EUROPA-PARLAMENTET

1999 *2004*

Det Midlertidige Udvalg om Echelon-Aflytningssystemet

FORELØBIG

18. maj 2001

UDKAST TIL BERETNING

om eksistensen af et globalt system til aflytning af privat og økonomisk kommunikation (Echelon-aflytningssystemet)

Det Midlertidige Udvalg om Echelon-Aflytningssystemet

Ordfører: Gerhard Schmid

DA

INDHOLD

Side

PROTOKOLSIDE

På mødet den 5. juli 2001 vedtog Europa-Parlamentet at nedsætte af Det Midlertidige Udvalg om Echelon-Aflytningssystemet. Med henblik på opfyldelse af dette mandat valgte det midlertidige udvalg på det konstituerende møde den 5. juli 2000 Gerhard Schmid til ordfører.

På mødet/møder den ... behandlede udvalget udkastet til betænkning.

På dette/sidstnævnte møde vedtog det forslaget til beslutning (for: ...; imod: ...; hverken/eller: ...)/vedtog det enstemmigt forslaget til beslutning.

Til stede under afstemningen var: ... (formand/mødeformand), ... (næstformand), ... (næstformand), ... (ordfører), ..., ... (for ...), ... (for ..., jf. forretningsordenens artikel 153, stk. 2), ... og ... .

Betænkningen indgivet den ....

Fristen for ændringsforslag til denne betænkning vil fremgå af forslaget til dagsorden for den mødeperiode, hvor den skal behandles/er fastsat til den ...kl. .....

FORSLAG TIL BESLUTNING

Europa-Parlamentets beslutning om eksistensen af et globalt system til aflytning af privat og økonomisk kommunikation (Echelon-aflytningssystemet)

Europa-Parlamentet,

– der henviser til Europa-Parlamentets afgørelse af 5. juli 2000 om nedsættelse af et midlertidigt udvalg om Echelon-aflytningssystemet og om dettes mandat,

– der henviser til EF-traktaten, der tilsigter etablering af et fælles marked med en høj grad af konkurrenceevne,

– der henviser til traktaten om Den Europæiske Union, navnlig dennes art. 6, stk. 2, der fastlægger EU's forpligtelse til at respektere menneskerettighederne, og afsnit V, bestemmelserne om en fælles udenrigs- og sikkerhedspolitik,

– der henviser til Den Europæiske Unions charter om grundlæggende rettigheder, hvis artikel 7 beskytter privat- og familielivet og udtrykkeligt præciserer respekten for kommunikation,

– der henviser til den europæiske menneskerettighedskonvention, navnlig dennes artikel 8, der beskytter privatsfæren, og de talrige andre internationale traktater, der sikrer beskyttelse af privatsfæren,

– der henviser til beretning fra Det Midlertidige Udvalg om Echelon-Aflytningssystemet om eksistensen af et globalt system til aflytning af privat og økonomisk kommunikation (Echelon-aflytningssystemet) (A5-0000/2001),

Eksistensen af et globalt system til aflytning af privat og økonomisk kommunikation (Echelon-aflytningssystemet)

A. der henviser til, at der ikke længere kan være tvivl om, at der eksisterer et verdensomspændende kommunikationsaflytningssystem, som fungerer gennem et samarbejde mellem USA, Det Forenede Kongerige, Canada, Australien og New Zealand inden for rammerne af UKUSA-aftalen og til, at det på grundlag af de foreliggende indicier forekommer sandsynligt, at systemets dæknavn faktisk er "Echelon", hvilket ganske vist er af sekundær betydning,

B. der henviser til, at systemet ikke benyttes til aflytning af militær kommunikation, men til aflytning af privat og erhvervsmæssig kommunikation, idet undersøgelsen dog har vist, at systemets langt fra kan have den kapacitet, medierne til dels antager,

Aflytningssystemets grænser

C. der henviser til, at aflytningssystemet er baseret på verdensomspændende aflytning af satellitkommunikation, at kommunikationen i områder med en stor kommunikationsintensitet kun i ringe grad transmitteres via satellitter og at størstedelen af kommunikationen dermed ikke kan aflyttes fra jordbaserede anlæg, men kun ved aflytning af kabel- og radiokommunikation, hvilket, - som undersøgelserne i denne beretning har

vist - kun er muligt inden for snævre grænser; der tillige henviser til, at personaleressourcerne til den endelige analyse af opfanget kommunikation medfører yderligere begrænsninger, og til, at Echelon-staterne derfor kun har adgang til en meget begrænset del af den kabel- og radiobaserede kommunikation, og kun kan analysere en begrænset del af kommunikationen,

Den mulige eksistens af andre aflytningssystemer

D. der henviser til, at aflytning af kommunikation er en almindelig anvendt spionageform blandt efterretningstjenester, og at et sådant system også vil kunne drives af andre stater, hvis disse råder over de nødvendige finansielle midler og har de geografiske forudsætninger herfor; der tillige henviser til, at Frankrig - i det mindste hvad angår de geografiske forudsætninger - på grund af sine oversøiske territorier som eneste EU-medlemsstat vil være i stand til alene at oprette et globalt aflytningssystem, og til at der derudover er indikationer på, at også Rusland kan drive et sådant system,

Forenelighed med EU-retten

E. der henviser til, at der, for så vidt angår foreneligheden af et system som Echelon med gældende EU-ret, må sondres mellem to aspekter: anvendes systemet kun til efterretningsformål, strider det ikke mod EU-retten, da statssikkerhedstjenesters aktiviteter ikke er omfattet af EF-traktaten, men henhører under EU-traktatens afsnit V (FUSP), idet der dog her endnu ikke findes relevante bestemmelser og dermed ingen berøringspunkter; henviser til, at systemet, hvis det derimod anvendes til konkurrencespionage, er i strid med medlemsstaternes pligt til loyalt samarbejde og tanken om et fælles marked med fri konkurrence, således at en medlemsstat, der deltager heri, bryder EU-retten,

Forenelighed med den grundlæggende ret til beskyttelse af privatsfæren (artikel 8 i den europæiske menneskerettighedskonvention)

F. der henviser til, at enhver aflytning af kommunikation er et alvorligt indgreb i den enkeltes privatsfære, og at menneskerettighedskonventionens artikel 8, der beskytter privatsfæren, kun tillader indgreb med henblik på beskyttelse af den nationale sikkerhed, og kun i det omfang, der fastlagt bestemmelser herom i national ret og disse bestemmelser er almindeligt tilgængelige og fastlægger, under hvilke omstændigheder og på hvilke betingelser myndighederne må foretage sådanne indgreb; der desuden henviser til, at indgrebene skal overholde proportionalitetsprincippet, at der derfor skal foretages en interesseafvejning, og at det ifølge Den Europæiske Menneskerettighedsdomstols praksis ikke er tilstrækkeligt, at indgreb blot er "hensigtsmæssige" eller "ønskværdige",

G. der henviser til, at et efterretningssystem, som aflytter enhver form for kommunikation uden at sikre overholdelse af proportionalitetsprincippet, ikke er foreneligt med den europæiske menneskerettighedskonvention (EMK), og at der ligeledes foreligger en krænkelse af EMK, hvis de bestemmelser, som kommunikationsovervågningen er baseret på, savner retsgrundlag, ikke er alment tilgængelige eller er formuleret på en sådan måde, at konsekvenserne for den enkelte ikke er overskuelige; der tillige henviser til, at de bestemmelser, som danner grundlag for den amerikanske efterretningstjenestes virke i udlandet, for det meste er fortrolige, og at det dermed kan sættes spørgsmålstegn ved, om proportionalitetsprincippet overholdes, hvormed der i så fald sandsynligvis er tale om en krænkelse af de af Menneskerettighedsdomstolens fastlagte principper om tilgængelighed til retsakterne og forudsigelighed af disses virkninger,

H. der henviser til, at medlemsstaterne ikke kan unddrage sig deres forpligtelser i henhold til EMK ved at lade andre landes sikkerhedstjenester, som er underlagt mindre strenge bestemmelser, arbejde på deres territorium, da legalitetsprincippet og dettes to elementer - tilgængelighed og forudsigelighed - i så fald vil blive gjort virkningsløse og Menneskerettighedsdomstolens retspraksis vil blive indholdsmæssigt udhulet,

I. der henviser til, at efterretningstjenesters ved lov legitimerede virksomhed kun er i overensstemmelse med de grundlæggende rettigheder, hvis der desuden findes et fyldestgørende kontrolsystem, som kan udligne faren ved, at en del af forvaltningen benytter sig af hemmelige aktiviteter; der henviser til, at Den Europæiske Menneskerettighedsdomstol udtrykkeligt har fremhævet betydningen af et effektivt kontrolsystem på efterretningsområdet, og at det derfor forekommer betænkeligt, at nogle medlemsstater ikke har et selvstændigt parlamentarisk kontrolorgan for efterretningstjenster,

Er EU-borgerne beskyttet tilstrækkeligt mod efterretningsvirksomhed?

J. der henviser til, at EU-borgernes beskyttelse afhænger af anvendelsen af gældende ret i de enkelte medlemsstater, at der er store forskelle på dette punkt, at nogle end ikke råder over parlamentariske kontrolorganer, og at der derfor næppe kan tales om tilstrækkelig beskyttelse; der desuden henviser til, at EU-borgerne har en grundlæggende interesse i, at deres nationale parlamenter har et formelt struktureret kontroludvalg, der overvåger og kontrollerer efterretningstjenesternes aktiviteter; der henviser til, at disse selv dér, hvor der findes kontrolorganer, i høj grad fristes til snarere at beskæftige sig med indenrigsefterretningstjenesternes virke end med udenrigsefterretningstjenesternes, da landets egne borgere som regel kun berøres af førstnævntes aktiviteter,

K. der henviser til, at institutionerne i forbindelse med et samarbejde mellem efterretningstjenester inden for rammerne af FUSP må vedtage bestemmelser, der beskytter EU-borgerne i tilstrækkelig grad,

Økonomisk spionage

L. der henviser til, at det er en del af udenrigsefterretningstjenesternes opgave at interessere sig for økonomiske data, herunder udviklingen inden for forskellige brancher, udviklingen på råstofmarkederne, overholdelse af økonomiske embargoer, regler for salg af varer med dobbelt anvendelse (dual use) m.m., og at der derfor ofte foretages overvågning af de virksomheder, der berøres heraf,

M. der mener, at det under ingen omstændigheder er acceptabelt, at efterretningstjenester lader sig anvende til konkurrencespionage ved at udspionere udenlandske virksomheder for at skaffe nationale virksomheder en konkurrencefordel, men at der ikke er belæg for, at det globale aflytningssystem har været anvendt hertil, selv om dette ofte er blevet hævdet,

N. der henviser til, at følsomme virksomhedsoplysninger ofte findes i selve virksomheden, og at konkurrencespionage derfor først og fremmest sker ved at der gøres forsøg på at få oplysninger via medarbejdere eller indslusede personer eller ved at trænge ind i interne edb-net; der henviser til, at kommunikationsovervågningssystemer kun kan anvendes til konkurrencespionage, når følsomme data kommer ud via kabelkommunikation eller trådløs kommunikation (satellit), og at dette kun sker systematisk i følgende tre tilfælde:

- i forbindelse med virksomheder, der arbejder inden for tre tidszoner, således at foreløbige resultater kan sendes fra Europa til Amerika og videre til Asien;
- i forbindelse med multinationale selskabers videokonferencer via V-Sat eller kabel;
- når der forhandles om vigtige kontrakter på stedet (f.eks. i bygge- og anlægssektoren, opbygning af telekommunikationsinfrastruktur, nyoprettelse af transportsystemer osv.) og der derfra skal føres samråd med virksomheders hovedkontor,

Mulighederne for selv af beskytte sig

O. der henviser til, at virksomhederne kun kan opnå sikkerhed, hvis hele arbejdsmiljøet sikres og alle kommunikationsmidler, som anvendes til overførsel af følsomme oplysninger, beskyttes; der henviser til, at der findes tilstrækkeligt sikre krypteringssystemer til rimelige priser på det europæiske marked; der tillige henviser til, at også private indtrængende må rådes til at kryptere deres e-mails, da en ikke-krypteret e-mail kan sidestilles med et brev uden konvolut; der henviser til, at der på Internettet findes relativt brugervenlige systemer, som endog stilles gratis til rådighed til privat brug,

Samarbejde mellem efterretningstjenesterne i EU

P. der henviser til, at EU er nået til enighed om at koordinere efterretningstjenesternes indsamling af oplysninger inden for rammerne af udviklingen af en fælles sikkerheds- og forsvarspolitik, men samtidig om at fortsætte samarbejdet på dette område med andre partnere,

Q. der henviser til, at et samarbejde mellem efterretningstjenesterne inden for EU også forekommer ønskeligt, dels fordi det vil være ulogisk at tale om en fælles sikkerhedspolitik uden inddragelse af sikkerhedstjenesterne, og dels fordi dette vil indebære mange fordele af erhvervsmæssig, økonomisk og politisk art; der henviser til, at dette også vil også være mere i overensstemmelse med tanken om at være en ligeværdig partner over for USA og vil kunne samle alle medlemsstater om et system, som udformes fuldt i overensstemmelse med EMK; der henviser til, at passende kontrol af et sådant samarbejde fra Europa-Parlamentets side må tilsikres,

R. der henviser til, at Europa-Parlamentet er i færd med at udarbejde sine egne bestemmelser om tilgængeligheden af fortrolige og følsomme oplysninger og dokumenter,

Om indgåelse og ændring af internationale aftaler om beskyttelse af borgere og virksomheder

1. opfordrer Europarådets generalsekretær til at forelægge Ministerudvalget en undersøgelse af, om det vil være hensigtsmæssigt at tilpasse den i artikel 8 i EMK garanterede beskyttelse af privatsfæren til de moderne kommunikationsmetoder og aflytningsmuligheder enten i en tillægsprotokol eller sammen med reglerne om databeskyttelse inden for rammerne af en revision af databeskyttelseskonventionen, forudsat at derved hverken sker en reduktion af det retsbeskyttelsesniveau, Menneskerettighedsdomstolen har sikret eller af den fleksibilitet, der er nødvendig for tilpasning til videre udviklinger;

2. opfordrer medlemsstaterne til at skabe en europæisk platform til at vurdere de lovmæssige bestemmelser om sikring af brev- og telehemmeligheden, til at vedtage en fælles tekst herom, som sikrer beskyttelse af privatsfæren, som fastlagt i artikel 7 i Den Europæiske Unions charter om grundlæggende rettigheder, for alle EU-borgere på medlemsstaternes

territorium som helhed og desuden garanterer, at efterretningstjenesters virksomhed er i overensstemmelse med de grundlæggende rettigheder og opfylder betingelserne i beretningens kapitel 8, særlig i 8.3.4., der er baseret på artikel 8 i EMK;

3. opfordrer Europarådets medlemsstater til at vedtage en tillægsprotokol, som gør det muligt for De Europæiske Fællesskaber at tiltræde EMK, eller at overveje andre foranstaltninger, som kan udelukke konflikter i retspraksis mellem Menneskerettighedsdomstolen i Strasbourg og Domstolen i Luxemburg.

4. opfordrer FN's generalsekretær til at pålægge det kompetente udvalg at forelægge forslag om tilpasning af artikel 17 i den internationale konvention om borgerlige og politiske frihedsrettigheder, som sikrer beskyttelse af privatsfæren, til den nye teknologiske udvikling;

5. opfordrer USA til at underskrive tillægsprotokollen til den internationale konvention om borgerlige og politiske frihedsrettigheder, således at enkeltpersoner kan anlægge sag mod USA for krænkelse af konventionen; opfordrer de relevante amerikanske ngo'er, navnlig ACLU (American Civil Liberties Union) og EPIC (Electronic Privacy Information Center) til at lægge pres på den amerikanske regering for at opnå dette;

National lovgivning om beskyttelse af borgere og virksomheder

6. opfordrer medlemsstaterne til at vurdere deres nationale lovgivning om efterretningsvirksomhed for overensstemmelse med de grundlæggende rettigheder;

7. opfordrer medlemsstaterne til at tilstræbe et fælles beskyttelsesniveau over for efterretningsaktiviteter, som er baseret på det højeste nationale beskyttelsesniveau, da de borgere, der er berørt af en udenrigsefterretningstjenestes virke, som regel er statsborgerne i andre stater og dermed også i andre medlemsstater;

8. opfordrer EU-institutionerne til i forbindelse med et samarbejde mellem efterretningstjenesterne inden for rammerne af FUSP at vedtage tilstrækkelige beskyttelsesbestemmelser til fordel for EU-borgerne; mener, at Europa-Parlamentet som det oplagte kontrolorgan fra sin side må skabe de nødvendige forudsætninger for overvågning af dette yderst følsomme område, således at det er realistisk, men også forsvarligt, at kræve de fornødne kontrolbeføjelser;

Særlige foranstaltninger til bekæmpelse af økonomisk spionage

9. opfordrer medlemsstaterne til at overveje, i hvilken udstrækning økonomisk spionage og bestikkelse med henblik på at skaffe kontrakter kan bekæmpes gennem europæisk og international ret, navnlig om der inden for rammerne af WTO er mulighed for regulering, som tager højde for den konkurrenceforvridende virkning af sådanne fremgangsmåder ved at annullere sådanne kontrakter;

10. opfordrer medlemsstaterne til i en fælles entydig erklæring at forpligte sig til ikke at udøve økonomisk spionage mod hinanden og derved at bekræfte deres forpligtelser over for EF-traktatens ånd og bestemmelser;

Foranstaltninger vedrørende anvendelsen af gældende ret og kontrollen hermed

11. opfordrer de nationale parlamenter, som ikke råder over selvstændige parlamentariske kontrolorganer til overvågning af efterretningstjenester, til at oprette sådanne;

12. anmoder de nationale kontroludvalg for efterretningstjenesterne om under udøvelsen af de kontrolbeføjelser, der er tillagt dem, at lægge stor vægt på beskyttelse af privatsfæren, uanset om der er tale om overvågning af egne statsborgere, EU-statsborgere eller borgere fra tredjelande;

13. opfordrer Tyskland og England til at gøre de amerikanske efterretningstjenesters fortsatte tilladelse til aflytning af kommunikation på deres territorium betinget af, at denne sker i overensstemmelse med EMK, dvs., at proportionalitetsprincippet overholdes, at retsgrundlaget er tilgængeligt og konsekvenserne er forudsigelige for den enkelte, og at der gennemføres en effektiv kontrol, da de selv bærer ansvaret for, at efterretningsvirksomhed på deres territorium, hvad enten den er tilladt eller blot tålt, sker i overensstemmelse med menneskerettighederne;

Fremme af borgernes og virksomhedernes selvbeskyttelse

14. opfordrer Kommissionen og medlemsstaterne til at udarbejde programmer, som skærper borgernes og virksomhedernes bevidsthed for sikkerhedsproblematikken og samtidig at tilbyde praktisk hjælp til udarbejdelse og gennemførelse af omfattende beskyttelseskoncepter;

15. opfordrer Kommissionen og medlemsstaterne til at udarbejde hensigtsmæssige foranstaltninger til fremme, udvikling og fremstilling af europæisk krypteringsteknologi og -software og navnlig at støtte projekter, der sigter mod at udvikle brugervenligt krypteringssoftware med offentlig kildetekst;

16. opfordrer Kommissionen og medlemsstaterne til at fremme softwareprojekter, hvis kildetekst er offentlig (såkaldt "open source software"), da det kun derved kan sikres, at der ikke er indbygget "backdoors";

17. opfordrer EU-institutionerne og de offentlige forvaltninger i medlemsstaterne til systematisk at anvende kryptering af e-mails for derved på længere sigt at lade kryptering blive normen;

Andre foranstaltninger

18. opfordrer virksomhederne til at samarbejde mere intensivt med kontraspionageorganer, og især at gøre disse bekendt med særlige angreb udefra med henblik på økonomisk spionage for derved at øge disse organers effektivitet;

19. opfordrer Kommissionen til at forelægge et forslag om oprettelse af en europæisk rådgivningsinstans for informationssikkerhed i erhvervslivet, som ud over at skærpe bevidstheden om problemet også skal yde praktisk hjælp;

20. anser det for hensigtsmæssigt, at der afholdes en international kongres om beskyttelse af privatsfæren mod telekommunikationsovervågning, for derved at skabe et platform, hvor ngo'er fra Europa, USA og andre stater kan drøfte de grænseoverskridende og internationale aspekter og koordinere aktivitetsområder og fremgangsmåder;

21. pålægger sin formand at sende denne beslutning til Rådet, Kommissionen, medlemsstaternes regeringer og parlamenter samt til ansøgerlandene og Europarådet.

BEGRUNDELSE

1. Indledning

1.1. Nedsættelse af udvalget

Den 5. juli 2000 vedtog Europa-Parlamentet en afgørelse om at nedsætte et midlertidigt udvalg om Echelon-aflytningssystemet. Baggrunden herfor var debatten om en undersøgelse af det såkaldte Echelon-system[1], som STOA[2] havde bestilt, og som blev forelagt af undersøgelsens forfatter, Duncan Campbell, i anledning af en høring i Udvalget om Borgernes Friheder og Rettigheder, Retsvæsen og Indre Anliggender om Den Europæiske Union og databeskyttelse.

1.2. Påstandene i de to STOA-undersøgelser om et globalt aflytningssystem med dæknavnet Echelon

1.2.1. Den første STOA-rapport fra 1997

I en rapport med titlen "Vurdering af teknologier til politisk kontrol", som STOA[3] havde ladet Omega Foundation udarbejde for Europa-Parlamentet, blev også Echelon beskrevet i kapitlet om nationale og internationale netværk inden for kommunikationsovervågning. Undersøgelsens forfatter opstillede heri den påstand, at al kommunikation i Europa, der foregår via E-mail, telefon og telefax, rutinemæssigt aflyttes af NSA (National Security Agency, den amerikanske efterretningstjeneste).[4] Gennem denne rapport blev Echelon kendt i hele Europa som formodet altomfattende globalt aflytningssystem.

1.2.2. STOA-rapporterne fra 1999

For at erfare mere om dette spørgsmål bestilte STOA i 1999 en undersøgelse i fem dele, som omhandler "overvågningsteknologiens udvikling og risikoen for misbrug af økonomiske oplysninger". Del 2/5, der har Duncan Campbell som forfatter, vedrører efterretningstjenesternes eksisterende kapacitet og navnlig Echelon-systemets måde at fungere på.[5]

Særlig opsigt vakte rapportens påstand om, at Echelon havde fjernet sig fra sit oprindelige formål, nemlig forsvar mod Østblokken, og i dag blev anvendt til industrispionage. Denne tese blev i rapporten underbygget med eksempler på industrispionage, og især Airbus og Thomsom CFS skal have lidt skade som følge heraf.

---

[1] Teknikkens stade inden for kommunikationsefterretninger (Comint) i forbindelse med den automatiserede behandling i efterretningsøjemed af aflyttede faste eller fælles bredbåndsforbindelser på flere sprog og dens anvendelse på indhentning og udvælgelse af Comint, herunder talegenkendelse (oktober 1999), PE 168.184.
[2] STOA (Scientific and Technological Options Assessment: vurdering af videnskabelige og teknologiske projekter) er en tjenestegren i Europa-Parlamentets Generaldirektorat for Forskning, som lader udføre forskningsprojekter).
[3] Scientific and Technological Options Assessment: vurdering af videnskabelige og teknologiske projekter.
[4] Steve Wright, An appraisal of technologies for political control (1998), s. 20.
[5] Teknikkens stade inden for kommunikationsefterretninger (Comint) i forbindelse med den automatiserede behandling i efterretningsøjemed af aflyttede faste eller fælles bredbåndsforbindelser på flere sprog og dens anvendelse på indhentning og udvælgelse af Comint, herunder talegenkendelse (oktober 1999), PE 168.184.

STOA-undersøgelsen resulterede i, at Echelon blev drøftet i næsten alle medlemsstaternes parlamenter, og i Frankrig og Belgien blev der endog udarbejdet betænkninger herom.

1.3. Udvalgets mandat

Samtidig med afgørelsen om at nedsætte et midlertidigt udvalg vedtog Europa-Parlamentet udvalgets mandat. I medfør heraf har det midlertidige udvalg til opgave:

"- at efterprøve eksistensen af det system til opfangelse af kommunikation, der betegnes Echelon-systemet, og hvis aktiviteter er beskrevet i STOA-rapporten "Overvågningsteknologiens udvikling og risikoen for misbrug af økonomiske oplysninger",

- at efterprøve et sådant systems forenelighed med fællesskabsretten, navnlig EF-traktatens artikel 286 og direktiv 95/46/EF og 97/66/EF, samt med EU-traktatens artikel 6, stk. 2, på baggrund af følgende spørgsmål:

  - er EU-borgernes rettigheder beskyttet mod efterretningstjenesters virksomhed?

  - er kryptering en passende og tilstrækkelig beskyttelse til at sikre borgernes privatliv, eller bør der træffes yderligere foranstaltninger, og i bekræftende fald hvilke foranstaltninger?

  - hvordan kan EU-institutionerne få bedre kendskab til de risici, disse aktiviteter indebærer, og hvilke foranstaltninger kan der træffes?

- at efterprøve, om den globale opfangelse af kommunikation frembyder en fare for den europæiske industri,

- i givet fald at fremsætte forslag til politiske og lovgivningsmæssige initiativer".

