide) und die Entwicklung der Ressourcen weltweit. Aber Wirtschaftsspionage ist nicht erst durch ECHELON zum Problem geworden. Bereits 1994 haben Erich Schmidt-Eenboom und Jo Angerer in „Die schmutzigen Geschäfte der Wirtschaftsspionage“ dazu umfangreiche Rechercheergebnisse veröffentlicht. 1999 hat Udo Ulfkotte mit „Marktplatz der Diebe“ die deutsche Wirtschaft als Opfer der internationalen Wirtschaftsspionage beschrieben, ohne die deutschen Täter zu benennen.

---

7 Vgl. Sunday Times v. 27.2.00; zitiert in jw. 4./5. März 2000: Rainer Rupp: Echelon – ein riesiger Staubsauger im Äther

Gravierender erscheinen jedoch die immens gewachsenen Möglichkeiten und Gefahren, dass Privatpersonen in den Strudel dieser Überwachung gezogen werden – und sie bleiben mit all ihren Querverbindungen und persönlichen Eigenheiten (man sollte nur an die Möglichkeiten denken, die die Auswertung diverser Chipspeicher über Reisetätigkeit, Gesundheitszustand, Bankkonten, Kaufverhalten, Interessen und Neigungen durch Internet-Zugänge etc. bieten!) in den Speichern der Geheimdienste. Hintergrund dieser Gefahren sind die verschwommenen Regelungen, die den Geheimdiensten Befugnisse zur Aufklärung der sogen. Organisierten Kriminalität erteilen. Die sehr willkürlich gefassten Definitionen der OK gehen meist weiter als die öffentlich genannten, wie Drogenhandel, Geldwäsche, Waffenhandel oder Terrorismus und bedienen damit die Speicherwut der Geheimdienste.

Zu den vielen Vorschlägen, wie einem solchen Überwachungs-System zu begegnen sei, gehört auch, mehr Verschlüsselungs-Technologien einzusetzen, die Telekommunikation also abhörsicher zu machen. Dazu ist anzumerken, dass in den USA seit den 80er Jahren die technischen und rechtlichen Möglichkeiten geschaffen werden (erinnert sei nur an die sogen. Clipper-Chip-Debatte), um durch einen intern eingebauten „Zugangsschlüssel“ die Verschlüsselungs-Software für den Inhaber dieses Schlüssels – und das ist die NSA – zugänglich zu machen. Die großen Software-Anbieter wie Microsoft, Lotus oder Netscape haben sich den Forderungen der NSA gebeugt. Wenn kleinere Software-Entwickler nicht spuren, werden sie vom Markt gedrängt.
Das 1995 verabschiedete EU-Memorandum über „ die rechtmäßige Überwachung des Fernmeldeverkehrs“ verlangt von jedem Kommunikationsanbieter die feste Einrichtung einer Abhör-Schnittstelle, die nach dieser Regelung natürlich nur für gesetzlich vorgesehene Abhörmaßnahmen Gültigkeit haben soll.

Aber: Nichts ist unmöglich!

Ausgewählte Literaturangaben zum Komplex SIGINT

James Bamford
NSA
Die Anatomie des mächtigsten Geheimdienstes der Welt
Goldmann Verlag, 2001

Jeffrey Richelson
The U.S. Intelligence Community
Harper Business, 1989

Bob Woodward
Geheimcode Veil
Reagan und die geheimen Kriege der CIA
DroemerKnaur, 1987

Erich Schmidt-Eenboom
Schnüffler ohne Nase
Der BND – die unheimliche Macht im Staate
Econ-Verlag, 1993

Erich Schmidt-Eenboom
Artikel:
Empfänglich für Geheimes – Die (west)deutschen Nachrichtendienste im Äther (Internet)

Klaus Eichner/Andreas Dobbert
Headquarters Germany
edition ost, 1997

Josef Foschepoth
Überwachtes Deutschland
Post- und Telefonüberwachung in der alten Bundesrepublik
Vandenhoeck & Ruprecht, 2013

Internet
www.intelligence-history.org
www.geheim-magazin.de
www.NSARCHIVE.wordpress.com
Netzpolitik.org
Wikipedia – Dagger Complex
Die Raven-Homepage
Luftpost - Friedenspolitische Mitteilungen aus der US-Militärregion Kaiserslautern/Ramstein

V. i. S. d. P. – Arbeitskreis Frieden der GBM, Helga Hörning