1.4. Hvorfor ikke et undersøgelsesudvalg?

Europa-Parlamentet besluttede at nedsætte et midlertidigt udvalg, fordi et undersøgelsesudvalg kun har til opgave at undersøge påstande om krænkelse af fællesskabsretten (EF-traktatens artikel 193) og derfor logisk kun kan beskæftige sig med spørgsmål, der falder ind under denne ret. Spørgsmål, som er omhandlet i EU-traktatens afsnit V (FUSP) og VI (politisamarbejde og retligt samarbejde i kriminalsager) er udelukket. I henhold til den interinstitutionelle afgørelse[1] kan et undersøgelsesudvalg desuden kun gøre sine særlige beføjelser vedrørende indkaldelse af eksperter og aktindsigt gældende, når tavshedspligt eller hensyn til offentlig eller national sikkerhed ikke er til hinder derfor, hvilket i hvert fald udelukker fremmøde af efterretningstjenester. Et undersøgelsesudvalg kan heller ikke udvide sit arbejde til at omfatte tredjelande, fordi disse lande pr. definition ikke kan

[1] Europa-Parlamentets, Rådets og Kommissionens afgørelse af 19. april 1995 om de nærmere vilkår for udøvelse af Europa-Parlamentets undersøgelsesbeføjelse (95/167/EF, Euratom, EKSF), artikel 3, stk. 3-5.

overtræde fællesskabsretten. Var der blevet tale om et undersøgelsesudvalg, ville det således have været ensbetydende med en indholdsmæssig begrænsning uden yderligere rettigheder, hvorfor et flertal af Europa-Parlamentets medlemmer afviste at nedsætte et sådant udvalg.

1.5. Arbejdsmetode og arbejdsplan

For at kunne udføre sit mandat fuldt ud har udvalget valgt nedenstående fremgangsmåde. I et arbejdsdokument, som forelægges af ordføreren og vedtages af udvalget, behandles følgende emneområder: 1) Konkret viden om Echelon, 2) Drøftelser på nationalt parlaments- og regeringsplan, 3) efterretningstjenester og deres virksomhed, 4) Kommunikationssystemer og muligheden for at opfange dem, 5) Kryptering, 6) Industrispionage, 7) Spionagemål og beskyttelsesforanstaltninger og 8) Retlige rammebetingelser for beskyttelse af privatlivet. Emnerne behandles løbende i de enkelte møder, idet rækkefølgen fastsættes ud fra praktiske synspunkter og således ikke er udtryk for den betydning, som de enkelte emner tillægges. Som forberedelse til de enkelte møder gennemgår og vurderer ordføreren systematisk eksisterende materiale. Under hensyntagen til de behov, som opstår i forbindelse med de enkelte emner, indbydes derpå repræsentanter fra de nationale administrationer (navnlig fra efterretningstjenesterne) og parlamenter til møderne i deres funktion som organer til kontrol af efterretningstjenesterne samt juridiske eksperter og eksperter på områderne kommunikations- og aflytningsteknik, forretningssikkerhed og krypteringsteknik i teori og praksis. Også journalister, som har forsket i dette emne, høres. Generelt er møderne offentlige, men holdes af og til også for lukkede døre, dersom dette skønnes hensigtsmæssigt af hensyn til arbejdet med at finde frem til bestemt information. Derudover vil udvalgets formand og ordføreren sammen rejse til London og Paris for her at træffe personer, som af forskellige årsager ikke har kunnet deltage i udvalgsmøderne, men som det kunne være formålstjenligt at inddrage i udvalgets arbejdet. Af samme årsag vil udvalgets formandskab, koordinatorerne og ordføreren rejse til USA. Endelig har ordføreren ført en lang række, delvis fortrolige individuelle samtaler.

1.6. Echelon-systemets tilskrevne egenskaber

Echelon-aflytningssystemet adskiller sig fra andre aflytningssystemer som følge af den ganske særlige karakter, som to egenskaber giver systemet:

For det første tillægges det den egenskab, at det har kapacitet til at gennemføre en så at sige total overvågning. Det hævdes, at det først og fremmest ved hjælp af satellitmodtagestationer og spionsatellitter skulle være muligt at opfange enhver meddelelse, der sendes af en hvilken som helst person via telefon, telefax, Internet eller E-mail, så man på den måde kan få kendskab til dens indhold.

Den anden egenskab, man tillægger Echelon, er, at systemet fungerer over hele verden som et samspil mellem flere stater (Det Forenede Kongerige, USA, Canada, Australien og New Zealand). Det betyder en merværdi i forhold til nationale systemer, idet de stater, der deltager i systemet (Echelon-staterne), gensidigt kan stille aflytningsanlæg til rådighed for hinanden, dele omkostningerne ved systemet og i fællesskab udnytte den opnåede viden. Dette internationale samarbejde er netop nødvendigt, hvis man vil overvåge satellitkommunikation globalt, fordi det er den eneste måde, hvorpå man kan sikre, at man opfanger begge dele af en samtale ved international kommunikation. Det er indlysende, at satellitmodtagestationer på grund af deres størrelse ikke kan opføres på en stats territorium, uden at denne stat har givet

sit samtykke hertil. Der må nødvendigvis foreligge en aftale og et samspil mellem flere stater, der er fordelt over hele jordkloden, og som hver især yder deres bidrag.

Eventuelle farer ved et system som Echelon for private og erhvervslivet skyldes imidlertid ikke kun, at der er tale om et særdeles kraftigt overvågningssystem, men i endnu højere grad, at det agerer i et rum, hvor der stort set hersker retsløshed. Et system til aflytning af international kommunikation, er for det meste ikke møntet på statens egne borgere. Som udlændinge har de, der aflyttes, dermed ingen national retsbeskyttelse. Den enkelte er således fuldstændig hjælpeløs over for systemet. Også den parlamentariske kontrol er i dette tilfælde utilstrækkelig, da vælgerne regner med, at det ikke rammer dem, men "kun" personer i andre lande. Derfor interesserer det dem ikke i særlig grad, og de repræsentanter, de vælger, følger i første række deres vælgeres interesse. Det er således ikke så mærkeligt, at de høringer om NSA's virksomhed, der har fundet sted i den amerikanske Kongres, kun beskæftiger sig med spørgsmålet om, hvorvidt amerikanske borgere også er berørt af systemet. Det, at et sådant system findes, vækker i sig selv ikke særligt anstød. Så meget des vigtigere er det at forholde sig hertil på europæisk plan.

2. Efterretningstjenester og deres virksomhed

2.1. Indledning

Til varetagelse af landets sikkerhed har de fleste regeringer ud over politimyndigheder også oprettet efterretningstjenester. Deres virke er ofte hemmeligt, og de tjener til at

- skaffe oplysninger for at afværge trusler mod statens sikkerhed
- foretage kontraspionage generelt
- afværge farer, som kunne true de væbnede styrker
- skaffe oplysninger om forhold i udlandet.

2.2. Hvad er spionage

Regeringerne har brug for systematisk at indsamle og evaluere oplysninger om bestemte forhold i andre lande. Der er tale om grundlaget for afgørelser, der vedrører de væbnede styrker, udenrigspolitikken osv. De har derfor oprettet efterretningstjenester. Disse tjenester evaluerer i første omgang systematisk informationskilder, som er offentligt tilgængelige. Ordføreren har fået oplyst, at dette i gennemsnit udgør mindst 80% af efterretningstjenesternes virksomhed.[1] Særlig vigtige informationer på de nævnte områder hemmeligholdes imidlertid af regeringer og erhvervsvirksomheder og er derfor ikke offentligt tilgængelige. For at komme i besiddelse af disse informationer må man stjæle dem. Spionage er ikke andet end organiseret tyveri af informationer.

2.3. Spionagemål

De klassiske mål for spionage er militære hemmeligheder, andre statshemmeligheder eller informationer om regeringers stabilitet eller mangel på samme. Dette gælder f.eks. nye våbensystemer, militærstrategier eller oplysninger om stationering af tropper. Lige så vigtige er oplysninger om forestående udenrigspolitiske eller valutapolitiske afgørelser eller insiderinformation om interne spændinger i en regering. Desuden har informationer af økonomisk betydning interesse. Hertil kan ud over oplysninger vedrørende enkelte sektorer også høre detaljer om ny teknologi eller handelstransaktioner med udlandet.

2.4. Spionagemetoder

Spionage er at skaffe sig adgang til informationer, som indehaveren egentlig vil beskytte mod fremmedes adgang. Denne beskyttelse må altså overvindes og brydes. Dette er tilfældet både ved politisk spionage og ved industrispionage. Derfor er spionage inden for de to områder kendetegnet af de samme problemer, og derfor anvendes den samme spionageteknik inden for begge områder. Logisk er der ingen forskel, blot er beskyttelsesniveauet i erhvervslivet for det meste lavere, hvorfor industrispionage ofte er nemmere at udføre. Især er bevidstheden om risikoen ved anvendelse af ikke-aflytningssikret kommunikation mindre udpræget i erhvervslivet, end det er tilfældet inden for de områder, der vedrører statens sikkerhed.

[1] "The Commission on the Roles and Capabilities of the US Intelligence Community" fastslog i sin rapport med titlen "Preparing for the 21st Century: An Appraisal of U.S. Intelligence", at 95% af al "economic intelligence" stammer fra offentlige kilder (kapitel 2: "The role of intelligence").

2.4.1. Menneskets rolle i spionagen

Beskyttelsen af hemmelige informationer er altid tilrettelagt på samme måde:

- kun få kontrollerede personer har adgang til hemmelige informationer
- der eksisterer faste regler for behandling af disse informationer
- informationerne forlader normalt ikke det beskyttede område og kun, hvis de er sikret og kodet. Derfor sigter organiseret spionage først mod at opnå direkte adgang uden omvej til de ønskede informationer via **personer** (såkaldt human intelligence). I den forbindelse kan der være tale om
    - personer (agenter) fra egen efterretningstjeneste/virksomhed, som sluses ind i det beskyttede område
    - personer, som hverves i målområdet.

De hvervede personer arbejder for det meste af følgende grunde for fremmede tjenester/virksomheder:

- seksuel forførelse
- bestikkelse med penge eller ydelser, der har pengeværdi
- afpresning
- appel til ideologier
- tildeling af særlig betydning eller ære (appel til utilfredshed eller mindreværdsfølelser).

Et grænsetilfælde er ufrivilligt samarbejde, hvorved der "udfrittes" oplysninger: Ved angiveligt harmløse lejligheder (samtaler i tilslutning til konferencer, under faglige arrangementer eller ved hotelbarer) lokkes en myndigheds eller et firmas medarbejdere til at tale ved at appellere til deres forfængelighed osv.

Ved at anvende personer har man den fordel, at man opnår direkte adgang til den ønskede information. Der er imidlertid også ulemper forbundet hermed:

- kontraspionage koncentrerer sig altid om personer og ledende agenter
- ved hvervede personer kan de svagheder, som var udgangspunktet for hvervningen, vise sig som en boomerang
- mennesker begår uvilkårligt fejl og ender derfor på et eller andet tidspunkt i kontraspionagens net.

Hvor det er muligt forsøger man derfor at erstatte brugen af agenter eller hvervede personer med en anonym spionage, der er uafhængig af personer. Dette foregår mest enkelt ved at analysere radiosignaler fra anlæg eller fartøjer af militær betydning.

2.4.2. Analysering af elektromagnetiske signaler

Den form for spionage med tekniske midler, der er bedst kendt i offentligheden, er anvendelse af satellitbilleder. Derudover opfanges og analyseres også elektromagnetiske signaler af enhver art (såkaldt signal intelligence, SIGNINT).

2.4.2.1. Elektromagnetiske signaler, der ikke tjener til kommunikation

Bestemte elektromagnetiske signaler, f.eks. signaler fra radarstationer, kan på det militære område levere værdifulde oplysninger om opbygningen af modpartens luftforsvar (såkaldt electronic intelligence, ELINT). Derudover er elektromagnetiske signaler, der kan give oplysning om troppers, flys, skibes eller ubådes position, en værdifuld informationskilde for

en efterretningstjeneste. Det har også betydning at følge andre staters billedoptagende spionsatellitter og at registre og tyde sådanne satellitters signaler.

Signalerne optages af stationære stationer, af lavt flyvende satellitter eller af kvasi-geostationære SIGNINT-satellitter. Denne del af efterretningstjenesternes virksomhed på det elektromagnetiske område fylder kvantitativt meget i deres aflytningskapacitet. Dermed er brugen af teknik imidlertid ikke udtømt.

2.4.2.2. Analysering af opfanget kommunikation

Mange staters efterretningstjenester aflytter andre staters militære og diplomatiske kommunikation. Mange af disse tjenester overvåger også andre staters civile kommunikation, for så vidt de har adgang hertil. I nogle stater har tjenesterne ret til også at overvåge kommunikationen til eller fra det eget land. I demokratier gælder bestemte forudsætninger og kontrolprocedurer for efterretningstjenesters overvågning af **egne** borgeres kommunikation. De nationale lovgivninger beskytter imidlertid kun borgere, som opholder sig på eget statsterritorium (se kapitel 8).

2.5. Bestemte efterretningstjenesters virksomhed

Den offentlige debat har navnlig drejet sig om amerikanske og britiske efterretningstjenesters aflytningsvirksomhed. Man kritiserer, at kommunikation (tale, telefax og E-mail) optages og analyseres. En **politisk** evaluering kræver en målestok, hvormed denne virksomhed kan bedømmes. Som sammenligningsgrundlag kan man benytte den aflytningsvirksomhed, som udøves af EU-landenes efterretningstjenester. Nedenstående tabel 1 giver en oversigt. Heraf fremgår, at amerikanske og britiske efterretningstjenester ikke er de eneste efterretningstjenester, der aflytter privat kommunikation.

Land	Udlandskommunikation	Statslig kommunikation	Civil kommunikation
Belgien	+	+	-
Danmark	+	+	+
Finland	+	+	+
Frankrig	+	+	+
Tyskland	+	+	+
Grækenland	+	+	-
Irland	-	-	-
Italien	+	+	+
Luxembourg	-	-	-
Nederlandene	+	+	+

Østrig	+	+	-
Portugal	+	+	-
Sverige	+	+	+
Spanien	+	+	+
UK	+	+	+
USA	+	+	+
Canada	+	+	+
Australien	+	+	+
New Zealand	+	+	+

Tabel 1: Efterretningstjenesters aflytningsvirksomhed i EU og i Echelon-staterne.

De enkelte spalter angiver:

Spalte 1: Det pågældende land

Spalte 2: Aflytning af udlandskommunikation

Spalte 3: Aflytning af statslig kommunikation (militær, ambassader osv.)

Spalte 4: Aflytning af civil kommunikation.

3. Tekniske forudsætninger for at aflytte telekommunikation

3.1. Forskellige kommunikationsmediers eksponering for aflytning

Når mennesker vil kommunikere med hinanden over en bestemt afstemt, er et kommunikationsmedie påkrævet. Det kan være:

- luft (lyd)
- lys (morseblinker og optisk glasfiberkabel)
- elektricitet (telegraf og telefon)
- en elektromagnetisk bølge (alle mulige former for radio).

Ønsker tredjemand adgang til kommunikationsmediet, kan han aflytte kommunikationen. Denne adgang kan være let eller vanskelig og kan være mulig fra en hvilken som helst position eller kun fra bestemte positioner. I det følgende behandles to diametralt modsatte tilfælde: på den ene side en spions tekniske muligheder på stedet, på den anden side mulighederne for et globalt arbejdende aflytningssystem.

3.2. Muligheder for at aflytte på stedet[1]

På stedet kan enhver kommunikation aflyttes, når den aflyttende person er rede til at overtræde loven og den aflyttede person ikke beskytter sig.

- **Samtaler** i lokaler kan aflyttes ved hjælp af skjulte mikrofoner eller ved registrering med laser af vinduernes svingninger.

- **Billedskærme** udsender stråling, som kan opfanges på en afstand af indtil 30 meter; dermed bliver skærmens indhold synligt.

- **Telefon, telefax og E-mail** kan aflyttes, hvis den aflyttende person tapper det kabel, som kommer fra bygningen.

- En **mobiltelefon** kan aflyttes i en afstand af op til …. kilometer.

- **Intern radiokommunikation** kan aflyttes inden for VHF-frekvensområdet (ultrakorte bølger).

Betingelserne for at anvende teknisk udstyr til spionage er ideelle på stedet, fordi aflytningsforanstaltningerne kan afgrænses til en målperson eller et målobjekt, og praktisk talt næsten enhver kommunikation kan opfanges. Den eneste ulempe er risikoen for at blive opdaget, når der er tale om installation af skjulte mikrofoner eller aftapning af et kabel.

[1] Manfred Fink, Lauschziel Wirtschaft - Abhörgefahren und -techniken, Vorbeugung und Abwehr, Richard Boorberg Verlag Stuttgart 1996.

3.3. Muligheder forbundet med et globalt arbejdende aflytningssystem

Til interkontinental kommunikation findes i dag forskellige kommunikationsmedier for alle kommunikationsformer (tale, telefax og data). Mulighederne for et globalt arbejdende aflytningssystem er begrænset af to faktorer:

- den begrænsede tilgængelighed til kommunikationsmediet

- nødvendigheden af at sortere den relevante kommunikation blandt en omfattende kommunikationsmængde.

3.3.1. Adgang til kommunikationsmedierne

3.3.1.1. Kommunikation via kabel

Alle former for kommunikation (tale, telefax, E-mail og data) overføres via kabel. Kabelbaseret kommunikation kan aflyttes, når det er muligt at få adgang til kablet. En sådan adgang er under alle omstændigheder mulig ved kabelforbindelsens endepunkt, når det ligger på den aflyttende stats territorium. På nationalt plan kan alle kabler **teknisk set** altså aflyttes, hvis aflytningen er tilladt ifølge loven. Udenlandske efterretningstjenester har imidlertid som regel ingen lovlig adgang til kabler på andre staters territorium. Illegalt kan de eventuelt opnå punktuel adgang under stor risiko for at blive opdaget.

Interkontinentale kabelforbindelser blev oprettet i telegrafens tidsalder og er baseret på undersøiske kabler. Det er altid muligt at skaffe sig adgang til disse kabler på de steder, hvor de dukker op af vandet. Arbejder flere stater sammen i et aflytningsforbund, vil der være adgang til alle endepunkter på de kabelforbindelser, som fremføres til de pågældende stater. Historisk var dette af betydning, fordi både de undersøiske telegrafkabler og de første undersøiske telefonkoaksialkabler mellem Europa og Amerika kom op fra havet i New Foundland (canadisk territorium), og forbindelserne til Asien gik via Australien, fordi det var nødvendigt at operere med indskudte forstærkere. I dag følger optiske glasfiberkabler den direkte vej uden hensyntagen til undersøiske bjerglandskaber og forstærkerkrav og dermed uden mellemstop i Australien eller New Zealand.

Elektriske kabler kan også tappes induktivt mellem en forbindelses endepunkter (dvs. elektromagnetisk med en spole, der lægges til kablet), uden at der oprettes en direkte elektrisk ledende forbindelse. Dette er også muligt fra ubåde, hvilket dog er forbundet med store omkostninger. Denne teknik blev anvendt af USA for at tappe et bestemt undersøisk kabel tilhørende Sovjetunionen, over hvilket der ukodet blev kommunikeret befalinger til russiske atomubåde. En generel anvendelse af denne teknik er dog - alene af økonomiske grunde - urealistisk.

Ved de optiske glasfiberkabler af den ældre generation, der anvendes i dag, er induktiv aflytning kun mulig på de steder, hvor der er indskudt forstærkere. Ved disse forstærkere ændres det optiske signal til et elektrisk signal, som forstærkes for igen at blev forvandlet til et optisk signal. Imidlertid er det spørgsmålet, om de enorme datamængder, som transporteres i et sådant kabel, kan sendes fra aflytningsstedet til evalueringsstedet, uden at der trækkes et selvstændigt glasfiberkabel. Af omkostningsmæssige grunde vil det kun i meget sjældne

tilfælde komme på tale at anvende ubåde med evalueringsteknik om bord, f.eks. i krig for at aflytte modstanderens strategiske, militære kommunikation. Efter ordførerens opfattelse vil det ikke kunne betale sig at indsætte ubåde til rutineovervågning af internationale telekommunikationsstrømme. Glasfiberkabler af den nyere generation benytter erbiumlasere som mellemforstærkere, hvor det ikke er muligt at foretage en elektromagnetisk tilkobling med henblik på aflytning! Sådanne glasfiberkabler kan således kun aflyttes ved forbindelsens endepunkter.

I praksis betyder dette for de såkaldte **Echelon-staters** aflytningsforbund, at de økonomisk forsvarligt kun kan aflytte ved endepunkterne af de undersøiske kabler, som kommer op af undergrunden på deres statsområde. I det væsentlige kan de således kun aftappe kabelbaseret kommunikation, som ankommer til eller forlader deres land. Det betyder, at deres adgang til denne kabelkommunikation **i Europa** er begrænset til **Det Forenede Kongeriges territorium (!)**, eftersom indenlandsk kommunikation hidtil for det meste er blevet overført via det indenlandske kabelnet. Med privatiseringen af telekommunikationssektoren kan der opstå undtagelser, men de vil være delvise og uforudsigelige!

Dette gælder i det mindste telefon og telefax. Ved kabelkommunikation via Internet gælder andre forhold. Sammenfattende kan følgende dog fastslås:

- Kommunikation på Internet afvikles ved hjælp af datapakker, i hvilken forbindelse de pakker, der er stilet til en modtager, kan tage forskellige veje i nettet.

- I begyndelsen af internettidsalderen blev uudnyttet kapacitet på det offentlige net anvendt til at overføre E-mail. Derfor var den vej, som de enkelte meddelelser og datapakker ville tage, helt uforudsigelige og vilkårlige. Den vigtigste internationale forbindelse på den tid var den såkaldte "science backbone" mellem Europa og USA.

- Med kommercialiseringen af Internettet og etableringen af internetudbydere fulgte også en kommercialisering af nettet. Internetudbydere etablerede eller lejede egne net. De forsøgte derfor i stigende grad at holde kommunikationen inden for deres eget net for at undgå at skulle betale brugerafgifter til andre netoperatører. En datapakkes vej på nettet bestemmes i dag derfor ikke kun af nettets kapacitet, men afhænger også af økonomiske overvejelser.

- En E-mail, som sendes fra en udbyders kunde til en anden udbyders kunde, forbliver som regel på firmanettet, også selv om dette ikke er den hurtigste vej. Ved hjælp af de såkaldte routere, som er computere, der er beliggende på nettets knudepunkter, og som bestemmer datapakkernes rute, tilrettelægges overgangen til andre net ved bestemte overgangspunkter (såkaldte "switches").

- På den tid, da ovennævnte "science backbone" eksisterede, var den globale internetkommunikations "switches" beliggende i USA. Derfor havde efterretningstjenesterne dér dengang adgang til en væsentlig del af den europæiske internetkommunikation. I dag afvikles kun en meget lille del af den interne europæiske kommunikation på Internet via USA.

- Den interne europæiske kommunikation afvikles for en mindre dels vedkommende via en "switch" i London, hvortil den britiske efterretningstjeneste GCHQ har adgang. Hovedparten af kommunikationen forlader ikke kontinentet. Således afvikles over 95% af den tyske internetkommunikation via en "switch" i Frankfurt.

I praksis betyder dette, at Echelon-staterne kun har adgang til en **meget begrænset del** af den kabelbaserede internetkommunikation.

3.3.1.2. Radiokommunikation [1]

I hvilken udstrækning radiokommunikation kan aflyttes, afhænger af de anvendte elektromagnetiske bølgers rækkevidde. Forløber de udsendte radiobølger langs med jordoverfladen (såkaldt **jordbølger**), er deres rækkevidde begrænset og afhænger af stedets topografi, bebyggelse og bevoksning. Går radiobølgerne i retning af verdensrummet (såkaldte **rumbølger**), kan signalerne sendes over meget store afstande ved hjælp af radiobølgernes refleksion fra ionosfærens lag. Ved at lade denne refleksion ske flere gange forøges rækkevidden betydeligt.

Rækkevidden er afhængig af bølgelængden:

- Langbølger (3 kHz - 300 kHz) forplanter sig kun via jordbølger, fordi rumbølger ikke reflekteres. De har ringe rækkevidde.

- Mellembølger (300 kHz - 3 mHz) forplanter sig via jordbølger og om natten også via rumbølger. De har mellemlang rækkevidde.

- Kortbølger (3 mHz - 30 mHz) forplanter sig først og fremmest via rumbølger; da de reflekteres flere gange, kan de modtages **over hele jorden**.

- Ultrakorte bølger (VHF-frekvens) (30 mHz - 300 mHz) forplanter sig kun via jordbølger, fordi rumbølger ikke reflekteres. De forplanter sig i en relativ lige linje som lyset; på grund af jordens krumning afhænger deres rækkevidde derfor af højden på senderens og modtagerens antenne. Afhængigt af effekten har de en rækkevidde på op til ca. 100 km (mobiltelefoner 30 km).

- Decimeter- og centimeterbølger (30 mHz - 30 gHz) forplanter sig i endnu højere grad end ultrakorte bølger på samme måde som lyset. De kan let samles og muliggør dermed målrettede transmissioner med ringe effekt (jordbaseret system baseret på mikrobølgeradiolinks). De kan kun modtages med en antenne, som står meget nær og parallelt med transmissionsleddene eller på selve transmissionsvejen eller i forlængelse heraf.

Lang- og mellembølger anvendes kun til radiosendere, radiofyr osv. Militær og civil radiokommunikation finder sted via kortbølge og navnlig de ultrakorte bølger og decimeter- og centimeterbølger.

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

Af ovenstående fremgår, at et globalt arbejdende kommunikationsaflytningssystem kun kan aflytte kortbølgeudsendelser. Alle øvrige radiofrekvenser kræver en lyttestation inden for en radius af 100 km eller mindre (f.eks. på et skib eller i en ambassade).

I praksis betyder det, at Echelon-staterne kun har adgang til en meget begrænset del af radiokommunikationen.

3.3.1.3. Kommunikation via geostationære telekommunikationssatellitter[1]

Som nævnt ovenfor kan decimeter- og centimeterbølger let samles til radiolinks. Opbygger man et sådant transmissionssystem til en stationær kommunikationssatellit placeret i stor højde, som modtager og omsætter radiosignalerne og sender dem tilbage til jorden, kan man overvinde store afstande uden brug af kabler. En sådan forbindelses rækkevidde er egentlig kan begrænset af, at satellitten ikke kan modtage og sende hele vejen rundt om jorden. Derfor anvender man flere satellitter for at kunne dække hele jorden (se kapitel 4 for nærmere detaljer). Hvis Echelon-staterne etablerer lyttestationer i de nødvendige egne af jorden, kan de i princippet aflytte al den telefon-, telefax- og datakommunikation, som går via sådanne satellitter.

3.3.1.4. Muligheder for at foretage aflytning fra fly og skibe

Det har i lang tid været kendt, at specialfly af typen AWACS indsættes til lokalisering af andre luftfartøjer over lange afstande. Disse maskiners radar er baseret på et system til identifikation af bestemte mål, som kan lokalisere og klassificere elektronisk stråling og korrelere den med radarkontakter. Der eksisterer ingen særskilt SIGNINT-kapacitet.[2]
Derimod har den amerikanske flådes langsomt flyvende spionfly EP-3 mulighed for at aflytte mikrobølger, ultrakorte bølger og kortbølger, og signalerne analyseres direkte om bord; flyet tjener rent militære formål.[3]

Derudover indsættes overvågningsskibe og i kystområder også ubåde til aflytning af militær radiokommunikation.[4]

3.3.1.5. Muligheder for at foretage aflytning fra spionagesatellitter

Så længe radiobølger ikke bundtes ved hjælpe af brugbare antenner, forplanter de sig i alle retninger, altså også i verdensrummet. Signal intelligence satellitter i lavt kredsløb kan kun opfange den sender, der skal aflyttes, i få minutter ad gangen. I tætbefolkede industriområder vanskeliggøres aflytningen af de mange sendere på samme frekvens i en sådan grad, at det næsten er umuligt at skelne enkelte signaler.[5] Disse satellitter er således ikke egnet til vedvarende overvågning af civil radiokommunikation.

Desuden anvender USA såkaldte kvasistationære SIGNINT-satellitter med høj omløbsbane (42.000 km).[6] Til forskel fra de geostationære kommunikationssatellitter har disse satellitter en inklination på 3-10 grader og flyver i en bane, hvis højeste afstand fra jorden er 39.000 -

[1] Hans Dodel, Satellitenkommunikation, Hüthig Verlag 1999.
[2] Skrivelse af 14.2.2001 fra statssekretær i det tyske forsvarsministerium, Walter Kolbow.
[3] Süddeutsche Zeitung nr. 80, af 5.4.2001, s. 6.
[4] Jeffrey T. Richelson, The U.S. Intelligence Community, Ballinger, New York 1989, s. 188 og s. 190.
[5] Skrivelse af 14.2.2001 fra statssekretær i det tyske forsvarsministerium, Walter Kolbow.
[6] Major Andronov, Zarubezhnoye voyennoye obozreniye, nr. 12, 1993, s. 37-43.

42.000 km og den laveste 30.000 - 33.000 km. Satellitterne står derfor ikke ubevægelige i rummet, men bevæger sig i en kompleks elliptisk bane. Dermed dækker de et større område i dagens løb og gør det muligt at pejle sig ind på radiosendere. Dette forhold og de i øvrigt offentligt tilgængelige kendetegn ved de pågældende satellitter afslører, at de anvendes til rent militære formål.

De modtagne signaler sendes stærkt bundtet tilbage til modtagestationen med en frekvens på 24 gHz.

3.3.2. Muligheder for automatisk analyse af opfanget kommunikation: anvendelse af filtre

Ved aflytning af udenlandsk kommunikation koncentrerer man sig ikke målrettet om en enkelt telefonforbindelse. I stedet optages al kommunikation (eller en del heraf), der passerer den overvågede satellit eller det aflyttede kabel, og filtreres ved hjælp af computere under anvendelse af kodeord. Det ville være helt umuligt at analysere al registreret kommunikation.

Det er let at sortere kommunikation på en given forbindelse. Med kodeord er det også muligt at registrere kommunikation via telefax og E-mail. Selv en bestemt stemme kan registreres, hvis systemet er afstemt efter stemmen.[1] Derimod kan det endnu ikke lade sig gøre automatisk at genkende ord, der stammer fra en vilkårlig stemme - i hvert fald ikke ifølge de oplysninger, ordføreren ligger inde med. Mulighederne for at filtrere kommunikation begrænses også af andre faktorer: computernes ultimative kapacitet, taleproblemet og især det lille antal analytikere, som kan læse og analysere filtrerede oplysninger.

Ved en vurdering af mulighederne for at anvende filtreringssystemer må der også tages højde for, at de fulde tekniske muligheder ved et sådant aflytningssystem, der arbejder efter "støvsugerprincippet", fordeler sig på en række emner. En del af kodeordene har med militær sikkerhed at gøre og en del med narkohandel og andre former for international kriminalitet; en del stammer fra handel med varer med dobbelt anvendelse, og en del vedrører overholdelse af handelsembargoer. Endelig har en del af kodeordene også med økonomisk virksomhed at gøre. Det betyder, at systemets kapacitet er fordelt på flere områder. En indsnævring af kodeordene til kun at vedrøre områder af økonomisk interesse vil slet og ret gå imod regeringernes krav til efterretningstjenesterne; selv afslutningen på den kolde krig var ikke nok til at tage et sådant skridt.[2]

3.3.3. Den tyske efterretningstjeneste som eksempel

Den tyske efterretningstjenestes afdeling 2 skaffer informationer ved aflytning af udenlandsk kommunikation. Dette var genstand for en undersøgelse af den tyske forfatningsdomstol. De enkeltheder, som blev offentliggjort i tilknytning til sagen[3], giver - sammenholdt med den redegørelse, som koordinatoren for efterretningstjenesterne i forbundskanslerens kontor, Ernst Uhrlau, gav i Echelon-udvalget den 21.11.2000 - et indtryk af efterretningsvæsenets udbytte ved aflytning af satellitkommunikation.

[1] Privat meddelelse til ordføreren, kilde beskyttet.
[2] Privat meddelelse til ordføreren, kilde beskyttet.
[3] BverfG, 1 Bv 2226/94 af 14.7.1999, punkt 1.

Andre efterretningstjenesters muligheder kan være større på bestemte områder som følge af deres ret til adgang til kabelbaseret kommunikation eller grundet et større antal analytikere. Især en analyse af de kabelbaserede kommunikationsstrømme øger den statistiske sandsynlighed for en fuldtræffer, men ikke nødvendigvis antallet af brugbare kommunikationer. I grunden er den tyske efterretningstjeneste (BND) for ordføreren et godt eksempel på, hvilke muligheder og strategier efterretningstjenester råder over ved aflytning af udenlandsk kommunikation, selv om de ikke vil afsløre det.

BND søger med **strategisk** telekommunikationsovervågning at skaffe oplysninger fra udlandet via udlandet. Til dette formål opfanges satellitkommunikation ved hjælp af en række søgetermer (som i Tyskland skal godkendes forinden af den såkaldte G10-kommission[1]). De relevante tal er som følger (situationen i år 2000): af de godt ti millioner internationale kommunikationsforbindelser, der finder sted til og fra Tyskland hver dag, afvikles ca. 800.000 via satellit. Heraf filtreres knap 10% (75.000) ved hjælp af en søgemaskine. Efter ordførerens opfattelse har denne begrænsning ikke rod i loven (teoretisk ville 100% have været tilladt - i det mindste før sagen ved forfatningsdomstolen), men er teknisk begrundet, f.eks. begrænset analysekapacitet.

Også antallet af anvendelige søgetermer er begrænset af tekniske årsager og kravet om tilladelse. I præmisserne til forfatningsdomstolens dom tales ved siden af de rent formelle søgetermer (forbindelser, der anvendes af udlændinge eller udenlandske virksomheder i udlandet) om 2.000 søgetermer på det område, der vedrører spredning af atomvåben, 1.000 søgetermer inden for våbenhandel, 500 termer inden for terrorisme og 400 på området handel med ulovlig narkotika. Når det gælder terrorisme og narkohandel, har processen imidlertid ikke givet mange resultater.

Med søgemaskinen søges efter godkendte søgetermer, der anvendes inden for telefax- og telexkommunikation. Automatisk genkendelse af ord i tale er endnu ikke muligt. Finder maskinen ikke søgebegreberne, ender kommunikationen teknisk set automatisk i papirkurven; den må ikke analyseres, fordi der ikke er noget retsgrundlag herfor. Dagligt registreres omkring fem kommunikationer med deltagere, som er omfattet af den tyske forfatnings beskyttelse. Den tyske efterretningstjenestes overvågningsstrategi går ud på at finde elementer, der udgør holdepunkter for yderligere overvågning. Den har ikke total overvågning af udenlandsk kommunikation som målsætning. Ifølge de oplysninger, ordføreren er i besiddelse af, gælder dette også andre efterretningstjenesters SIGNINT-aktiviteter.

[1] Tysk lov af 13.8.1968 om begrænsning af brev-, post- og kommunikationshemmeligheden (lov til artikel 10 i den tyske grundlov).

4. Den tilgrundliggende teknologi for satellitkommunikation

4.1. Kommunikationssatellitters betydning

Kommunikationssatellitter udgør i dag en afgørende faktor i de globale telekommunikationsstrømme og er af vital betydning for transmission af fjernsyns- og radioprogrammer og for multimedieaktiviteterne. På trods heraf er satellitkommunikationens andel i den internationale kommunikation i Centraleuropa aftaget stærkt i de senere år. I mange områder udgør denne andel nu sågar under 10%.[1] Dette hænger sammen med fordelene ved optiske glasfiberkabler, som transmitterer langt større kommunikationsmængder med bedre forbindelse.

Talekommunikation afvikles i dag også digitalt. Kapaciteten for digitale forbindelser, der går via satellit, er pr. transponder på satellitten begrænset til **1890** talekanaler med ISDN-standard (64 kbits/sek). Sammenholdt hermed kan der på et enkelt glasfiberkabel i dag sendes **241.920** talekanaler med samme standard. Det svarer til et forhold på **1:128**!

Dertil kommer, at forbindelsernes kvalitet er ringere via satellit end via undersøiske glasfiberkabler. Som følge af signalernes lange transmissionstid på flere hundrede millisekunder spiller kvalitetstabet ikke den store rolle ved normal taletransmission - selv om man kan høre det. Når det gælder data- og telefaxforbindelser, som afvikles ved en kompliceret "handshaking"-procedure, har kablet klare fordele for så vidt angår forbindelsens sikkerhed. Imidlertid er kun 15% af verdens befolkning sluttet til det globale kabelnet.[2]

Til bestemte anvendelsesformål vil satellitsystemer derfor i lang tid trods alt frembyde flere fordele end kabler. Dette viser følgende eksempler fra det civile område:

- National, regional og international telefon- og datakommunikation i områder med små kommunikationsmængder, dvs. hvor det ikke ville kunne betale sig at etablere en kabelforbindelse på grund af den ringe kapacitetsudnyttelse.

- Tidsbegrænset kommunikation i forbindelse med naturkatastrofer, arrangementer, omfattende byggeri og anlægsarbejder, osv.

- FN-missioner i områder med underudviklet kommunikationsinfrastruktur.

- Fleksibel/mobil erhvervskommunikation under anvendelse af meget små sendestationer (VSAT, se nedenfor).

Disse anvendelsesområder for satellitter inden for kommunikation kan forklares med, at de har følgende egenskaber: En enkelt geostationær satellit kan dække næsten 50% af jordens overflade, og uvejsomt terræn udgør ingen hindring. I dette område er 100% af brugerne dækket, både til lands, til vands og i luften. Satellitter er funktionsdygtige i løbet af få måneder og er ikke afhængige af infrastrukturen på stedet; de er desuden mere pålidelige end kabler og kan udskiftes uden problemer.

[1] Se begrundelsen for ændringen af G10-loven i Tyskland.
[2] Deutsche Telekoms hjemmeside: www.detesat.com/deutsch/

Følgende egenskaber ved satellitkommunikation må betegnes som ulemper: de relativt lange signaltransmissionstider, tilbagegangen i satellitkommunikationens udbredelse, 12-15 års kortere levetid end kablet, større risiko for beskadigelse og stor aflytningsrisiko.

4.2. Hvordan en satellitforbindelse fungerer

Som allerede nævnt (se kap. 3) kan mikrobølger nemt bundtes ved brug af de rigtige antenner. Derfor kan man erstatte kabler med mikrobølgeradiolinks. Er sende- og modtageantenne ikke placeret på en vandret linje, men - som det er tilfældet på jorden - på overfladen af en kugle, "forsvinder" modtageantennen på grund af jordens krumning under horisonten fra og med en bestemt afstand. De to antenner kan dermed ikke længere "se" hinanden. Det samme ville f.eks. være tilfældet med en interkontinental radioforbindelse mellem Europa og USA. Antennerne skulle stå på 1,8 km høje master for at kunne etablere en forbindelse. Alene af den grund er det ikke muligt at etablere en interkontinental radioforbindelse - helt bortset fra, at signalet under transmissionen dæmpes som følge af påvirkningen fra luft og vanddampe. Lykkes det derimod at placere en slags spejl til brug for transmissionen på en "fast position" i stor højde i verdensrummet, kan der sendes over store strækninger trods jordens krumning på samme måde som, man kan se om hjørner med et trafikspejl. Det her beskrevne princip gennemføres ved at anvende såkaldte geostationære satellitter.

4.2.1. Geostationære satellitter

Lader man en satellit kredse én gang om jorden på 24 timer i en cirkelformet bane parallelt med ækvator, følger den nøjagtigt jordens omdrejning. Set fra jordens overflade vil satellitten da i 36.000 kilometers højde stå stille - den har en **geostationær** position. De fleste kommunikations- og fjernsynssatellitter hører til denne type satellitter.

4.2.2. En satellitkommunikationsforbindelses signalvej

Transmission af signaler via satellitter kan beskrives på følgende måde:

Det signal, der kommer fra en ledning, sendes til satellitten fra en jordbaseret sendestation med en parabolantenne via en opadgående transmissionsvej, det såkaldte **uplink**. Satellitten modtager signalet, forstærker det og sender det tilbage til en anden jordbaseret station via en nedadgående transmissionsvej, det såkaldte **downlink**. Derfra går signalet så igen tilbage til et kabelnet.

Ved mobilkommunikation transmitteres signalet til satellitten direkte fra den mobile kommunikationsenhed og kan derfra via en jordstation igen indføres i en ledning eller videresendes direkte til en anden mobil enhed.

4.2.3. De vigtigste eksisterende satellitkommunikationssystemer

Den kommunikation, der stammer fra de **offentligt tilgængelige kabelnet** (ikke nødvendigvis statslige) sendes om nødvendigt via satellitsystemer med forskellig rækkevidde fra og til stationære sendestationer på jorden for så igen at tilgå kabelnettene. Man skelner mellem

- globale (f.eks. INTELSAT)
- regionale (kontinentale) (f.eks. EUTELSAT) og
- nationale (f.eks. ITALSAT)

satellitsystemer.

De fleste af disse satellitter har en geostationær position; 120 private selskaber i hele verden driver ca. 1000 sådanne satellitter.[1]

Derudover er jordens nordligste del dækket af satellitter, der kredser i en meget excentrisk bane (russiske molnyia kredsløb), således at disse satellitter under halvdelen af deres kredsløb er synlige for brugeren i denne del af verden. Med to satellitter vil der derfor her kunne opnås en komplet regional dækning, som ikke er mulig fra en geostationær position over ækvator.

Desuden findes i form af det globale INMARSAT-system et **mobilkommunikationssystem**, der i øvrigt oprindelig var oprettet for at blive brugt til søs, hvormed der kan etableres satellitbaserede forbindelser overalt i verden. Dette system arbejder ligeledes med geostationære satellitter.

Det satellitbaserede mobiltelefonsystem ved navn IRIDIUM, som fungerede på grundlag af flere satellitter, der var placeret i tidsforskudte lave kredsløb, indstillede for nylig sin virksomhed af økonomiske årsager grundet manglende kapacitetsudnyttelse.

Endelig eksisterer der et hurtigt udviklende marked for såkaldte VSAT-forbindelser (VSAT = very small aperture terminal). Der anvendes her meget små jordbaserede sendestationer med antenner med en diameter på mellem 0,9 og 3,7 m, som drives af firmaer til eget behov (f.eks. videokonferencer) eller af udbydere af mobilkommunikation til dækning af tidsbegrænsede kommunikationsbehov (f.eks. møder). I 1996 var 200.000 sådanne sendestationer i drift i hele verden. Volkswagen AG driver 3.000 VSAT-enheder, Renault 4.000, General Motors 100.000 og den største europæiske oliekoncern 12.000. Kommunikationen afvikles åbent, medmindre kunden selv sørger for kryptering.[2]

4.2.3.1. Globalt arbejdende satellitsystemer

Disse satellitsystemer dækker hele jordkloden på grundlag af satellitter, der er placeret over Atlanterhavet, Det Indiske Ocean og Stillehavet.

INTELSAT[3]

INTELSAT (International Telecomunications Satellite Organisation) blev oprettet i 1964 som en myndighed med en organisationsstruktur svarende til FN´s og med det formål at drive international kommunikation. Medlemmer var de nationale postvæsener i regeringseje. I dag er 144 regeringer medlem af INTELSAT. I 2001 bliver INTELSAT privatiseret.

INTELSAT har i øjeblikket 19 geostationære satelliter, der forbinder over 200 lande, og hvis ydelser udlejes til medlemmerne af INTELSAT. Medlemmerne driver deres egne jordstationer. Gennem INTELSAT Business Service (IBS) har også ikke-medlemmer (f.eks. telefonselskaber, store firmaer, internationale koncerner) siden 1984 kunnet benytte

[1] G. Thaller, Satelliten im Erdorbit, Franzisverlag, München 1999.
[2] H. Dodel, privat meddelelse.
[3] INTELSATs hjemmeside: http:www.intelsat.com

satellitterne. INTELSAT tilbyder globale tjenester på områder som kommunikation, fjernsyn etc. Transmissionen af telekommunikation sker på C- og Ku-båndet (se nedenfor).

INTELSAT-satelliterne er de vigtigste internationale kommunikationssatelliter. Over disse afvikles størstedelen af den satellitbaserede internationale kommunikation.
Satelliterne dækker det atlantiske, indiske og pacifiske område (se tabel, kapitel 5.3).

Over Atlanterhavet befinder der sig mellem 304°E og 359°E 10 Satelliter, det indiske område dækkes af 6 Satelliter mellem 62°E og 110,5°E, Stillehavsområdet af 3 satelliter zwischen 174°E und 180°E. Via flere enkeltsatellitter i Atlanterhavsområdet dækkes behovet her.

INTERSPUTNIK[1]

I 1971 blev den internationale satellitenkommunikationsorganisation INTERSPUTNIK oprettet af 9 lande som agentur i det tidligere Sovjetunionen med opgaver svarende til INTELSAT´s. I dag er INTERSPUTNIK en mellemstatslig organisation, som regeringerne i alle stater kan blive medlem af. Den har nu 24 medlemsstater (bl.a. Tyskland) og ca. 40 brugere (bl.a. Frankrig og England), der er repræsenteret ved deres postvæsener, hhv. teleselskaber. Hjemstedet er Moskva.

Telekommunikationstransmissionerne sker på C- og Ku-båndet (se nedenfor).

Med satelliterne (Gorizont, Express, Express A under Den Russiske Føderation og LMI-1 under Lockhead-Martin Joint venture), dækkes ligeledes hele kloden: over Atlanterhavsområdet er der 1 satellit, og der er planer om en til, over det indiske område er der 3 satellitter , i Stillehavsområdet 2 (se tabel, kapitel 5.3).

INMARSAT

INMARSAT (Interim International Maritime Satellite) har siden 1979 med sit satellitsystem muliggjort verdensomspændende **mobil** kommunikation til havs, i luften og til lands samt sikret et nødradiosystem. INMARSAT er opstået på grundlag af et initiativ fra „International Maritime Organisation“ som mellemstatslig organisation. Nu er INMARSAT privatiseret og har sit hjemsted i London.

INMARSAT-systemet består af ni satellitter i geostationære omløbsbaner. Fire af satellitterne – INMARSAT III-generationen – dækker hele kloden med undtagelse af de ekstreme polområder. Hver af satellitterne dækker ca. 1/3. På grund af deres position over de fire ocean-regioner (vestlige og østlige Atlanterhav, Stillehavet, Det Indiske Ocean) dækker de globalt. Samtidig har hver INMARSAT også en række „Spot-Beams“, hvilket muliggør samling af energi i områder med større kommunikationsvolumen.

Telekommunikationstransmissionen sker på L- og Ku-båndet (se nedenfor, 4.2.4.).

4.2.3.2. Regionale Satellitsystemer

Via regionale satellitsystemers transmissionsområder dækkes de enkelte regioner/kontinenter. Den kommunikation, de transmitterer, kan derfor kun modtages i disse regioner.

[1] INTERSPUTNIK´s hjemmeside: http://www.intersputnik.com

EUTELSAT[1]

EUTELSAT blev oprettet i 1977 af 17 europæiske postvæsener med sigte på at dække Europas specifikke behov for satellitkommunikation og støtte den europæiske rumfartsndustri. Det har hjemsted i Paris og har ca. 40 medlemsstater. I 2001 skal EUTELSAT privatiseres.

EUTELSAT driver 18 geostationære satellitter, der dækker Europa, Afrika og store dele af Asien og har forbindelse til Amerika. Satellitterne befinder sig mellem 12,5°W og 48°E. EUTELSAT tilbyder hovedsagelig fjernsyn (850 digitale og analoge kanaler) og radio (520 kanaler), men benyttes derudover også til kommunikation – i første række inden for Europa (inklusive Rusland): f.eks. til videokonferencer, til store virksomheders private netværk (f.eks. General Motors, Fiat), for presseagenturer (Reuters, AFP), for udbydere af finansielle data samt til mobile datatransmissionstjenester.
Telekommunikationstransmissionen sker på Ku-båndet.

ARABSAT[2]

ARABSAT er en pendant til EUTELSAT i den arabiske region, oprettet i 1976. Medlemmer er 21 arabiske Lande. ARABSAT-satellitter benyttes både til transmission af fjernsyn og til kommunikation.

Telekommunikationstransmissionen sker hovedsagelig på C-båndet.

PALAPA[3]

Det indonesiske PALAPA-system har været i drift siden 1995 og er den sydasiatiske pendant til EUTELSAT. Det dækker Malaysia, Kina, Japan, Indien, Pakistan og andre lande i regionen.

Telekommunikationstransmissionen sker på C- og Ku-båndet.

4.2.3.3 Nationale satellitsystemer[4]

Mange stater benytter til dækning af nationale behov egne satellitsystemer med begrænsede dækningsområder.

Den franske telekommunikationssatellit **TELECOM** tjener bl.a. til at forbinde de franske departmenter i Afrika og Sydamerika med moderlandet. Telekommunikationstransmissionen sker på C- og Ku-båndet.

ITALSAT driver telekommunikationssatellitter, der med forbundne, begrænsede dækningsområder dækker hele den italienske støvle. Modtagelse er derfor kun mulig i Italien. Transmissionen sker på Ku-båndet.

AMOS er en israelisk satellit, hovedsagelig til stationær kommunikation; den dækker

[1] EUTELSAT´s hjemmeside: http://www.com

[2] ARABSAT´s hjemmeside: http://www.arabsat.

[3] H.Dodel, Satellitenkommunikation, Hüthigverlag 1999

[4] H.Dodel og efterforskning på Internet.

Mellemøsten. Telekommunikationstransmissionen sker på Ku-båndet.

De spanske satellitter **HISPASAT** dækker Spanien og Portugal (Ku-spots) og transmitterer spanske tv-programmer til Nord- og Sydamerika.

4.2.4 Tildeling af Frekvenser

International Telecommunication Union er ansvarlig for fordeling af frekvenser. For at skabe en vis orden er verden, for så vidt angår telekommunikation, inddelt i tre regioner:

1. Europa, Afrika, det tidligere Sovjetunionen, Mongoliet

2. Nord- und Sydamerika samt Grønland

3. Asien med undtagelse af lande i Region 1, Australien og det sydlige Stillehav.

Denne historisk baserede opdeling blev overtaget til satellitkommunikationsformål og medfører en ophobning af satelliter i bestemte geostationære zoner.

Die vigtigste frekvenser til satellitkommunikation er:

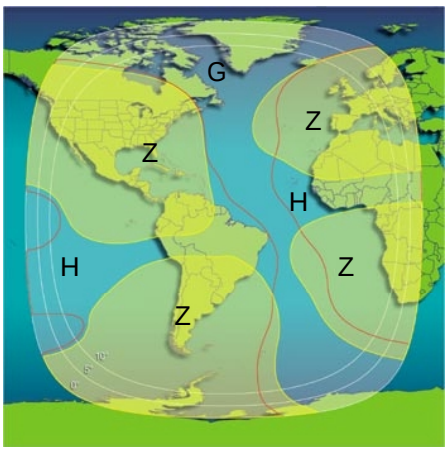
- L-båndet (0.4 - 1.6 GHz) til mobil satellitkommunikation, f.eks. over INMARSAT.
- C-båndet (3,6 - 6,6 GHz) til sendestationer, f.eks. over INTELSAT
- Ku-båndet (10 – 20 GHz) til sendestationer, f.eks. INTELSAT-Ku-Spot og EUTELSAT
- Ka-båndet (20 - 46 GHz) til sendestationer, f.eks. over nationale satellitter som ITALSAT
- V-båndet (46 – 56 GHz) til små jordbaserede sendestationer (V-SATs)

4.2.5. Satellitternes dækningsområder (footprints)

Som dækningsområde eller „footprint“ betegner man det område på Jorden, der dækkes af satellitantennen. De kan omfatte op til 50 % af Jordens overflade eller gennem koncentration af signalet begrænses til små, regionalt begrænsede spots.

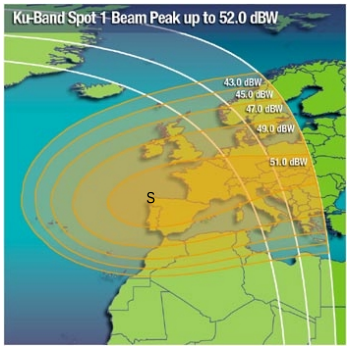
Jo højere det udsendte signals frekvens er, desto stærkere lader det sig koncentrere, og desto mindre bliver dækningsområdet. Gennem koncentration af det transmitterede satellitsignal til mindre dækningsområder kan signalets energi øges. Jo mindre dækningsområde, desto stærkere kan signalet være, og desto mindre kan modtagelsesantennerne være.

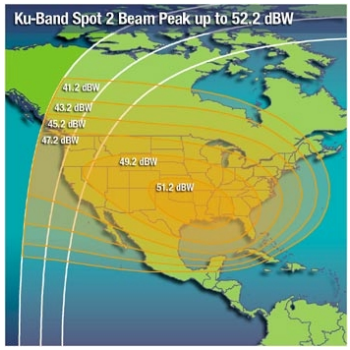
For så vidt angår INTELSAT-satellitterne forholder dette sig mere præsist som følger:

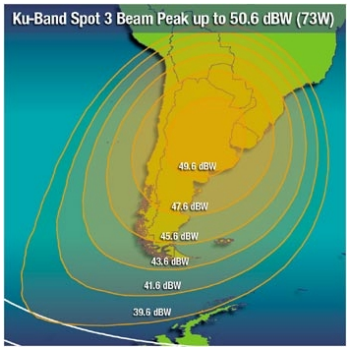


INTELSAT-satellitternes footprint er underdelt i forskellige Beams:

Alle satellitters Global-Beam (G) dækker omkring en tredjedel af jordoverfladen, Hemi-Beams (H) hver et område, der er mindre end halvdelen af Global-Beam-omådet. Zone-Beams (Z) er Spots i bestemte zoner på Jorden; de er mindre end Hemi-Beams. Derudover er der de såkaldte Spot-Beams; det er præcise, små footprints (se nedenfor).







C-båndets frekvenser finder man i Global-, Hemi- samt Zone-Beams. I Spot-Beams findes Ku-båndets frekvenser.

4.2.6 De nødvendige antennestørrelser til radiostationer

Som modtageantenner på jorden anvendes parabolantenner. Parabolspejlet reflekterer alle indgående bølger og koncentrerer dem i sit brændpunkt. I brændpunktet befinder sig det egentlige modtagesystem. Jo større signalets energi er på modtagestedet, desto mindre kan parabolantennens diameter være.

Med henblik på den undersøgelse, der udføres med denne betænkning, er det afgørende, at en del af den interkontinentale kommunikation går over C-båndet i INTELSAT-satellitternes og andre satellitters (f.eks. INTERSPUTNIK´s) Global Beam, til modtagelse af hvilken der til dels kræves paraboler med en diameter på over 30 m (se kapitel 5). 30m-antenner var også nødvendige for de første lyttestationer for kommunikationssatelliter, da den første generation af INTELSAT kun havde Global-Beams og signaltransmissionen var mindre udviklet end i dag. Disse paraboler med en diameter på til dels over 30 m benyttes stadig på de pågældende stationer, også selv om de ikke længere er teknisk nødvendige.

De typiske antenner, der i dag kræves til INTELSAT-kommunikation på C-båndet, har en diameter på mellem 13 og 18 m. I enkelte tilfælde (f.eks. til INTELSAT 511) kræves der en større antenne til Global-Beam. Til de nyeste INTELSAT-satelliter er antenner med en diameter på indtil 5 m tilstrækkelige, også til Zone-Beams på C-båndet

.

Til modtagelse af C-bånd-kommunikation fra Intersputnik kræves antenner med en diameter

på mellem 2 og 25 m.

Til INTELSAT-satelliternes Ku-Spots og til andre satelliter (EUTELSAT-Ku-bånd, AMOS Ku-bånd etc.) kræves antenner med et gennemsnit på 2 til 10 m.

Til små stationære sendestationer, der arbejder på V-båndet og hvis signal på grund af den høje frekvens kan koncentreres endnu stærkere end på Ku-båndet, er antennediametre på 0,9-3,7 m (f.eks. VSATs under EUTELSAT eller INMARSAT) tilstrækkelige.

5. Indiciebevis på eksistensen af mindst ét globalt aflytningssystem

5.1 Hvorfor indiciebevis?

Hemmelige tjenester offentliggør af naturlige årsager intet om deres arbejde. Der er derfor idet mindste ingen officiel erklæring fra Echelon-staternes efterretningstjenester om, at de i fællesskab driver et globalt aflytningssystem. Påvisning må derfor ske gennem indsamling af så mange indicier som muligt, der fortættes til et overbevisende indiciebevis.

Kæden af indicier består af tre elementer:

- påvisning af, at Echelon-staternes efterretningstjenester aflytter privat og forretningsmæssig kommunikation.

- påvisning af, at der på de dele af Jorden, der er nødvendige på grund af det civile satellitkommunikationssystems funktionsmåde, findes lyttestationer, der drives af en Echelon-stat.

- påvisning af, at der findes en efterretningsmæssig forbindelse mellem disse stater, der går ud over rammerne for det sædvanlige. Om dette går så vidt, at der indgås aflytningsaftaler mellem parterne, der derefter fremsender det optagne råmateriale uden selv at evaluere det, er uden betydning for beviset af eksistensen af et samarbejde. Dette spørgsmål spiller kun en rolle, når der er tale om klarlæggelse af hierarkierne inden for et sådant aflytningssamarbejde.

5.1.1. Påvisning af efterretningstjenesternes aflytningsaktiviteter

I hvert fald i demokratier arbejder efterretningstjenester på grundlag af love, der definerer deres formål og/eller deres beføjelser. Det kan derfor let bevises, at der i mange af disse stater findes efterretningstjenester, der aflytter civil kommunikation. Dette gælder også for de fem såkaldte Echelon-stater, der alle har sådanne tjenester. I hver enkelt af disse stater kræves der intet yderligere bevis for, at de aflytter intern kommunikation og kommunikation ud af landet. Fra det nationale territorium kan der i forbindelse med satellitkommunikation også aflyttes en del af den informationsstrøm, der er bestemt til modtagere i udlandet. I alle fem Echelon-stater er der ingen retlige begrænsninger, der hindrer dette. Den indre logik i metoden for strategisk kontrol med udlandstelekommunikationen og i formålet med den, som til dels er offentliggjort, viser klart, at disse tjenester også gør det således.[1]

5.1.2. Påvisning af eksistensen af stationer i de geografisk nødvendige

[1] Ordføreren råder over oplysninger, der bekræfter, at dette er korrekt. Kilden er beskyttet.

områder

Den eneste begrænsning for forsøget på at opbygge verdensomspændende overvågning af kommunikation, der er baseret på satellitter, ligger i teknikken for denne kommunikation. Der er intet sted, hvorfra **al** satellitkommunikation i verden kan aflyttes (se kapitel 4.2.5).

Et globalt arbejdende aflytningssystem vil kunne opbygges på tre betingelser:

- operatøren har nationalt territorium i alle de nødvendige dele af verden,
- operatøren har delvis nationalt territorium i alle de nødvendige dele af verden, og supplerende en gæsteret i de manglende dele af verden og kan drive eller medbenytte stationer her,
- operatøren er et efterretningsmæssigt samarbejde mellem stater og driver systemer i de nødvendige dele af verden.

Ingen af Echelon-staterne vil kunne drive et globalt system alene. USA har i hvert fald officielt ingen kolonier. Canada, Australien og New Zealand har heller intet nationalt territorium uden for selv landet i snævrere forstand. Heller ikke Det Forenede Kongerige vil kunne drive et globalt aflytningssystem alene (se kapitel 6).

5.1.3. Bevis for et snævert efterretningssamarbejde

Det er derimod ikke klart, om og hvordan Echelon-staterne i givet fald samarbejder på efterretningsområdet. Normalt gennemføres tjenesternes samarbejde bilateralt og på grundlag af udveksling af evalueret materiale. Et multilateralt samarbejde vil være meget usædvanligt; når hertil kommer regelmæssig udveksling af råmateriale, opstår en helt ny kvalitet. Et samarbejde af denne art kan kun påvises via indicier.

5.2. Hvorledes identificerer man en station til aflytning af satellitkommunikation?

5.2.1. Kriterium 1: Adgang til anlæggene

Postvæseners, radio- og tv-stationers og forskningsinstitutioners anlæg, der er udstyret med store antenner, er tilgængelige for besøgende, i hvert fald efter aftale; det er aflytningsstationer ikke. De drives for det meste formelt af militæret, som også teknisk foretager aflytningen. Således drives stationerne for USA f.eks. af Naval Security Group (NAVSECGRU) eller af Air Intelligence Agency under US Airforce (AIA). For så vidt angår de britiske stationer, driver det britiske Royal Airforce anlæggene for den britiske efterretningstjeneste, GCHQ. Dette arrangement muliggør en militær skarp bevogtning af anlæggene og tjener samtidig som camouflage.

5.2.2. Kriterium 2: Antennernes art

I anlæg, der opfylder kriterium 1, kan man finde forskellige typer antenner, der på karakteristisk vis adskiller sig i form. Formen giver oplysning om aflytningsanlæggets formål. Således anvendes anordninger af høje stavantenner i en ring med stor diameter (såkaldte Wullenweber-antenner) til retningspejling af radiosignaler.
Ligeledes ringformede anordninger af rhombisk formede antenner (såkaldte pusher-antenner) tjener samme formål. Antenner til modtagelse fra alle retninger eller retningsantenner, der ligner kæmpemæssige klassiske tv-antenner, tjener til aflytning af ikke-retningsbestemte radiosignaler. **Til modtagelse af satellitsignaler anvendes derimod udelukkende parabolantenner.** Står parabolantennerne i åbent landskab, kan man på grundlag af deres placering, deres hældningsvinkel (elevation) og deres kompasvinkel (azimut) beregne, hvilken satellit, de modtager. Dette vil f.eks. være muligt i Morwenstow (UK) eller i Yakima (USA) og Sugar grove (USA). For det meste er parabolantennerne imidlertid skjult under et kugleformet hvidt dække, såkaldte radomer. Disse tjener som beskyttelse af antennerne, men også som camouflage.

Befinder der sig parabolantenner eller radomer på en lyttestations område, aflyttes der med sikkerhed her signaler fra satellitter. Det ses imidlertid ikke, hvilken form for signaler, der er tale om.

5.2.3. Kriterium 3: Antennestørrelsen

Antenner til satellitmodtagelse i et kriterium 1-anlæg kan tjene forskellige formål:
- modtagelse af militær kommunikation,
- modtagelse fra spionagesatellitter (billeder, radar),
- modtagelse fra militære SIGINT-satellitter,
- aflytning af civile kommunikationssatellitter.

Udefra kan man ikke på antennerne/radomerne se, hvilken opgave de tjener. Imidlertid er der teknisk betingede minimumsstørrelser for antenner, der skal modtage den såkaldte "Global Beam" på C-båndet af den på satellitter baserede civile internationale kommunikation. I forbindelse med første generation af disse satellitter krævedes antenner med en diameter på 25-30 m., i dag er en diameter på 15-18 m. tilstrækkelig. Den automatiske computerfiltrering af de opfangede signaler kræver en så god signalkvalitet som muligt, derfor vælger man til efterretningsbrug antennestørrelser, der ligger i overkanten. Da antennerne er monteret på master, er radomernes diameter endnu større en antennernes.

5.2.4. Konklusion

Ifølge ordførerens oplysninger har antenner af denne størrelse ingen militær funktion. Ses de defor på et kategori 1-område, aflyttes der her civil satellitkommunikation.

5.3. Offentligt tilgængelige oplysninger om kendte lyttestationer

5.3.1. Metode

For at konstatere, hvilke stationer der opfylder de i kapitel 5.2. anførte kriterier, indgår i det verdensomspændende aflytningssystem og hvilke opgaver, de har, er der foretaget en gennemgang af den relevante, til dels modstridende litteratur (Hager[1], Richelson[2], Campbell[3]), deklassificeede dokumenter[4], Federation of American Scientists hjemmeside[5] samt opreratørernes[6] (NSA, AIA, m.fl.) hjemmesider og andre Internet-oplysninger. Derudover er kommunikationssatellitternes footprints blevet uddraget, de nødvendige antennestørrelser beregnet og sammen med de mulige stationer opført på verdenskort.

5.3.2. Præcis analyse

For evalueringen gælder følgende principper, der hænger sammen med de fysiske rammer for satellitkommunikation (se også kapitel 4):

- En satellitantenne kan kun opfange det, der befinder sig inden for det respektive dækningsområde, den står i. For at kunne opfange kommunikation, der hovedagelig transmitteres på C- og Ku-båndet må der etableres en antenne i det dækningsområde, der rummer C- hhv.. Ku-båndet.
- Til enhver Global-Beam kræves en satellitantenne, også når to satellitters Beams overlapper hinanden.
- Har en satellit flere dækningsområder end blot Global-Beam, hvilket er karakteristisk for vore dages generation af satellitter, kan en enkelt satellitantenne ikke længere opfange den samlede kommunikation, der transmitteres over denne, da en enkelt satellitantenne ikke kan stå i alle satellittens dækningsområder. Til modtage Hemi-Beams og Global-Beams fra en satellit kræves altså to satellitantenner i forskellige områder (sml. redegørelsen for dækningsområder i kapitel 4). Kommer der yderligere Beams til (Zone- og Spot-Beams), kræves der yderligere satellitantenner. Forskellige Beams fra en satellit, der overlapper hinanden, kan imidlertid modtages med én satellitantenne, da det er teknisk muligt at skille de forskellige frekvensbånd ved modtagelsen.

Derudover gælder de i kapitel 5.2. anførte forudsætninger: manglende adgang til anlæggene, da de drives af militæret[7], at der kræves en parabolantenne til modtagelse af satellitsignaler ,

---

[1] 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

[2] 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

[3] 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, forelagt Europa-Parlamentets Echelon-udvalg den 22. januar 2001
Federation of American Scientists, http://www.fas.org/irp/nsa/nsafacil.html

[4] 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

[5] Federation of American Scientists

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

[7] Anvendte forkortelser: 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

og at kravene til størrelsen af satellitantennerne til modtagelse af C-båndet i Global-Beam for første generation af INTELSAT var over 25 m., for senere generationer 15-18 m.

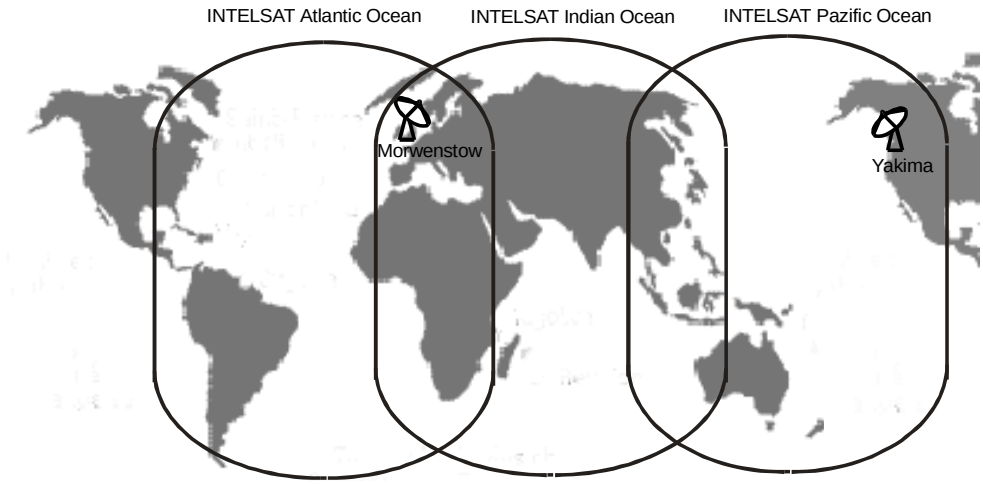
5.3.2.1. INTELSAT-udviklingens parallellitet med bygningen af stationer

Et globalt aflytningssystem må vokse med fremskridtene inden for kommunikation. Indledningen af satellit-kommunikation må derfor logisk ledsages af bygning af stationer, og indførelse af nye satellitgenerationer med udvikling af nye stationer og rejsning af nye satellitantenner, der opfylder de respektive krav. Antallet af stationer og af satellitantenner må hele tiden kunne vokse, når det er nødvendigt for modtagelsen af kommunikation.
Og omvendt, når der dér, hvor der opstår nye dækningsområder, bygges nye stationer og nye satellitantenner, er dette intet tilfælde, men kan tages som indicium for tilstedeværelsen af en aflytningsstation for kommunikation.
Da INTELSAT-satelliterne var de første kommunikationssatellitter,der desuden dækkede hele kloden, er det logisk, at bygning og udvidelse af stationerne følger udviklingen i INTELSAT-generationerne.

Den første generation

Allerede i 1965 blev den første INTELSAT-satellit (Early Bird) bragt i geostationært kredsløb. Dens transmissionskapacitet var ringe, og dens dækningsområde strakte sig kun over den nordlige halvkugle.
Med INTELSAT-generationerne II og III, der blev sat i drift i 1967, hhv. 1968, opnåedes for første gang global dækning. Satellitternes Global-Beams dækkede det atlantiske, det pacifiske og det indiske område. Mindre dækningsområder fandtes ikke. Til modtagelse af den samlede kommunikation krævedes derfor tre satellitantenner. Da to Global-Beams overlappede hinanden over det europæiske område, kunne man i dette område på én station med to satellitantenner, der vendte forskelligt, modtage de globale dækningsområder fra to satellitter.

Den første globalt arbejdende INTELSAT-satellitgeneration



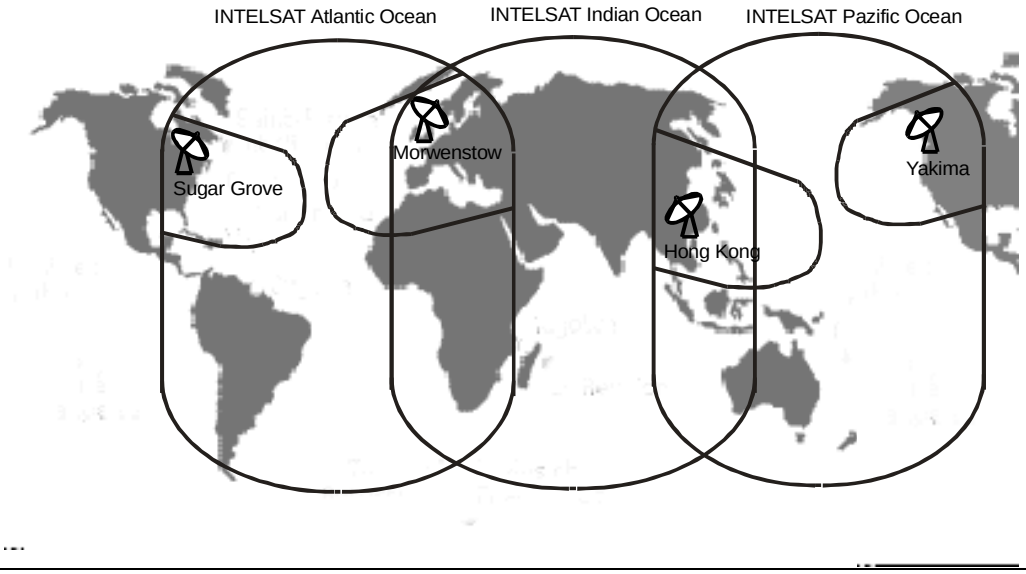
I 1970 blev **Yakima** i det nordvestlige USA oprettet, i 1972/73 **Morwenstow** i Sydengland. Yakima havde dengang én stor antenne (rettet mod Stillehavet), Morwenstow havde to store antenner (en mod Atlanterhavet, en mod Det Indiske Ocean). På grund af de to stationers

beliggenhed var modtagelse af den samlede kommunikation mulig. I 1974 byggedes derudover den første satellitantenne i Menwith Hill.

Den anden globale generation

Den anden generation af INTELSAT-satellitter (IV og IVA) blev udviklet i 70erne og bragt i geostationært kredsløb (1971 und 1975). De nye satellitter, der ligeledes sikrede global dækning og rådede over væsentligt flere telefonkanaler (4000 – 6000), havde ud over Global-Beams også Zone-Beams over den nordlige halvkugle (se kapitel 4). En Zone-Beam dækkede det østlige USA, en anden det vestlige USA, en Vesteuropa og en Østasien. Med to stationer med tre satellitantenner var modtagelse af den samlede kommunikation ikke længere mulig. Med de eksisterende stationer i Yakima kunne Zone-Beam'en til det vestlige USA modtages, med Morwenstow Zone-Beam'en over Europa. Til modtagelse af yderligere to Zone-Beams var det nødvendigt at bygge en station i det østlige USA og en i det østasiatiske område.

Den anden globalt arbejdende INTELSAT-satellitgeneration



I de sene 70ere byggedes **Sugar Grove** det østlige USA (stationen fandtes allerede til aflytning af rusisk kommunikation); den blev sat i drift i 1980. Ligeledes i de sene 70ere blev der oprettet en station i **Hongkong**.
Med de fire stationer – Yakima, Morwenstow, Sugar Grove og Hongkong - var global aflytning af INTELSAT-kommunikation mulig i 80'erne.

De senere INTELSAT-satellitter med Zone-Beams og Spot-Beams ud over Global- und Hemi-Beams gjorde yderligere stationer i forskellige dele af verden nødvendige. Her er det vanskeligt at erkende en sammenhæng mellem bygning af yderligere stationer, hhv. af nye satellitantenner.
Da man derudover kun vanskeligt får adgang til informationer om stationer, er det ikke muligt præcist at finde ud af, hvilke satellitter med hvilke Beams der modtages af hvilke stationer.

Man kan dog konstatere, i hvilke Beams kendte stationer ligger.

5.3.2.2. Den globale dækning med stationer, der entydigt aflytter kommunikationssatellitter

I dag sikres den globale satellitkommunikation via satellitter fra INTELSAT, INMARSAT og INTERSPUTNIK. Opdelingen i tre dækningsområder (det indiske, pacifiske og atlantiske område) er bevaret som ved de første satellitgenerationer.
I hvert enkelt dækningsområde findes stationer, der opfylder de for lyttestationer karakteristiske kriterier:

Satellitter over Det indiske Ocean:

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

Satellitter over Stillehavsområdet:

INTELSAT 802 (174°), 702 (176°), 701 (180°) GORIZONT 41 (130°E), 42 (142°E), LM-1 (75°E) INMARSAT Stillehavsområdet	Waihopai, New Zealand Geraldton, Australien Pine Gap, Australien Misawa, Japan Yakima, USA - kun Intelsat og Inmarsat

Satellitter over Atlanterhavet:

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 det atlantiske område	Sugar Grove, USA Buckley Field, USA Sabana Seca, Puerto Rico Morwenstow, England Menwith Hill, England
INTELSAT 707 (359°)	Morwenstow, England Menwith Hill, England

Dette viser, at global aflytning af kommunikation er mulig.

Derudover er der andre stationer, som ganske vist ikke overholder kriteriet om antennestørrelse, men som alligevel kan være en del af det globale aflytningssystem. Med disse stationer vil f.eks. kunne modtages Zone- eller Spot-Beams fra satellitter, hvis Global-Beams aflyttes af andre stationer, eller til aflytning af hvis Global-Beam der ikke kræves store satellitantenner.

5.3.2.3. Stationerne i detaljer

I den detaljerede beskrivelse af stationer sondres mellem stationer, der entydigt aflytter

kommunikationssatellitter (kriterier jf. kapitel 5.2) og stationer, hvis opgaver ikke kan dokumenteres med ovenanførte kriterier.

5.3.2.3.1. Stationer til aflytning af kommunikationssatellitter

De i kapitel 5.2. anførte kriterier, der kan betragtes som indicier på stationer til aflytning af kommunikationssatellitter passer på følgende stationer:

Yakima, USA (120°W, 46°N)

Stationen blev oprettet i 1970, samtidig med første satellitgeneration. Siden 1995 har Air Intelligence Agency (AIA) været på stedet med 544th Intelligence Group (Detachment 4). Naval Security Group (NAVSECGRU) er ligeledes stationeret her. På området findes 6 satellitantenner, hvis størrelse kilderne ikke giver oplysninger om. Hager beskriver satellitantennerne som store og oplyser, at de er rettet mod Intelsat-satellitter over Stillehavet (2 antenner), Intelsat-satellitter over Atlanterhavet og mod Inmarsat-satellit 2.
Oprettelsen af Yakima samtidig med den første Intelsat-satellitgeneration samt den generelle beskrivelse af 544th Intelligence Group's opgaver taler for, at Yakima deltager i den globale overvågning af kommunikation. Et yderligere indicium på dette er Yakimas beliggenhed tæt på en satellitmodtagelsesstation, der ligger 100 miles nordligere.

Sugar Grove, USA (80°W, 39°N)

Sugar Grove blev oprettet samtidig med at anden generation af Intelsat-satellitterne blev sat i drift i de sene 70ere. Her er stationeret NAVSECGRU samt AIA med 544th Intelligence Group (Detachment 3). Stationen har efter forskellige kilders oplysninger 10 satellitantenner, hvoraf tre er større end 18m (18,2 m, 32,3 m og 46 m) og benyttes dermed entydigt til aflytning af kommunikationssatellitter. Det hører til opgaverne for Detachment 3 under 544th IG på stationen at stille „Intelligence Support“ til rådighed for indsamling af oplysninger fra kommunikationssatelliter gennem Navy-stationer.[1]
Derudover ligger Sugar Grove i nærheden af (60 miles fra) satellitmodtagelsesstationen i Etam.

Sabana Seca, Puerto Rico (66°W, 18°N)

I 1952 blev NAVSECGRU stationeret i Sabana Seca. Siden 1995 også AIA med 544th IG (Detachment 2). Stationen har mindst en satellitenantenne med en radius på 32 m og 4 andre små satellitantenner.
Ifølge officielle oplysninger er stationens opgave bearbejdelse af satellitkommunikation („performing satellite communication processing“), „cryptologic and communications service“ samt at støtte Navy- og DoD-opgaver (bl.a. indsamling af COMSAT-information (beskrivelse fra 544th IG)). Fremover skal Sabana Seca være den første station til analyse og behandling af satellitkommunikation.

Morwenstow, England (4°W, 51°N)

Morwenstow blev som Yakima oprettet samtidig med den første Intelsat-generation i begyndelsen af 70erne. Operatør på Morwenstow er den britiske efterretningstjeneste (GCHQ). I Morwenstow står ca. 30 satellitantenner, hvoraf to med en diameter på 30 m; der

[1] „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

findes ingen oplysninger om de øvrige antenner.
Om stationens opgaver oplyses intet officielt, størrelsen og antallet af satellitantennerne og disses placering kun 110 km fra Telekom-stationen i Goonhilly levner ingen tvivl om, at den fungerer som aflytningsstation for kommunikationssatellitter.

Menwith Hill, England (2°W, 53°N)
Menwith Hill blev oprettet i 1956, i 1974 var der allerede 8 satellitantenner. Nu er der ca. 30 satellitantenner, hvoraf nogle har en diameter på over 20 m. I Menwith Hill arbejder briter og amerikanere sammen. Amerikanerne har her stationeret NAVSECGRU, AIA (451st IOS) samt INSCOM, som driver stationen. Jorden, Menwith Hill befinder sig på, tilhører Englands Forsvarsministerium og er udlejet til USA´s regering. Ifølge officielle kilder er Menwith Hill´s opgave „to provide rapid radio relay and to conduct communications research". Ifølge Richelson og Federation of American Scientists er Menwith Hill såvel jordstation for spionagesatellitter som jordstation for russiske kommunikationssatellitter.

Geraldton, Australien (114°O, 28°S)
Stationen har eksisteret siden begyndelsen af 90'erne. Stationen ledes af den australske hemmelige tjeneste (DSD), briter, der tidligere var stationeret i Hongkong (se ovenfor) hører nu til mandskabet på denne station. Seks satellitantenner, hvoraf mindst én med en diameter på ca. 20 m (skønnet), er ifølge Hager rettet mod satellitter over Det Indiske Ocean og over Stillehavet.
Ifølge en ekspert, der var taget under ed af det australske Parlament, aflyttes der i Geraldton kommunikationssatellitter.[1]

Pine Gap, Australien (133°O, 23°S)
Stationen i Pine Gap blev oprettet i 1966. Den drives af den australske hemmelige tjeneste (DSD); ca. halvdelen af de dér stationerede ca. 900 personer er amerikanere fra CIA og NAVSECGRU.[2]
Pine Gap har 18 satellitantenner, heraf en med en diameter på ca. 30 m og en med en diameter på ca. 20 m. Ifølge officielle oplysninger samt oplysninger fra flere kilder har stationen fra begyndelsen været jordstation for SIGINT-satellitter. Herfra kontrolleres og styres flere spionagesatellitter og deres signaler modtages, forarbejdes og analyseres. De store satellitantenner taler imidlertid også for aflytning af kommunikationssatellitter, da SIGINT-satellitter ikke kræver store satellitantenner. Indtil 1980 var australiere udelukket fra signalanalyseafdelingen, siden har disse haft fri adgang til alt, undtagen til amerikanernes nationale kryptografirum.

Misawa, Japan (141°O, 40°N)
Stationen i Misawa har eksisteret siden 1948. Der er stationeret japanere og amerikanere. Fra amerikansk side er er tale om NAVSECGRU, INSCOM samt grupper af AIA (544th IG, 301st IS,). På området befinder sig ca. 14 satellitantenner, hvoraf nogle med en diameter på ca. 20 m (skønnet). Misawa tjener officielt som „Cryptology Operations Center". Ifølge Richelson benyttes Misawa til aflytning af de russiske Molnyia-satellitter og andre russiske kommunikationssatelliter.

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

Waihopai, Neuseeland (173°O, 41°S)
Waihopai har eksiseret siden 1989. Siden da har der været en stor antenne med en diameter på 18 m, en anden, mindre, er kommet til senere. Ifølge Hager er den store antenne rettet mod Intelsat 701 over Stillehavet.

Buckley Field, USA, Denver Colorado (104°W, 40°N)
Stationen blev oprettet i 1972 . Her er stationeret 544th IG (Det. 45). På området findes omkring 5 satellitantenner, hvoraf 4 har en diameter på ca. 20 m. Stationens officielle opgave er at indsamle, evaluere og analysere data om nukleare forhold, der er modtaget via SIGINT-satellitter. Satellitantennernes størrelse tyder på en rolle i forbindelse med aflytning af civil kommunikation.

Hongkong (22°N, 114°O)
Stationen blev oprettet i de sene 70'ere, samtidig med anden INTELSAT-generation og var udstyret med store satellitantenner. Der foreligger ingen oplysninger om de præcise størrelser. I 1994 indledtes en afvikling af stationen i Hongkong, antennerne blev flyttet til Australien. Hvilken station der har overtaget Hongkongs opgaver er ikke klart: Geraldton, Pine Gap eller Misawa i Japan.
Måske blev opgaverne fordelt på flere stationer.

5.3.2.3.2. Andre stationer

Følgende stationers funktion kan ikke entydigt fastlægges på grundlag af ovennævnte kriterier:

Leitrim, Canada (75°W, 45°N)
Leitrim er led i et udvekslingsprogram mellem canadiske og amerikanske militære enheder. Derfor er der i Leitrim ifølge US-Navy stationeret ca. 30 personer. I 1985 blev den første af 4 satellitantenner installeret, hvoraf de to største kun har en diameter på ca. 12 m (skønnet) .

Bad Aibling, Tyskland (12°O, 47°N)
Stationen i nærheden af Bad Aibling, hvor ca. 750 amerikanere arbejder, blev overtaget af US-Army i 1952 (fra 1972 til 1994 var den under Department of Defense). I Bad Aibling er stationeret NAVSECGRU, INSCOM (66th IG, die 718 IG) samt forskellige grupper af AIA (402nd IG, 26th IOG). Der er 14 satellitantenner, hvoraf ingen er større end 18 m. Ifølge officielle oplysninger har Bad Aibling følgende opgaver: “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”. Ifølge Richelson er Bad Aibling modtagestation for SIGINT-satellitter og for russiske kommunikationssatellitter.

Ayios Nikolaos, Cypern (32°O, 35°N)
Ayios Nikolaos på Zypern er en britisk station. Stationen har 9 satellitantenner, hvis størrelse er ukendt, dens opgaver er fordelt på to enheder, „Signals Regiment Radio" og "Signals Unit (RAF)“.
Agios Nikolaos placering i nærheden af de arabiske stater og det forhold, at Agios Nikolaos er den eneste station inden for bestemte dækningsområder (navnlig Spot-Beams) i denne region, taler for, at denne station spiller en rolle i efterretningsarbejdet.

Shoal Bay, Australien (134°O, 13°S)
Shoal Bay drives udelukkende af den australske efterretningstjeneste. Stationen skal have 10 satellitantenner, om hvis størrelse der ikke foreligger noget nærmere. Af de satellitantenner, der ses på fotos, har de 5 største en diameter på maksimalt 8 m, den synlige sjette er mindre. Ifølge Richelson er antennerne rettet mod de indonesiske PALAPA-satellitter. Om stationen er en del af det globale system til aflytning af civil kommunikation er ikke klart.

Guam, Stillehavet(144°O, 13°S)
Guam har eksisteret siden 1898. I dag er det en Naval Computer and Telecommunication Station, hvor der er stationeret 544th IG under AIA og Navy-soldater.
Stationen har mindst to satellitantenner, hvis størrelse der ikke findes oplysninger om. Guams funktion er derfor ikke klar.

Kunia, Hawai (158°W, 21°N)
Denne station har siden 1993 været i drift som Regional Security Operation Center (RSOC), dervet af NAVSECGRU og AIA. Til dens opgaver hører tilrådighedstillelse af information og kommunikation samt kryptologisk støtte. Kunias funktion er ikke klar.

Medina Annex, USA Texas (98°W, 29°N)
Medina er som Kunia et Regional Security Operation Center – oprettet i 1993 - , drevet af NAVSECGRU og AIA-enheder med opgaver i Stillehavet.

Fort Gordon (81°W, 31°N)
Fort Gordon er ligeledes et Regional Security Operation Center, drevet af INSCOM og AIA (702nd IG, 721st IB, 202nd IB, 31st IS) med uklare opgaver.

Fort Mead, USA (76°W, 39°N)
Fort Mead er Headquater for NSA.

5.3.3. Sammenfatning af resultaterne

Af de indsamlede data om stationer, satellitter og de ovenfor anførte forudsætninger kan drages følgende konklusioner:

1. Der findes i hvert dækningsområde aflytningsstationer for i hvert fald nogle Global-Beams med hver mindst én antenne med en diameter på over 18 m, der drives af amerikanere eller briter, hhv. hvor amerikanere eller briter udfører efterretningstjenstelige aktiviteter. Det er et stærkt indicium på eksistensen af et globalt aflytningssystem.
2. Udviklingen i INTELSAT-kommunikationen og den samtidige bygning af aflytningsstationer dokumenterer systemets globale sigte.
3. På grundlag af punkt 1 og 2 er det muligt entydigt at identificere bestemte stationer som stationer, der aflytter international satellitkommunikation.
4. Oplysningerne i de deklassificerede dokumenter og fra operatørerne (AIA, NSA, Navy osv.) kan tages som belæg for de dér anførte stationer.
5. Nogle stationer ligger samtidig i Beams hhv. Spots fra forskellige satellitter, således at en stor del af kommunikationen kan opfanges.
6. Der er andre stationer, der ikke har store antenner, men alligevel kan være en del af systemet, da de kan opfange kommunikation fra Beams og Spots. Her må man afstå fra

indiciet om antennestørrelse og gribe til andre indicier.

7. Nogle af de nævnte stationer ligger beviseligt i umiddelbar nærhed af regulære modtagestationen for kommunikationssatelliter.

5.4. UKUSA-aftalen

UKUSA-aftalen er betegnelsen på en SIGINT-aftale, der blev indgået i 1948 mellem Storbritannien (United Kingdom, UK), De Forenede Stater (USA) samt Australien, Canada og New Zealand.

5.4.1. UKUSA-aftalens historiske udvikling[1]

UKUSA-aftalen er en fortsættelse af det meget snævre samarbejde mellem De Forenede Stater og Storbritannien under Anden Verdenskrig, der allerede indledtes under Første Verdenskrig.
Initiativet til oprettelse af en SIGINT-alliance blev taget af amerikanerne i august 1940 på et møde mellem amerikanere og briter i London.[2] I februar 1941 leverede de amerikanske kryptoanalyster en krypteringsmaskine (PURPLE) til Storbritannien. I foråret 1941 indledtes det kryptoanalytiske samarbejde.[3] Det efterretningstjenestelige samarbejde styrkedes gennem flådernes fælles indsats i det nordlige Atlanterhav i sommeren 1941. I juni 1941 kunne briterne bryde den tyske flåde kode, ENIGMA.

Amerikas indtræden i krigen styrkede SIGINT-samarbejdet yderligere. I 1942 begyndte amerikanske kryptoanalytikere under „naval SIGINT agency" at arbejde i Storbritannien.[4] Kommunikationen mellem U-båds-Tracking-Rooms i London, Washington og fra maj 1943 også i Ottawa i Canada, blev så snæver, at de ifølge en tidligere involveret arbejdede som én organisation.[5]
I foråret 1943 blev BRUSA-SIGINT-aftalen undertegnet, og der blev foretaget en udveksling af personale. Aftalens indhold omfatter bl.a. opdeling af arbejdet, hvilket er sammenfattet i de tre første afsnit: Der er tale om udveksling af al information i forbindelse med opdagelse, identifikation og aflytning af signaler samt brydning af koder og krypteringer. Amerikanerne var hovedansvarlige for Japan, briterne for Tyskland og Italien[6].

Efter krigen udgik initiativet til bevarelse af SIGINT-alliancen hovedsagelig fra Storbritannien. Grundlaget for det blev aftalt på en verdensrejse for britiske efterretningsfolk

---

[1] 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

[2] samme, s. 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)

[3] samme, s. 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" (

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

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

[6] Samme, s. 101-2: Interivews med 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

(bl.a. Sir Harry Hinsley, hvis bøger danner grundlag for den citerede artikel) i foråret 1945. Et mål var at sende SIGINT-personale fra Europa mod Stillehavet til krigen mod Japan. I denne forbindelse blev det aftalt med Australien at stille ressourcer og personale (briter til rådighed for de australske tjenester. Tilbagerejsen førte over New Zealand og Canada.
I september 1945 underskrev Truman et strengt hemmeligt memorandum, der udgør hjørnestenen for SIGINT-alliancen i fredstider.[1] I den forbindelse blev der mellem briter og amerikanere indledt forhandlinger om en aftale. En britisk delegation optog derudover kontakt til canadierne og australierne for at drøfte en mulig deltagelse. I februar og marts 1946 afholdtes en strengt hemmelig angloamerikansk SIGINT-konference med henblik på at drøfte detaljer. Briterne havde mandat fra canadierne og australierne. Resultatet af konferencen var en stadig klassificeret aftale på ca. 25 sider, der fastlagde detaljerne i en SIGINT-aftale mellem De Forenede Stater og det britiske Commonwealth. Yderligere forhandlinger fulgte de næste to år, således at den endelige UKUSA-aftales tekst kunne undertegnes i juni 1948.[2]

5.4.2. Belæg for aftalens eksistens

Hidtil er der fra de kontraherende staters side ikke blevet sket nogen officiel anerkendelse af UKUSA-aftalen. Alligevel er der flere belæg på dens eksistens.

5.4.3.1 US-Navy's akronymfortegnelse

UKUSA står ifølge US-Navy[3] for „United Kingdom – USA“ betegner en „5-nation SIGINT agreement“.

5.4.2.2. Udtalelse af DSD's direktør

Direktøren for den australske efterretningstjeneste (DSD) har bekræftet aftalens eksistens i et interview: Ifølge hans oplysninger samarbejder den australske hemmelige tjeneste under UKUSA-aftalen med andre oversøiske efterretningstjenester .[4]

5.4.2.3. Betænkning fra Canadian Parliamentary Security and Intelligence Committee

I denne betænkning oplyses, at Canada i efterretningsspørgsmål samarbejder med nogle af sine nærmeste og længstvarende allierede. Betænkningen anfører disse allierede: De Forenede Stater (NSA), Storbritannien (GCHQ), Australien (DSD) og New Zealand (GCSB). Aftalens navn nævnes ikke i betænkningen.

5.4.2.4. Udtalelser af den tidligere vicedirektør i NSA, Dr. Louis Torella

I interviews med Christopher Andrew, Professor ved Cambridge University, i november 1987 og april 1992 bekræfter den tidligere vicedirektør for NSA, Dr. Louis Torella, der var til stede

---

[1] 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))
[2] 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
[3] „Terms/Abbreviations/Acronyms“ offentliggjort af US Nave and Marine Corps Intelligence Training Centre (NMITC) bei http://www.cnet.navy.mil/nmitc/training/u.html
[4] Martin Brady, Direktor des DSD, Canberra 16. marts 2000.

ved undertegnelsen, aftalens eksistens.[1]

5.4.2.5. Skrivelse fra den tidligere GCHQ-direktør, Joe Hooper

Den tidligere GCHQ-direktør Joe Hooper, nævner UKUSA-aftalen i en skrivelse af …. til den tidligere NSA-direktør, Marshall S.Carter.

5.4.2.6.Ordførerens samtalepartnere

Ordføreren har drøftet aftalen med flere personer, der på grund af deres opgaver må kende UKUSA-aftalen og dens indhold. Herunder er aftalens eksistens i alle tilfælde blevet indirekte bekræftet af svarenes art.

5.5 Evaluering af deklassificeret amerikansk materiale

5.5.1. Dokumenternes art

Inden for rammerne af „Freedom of Information Acts" fra 1966 (5 U.S.C. § 552) og af Forsvarsministeriets bestemmelser (DoD FOIA Regulation 5400.7-R fra 1997) er tidligere klassificerede dokumenter deklassificeret og dermed gjort tilgængelige for offentligheden. Via det i 1985 grundlagte National Security Archive ved George Washington University i Washington D.C. er dokumenterne tilgængelige for offentligheden. Forfatteren Jeffrey Richelson, tidligere medlem af National Security Archives, har via Internet gjort 16 dokumenter tilgængelige, der giver indblik i ledelsen af og mandatet for NSA (National Security Agency).[2]. Derudover nævnes „Echelon" i to dokumenter. Disse dokumenter citeres igen og igen af forskellige forfattere, der har skrevet om Echelon, og tages som bevis for eksistensen af det globale spionagesystem Echelon. Derudover finder man i de dokumenter, Richelson stiller til rådighed, nogle, der bekræfter eksistensen af NRO (National Reconnaissance Office) og beskriver dettes funktion som manager og operatør af SIGINT-satellitter.[3]

5.5.2. Dokumenternes indhold

Dokumenterne indeholder fragmentarisk beskrivelser eller omtale af følgende spørgsmål:

5.5.2.1. NSA's opgave og arbejde (dokument 1, 4, 10, 11 og 16)

I National Security Council Intelligence Directive 9 (NSCID 9) af 10. marts 1950 defineres udlandskommunikation med henblik på COMINT; ifølge denne definition omfatter udlandskommunikation **enhver regeringskommunikation i bredeste forstand (ikke kun militært) samt al anden kommunikation, der kan rumme oplysninger af militær, politisk, videnskabelig eller økonomisk værdi.**

Direktivet (NSCID 9 ændr. 29.12.52) fastlægger udtrykkeligt, at FBI er eneansvarlig for indre sikkerhed.

---

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

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

[3] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/index.html

Direktivet fra Department of Defense (DoD) af 23. december 1991 om NSA Central Security Service (CSS) definerer konceptet for NSA som følger:

- NSA er et separat organiseret tjenestested under Department of Defense under ledelse af en „Secretary of Defense.
- NSA sørger dels for opfyldelse af USA's SIGINT-mission, dels stiller den sikre kommunikationssystemer til rådighed for ministerier og tjenestegrene.
- NSA's SIGINT-aktiviteter omfatter ikke produktion af færdige informationer. Dette henhører under andre ministerier og tjenestegrene.

Derudover skitserer DoD-direktivet fra 1991 strukturen i NSA, hhv. CSS.

I sin redegørelse til „House Permanent Select Committee on Intelligence“ den 12. April 2000 definerede NSA-direktor Hayden NSA's opgaver som følger:

- via elektronisk overvågning samles udlandskommunikation til militær og politikere (policymakers);
- NSA leverer oplysninger til „U.S. Government consumers“ om international terrorisme, narkotika, våbenspredning;
- det er ikke NSA's opgave at indsamle al elektronisk kommunikation
- NSA må kun videregive oplysninger til modtagere, der er godkendt af USA's regering, ikke direkte til amerikanske firmaer.

I et memorandum, viceadmiral i U.S. Navy, W.O.Studeman, afgav for regeringen den 8.april 1992, henvises til NSA's voksende globale opgave (access) ud over støtte til militære operationer.

5.5.2.2. Intelligense Agencies' beføjelser (dokument 7)

Af United States Signals Intelligence Directive 18 (USSID 18) fremgår, at såvel kabel- som radiosignaler aflyttes.

5.5.2.3. Samarbejde med andre tjenester (dokument 2a og 2b)

Til opgaverne for U.S. Communications Intelligence Board hører bl.a. at overvåge alle „arrangements“ med udenlandske regeringer på COMINT-området. Til de opgaver, direktøren for NSA har, hører at afvikle alle forbindelser med udenlandske COMINT-tjenester.

5.5.2.4. Enheder, der er aktive på „Echelon-Sites“ (dokument 9, 12)

I NAVSECGRU INSTRUCTIONs C5450.48A beskrives opgaver, funktion og mål for Naval Security Group Activity (NAVSECGRUACT), 544th Intelligence Group i Sugar Grove, West Virginia. Her anføres, at en speciel opgave er: „Maintain and operate an Echelon-Site“; derudover anføres bearbejdning af efterretningsmæssige oplysninger som en opgave.

I dokumentet „History of the Air Intelligence Agency – 1 January to 31 December 1994 (RCS: HAF-HO(A&SA)7101 Volume 1) anføres under punktet “Activation of Echelon Units“ Air Intelligence Agency (AIA), Detachment 2 og 3:

Dokumenterne giver ingen oplysninger om, hvad en „Echelon-site“ er, hvad der gøres på en „Echelon-site“, hvad dæknavnet Echelon står for. Dokumenterne oplyser intet om UKUSA-aftalen.

5.5.2.5. Angivelse af stationer (dokument 6, 9, 12)

- Sugar Grove, West Virginia i NAVSECGRU INSTRUCTIONs C5450.48A
- Misawa Air Base, Japan, i 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), samme
- Guam, samme
- Yakima, Washington, samme
- Fort Meade, Maryland, en COMINT Report fra NSA fra Fort George G. Meade, Maryland af 31. august 1972 bekræfter COMINT-aktiviteterne der.

5.5.2.6. Beskyttelse af USA-borgeres privatliv (dokument 7, 7a -f, 11,16)

I NAVSECGRU INSTRUCTIONs C5450.48A hedder det, at borgernes privatliv skal garanteres.

I forskellige dokumenter anføres at og hvordan amerikanske borgeres privatliv skal beskyttes (Baker, General Counsel, NSA, skrivelse af 9. september 1992, United States Signals Intelligence Direcive (USSID) 18, 20. Oktober 1980, og forskellige supplementer[1].

5.5.2.7. Definitioner (dokument 4, 5a,7)

Department of Defense Directive af 23. december 1991 giver præcise definitioner på SIGINT, COMINT, ELINT og TELINT, hvilket ligeledes gælder National Security Council Intelligence Directive No.6 af 17. februar 1972.

Ifølge disse dokumenter betyder COMINT indsamling og bearbejdning af udlandskomminikation (passed by electromagnetic means), inklusive aflytning og bearbejdning af ukodet skreven kommunikation, presse og propaganda.

5.5.3. Sammenfatning

1. Allerede for 50 år siden var interessen ikke blot rettet mod oplysninger vedrørende politik og sikkerhed, men også vedrørende videnskab og økonomi.
2. Dokumenterne beviser, at NSA samarbejder med andre tjenester om COMINT.
3. De dokumenter, der giver oplysninger om, hvordan NSA er organiseret, hvilke opgaver det har, og at det er underlagt Department of Defense går i det store og hele ikke ud over, hvad man kan udlede af offentligt tilgængelige kilder på NSA's hjemmeside.
4. Kabelkommunikation må aflyttes.
5. 544th Intelligence group og Detachment 2 og 3 under Air Intelligence Agency deltager i indsamlingen af efterretningsmæssige oplysninger.
6. Begrebet „Echelon“ dukker op i forskellige forbindelser.
7. Sugar Grove i West Virginia, Misawa Air Base i Japan, Puerto Rico (dvs. Sabana Seca),

[1] 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).

Guam, Yakima i staten Washington nævnes som SIGINT-stationer.

8. Dokumenterne giver oplysning om, hvordan amerikanske borgeres privatliv skal beskyttes.

Dokumenterne giver intet bevis, men stærke indicier, der sammen med andre indicier giver grundlag for konklusioner.

5.6. Oplysninger fra forfattere og journalister

5.6.1. Bogen af Nicky Hager

I Nicky Hager's bog "Secret Powers – New Zealand's role in the international spy network", der udkom i 1996, beskrives Echelon-systemet for første gang grundigt. Ifølge Hager går begyndelsen tilbage til 1947, hvor Det Forenede Kongerige sammen med De Forenede Stater i tilknytning til krigssamarbejdet traf aftale om i fællesskab at fortsætte de hidtidige COMINT-aktiviteter på globalt plan. Landene skulle samarbejde om oprettelse af et så globalt aflytningssystem som muligt, idet de ville være fælles om de nødvendige specifikke faciliteter og de deraf følgende nødvendige udgifter og i fællesskab skulle have adgang til resultaterne. Senere tilsluttede Canada, Australien og New Zealand sig UKUSA-aftalen.

Ifølge Hager er aflytning af satellitkommunikation nøglepunktet i det nuværende system. Allerede i 70'erne begyndte man at aflytte afsendte meddelelser i jordbaserede stationer via Intel-satellitter - det første globale satellitkommunikationssystem[1]. Disse meddelelser blev derefter med computer gennemsøgt for fastlagte nøgleord og adresser med henblik på at kunne udskille de relevante meddelelser. Derefter blev overvågningen udvidet til andre satellitter, som f.eks. fra Inmarsat[2], der var koncentreret om maritim kommunikation.

Hager henviser i sin bog til, at aflytning af satellitkommunikation kun er én - om end vigtig - komponent i aflytningssystemet. Derudover er der talrige installationer til aflytning af radio- og kabelkommunikation, der ganske vist er mindre dokumenteret og vanskeligere at påvise, da de ikke falder i øjnene som aflytningsstationerne. "Echelon" bliver dermed til et synonym for et globalt aflytningssystem..

5.6.2. Oplysninger fra Duncan Campbell

Duncan Campbell har i STOA-studie 2/5 fra 1999, der beskæftiger sig indgående med den tekniske side, redegjort for, at og hvordan ethvert medium, der anvendes til transmission af kommunikation, kan aflyttes. I et af sine sidste arbejder gør han det imidlertid klart, at også Echelon har sine grænser; den oprindelige opfattelse af, at komplet overvågning er mulig, har vist sig at være falsk, "hverken Echelon eller det elektroniske spionagesystem, det er en del af, er i stand til dette. Der findes heller ikke udstyr, der har kapacitet til at bearbejde og genkende indholdet af enhver sproglig meddelelse eller enhver telefonsamtale." [3]

5.6.3. Oplysninger fra Jeff Richelson

Forfatteren Jeffrey Richelson, tidligere medlem af National Security Archives, har pr. Internet

[1] Sml http://www.intelsat.int/index.htm.
[2] Sml http://www.inmarsat.org/index3.html.
[3] Duncan Campbell, Inside Echelon. Om historie, teknik og funktion i forbindelse med det globale aflytnings- og filtersystem, der er kendt som Echelon, 1

gjort 16 tidligere klassificerede dokumenter tilgængelige; disse giver et indblik i NSA's (National Security Agency)[1] opståelse, udvikling, management og mandat.
Derudover har han skrevet forskellige bøger og artikler om efterretningstjenestelige aktiviteter i USA. I sin bog fra 1985 „The Ties That Bind“[2] beskriver han udførligt UKUSA-aftalens tilblivelse og de aktiviteter, de hemmelige tjenester i USA, Storbritannien, Canada, Australien og New Zealand gennemfører under denne aftale.
I sin meget omfattende bog fra 1999 „ The U.S. Intelligence Community“[3] giver han et overblik over USA's efterretningstjenestelige aktiviteter, han beskriver tjenesternes organisationsstrukturer, deres methoder til indsamling og analyse af information. I kapitel 8 kommer han detaljeret ind på efterretningstjenesternes SIGINT-kapaciteter og beskriver nogle modtagestationer. I kapitel 13 beskriver han USA's forbindelser til andre efterretningstjenester, bl.a. UKUSA-aftalen. Betegnelsen Echelon nævner han et sted som kodeord for et computerbaseret udvekslingssystem.

I artiklen „Desperately seeking Signals“[4], der udkom i 2000, beskriver han i kortform UKUSA-aftalen, nævner satellitaflytningsanlæg til kommunikationssatellitter og beskriver muligheder og grænser for aflytning af civil kommunikation.

5.6.4. Oplysninger fra James Bamford

følger.

5.6.5. Oplysninger fra Bo Elkjaer og Kenan Seeberg

De to danske journalister, Bo Elkjaer og Kenan Seeberg oplyste den 22. januar 2001 over for udvalget, at Echelon allerede var stærkt udviklet i 80'erne, og at Danmark havde samarbejdet med USA siden 1984.

5.7. Udtalelser af tidligere efterretningsmedarbejdere

5.7.1 Margaret Newsham (tidligere medarbejder i NSA)

Margaret Newsham[5] var fra 1974 til 1984 ansat hos Ford og Lockheed og arbejdede i denne periode ifølge egne oplysninger for NSA. Hun var uddannet til dette arbejde i NSA's hovedkvarter i Fort George Meade i Maryland, USA, og i 1977-1978 beskæftiget i Menwith Hill, den amerikanske jordstation på britisk territorium. Der konstaterede hun, at en samtale, som US-senator Strohm Thurmond førte, blev aflyttet. Allerede i 1978 kunne Echelon opfange enkeltpersoners telekommunikation, der gik via satellit.

For så vidt angik hendes egen rolle hos NSA, var hun ansvarlig for at opbygge systemer og programmer, at konfigurere dem og at installere dem på store computere.
Softwareprogrammerne kaldtes SILKWORTH og SIRE, Echelon var derimod betegnelsen på

[1] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html
[2] Jeffrey T. Richelson, Desmond Ball 1985: The Ties That Bind, Boston UNWIN HYMAN, Sydney Wellington London
[3] Jeffrey T. Richelson 1999 (4th ed.): „The U.S. Intelligence Community“, Westview Press
[4] Jeffrey T. Richelson 2000: „Desperately seeking Signals“ The Bulletin of the Atomic Scientists, March/April 2000, Vol. 56, No. 2, pp. 47-51
[5] Sml. Bo Elkjaer, Kenan Seeberg, Echelon was my baby – Interview med Margaret Newsham, Ekstra Bladet, 17.1.1999

netværket.

5.7.2. Wayne Madsen (tidligere NSA-medarbejder)

Wayne Madsen[1], tidligere medarbejder i NSA, bekræfter ligeledes eksistensen af Echelon. Han mener, at indsamling af økonomiske data har højeste prioritet og udnyttes af amerikanske virksomheder. Han giver navnlig udtryk for bekymring over, at Echelon kan udspionere ngo'er som Amnesty International og Greenpeace. Som begrundelse anfører han, at NSA har måttet indrømme, at det havde over 1000 sider oplysninger om prinsesse Diana, der med sin kampagne mod landminer gik imod den amerikanske politik.

5.7.3. Mike Frost (tidligere medarbejder i den canadiske efterretningstjeneste

Mike Frost var i over 20 år beskæftiget i den canadiske efterretningsatjeneste, CSE[2]. Aflytningsstationen i Ottawa er kun en del af et verdensomspændende netværk af spionagestationer.[3] I et interview med CBS oplyste han, at der "overalt i verden, hver dag sker aflytning af telefonsamtaler, e-mails und telefax'er via Echelon, et hemmeligt overvågningsnetværk under regeringen".[4] Dette omfatter også civil kommunikation. Som eksempel anførte han i et interwiev med en australsk sender, at CSE faktisk i en databank over mulige terrorister registrerede navn og telefonnummer på en kvinde, der havde anvendt et tvetydigt udtryk i en telefonsamtale med en ven. Computeren havde ved gennemsøgning af kommunikationen fundet et stikord og gengivet samtalen; den for analyse ansvarlige person var ikke sikker og havde derfor registreret hendes personlige data.[5]

Echelon-staternes efterretningstjenester hjalp også hinanden på den måde, at den ene spionerede for den anden, således at man i det mindste ikke kunne bebrejde den nationale efterretningstjeneste noget. Således skal GCHQ have anmodet den canadiske CSE om for den at udspionere to engelske ministre, da premierminister Thatcher ville vide, om de var på hendes side.[6]

5.7.4. Fred Stock (tidligere medarbejder i den canadiske efterretningstjeneste)

Fred Stock blev ifølge egne oplysninger udelukket fra den canadisken efterretningstjeneste, CSE, fordi han havde udtalt sig imod den nye prioritering af økonomiske oplysninger og civile mål. Opfanget kommunikation havde rummet oplysninger om forretninger med andre lande, bla. også forhandlingerne om NAFTA, kinesiske kornopkøb og franske våbensalg. Ifølge Stock havde tjenesten også rutinemæssigt fået oplysninger om Greenpeace-skibes protester til søs.[7]

---

[1] NBC-fjernsynsinterwiev "60 Minutes" af 27.2.2000; http://cryptome.org/Echelon-60min.htm
[2] Communication Security Establishment, under det canadiske forsvarsministerium, driver Sigint
[3] NBC-fjernsynsinterwiev "60 Minutes" af 27.2.2000; http://cryptome.org/Echelon-60min.htm
[4] Rötzer, Die NSA geht wegen Echelon an die Öffentlichkeit; http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special
[5] NBC-fjernsynsinterwiev "60 Minutes" af 27.2.2000; http://cryptome.org/Echelon-60min.htm
[6] Interview i den australske sender Channel 9 af 23..3.1999; http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm
[7] Bronskill, Canada a key snooper in huge spy network, Ottawa citizen, 24.10.2000, http://www.ottawacitizen.com/national/990522/2630510.html

5.8 Regeringsoplysninger

5.8.1. Udtalelser fra amerikanisk side

Den tidligere CIA-direktør, James Woolsey, oplyste på en pressekonference,[1] som han afgav på anmodning af US-State Department, at USA driver spionage i Kontinentaleuropa. "Economic Intelligence" opnås for 95 procents vedkommende gennem evaluering af offentligt tilgængelige informationskilder, kun 5% er stjålne hemmeligheder. Økonomiske data i andre lande udspioneres, når der er tale om overholdelse af sanktioner og dual-use-varer, samt om at bekæmpe bestikkelse i forbindelse med indgåelse af ordrer. Disse oplysninger videregives imidlertid ikke til amerikanske virksomheder. Woolsey understreger, at det, selv når man under udspionering af økonomiske data støder på økonomisk anvendelige oplysninger, vil være meget tidskrævende for en analytiker at analysere den store mængde data med henblik herpå, og at det desuden ville være misbrug at bruge tid på spionage mod venligtsindede handelspartnere. Derudover påpeger han, at det, selv hvis man gjorde det, på grund af det internationale samarbejde ville være vanskeligt at afgøre, hvilken virksomhed, der hørte hjemme i USA, og som man derfor skulle videresende oplysningerne til.

I en senere artikel til The Wall Street Journal Europe[2] gentog Woolsey, at USA udspionerer Europa, men at dette skete for at afdække bestikkelse. Han oplyser også, at USA anvender computere til at gennemsøge data for nøgleord.

5.8.2. Udtalelser fra engelsk side

Det fremgår af forskellige forespørgsler i House of Commons[3], at RAF-stationen Menwith Hill henhører under det engelske forsvarsministerium, men som kommunikationsinstallation stilles til rådighed for NSA[4], der udpeger stationslederen [5] [6]. I midten af 2000 var der i RAF Menwith Hill beskæftiget 415 militærpersoner fra USA, 5 militærpersoner fra UK, 989 US-civilister und 392 UK-civilister, idet tilstedeværende GCHQ-medarbejdere ikke medregnedes.[7] Tilstedeværelsen af US-tropper blev reguleret via NATO-traktaten og specielle hemmelige[8] administrative aftaler, der blev anset for hensigtsmæssige for de eksisterende forbindelser mellem regeringerne i UK og USA med henblik på et fælles forsvar.[9] Stationen er en integral del af det amerikanske forsvarsministeriums verdensomspændende netværk, der understøtter UK, USA og NATO-interesser.[10]

Iårsberetningen for 1999/2000 understreges udtrykkeligt den værdi, det snævre samarbejde under UKUSA-aftalen har, og som genspejles i kvaliteten af de efterretningsmæssige resultater. Der henvises navnlig til, at GCHQ, da NSA-anlæggene faldt ud i tre dage, udover UK-kunderne også direkte betjente US-kunderne.[11]

---

[1] Transcript, 7.3.2000, http://cryptome.org/Echelon-cia.htm
[2] James Woolsey, Why America Spies on its Allies, The Wall Street Journal, 22.3.2000, 31
[3] Commons Written Answers, House of Commons Hansard Debares
[4] 12.7.1995.
[5] 25.10.1994
[6] 3.12.1997
[7] 12.5.2000
[8] 12.7.1995
[9] 8.3.1999, 6.7.1999
[10] 3.12.1997
[11] Intelligence and Security Committee, Annual Report 1999-2000, s. 14, forelagt parlamentet af premierministeren i november 2000

5.8.3. Udtalelser fra australsk side[1]

Martin Brady, direktør for den australske efterretningstjeneste, DSD[2], bekræftede i en skrivelse til programmet "Sunday" på den australske senders "Channel 9", at DSD i UKUSA-regi samarbejder med andre efterretningstjenester. I samme skrivelse understreges, at samtlige Australiens efterretningsmæssige tjenester drives af australske tjenester alene eller sammen med amerikanske tjenester. I de tilfælde, hvor anlæg drives i fællesskab, er den australske regering fuldt bekendt med alle aktiviteter, og australsk personale deltager på alle niveauer.[3]

5.8.4. Udtalelser fra nederlandsk side

Den 19. januar 2001 forelagde den nederlandske forsvarsminister det nederlandske parlament en rapport om tekniske og retlige aspekter af global aflytning af moderne telekommunikationssystemer.[4] Den nederlandske regering indtager heri den holdning, at det, selv om den ikke er i besiddelse af egen viden, på grundlag af de disponible oplysninger fra anden side er meget sandsynligt, at Echelon-netværket eksisterer, men at der også er andre systemer med samme muligheder. Den nederlandske regering kommer til den konklusion, at global aflytning af kommunikationssystemer ikke er begrænset til de stater, der deltager i Echelon-systemet, men også gennemføres af regeringsmyndigheder i andre lande.

5.8.5. Udtalelser fra italiensk side

Luigi Ramponi, tidligere direktør for den italieniske efterretningstjeneste SISMI, giver i et interwiev i dagbladet "il mondo" udtryk for, at der ikke er tvivl om, at "Echelon" eksisterer.[5] Ramponi erklærer udtrykkeligt, at han i sin egenskab af chef for SISMI vidste besked om Echelon's eksistens. Siden 1992 havde han været orienteret om stærke aflytningsaktiviteter vedrørende bølger af lav, mellem og høj frekvens. Da han i 1991 begyndte hos SISMI, beskæftigede man sig mest med Det Forenede Kongerige og De Forenede Stater.

5.9. Parlamentsrapporter

5.9.1. Rapporter fra det belgiske kontroludvalg Comité Permanent R

Det belgiske kontroludvalg, Comité Permanent R, har allerede behandlet Echelon i to rapporter.

Rapporten "Rapport d'activités 1999" drejede hele kapitel 3 sig om, hvordan de belgiske efterretningstjenester reagerer på den mulige eksistens af et Echelon-system til kommunikationsovervågning. Rapporten på godt 15 sider konkluderer, at de to belgiske efterretningstjenester, Sûreté de l'Etat og Service général du Renseignement (SGR), kun har modtaget information om Echelon via offentlige dokumenter.

---

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

[2] Defence Signals Directorate, australsk efterretningstjeneste, der driver SIGINT.

[3] Skrivelse fra Martin Brady, direktør for DSD af 16.marts 1999 til Ross Coulthart, Sunday Program; Sml. også:
http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp;
http://sunday.ninemsn.com/01_cover_stories/article_335.asp

[4] Skrivelse til det nederlandske Andetkammer om "Het grootschalig afluisteren van moderne telecommunicatiesystemen" af 19.01.01.

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

Den anden rapport "Rapport complémentaire d'activités 1999" beskæftiger sig væsentligt mere indgående med Echelon-systemet. Den tager stilling til STOA-undersøgelserne og bruger en del af fremstillingen på at beskrive de tekniske og lovgivningsmæssige rammebetingelser for aflytning af telekommunikation. Rapporten konkluderer, at Echelon rent faktisk eksisterer og også er i stand til at aflytte alle informationer, der transmitteres via satellit (ca. 1% af alle internationale telefonsamtaler), hvis der anvendes søgeord, og at dets kapacitet med hensyn til kryptering er betydeligt større end angivet fra amerikansk side. Der er fortsat tvivl om udsagnene om, at der ikke finder industrispionage sted i Menwith Hill. Det understreges udtrykkeligt, at det er umuligt at konstatere med sikkerhed, hvilke aktiviteter Echelon driver.

5.9.2. Rapport fra den franske Nationalforsamlings Udvalg for Nationalt Forsvar

I Frankrig forelagde Udvalget for Nationalt Forsvar en rapport om aflytningssystemer for Nationalforsamlingen[1].

Efter en udførlig drøftelse af en lang række aspekter konkluderer ordføreren, Arthur Paecht, at Echelon eksisterer, og at der er tale om det eneste kendte multinationale overvågningssystem. Systemets kapacitet er reel, men har dog nået sine grænser, ikke kun fordi indsatsen ikke længere kan stå mål med den eksplosive vækst i kommunikationen, men også fordi bestemte mål har fundet ud af at beskytte sig.

Echelon-systemet har fjernet sig fra sine oprindelige mål, der var udformet ud fra konteksten under den kolde krig, således at det ikke er umuligt at anvende de indsamlede informationer til politiske og økonomiske formål mod andre NATO-stater.

Echelon kan absolut udgøre en fare for grundlæggende frihedsrettigheder, og der opstår adskillige problemer i denne forbindelse, som der skal findes et svar på. Det er forkert at forestille sig, at de stater, der er medlem af Echelon, vil opgive deres aktiviteter. Flere indicier synes snarere at pege i retning af, at der bliver skabt et nyt system med nye samarbejdspartnere for at overvinde Echelons grænser med nye midler.

[1] 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 Assemblé nationale, enregisté à la Présidence de l'Assemblée nationale le 11 octobre 2000.

6. Kan der findes andre globale aflytningssystemer?

6.1. Forudsætninger for et sådant system

6.1.1. Teknisk-geografiske forudsætninger

Til aflytning af international kommunikation, der transmitteres via førstegenerationssatellitter kræves der modtagestationer i Atlanterhavsområdet, i Det Indiske Ocean og i Stillehavsområdet. I forbindelse med den nyere generation af satellitter, der muliggør transmission i underområder, stilles der yderligere krav til aflytningsstationernes geografiske placering, hvis den samlede kommunikation, der transmitteres via satellit, skal aflyttes.

Et yderligere globalt arbejdende aflytningssystem vil være tvunget til at oprette stationer uden for Echelon-staternes territorium.

6.1.2. Politisk-økonomiske forudsætninger

Oprettelse af et sådant verdensomspændende arbejdende aflytningssystem må imidlertid også være økonomisk og politisk hensigtsmæssigt for operatørerne. Brugerne af et sådant system må have globale økonomiske, militære eller andre sikkerhedsinteresser, eller i det mindste tro, at de hører til de såkaldte verdensmagter. Dermed begrænses kredsen i princippet til Kina og G8-staterne uden USA og UK.

6.2. Frankrig

Frankrig har egne territorier, departementer og andre lokale strukturer i alle de tre ovenfor anførte områder.

I Atlanterhavsområdet ligger øst for Canada Saint Pierre og Miquelon (65° W / 47° N), nordøst for Sydamerika Guadeloupe (61° W / 16° N) og Martinique (60° W / 14° N) og ved Sydamerikas nordkyst Guyana (52° W / 5° N).

I Det Indiske Ocean ligger øst for det sydlige Afrika Mayotte (45° O / 12° S) og La Réunion (55° O / 20° S) og helt sydpå Terres Australes og Antarticques Francaises. I Stillehavsområdet ligger Ny Kaledonien (165° O / 20° S), Wallis og Futana (176° W / 12° S) samt Fransk Polynesien (150° W / 16° S).

Der foreligger kun meget lidt om eventuelle franske stationer under den franske efterretningstjeneste DGSE (Direction générale de la sécurité extérieur) i disse oversøiske områder. Ifølge oplysninger fra franske journalister[1] findes der stationer i Kourou i Fransk Guyana og i Mayotte. Der foreligger intet om stationernes størrelse, antallet af satellitenantenner og disses størrelse. Andre statione hævdes at ligge i Frankrig i Domme i nærheden af Bordeaux og i Alluetts-le-Roi i nærheden af Paris. Antallet af satellitparaboler anslår Jauvert til i alt 30. Forfatteren Schmidt-Enboom[2] hævder, at der også drives en station i Ny Kaledonien.

Teoretisk set vil Frankrig også kunne drive et globalt aflytningssystem. Ordføreren disponerer imidlertid ikke over tilstrækkelige offentligt tilgængelige oplysninger til at kunne fremsætte seriøse påstande.

6.3. Rusland

Den russiske efterretningstjeneste FAPSI, der er ansvarlig for kommunikationssikkerhed og SIGINT, hævdes sammen med den russiske militære efterretningstjeneste GRU at drive aflytningsstationer i Letland, Vietnam og Cuba.

I Atlanterhavsområdet ligge ifølge oplysninger fra Federation of American Scientists en station i Lourdes på Cuba (82°W, 23°N), som drives sammen med den cubanske efterretningstjeneste. I Det Indiske Ocean ligger stationer i Rusland, som der ikke foreligger nærmere oplysninger om, samt en station i Skrunda in Letland. I Stillehavsområdet hævdes der at være en station i Cam Rank Bay i Nord Vietnam. Der foreligger ingen enkeltheder om stationerne, for så vidt angår antal antenner og disses størrelse.

Sammen med stationerne i selve Rusland muliggør dette teoretisk set global dækning. Heller ikke her er de foreliggende oplysninger tilstrækkelige til seriøse påstande.

6.4. De øvrige G-8 stater og Kina

Hverken de øvrige G8-stater eller Kina har eget territorium eller nære forbundsfæller i de nødvendige dele af verden, der muliggør drift af et globalt aflytningssystem.

---

[1] Jean Guisnel, Léspionage nést 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.
[2] E.Schmidt-Eenboom, i: Streng Geheim, Museumsstiftung Post und Telekommunikation, Heidelberg 1999, s.180.

7. Foreneligheden af kommunikationsaflytningssystemer af "Echelon"-typen med EU-retten

7.1. Bemærkninger

Udvalgets mandat omfatter bl.a. den udtrykkelige opgave at undersøge foreneligheden af et kommunikationsaflytningssystem af "Echelon"-typen med EU-retten.[1] Det vil navnlig blive vurderet, om et sådant system vil være foreneligt med de to databeskyttelsesdirektiver, 95/46/EF og 97/66/EF, med EF-traktatens art. 286 og Unionstraktatens art. 8, stk. 2.

Det forekommer nødvendigt at foretage vurderingen ud fra to forskellige synspunkter. Det første aspekt fremgår af det i kapital 5 anførte indiciebevis, hvoraf det fremgår, at det system, der kaldes "Echelon", er udformet som et kommunikationsaflytningssystem, som via indsamling og evaluering af kommunikationsdata skal give den amerikanske, canadiske, australske og newzealandske efterretningstjeneste oplysninger om forhold i udlandet. Der er dermed tale om et klassisk spionageinstrument for efterretningstjenester.[2] Som et første skridt undersøges derfor et sådan efterretningssystems forenelighed med EU-retten.

Derudover har Campell i den forelagte STOA-rapport kritiseret, at dette system er blevet misbrugt til konkurrencespionage, og at de europæiske landes økonomier som følge deraf har lidt store tab. Desuden har den tidligere CIA-direktør R. James Woolsey udtalt, at USA ganske vist udspionerer europæiske virksomheder, men kun for at sikre ligevægt på markedet, da kontrakter kun kunne opnås via bestikkelse.[3] Er det korrekt, at systemerne anvendes til konkurrencespionage, dukker spørgsmålet om foreneligheden med EU-retten op på ny. Dette andet aspekt vil derfor blive behandlet separat i en senere fase.

7.2. Det efterretningstjenestelige systems forenelighed med EU-retten

7.2.1. Forenelighed med EF-retten

Aktiviteter og foranstaltninger vedrørende statssikkerhed, hhv. strafforfølgelse, omfattes principielt ikke af EF-traktatens bestemmelser. Da Det Europæiske Fællesskab på grund af princippet om begrænset enekompetence kun kan agere, hvor det har kompetence til det, har det derfor i databeskyttelsesdirektiverne, der er baseret på EF-traktaten, navnlig dennes art. 95 (ex-artikel 100 A), udtrykkeligt undtaget disse områder fra anvendelsesområdet. Direktiv 59/46/EG om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger[4] og direktiv 97/66/EF om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren[5]

[1] Sml. ovenfor, kapitel 1, 1.3.

[2] Sml. Kapitel 2.

[3] *Sml. kapitel 5, 5.6. og 5.8.*

[4] EFT L 281 af 23.11.1995, s. 31.

[5] EFT L 24 af 30.1.1998, s. 1.

gælder ikke for behandling[1]/aktiviteter[2],"der vedrører den offentlige sikkerhed, forsvar, statens sikkerhed (herunder statens økonomiske interesser, når behandlingen er forbundet med spørgsmål vedrørende statens sikkerhed) og statens aktiviteter på det strafferetlige område". Samme formulering er overtaget i det direktivforslag om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor[3] , Parlamentet i øjeblikket har til behandling. En medlemsstats deltagelse i et aflytningssystem, der tjener statens sikkerhed, kan dermed ikke stride mod databeskyttelsesdirektiverne.

Lige så lidt kan der være tale om en overtrædelse af EF-traktatens art. 286, der udvider anvendelsesområdet for databeskyttelsesdirektiverne til også at omfatte Fællesskabets institutioner og organer. Det samme gælder for forordning 45/2001 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger.[4] Også denne forordning kan kun anvendes, for så vidt som organerne handler inden for rammerne af EF-traktaten.[5] For at hindre misforståelser skal det her udtrykkeligt understeges, at det aldrig fra nogen side er hævdet, at fællesskabsorganer og
-institutioner deltager i et aflytningssystem, og at ordføreren heller ikke har holdepunkter i denne retning.

7.2.2. Forenelighed med anden EU-ret

For så vidt angår områderne omfattet af afsnit V (fælles udenrigs- og sikkerhedspolitik) og VI (politisamarbejde og samarbejde og retligt samarbejde i kriminalsager), er der ingen databeskyttelsesbestemmelser, der kan sammenlignes med EF-direktiverne. Europa-parlamentet har allerede gentagne gange påpeget, at der her er et stor behov for handling.[6]
Beskyttelsen af personers grundlæggende rettigheder og frihedsrettigheder sikres på disse områder kun gennem EU-traktatens artikel 6 og 7, navnlig art. 6, stk. 2, hvori Unionen forpligter sig til at respektere de grundlæggende rettigheder, således som disse garanteres ved den europæiske menneskerettighedskonvention, og som de følger af medlemsstaternes fælles forfatningsmæssige traditioner. I tilknytning til medlemsstaternes forpligtelse til at respektere de grundlæggende rettigheder og navnlig den europæiske menneskerettighedskonvention (sml. nedenfor i kapitel 8) opstår der dermed en forpligtelse for Unionen til at respektere de grundlæggende rettigheder i forbindelse med dens lovgivningsmæssige og administrative aktiviteter. Da der imidlertid hidtil ikke på EU-plan er sket nogen regulering af kompetencen til overvågning af telekommunikation til sikkerhedsmæssige eller efterretningstjenstelige

[1] Art. 3, stk. 2, i direktiv 95/46.
[2] Art. 1, stk. 3, i direktiv 97/66.
[3] KOM (2000) 385 EFT C 365 E/223.

[4] Forordning (EG) nr. 45/2001, EFT 2001 L 8, s.1.

[5] Art. 3, stk. 1; sml. også betragtning 15: Når denne behandling finder sted i fællesskabsinstitutioner og -organer som led i udøvelsen af aktiviteter, som ikke hører under denne forordnings anvendelsesområde, navnlig de aktiviteter, der er omhandlet i afsnit V og VI i traktaten om Den Europæiske Union, sikres beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder under overholdelse af artikel 6 i traktaten om Den Europæiske Union. Aktindsigt, herunder betingelserne for aktindsigt i dokumenter, som indeholder personoplysninger, hører under de bestemmelser, der er vedtaget på grundlag af traktatens artikel 255, hvis anvendelsesområde også omfatter afsnit V og VI i traktaten om Den Europæiske Union.
[6] Sml. f.eks. punkt 25 i beslutningen om Rådets og Kommissionens forslag til handlingsplan for, hvorledes Amsterdam-traktatens bestemmelser om indførelse af et område med frihed, sikkerhed og retfærdighed bedst kan gennemføres (13844/98 - C4-0692/98 - 98/0923(CNS)),EFT. C 219 af 30.7.1999, s. 61 ff.

formål[1], er spørgsmålet om overtrædelse af EU-traktatens art. 6, stk. 2, ikke i øjeblikket relevant.

7.3. Spørgsmålet om foreneligheden, hvis systemet misbruges til økonomisk spionage

Hvis en medlemsstat støtter et aflytningssystem, der også driver konkurrencespionage, ved at anvende de nationale efterretningstjenester hertil, hhv. stiller territorium til rådighed for fremmede efterretningstjenester med dette sigte, vil der dog være tale om overtrædelse af EF-retten. Medlemsstaterne er nemlig i henhold til EF-traktatens art. 10 forpligtet til omfattende loyalitet, navnlig til at afholde sig fra alle foranstaltninger, der kan bringe virkeliggørelsen af traktatens mål i fare. Selv om aflytning af telekommunikation ikke sker til fordel for det nationale erhvervsliv (hvilket i øvrigt i virkningen ville svare til statsstøtte, og dermed ville udgøre en overtrædelse af EF-traktatens artikel 87), men til fordel for tredjelande, ville en sådan aktivitet være i direkte modstrid med det koncept om det fælles marked, der ligger til grund for EF-traktaten, da den vil medføre forvridning af konkurrencen.

En sådan adfærd vil i øvrigt efter ordførerens mening udgøre en krænkelse af databeskyttelsesdirektivet for telekommunikationsområdet[2], da spørgsmålet om direktivernes anvendelighed må løses efter funktionelle synspunkter og ikke efter organisatoriske. Dette fremgår ikke blot af ordlyden af retsakten om anvendelsesområdet, men også af retsaktens hensigt. Anvender efterretningstjenester deres kapaciteter til økonomisk spionage, gennemføres aktiviteterne ikke med henblik på sikkerhed og strafforfølgelse, men med et forkert formål og omfattes dermed fuldt ud af direktivets anvendelsesområde. Dette forpligter i art. 5 medlemsstaterne til at sikre telekommunikationshemmeligheden, navnlig ved at forbyde "aflytning, registrering, lagring og andre måder, hvorpå samtaler kan opfanges eller overvåges af andre end brugerne". Ifølge art. 14 må der kun ske undtagelse, når dette er nødvendigt af hensyn til statens sikkerhed, forsvaret og retsforfølgning. Da økonomisk spionage ikke legitimerer undtagelser, ville der i så fald være tale om overtrædelse af fællesskabsretten.

7.4. Resultat

Sammenfattende kan det siges, at et efterretningssystem af Echelon-typen i den nuværende situation derfor ikke kan stride mod EU-retten, da det ikke udviser de berøringspunkter med EU-retten, der kræves for at der er tale om uforenelighed. Dette gælder ganske vist kun, så længe systemet virkelig udelukkende anvendes med sigte på statens sikkerhed. Anvendes det

[1] For så vidt angår overvågning af telekommunikation, findes der på EU-plan i øjeblikket kun to retsakter, hvoraf ingen regulerer spørgsmålet om kompetence:

- Rådets resolution af 17. januar 1995 om lovlig aflytning af telekommunikation (EFT C 329 af 4.11.1996), der i bilaget indeholder tekniske krav til gennemførelse af lovlige overvågningsforstaltninger i moderne telekommunikationssystemer, og

- Rådets retsakt af 29. maj 2000 om udarbejdelse i henhold til artikel 34 i traktaten om Den Europæiske Union af konventionen om gensidig retshjælp i straffesager mellem Den Europæiske Unions medlemsstater (EFT C 2000 C 197/1, art. 17 f), hvori det reguleres, på hvilke vilkår retshjælp i straffesager vedrørende telekommunikationsovervågning skal være mulig. De aflyttedes rettigheder begrænses på ingen måde herved, da den medlemsstat, i hvilken den aflyttede befinder sig, altid kan nægte retshjælp, hvis denne ikke er lovlig i henhold til den pågældende stats nationale ret.

[2] Direktiv 97/66/EF, EFT L 24 1998, s. 1.

derimod til andet formål og til konkurrencespionage mod udenlandske virksomheder, strider det mod EU-retten. Hvis en medlemsstat deltager i noget sådant, overtræder den fællesskabsretten.

8. Efterretningstjenesters kommunikationsovervågning og foreneligheden heraf med den grundlæggende ret til privatsfæren

8.1. Kommunikationsovervågning som et indgreb i den grundlæggende ret til privatsfæren

Enhver aflytning af kommunikation, ja sågar enhver tapning af data, som foretages af efterretningstjenester til dette formål[1] er et alvorligt indgreb i den enkeltes privatsfære. Kun i en "politistat" er uindskrænket aflytning fra statens side tilladelig. I EU-medlemsstaterne, som derimod er fuldtudviklede demokratier skal statsorganer og derved også efterretningstjenester ubetinget respektere retten til privatlivets fred, som som regel er nedfældet i medlemsstaternes forfatninger. Privatsfæren nyder således en særlig beskyttelse, og indgreb i denne ret er kun tilladt efter overvejelse af retsgoderne og under hensyntagen til proportionalitetsprincippet.

Også i Echelon-staterne er man sig denne problematik bevidst. De gældende bestemmelser for beskyttelse af privatsfæren finder imidlertid kun anvendelse på landets egne borgere, og den europæiske borger kan derfor som regel ikke påberåbe sig disse bestemmelser. I de amerikanske love, der fastlægger betingelserne for elektronisk overvågning, afvejes den interesse, som staten har i en funktionsdygtig efterretningstjeneste, ikke mod betydningen af en effektiv generel beskyttelse af grundlæggende rettigheder, men mod den fornødne beskyttelse af amerikanske statsborgeres privatsfære ("US-Persons").[2]

8.2. Beskyttelse af privatsfæren gennem internationale aftaler

Respekten for privatsfæren som grundret er optaget i mange folkeretlige aftaler[3] På verdensplan bør navnlig henvises til den internationale konvention om borgerlige og politiske rettigheder"[4] , som blev vedtaget inden for rammerne af FN i 1966. Artikel 17 i denne konvention omhandler beskyttelsen af privatsfæren. I forbindelse med klager over andre stater har alle Echelon-stater har underlagt sig de beslutninger, der træffes af den Menneskerettighedskomité, som er nedsat i henhold til konventionens artikel 41. USA har

[1] 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."

[2] Se rapport til den amerikanske kongres af slutningen af februar 2000: "Legal Standards for the Intelligence Community in Conducting Electronic Surveillance", http://www.fas.org/irp/nsa/standards.html, der henviser til Foreign Intelligence Surveillance Act (FISA), i Titel 50 Kapitel 36 U.S.C. § 1801 ff og Exec. Order No. 12333, 3 C.F.R. 200 (1982), i Titel 50, Kapitel 15 U.S.C. § 401 ff , http://www4.law.cornell.edu/uscode/50/index.html.

[3] Art. 12 Verdenserklæring om menneskerettigheder; Art. 17 FN's internationale konvention om borgerlige og politiske rettigheder; Art. 7 i EU-charteret, Art. 8 EMK; OECD-rådets henstilling om retningslinjer vedrørende informationssystemers sikkerhed, vedtaget den 26./27.11.1993 C(92) 188/Final; Art. 7 i Europarådets konvention om beskyttelse af det enekelte menneske i forbindelse med elektronisk databehandling; Jfr. STOA-rapportenom overvågningsteknologiens udvikling samt risikoen for misbrug af økonomiske oplysninger; 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

[4] FN's internationale konvention om borgerlige og politiske rettigheder, vedtaget af FN's generalforsamling den 16. 12. 1966

dog ikke underskrevet tillægsprotokollen[1], som udvider Menneskerettighedskomiteens beføjelser til også at omfatte klager fra den enkelte borger. Den enkelte har derfor i tilfælde af krænkelse af konventionen ingen mulighed for at indbringe en sag mod USA for Menneskerettighedskomiteen.

Også på EU-plan forsøger man at gennemføre en særlig europæisk beskyttelse af grundretten ved indførelse af et EU-charter om grundlæggende rettigheder. I charterets artikel 7 under overskriften "Respekt for privatlivet og familielivet", nævnes retten til respekten for den enkeltes kommunikation sågar eksplicit[2]. Desuden fastlægges i artikel 8 grundretten til "Beskyttelse af personoplysninger". Det kunne beskytte den enkelte borger i de tilfælde, hvor vedkommendes personoplysninger behandles (elektronisk eller på anden vis), hvad der som regel er tale om ved aflytning og altid er tilfældet ved anden opsnapning.

Charteret er indtil videre ikke inkorporeret i traktaten. Dets bindende virkning gælder derfor kun de tre institutioner, som ved den højtidelige deklaration i Nice den 7. december 2000 har underkastet sig dets bestemmelser: Rådet, Kommissionen og Europa-Parlamentet. De er , så vidt det er ordføreren bekendt, ikke involveret i efterretningsvirksomhed. Også hvis charteret får fuld virkning ved optagelse i traktaten, må der tages hensyn til dets begrænsede anvendelsesområde. I henhold til artikel 51 er charteret "rettet til Unionens institutioner og organer ... samt til medlemsstaterne, dog kun når de gennemfører EU-retten." Charteret ville derved have relevans for forbuddet mod konkurrenceforvridende statsstøtte (jf. kapitel 7.7.3.)

Den europæiske menneskerettighedskonvention er det eneste effektive instrument på internationalt plan i forbindelse med beskyttelse af privatsfæren.

8.3. Den europæiske menneskerettighedskonvention (EMK)

8.3.1. EMK's betydning for EU

Den beskyttelse af de grundlæggende rettigheder, som ydes ved EMK, får særlig betydning derved, at alle EU-medlemsstater har ratificeret konventionen og at den danner et ensartet europæisk beskyttelsesniveau. Signatarstaterne har indgået en folkeretlig forpligtelse til at sikre de rettigheder, der er fastlagt i EMK og har underlagt sig de domme, der afsiges af Menneskerettighedsdomstolen i Strasbourg. Nationale bestemmelser kan derfor efterprøves af Menneskerettighedsdomstolen på deres overensstemmelse med EMK og signatarstaterne kan i tilfælde af en krænkelse af menneskerettighederne dømmes og forpligtes til at udbetale en erstatning. Desuden har EMK vundet i betydning, idet De Europæiske Fællesskabers Domstol i sine afgørelser i forbindelse med efterprøvning af love gentagne gange har henvist dertil sammen med medlemsstaternes retsgrundsætninger. Med Amsterdam-traktaten blev EU's forpligtelse til at respektere de grundlæggende rettigheder, således som de er garanteret i EMK, optaget i traktaten, jf. artikel 6, stk. 2.

8.3.2. Rækkevidden af EMK's rumlige og personlige beskyttelse

Rettighederne, der garanteres i EMK, er universelle menneskerettigheder og er derfor ikke

[1] Fakultativ protokol til den internationale konvention om borgerlige og politiske rettigheder, vedtaget af FN's generalforsamling den 19.12.1966.
[2] "Enhver har ret til privatliv og familieliv, sit hjem og sin kommunikation."

bundet til et statsborgerforhold. De garanteres enhver person under de kontraherende parters jurisdiktion. Det betyder, at menneskerettighederne skal garanteres i en stats territorium som helhed, og at lokale undtagelser er en overtrædelse af konventionen. Desuden gælder de også uden for en kontraherende stats territorium, i det omfang hvor der er tale om statens højhedsområde. Rettighederne i henhold til EMK i forhold til en signatarstat tilkommer også personer uden for territoriet, hvis en signatarstat uden for sit territorium griber ind i privatsfæren[1].

Det sidste er navnlig vigtigt, fordi der er den særlige aspekt ved grundretsspørgsmålet i forbindelse med telekommunikationsovervågning, at der kan være langt mellem den stat, der er ansvarlig for overvågningen, den overvågede og stedet for den konkrete aflytning. Det gælder navnlig for international kommunikation, men i visse omstændigheder også for national kommunikation, hvis oplysningerne overføres via udenlandske ledninger. Det er typisk tilfældet ved udenlandske efteretningstjenesters fremgangsmåde. Og det kan ikke udelukkes, at en efterretningstjeneste videregiver oplysningerne fra en overvågning til andre stater.

8.3.3. Telekommunikationsovervågning og artikel 8 i EMK

I henhold til artikel 8, stk. 1 i EMK har "enhver […] ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance." Beskyttelsen af telefonsamtaler og telekommunikation nævnes ikke eksplicit, men er efter Menneskerettighedsdomstolens afgørelser i kraft af begrebet "privatliv" og "korrespondance" omfattet af den beskyttelse, som ydes ved artikel 8 i EMK.[2] Beskyttelsen af denne grundret omfatter ikke kun kommunikationens indhold, men også registrering af yderligere data vedrørende samtalen. Det betyder, at der også er tale om en krænkelse af privatsfæren, hvis en efterretningstjeneste kun registrerer data, såsom forbindelsens tidspunkt og varighed og de valgte numre.[3] Grundretten i henhold til artikel 8, stk. 2 i EMK er ikke uindskrænket. Indgreb i denne ret kan være tilladt, hvis der er retsgrundlag dertil i den nationale lovgivning.[4] Bestemmelsen skal være almen tilgængelig og dens konsekvenser skal være forudsigelige.[5]

Medlemsstaterne er ikke frit stillet med hensyn til gennemførelsen af disse indgreb. I artikel 8 i EMK er de kun tilladt til formål, der er opført i stk. 2; det er navnlig hensynet til den nationale sikkerhed, den offentlige tryghed og orden, forebyggelse af forbrydelser, men også

---

[1] Jf. Menneskerettighedsdomstolen, Loizidou/Türkei, 23.3.1995, Z 62 med yderligere henvisninger "...the concept of 'jursidiction' 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" med henvisning til Menneskerettighedsdomstolen, Drozd og Janousek, 26.6.1992, Z 91. Jf. Jacobs, The European Convention on Human Rights (1996), 21 ff

[2] Jf. Menneserettighedsdomstolen , Klass m.fl.., 6.9.1978, Z 41.

[3] Jf. Menneskerettighedsdomstolen, Malone, 2.8.1984, Z 83 ff; og Davy, B/Davy/U, Aspekte staatlicher Informationssammlung und Art. 8 MRK, JBl 1985, 656.

[4] Efter Menneskerettighedsdomstolens retspraksis (særlig Sunday Times, 26.4.1979, Z 46 ff, Silver m.fl.., 25.3.1983, Z 85 ff) omfatter begrebet "lov" i Art. 8, stk. 2 , ikke kun lov i ordets formelle forstand, men også retsforskrifter på et lavere trin, i visse tilfælde sågar uskrevet ret. Den pågældende skal dog til enhver tid kunne vide, under hvilke omstændigheder et sådant indgreb er muligt. Jf. Wessley, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht? ÖJZ 1999, 491 ff, 495

[5] Silver m.fl.., 25.3.1983, Z 87 f

landets økonomiske velfærd[1], hvilket imidlertid ikke berettiger økonomisk spionage, da artiklen kun omfatter indgreb, som "er nødvendigt i et demokratisk samfund". Til hvert indgreb vælges det mest lempelige middel, der kan føre til resultat, og der må desuden være fyldestgørende garantier mod misbrug.

8.3.4. Betydningen af artikel 8 i EMK for efterretningsvirkomhed

Hvis efterretningstjenesterne i deres virke skal respektere de grundlæggende rettigheder, betyder disse generelle principper følgende : hvis det af hensyn til den nationale sikkerhed synes at være nødvendigt, at efterretningstjenester skal kunne aflytte telekommunikationsindhold eller i det mindste registrere oplysninger om forbindelser, skal en sådan bestemmelse optages i den nationale lovgivning. Bestemmelsen skal være almen tilgængelig og konsekvenserne for borgeren skal være forudsigelige, samtidig med at der tages hensyn til de særlige krav med hensyn til fortrolighed. Menneskerettighedsdomstolen har i en udtalelse om, hvorvidt tjenestemænds hemmelige kontrol i forbindelse med sager, der berører den nationale sikkerhed, er i overensstemmelse med konventionens artikel 8, fastslået, at man i dette særlige tilfælde ikke kan påberåbe sig kravet om forudsigelighed som i andre tilfælde.[2] Domstolen har også krævet, at det altid skal fremgå af loven, under hvilke omstændigheder og på hvilke betingelser den offentlige anklager kan indlede et hemmeligt og derved potentielt farligt indgreb i privatsfæren.[3]

Hvis efterretningsvirksomhed skal ske i overensstemmelse med menneskerettighederne, må man være opmærksom på, at skønt hensynet til den nationale sikkerhed er en berettigelse, skal den i henhold til artikel 8, stk. 2 i EMK følge proportionalitetsprincippet. Heller ikke den nationale sikkerhed kan bruges som berettigelse, med mindre det er nødvendigt i et demokratisk samfund. Menneskerettighedsdomstolen har entydig fastslået, at en stats interesse i at beskytte den nationale sikkerhed må afvejes mod indgrebets vægt og borgerens interesse i respekten for hans/hendes privatsfære.[4] Indgrebene er ikke begrænset til det strengt nødvendige, men det er ikke tilstrækkeligt, at de blot er nyttige eller ønskværdige.[5] Den opfattelse, at aflytning af al telekommunikation er den bedste beskyttelse mod organiseret kriminalitet, ville værre i strid med artikel 8 i EMK, selv om den skulle være tilladt i henhold til national lovgivning.

På grund af efterretningsaktiviteternes særlige karakter, som kræver hemmeligholdelse og derved en særlig afvejelse af interesser, er der desto mere brug for gode kontrolmuligheder. Domstolen har eksplicit påpeget, at et hemmeligt overvågningssystem med henblik på den nationale sikkerhed rummer den fare, at det under foregivende af at forsvare demokratiet undergraver eller sågar forstyrrer det. Derfor er det nødvendigt med adækvate og effektive garantier mod sådant misbrug.[6] En efterretningstjenestes legitime virksomhed er kun i

[1] Menneskerettighedsdomstolen har i et tilfælde accepteret "den økonomiske velfærd" som berettiget grund. Det drejede sig om videregivelse af medicinske oplysninger, som var vigtige for tildeling af offentlige ydelser. M.S./Schweden, 27.8.1997, Z 38, og i et tilfælde, hvor der var tale om udvisning fra Nederlanden af en person , som levede af bistandsydelser, efter at grunden for hendes opholdstilladelse var bortfaldet. Ciliz/Nederlandene, 11.7.2000, Z 65.

[2] Menneskerettighedsdomstolen, Leander, 26.3.1987, Z 51

[3] Menneskerettighedsdomstolen, Malone, 2.8.1984, Z 67

[4] Menneskerettighedsdomstolen, Leander, 26.3.1987, Z 59, Sunday Times, 26.4.1979, Z 46 ff

[5] Menneskerettighedsdomstolen, Silver m.fl., 24.10.1983, Z 97

[6] Menneskerettighedsdomstolen, Leander, 26.3.1987, Z 60.

overensstemmelse med de grundlæggende rettigheder, hvis den pågældende EMK-stat har etableret fyldestgørende kontrolsystemer og andre garantier mod misbrug. Domstolen henviste i den sammenhæng til Sverige og tillagde tilstedeværelsen af parlamentarikere i politiets kontrolorgan, og overvågningen ved justitsministeren, parlamentets ombudsmand og retsudvalget stor betydning. Ud fra denne betragtning forekommer det betænkeligt, at Frankrig, Grækenland, Irland, Luxemburg og Spanien ikke har et tilsynsudvalg for efterretningstjenester[1] og at de heller ikke har et kontrolsystem, som kan sidestilles med den parlamentariske ombudsmand i de nordiske lande.[2] Det er derfor glædeligt, at forsvarsudvalget i den franske Assemblée Nationale bestræber sig på nedsættelse af et kontroludvalg[3], navnlig fordi Frankrig i teknisk og geografisk henseende råder over bemærkelsesværdige kapaciteter inden for efterretningsvirksomhed.

8.4. Pligten til at være på vagt over for udenlandske efterretningstjenester

8.4.1. Omgåelse af artikel 8 i EMK ved at inddragelse af udenlandske efterretningstjenester

Som det allerede er udførligt belyst, skal signatarstaterne opfylde en række forudsætninger for at sikre, at deres efterretningstjenester opfylder forpligtelserne i henhold til artikel 8 i EMK. Det siger sig selv, at disse efterretningstjenester ikke kan frigøre sig for disse forpligtelser ved at gribe tilbage til andre efterretningstjenester, som er underlagt mindre strenge regler. Ellers ville legalitetsprincippet og dets to elementer - tilgængelighed og forudsigelighed - være gjort virkningsløse og Menneskerettighedsdomstolens retspraksis indholdsmæssigt svækket.

Det betyder for det første, at udveksling af data mellem efterretningstjenester er underkastet begrænsninger. En efterretningstjeneste kan kun få oplysninger fra en anden efterretningstjeneste, hvis videregivelsen er i overensstemmelse med landets egen lovgivning. Den ved lov fastsatte rækkevidde af efterretningstjenesternes aktioner må ikke udvides ved aftaler med andre tjenester. Ligeledes må den kun udføre efterretningsvirksomhed for en anden efterretningstjeneste efter dennes anvisninger, når den har forvisset sig om , at de er i overensstemmelse med gældende national ret. Selv om oplysninger er beregnet til en anden stat, ændrer det intet ved det forhold, at et indgreb, som ikke er forudsigeligt for borgeren, er en krænkelse af denne persons grundret.

For det andet må EMK-staterne ikke lade fremmede efterretningstjenester udføre deres virke på deres højhedsområde, hvis der foreligger begrundet formodning om, at de udenlandske tjenesters virksomhed ikke opfylder forpligtelserne i henhold til EMK..[4]

---

[1] Ordføreren er bekendt med, at hverken Luxemburg eller Irland har en udenlandsk efterreetningstjeneste og at de ikke driver Sigint. Kravet om en særlig kontrolinstans vedrører her kun efterretningstjenester inden for landets grænser.

[2] For kontrollen med efterretnignstjenester i medlemsstaterne jf. kapitel 9.

[3] Jf. det franske lovforslag ("Proposition de loi tendant à la création de délégations parlementaires pour le renseignement") og betænkningen herom af parlamentsmedlem Arthur Paecht, N° 1951 Assmeblée nationale, 11. Legislaturperiode, registreret den 23. november 1999

[4] Jf. også 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.

8.4.2. Konsekvenserne af at tåle ikke-europæiske efterretningstjenesters virke på EMK-staternes territorium

8.4.2.1. Menneskerettighedsdomstolens relevante retspraksis

Med ratificering af EMK har signatarstaterne forpligtet sig til at lade udøvelsen af deres suverænitet være underkastet en grundretsefterprøvning. De kan ikke tilsidesætte denne forpligtelse ved at afstå fra deres suverænitet. Disse stater er fortsat ansvarlige for deres territorium og derved forpligtet overfor EU-borgerne, også i det tilfælde, hvor udøvelse af suveræniteten sker ved en anden stats efterretningstjeneste. Menneskerettighedsdomstolen bekræfter imidlertid i sin retspraksis, at signatarstaterne er pligtige til at træffe positive foranstaltninger for at beskytte privatsfæren, således at grundretten i henhold til artikel 8 i EMK ikke krænkes af private (!), dvs. også på horisontalt plan, hvor den enkelte ikke står overfor myndighederne, men en anden person.[1] Hvis en stat tillader, at en udenlandsk efterretningstjeneste udøver sin virksomhed på dette lands territorium, er der meget større behov for beskyttelse, fordi det i så fald er en anden myndighed, der udøver sin overhøjhed. Det forekommer kun at være logisk, at staten må føre tilsyn med overvåge, at den efterretningsvirkomhed, der udøves på dens territorium, er konform med menneskerettighederne.

8.4.2.2. Konsekvenser for aflytningsanlæg

I Tyskland har man i Bad Aibling stillet et eget territorium til rådighed udelukkende til brug for satellitovervågning. I Menwith Hill i Storbritannien blev der givet tilladelse til anvendelse af et areal til samme formål. Hvis en amerikansk efterretningstjeneste via disse anlæg foretager aflytning af ikke-militær kommunikation fra private eller virksomheder, som har oprindelse i en stat, der har tiltrådt EMK, udløser det tilsynspligten i henhold til EMK. Det betyder i praksis, at Tyskland og Det Forenede Kongerige som kontraherende parter i EMK er pligtige til at forvisse sig om, at den amerikanske efterretningstjeneste i sit virke respekterer de grundlæggende rettigheder. Det er desto mere vigtigt, eftersom repræsentanter for ngo'er og medierne gentagne gange har udtrykt deres bekymring over NSA's fremgangsmåde.

8.4.2.3. Konsekvenser for aflytning foranlediget af udenlandske tjenester

I Morgenstow i Storbritannien gennemføres efter oplysningerne fra GCHQ aflytning af civil kommunikation i samarbejde med NSA og strikt efter dennes anvisninger og disse oplysninger videregives som råmateriale til USA. Også i de tilfælde, hvor arbejdet udføres for tredjepart, er man pligtig til at efterprøve, om opgaven opfylder kravet om respekt for de grundlæggende rettigheder.

8.4.2.4. Særlig omhu ved tredjelande

Er der tale om EMK-stater, kan man til en vis grad gensidigt gå ud fra, at den anden stat også opfylder sine forpligtelser i henhold til konventionen. Det gælder i hvert fald, indtil det er bevist, at en EMK-stat systematisk og vedvarende overtræder EMK. USA er imidlertid ikke kontraherende part i EMK og har heller ikke underkastet sig et tilsvarende kontrolsystem. De amerikanske efterretningstjenesters aktiviteter er underlagt meget nøje regler, for så vidt det angår amerikanske borgere hhv. personer, som har legalt ophold i USA. Der gælder imidlertid andre regler for NSA's virksomhed i udlandet, og mange af disse regler er tilsyneladende

[1] Menneskerettighedsdomstolen, Abdulaziz, Cabales og Balkandali, 28.5.1985, Z 67; X u Y/Nederlandene, 26.3.1985, Z 23; Gaskin vs Det Forenede Kongerige 7.7.1989, Z 38; Powell og Rayner, 21.2.1990, Z 41

fortrolige og derved utilgængelige. Det forekommer endnu mere foruroligende, at den amerikanske efterretningstjeneste er underlagt kontrol fra udvalg i Kongressen og Senatet, men at disse parlamentariske udvalg kun udviser ringe interesse for NSA's aktivitet i udlandet.

Det synes derfor at være på sin plads at appellere til Tyskland og England om at tage de forpligtelser, der udspringer af EMK, alvorligt og gøre NSA's udførelse af yderligere efterretningsvirksomhed på deres territorium betinget af, at den opfylder EMK-bestemmelserne. I den sammenhæng er der tre centrale aspekter, som man bør holde sig for øje:

1. I henhold til EMK må indgreb i privatsfæren kun ske på grundlag af retsforskrifter, som er almen tilgængelige og hvis konsekvenser er forudsigelige for borgeren. Dette krav er kun opfyldt, hvis USA gør det klart for den europæiske befolkning, hvordan og under hvilke forhold aflytningen finder sted. I det omfang, hvor dette virke er uforeneligt med EMK, må bestemmelserne tilpasses til det europæiske beskyttelsesniveau.

2. I henhold til EMK må indgreb ikke gå længere, end hvad der er nødvendigt. Derfor må man vælge det lempeligste middel. For EU-borgeren må et indgreb, der gennemføres fra europæisk side, skønnes at være mindre alvorligt end et indgreb fra amerikansk side, da borgeren i første tilfælde kan påberåbe sig sin grundret hos nationale instanser.[1] Indgreb må derfor i videst muligt omfang ske fra tysk hhv. engelsk side, følgelig i hvert fald de indgreb, der sker af hensyn til strafferetsplejen. Fra amerikansk side har man gentagne gange forsøgt at bruge påstande om korruption og bestikkelse som berettigelse for aflytning af telekommunikation.[2] Det bør påpeges overfor USA, at alle EU-stater råder over en velfungerende strafferetspleje. Foreligger der grund til mistanke, må USA overlade retsforfølgelsen til værtslandene. Foreligger der ingen grund til mistanke, må overvågningen anses for at være uforholdsmæssig, følgelig en krænkelse af menneskerettighederne, og derfor ikke tilladt. Der foreligger derfor kun forenelighed med EMK, hvis USA begrænser sig til overvågningsforanstaltninger, som er nødvendige for den nationale sikkerhed, men afstår fra overvågning med henblik på strafferetlig forfølgelse.

3. Som allerede anført, stiller Menneskerettighedsdomstolen i sin retspraksis tilstedeværelse af fyldestgørende kontrolsystemer og garantier mod misbrug som forudsætning for overensstemmelse med de grundlæggende rettigheder. Det betyder, at den amerikanske telekommunikationsovervågning fra europæisk territorium kun er i overensstemmelse med menneskerettighederne, hvis USA i de tilfælde, hvor den fra europæisk territorium tapper kommunikation af hensyn til den nationale sikkerhed, sikrer en tilsvarende effektiv kontrol hhv. hvis NSA i sit virke på europæiske territorium underkaster sig de kontrolforanstaltninger, der gælder i den stat, hvor tapningen finder sted (dvs. Tyskland hhv. Storbritannien).

Kun efter opfyldelse af de i disse tre punkter nedfældede krav kan man sikre, at USA's fremgangsmåde ved aflytning af telekommunikation er i overensstemmelse med EMK og at det ved EMK garanterede ensartede beskyttelsesniveau i Europa opretholdes.

[1] Derved opfyldes også kravene i Art. 13 i EMK, som giver enhver, der krænkes i sine rettigheder adgang til effektiv oprejsning for en national myndighed.

[2] Woolsey (forhenværende direktør for CIA), Why America Spies on its Allies, The Wall Street Journal Europe, 22.3.2000, 31

9. Er EU's borgere tilstrækkeligt beskyttede over for efterretningsvirksomhed?

9.1. Beskyttelse over for efterretningsvirksomhed: en opgave for de nationale parlamenter

Om end efterretningstjenesternes aktiviteter i fremtiden kan henføres under FUSP (den fælles udenrigs- og sikkerhedspolitik), er der endnu ikke udarbejdet bestemmelser herom på EU-plan[1], og ordninger om beskyttelse af borgere over for efterretningstjenesternes aktiviteter afhænger alene af de nationale retssystemer.

De nationale parlamenter har her en dobbelt funktion: som lovgiver træffer de afgørelser om efterretningstjenesternes karakter og beføjelser og udformningen af ordninger vedrørende kontrol heraf. Som det er redegjort detaljeret for i de forrige kapitler, skal de nationale parlamenter, når det drejer sig om spørgsmål, hvorvidt telekommunikationskontrol er tilladt overholde de begrænsninger, der er fastsat i artikel 8 i den europæiske menneskerettighedskonvention, dvs. relevante bestemmelser skal være nødvendige og forholdsmæssige og deres konsekvenser for den enkelte skal være forudsigelige, og desuden skal der fastlægges tilstrækkelige og effektive kontrolforanstaltninger vedrørende kontrolmyndighedernes beføjelser.

Desuden spiller de nationale parlamenter i de fleste lande en aktiv rolle som kontrolmyndighed, da kontrol med den udøvende myndighed (og dermed også med efterretningstjenesterne) udover lovgivningen udgør et parlaments anden "klassiske" opgave. Der er imidlertid store forskelle i udøvelsen af denne kontrol i EU's medlemsstater, ofte findes der parlamentariske og ikke-parlamentariske organer side om side.

9.2. De nationale myndigheders beføjelser til gennemførelsen af overvågningsforanstaltninger

Overvågningsforanstaltningerne skal fra statens side som en generel regel have til formål at håndhæve loven, opretholde ro og orden og beskytte national sikkerhed[2] (over for udlandet).

I alle medlemsstater kan princippet om hemmelig telekommunikation brydes, når formålet er at håndhæve loven, forudsat der er tilstrækkelig bevis for, at en person har begået en forbrydelse (eventuelt under særlige alvorlige omstændigheder). Da indgreb i udøvelsen af retten til privatsfæren er alvorlig, kræves generelt en dommerkendelse til en sådan aktion[3] og kendelsen indeholder præcise oplysninger om kontrollens tilladte varighed, de relevante kontrolforanstaltninger og tilintetgørelse af indsamlede data.

[1] Se kapitel 7.
[2] Disse målsætninger anerkendes også i artikel 8, stk. 2, i den europæiske menneskerettighedskonvention som grunde, der berettiger indgreb i privatlivet. Jf. også ovennævnte kapitel 8.3.2.
[3] Britisk ret er en undtagelse, da indenrigsministeren har beføjelse til at udstede sådanne afgørelser (Regulation of Investigatory Powers Act 2000, Section 5 (1) og (3) (b).

For at garantere national sikkerhed og orden udvides statens ret til at indhente oplysninger udover individuelle undersøgelser i tilfælde af konkret mistanke om at en forbrydelse er begået. Nationale love giver staten tilladelse til at træffe supplerende foranstaltninger for at sikre oplysninger om bestemte personer eller grupper med henblik på på et tidligt tidspunkt at afsløre ekstremistbevægelser eller undergrundsbevægelser, terrorisme og organiseret kriminalitet. Indsamlingen af relevante data samt analyse heraf foretages af særlige indenrigsefterretningstjenester.

Endelig gennemføres en stor del af kontrolforanstaltninger med henblik på at beskytte statens sikkerhed. Som generel regel henhører ansvaret for at bearbejde, analysere og forelægge relevant oplysning om udlandet under statens egen udenrigsefterretningstjeneste[1]. Målet for overvågningen er som regel ingen konkret enkeltperson, men snarere et bestemt område eller bestemte frekvenser. Alt afhængig af, hvilke midler og juridiske beføjelser de eksterne efterretningstjenester råder over kan overvågning omfatte et vidt spektrum, der varierer fra ren militær overvågning af kortbølgeradiotransmissioner til overvågning af alle udenlandske telekommunikationsforbindelser. I visse medlemsstater er overvågning af telekommunikationsmidler alene for at indhente oplysninger ganske enkelt forbudt[2], i andre medlemsstater – i visse tilfælde efter tilladelse fra en uafhængig kommission[3] foretages overvågningen på grundlag af en ministeriel ordre[4] for nogle kommunikationsveje endog uden nogen form for indskrænkning[5]. De forholdsvis vide beføjelser, som visse udenlandske efterretningstjenester nyder, kan begrundes af, at deres aktiviteter er målrettet mod overvågning af udenlandsk kommunikation og således kun vedrører en lille del af deres egne borgere og bekymringen herom derfor er væsentlig mindre.

9.3. Kontrol med efterretningstjenesterne

Det er derfor særlig vigtig med en effektiv og omfattende kontrol, for det første fordi en efterretningstjeneste arbejder hemmeligt og på længere sigt, således at de berørte personer først længe efter overvågning eller alt afhængig af retssituationen slet ikke erfarer, at de er mål for en overvågning, og for det andet fordi overvågningsforanstaltninger ofte vedrører bredere, vagt definerede persongrupper, således at staten meget hurtigt kan indhente en stor mængde personlige oplysninger.

Uafhængig af formen står alle kontrolorganer naturligvis over for samme problem, at det på grund af efterretningstjenesternes særlige karakter, ofte er yderst vanskeligt at fastslå, om alle oplysninger er forelagt, eller om en del tilbageholdes. Derfor må bestemmelserne herom udarbejdes meget omhyggeligt. Principielt kan man gå ud fra, at overvågningen er yderst effektiv og indebærer en vidtgående garanti for, at indgreb er i overensstemmelse med loven,

[1] Med hensyn til udførlig redegørelse for de eksterne efterretningstjenesters aktivitet, se kapitel 2.
[2] Bl.a. i Østrig og Belgien.
[3] Bl.a. i Tyskland, lov om indskrænkning af post- og telekommunikationshemmelighed (lov om artikel 10 i grundloven). I henhold til artikel 9 skal Kommissionen orienteres (undtagen ved fare for at forsinkelsen kan hindre aktionen) inden overvågningen gennemføres.
[4] Bl.a. i Storbritannien (Regulation of Investigatory Powers Act, Section 1) og i Frankrig for kabelkommunikation (Artikel 3 une 4 Loi 91-646 af 10. juli 1991, loi relative au secret des correspondances émises par la voie des télécommunications).
[5] Bl.a. for kabelkommunikation i Frankrig (Artikel 20 Loi 91-646 af 10. juli 1991, loi relative au secret des correspondances émises par la voie des télécommunications).

hvis beføjelser til at beordre overvågning af telekommunikationsmidler er forbeholdt de øverste administrative myndigheder, hvis overvågning alene kan gennemføres på grundlag af en dommerkendelse og hvis et uafhængigt organ kontrollerer gennemførelsen af overvågningsforanstaltningerne. Desuden er det ud fra demokratiske og forfatningsmæssige hensyn ønskeligt, at efterretningstjenestens arbejde som helhed underlægges kontrol af et parlamentarisk organ i overensstemmelse med princippet om magtfordeling.

Dette er i vid omfang gennemført i Tyskland.
Telekommunikationsovervågningsforanstaltninger beordres af den ansvarlige forbundsminister. Med mindre der er risiko for, at yderligere forsinkelse kan hindre aktionen, må en uafhængig kommission, der ikke er bundet af regeringsinstruktioner forud for gennemførelsen af overvågningsforanstaltninger ("G-10-Kommission"[1]) underrettes, således at den kan afgøre, om der er behov for den foreslåede foranstaltning og om den er tilladt. I de tilfælde, hvor den tyske forbundsefterretningstjeneste, BND, har tilladelse til at gennemføre overvågning af ikke-kabeltelekommunikation gennem filtrering på grundlag af søgebegreber træffer Kommissionen afgørelse om disse søgebegreber er tilladte. G-10-Kommissionen er ligeledes ansvarlig for at kontrollere, at de personer, der er underkastet kontrol, får meddelelse herom i henhold til loven, og at BND tilintetgør indsamlede data.

Derudover findes der et parlamentarisk kontrolorgan (PKGr)[2], som består af ni medlemmer af Forbundsdagen og fører tilsyn med alle Tysklands tre efterretningstjenesters aktiviteter. PKGr har ret til aktindsigt, til at høre medarbejdere af efterretningstjenesten, at aflægge besøg hos tjenesten og har ret til at indhente oplysninger, og disse kan kun nægtes af tvingende grunde vedrørende adgang til information, hvis det er nødvendigt for at beskytte en tredjeparts ret til privatliv, eller hvis det vedrører kerneområdet af regeringens ansvar. PKGr's drøftelser er hemmelige og medlemmerne er forpligtet til at udvise fuld fortrolighed – også efter at de har nedlagt deres hverv. Halvvejs og ved udløbet af valgperioden forelægger PKGr den tyske Forbundsstat en beretning om sin kontrolaktivitet.

En sådan omfattende praktisk ubrudt kontrol med efterretningstjenesten er imidlertid en undtagelse i medlemsstaterne.

I Frankrig[3] kræves f.eks. kun tilladelse fra premierministeren til overvågningsforanstaltninger som indebærer aftapning af kabelkommunikation. Kun foranstaltninger af denne art er underkastet kontrol af en kommission, der er nedsat til dette formål (Commission nationale de contrôle des interceptions de sécurité), hvis medlemmer omfatter et medlem af parlamentet og en senator. Ansøgning om tilladelse til at gennemføre aflytning forelægges Kommissionens formand af en minister eller dennes repræsentant. Hvis der er tvivl om lovligheden af den forestående foranstaltning kan formanden indkalde til et møde i kommissionen, som udsteder henstillinger, og ved mistanke om en strafbar handling, orienterer statsanklageren. Aflytningsforanstaltninger af hensyn til nationale interesser, som indebærer aflytning af radioudsendelser og således også af satellitkommunikationer, er ikke underkastet nogen form

[1] Udtømmende oplysninger: Parlamentarisk kontrol med efterretningstjenesten i Tyskland (9.9.2000, udgivet af Den Tyske Forbundsdag, den parlamentariske kontrolgruppes sekretariat).
[2] Lov om kontrol med Forbundsstatens efterretningstjenestes aktiviteter (PKGrG) af 17. juni 1999, BGB1 I 1334, idgF.
[3] Loi 91-646 af 10. juli 1991, loi relative au secret des correspondances émises par la voie des télécommunications.

for begrænsning, og heller ikke en kontrolkommission.

Den franske efterretningstjenesters arbejde er i øvrigt ikke underlagt kontrol af et parlamentarisk kontroludvalg, men der arbejdes herpå. Nationalforsamlingens forsvarsudvalg har allerede godkendt et sådant forslag[1], men forslaget er endnu ikke behandlet i plenum.

I Det Forenede Kongerige kræver enhver overvågning af telekommunikation på britisk jord en tilladelse fra indenrigsministeriet. Imidlertid fremgår det ikke klart af lovens formulering, hvorvidt målrettet aflytning af kommunikationsmidler, som kontrolleres via nøgleord, også omfattes af begrebet "aflytning" som defineret i "Regulation of Investigatory Powers Act 2000" (RIP), hvis oplysningerne ikke analyseres på britisk jord, men blot transmitteres til udlandet som "råmateriale". Kontrol med overholdelse med RIP's bestemmelser gennemføres "ex-post" af kommissærer, som udnævnes af premierministeren og enten en fungerende eller tidligere overretsdommere. Den kommissær, der er ansvarlig for aflytning (Interception Commissioner), kontrollerer tildeling af tilladelser til aflytning og bistår ved undersøgelser vedrørende klager over aflytningsforanstaltninger. Intelligence Service Commissioner overvåger tilladelser til efterretningstjenestens og sikkerhedstjenesternes aktiviteter og bistår undersøgelser vedrørende klager over disse tjenester. Investigatory Powers Tribunal, som ledes af en overretsdommer, undersøger alle klager vedrørende aflytningsforanstaltninger og ovennævnte tjenesters aktiviteter.

Intelligence and Security Committee (ISC)[2], som kontrollerer alle tre civile efterretningstjenesters (M15, M16 og GCHQ) aktiviteter, står for den parlamentariske kontrol. Dette udvalg er navnlig ansvarlig for gennemgang af udgifter og administration samt kontrol af sikkerhedstjenestens, efterretningstjenestens og GCHQ's aktiviteter. Udvalget består af ni medlemmer fra Underhuset og Overhuset, hvoraf ingen må være minister. Til forskel for andre staters kontroludvalg, der som regel vælges af det nationale parlament eller udnævnes af parlamentets formand, udnævnes de af premierministeren i samråd med lederen af oppositionen.

Disse eksempler viser allerede klart, at beskyttelsesniveauet varierer ret betydeligt. Med hensyn til parlamentarisk kontrol ønsker ordføreren at understrege, at det er meget vigtigt, at der findes særlige kontroludvalg, der er ansvarlige for tilsyn med efterretningstjenesternes aktiviteter. De har frem for hovedudvalgene den fordel, at de nyder større tillid hos efterretningstjenesterne, da deres medlemmer er bundet af reglen om fortrolighed og møderne finder sted for lukkede døre. Desuden har de med henblik på udførelsen af deres særlige opgaver specielle rettigheder, der er altafgørende for kontrol med hemmelige aktiviteter.

Det er glædeligt, at de fleste af EU's medlemsstater har nedsat et særligt parlamentarisk kontroludvalg, der skal gennemgå efterretningstjenesternes aktiviteter. I Belgien[3], Danmark[4],

[1] Jf. lovforslag "Proposition de loi tendant à la création de délégations parlementaires pour le renseignement" og betænkning herom af Arthur Paecht nr. 1951 Assemblée nationale, 11. lovgivningsperiode, registreret den 23. november 1999.
[2] Intelligence services act 1994, Section 10.
[3] Comité permanent de contrôle des services de renseignements et de sécurité, Comité permanent R, Loi du 18. juli 1991/IV, organique de contrôle des services de police et de renseignements.
[4] Udvalget vedrørende efterretningstjenesterne, Lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester, lov 378 af 6/7/88.

Tyskland[1], Italien[2], Nederlandene[3] og Portugal[4] findes der et parlamentarisk kontroludvalg, som både er ansvarlig for kontrol med militære og civile efterretningstjenester. I Det Forenede Kongerige[5] overvåger det særlige kontroludvalg kun (om end væsentlig mere omfattende) civile efterretningstjenester, mens den militære efterretningstjeneste overvåges af det normale forsvarsudvalg. I Østrig[6] henhører de to grene af efterretningstjenesten under to separate kontroludvalg, som imidlertid er organiseret på samme måde og har de samme rettigheder. I de nordiske lande Finland[7] og Sverige[8] varetages opgaver vedrørende parlamentarisk kontrol af ombudsmænd, som er uafhængige og vælges af parlamentet. I Frankrig, Grækenland, Irland, Luxembourg og Spanien findes der ikke noget parlamentarisk udvalg, og kontrolopgaverne varetages her kun af hovedudvalgene som led i det almindelige parlamentariske arbejde.

9.4. Vurdering af situationen for de europæiske borgere

Situationen i Europa synes utilfredsstillende for de europæiske borgere. De nationale efterretningstjenesters beføjelser inden for overvågning af telekommunikation varierer ret betydeligt i omfang, og det samme gælder kontroludvalgenes beføjelser. Ikke alle de medlemsstater, som har en efterretningstjeneste, har nedsat uafhængige parlamentariske kontrolorganer med passende overvågningsbeføjelser. Man er endnu langt fra et ensartet beskyttelsesniveau.

Fra et europæisk synspunkt er dette så meget mere beklageligt som denne situation ikke først og fremmest berører de pågældende medlemsstaters borgere, som kan påvirke beskyttelsesniveauet gennem deres stemme ved valg. Den uheldige virkning rammer først og fremmest statsborgere fra andre lande, eftersom efterretningstjenester i sagens natur arbejder udenlands. Enkeltpersoner er for det meste værgeløse over for udenlandske systemer, og her er behovet for beskyttelse endnu større. Man må heller ikke glemme, at EU-borgere på grund af efterretningstjenesternes særlige karakter kan rammes af flere efterretningstjenesters aktiviteter samtidig. I denne forbindelse er det ønskeligt med et ensartet beskyttelsesniveau i overensstemmelse med demokratiske principper. Det bør også overvejes, om databeskyttelsesbestemmelser kunne gennemføres på EU-plan.

---

[1] Das parlamentarische Kontrollgremium (PKGr), Gesetz über die Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG) af 17. juni 1999 BGB1 I 1334 idgF.

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

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

[4] Conselho de Fiscalização dos Serviços de Informações (CFSI), Lov 30/84 af 5. september 1984, ændret ved Lov 4/95 af 21. februar 1995, Lov 15/96 af 30. april 1996 og Lov 75-A/97 af 22. juli 1997.

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

[6] Stående underudvalg under det nationale forsvarsudvalg, der er ansvarlig for kontrol med efterretningsforanstaltninger for at beskytte militær sikkerhed og det stående underudvalg under udvalget om interne anliggender, der er ansvarlig for kontrolforanstaltninger for at beskytte forfatningsorganer og deres handlekraft (Art. 52a B-VG, §§ 32b ff forretningsordenen 1975.

[7] Ombudsmand, retslig grundlag for politikontrol (SUPO): Poliisilaki 493/1995 §33 og Laki pakkokeinolain 5 a luvun muuttamisesta 366/1999 §15, for militæret: Poliisilaki 493/1995 §33 og Laki poliisin tehtävien suorittamisesta puolustusvoimissa 1251/1995 §5.

[8] Rikspolisstyrelsens ledning, Förordning (1989:773) med instruktion for Rikspolisstyrelsen (Forordning (1989:773) om nationale politimyndigheder).

Desuden vil spørgsmålet om beskyttelse af europæiske borgere blive placeret i en fuldstændig ny sammenhæng, når de første skridt som led i en fælles sikkerhedspolitik tages i retning af samarbejde mellem medlemsstaternes efterretningstjenester. Borgerne vil så forvente, at de europæiske institutioner vedtager passende sikkerhedsbestemmelser. Europa-Parlamentet skal som fortaler for konstitutionelle principper således kræve, at det som et demokratisk valgt organ tildeles de beføjelser, der er nødvendige for at gennemføre passende kontrol. Europa-Parlamentet skal imidlertid også skabe forudsætningerne for en fortrolig behandling af følsomme data af denne art og af andre hemmelige dokumenter i et særligt udvalg, hvis medlemmer har tavshedspligt. Først når disse forudsætninger er opfyldt, vil det være realistisk og med henblik på et effektivt samarbejde mellem efterretningstjenesterne – som er en forudsætning for en seriøs fælles sikkerhedspolitik – forsvarligt at kræve disse kontrolrettigheder.

10. Beskyttelse mod økonomisk spionage

10.1. Spionagens mål: erhvervslivet

Hvad angår fortrolighed kan en virksomheds informationer opdeles i tre kategorier. For det første oplysninger, der bevidst gives **størst mulig udbredelse**. Dertil hører fakta om virksomhedens produkter (f.eks. produktets egenskaber, pris, osv.) og annonceoplysninger, som bidrager til virksomhedens image.

Der findes også informationer, som **hverken beskyttes eller aktivt udbredes,** fordi de ingen betydning har for virksomhedens konkurrencestilling. Som eksempel kan nævnes datoen for virksomhedens årlige skovtur, kantinens menu, eller faxens mærke.

Og til sidst findes der oplysninger, som **beskyttes mod, at andre får kendskab dertil** .Disse oplysninger beskyttes mod konkurrencen, men også mod staten, hvis en virksomhed ikke vil overholde loven (skat, embargoregler, m.m). Der findes også forskellige grader af fortrolighed frem til strikt hemmeligholdelse, f.eks. af forskningsresultater forud for patentering eller ved fremstilling af våben eller våbendele.[1].

Spionagen afhænger af arten af de oplysninger, som en virksomhed ønsker at hemmeligholde. Er den angribende part en konkurrerende virksomhed, taler man om **konkurrencespionage** (også erhvervsspionage eller industrispionage). Er angriberen en statslig efterretningstjeneste, taler man om **økonomisk spionage**.

10.1.1. De enkelte spionagemål

Strategiske oplysninger, som er vigtige for økonomisk spionage, kan opdeles i følgende erhvervssektorer og virksomhedsområder:

10.1.1.1. Erhvervssektorer

Det er klart, at der er stor interesse for oplysninger om følgende områder: bioteknologi, genteknologi, medicinteknik, miljøteknik, avanceret computerteknik, software, optoelektronik, billedsensor- og signalteknik, oplagring af data, teknisk keramik, legeringer med stor kapacitet, nanoteknologi. Denne liste er ikke udtømmende og ændrer sig i øvrigt fortløbende i trit med den teknologiske udvikling. På disse områder drejer spionagen sig navnlig om tyveri af forskningsresultater eller særlige produktionsteknikker.

10.1.1.2. Virksomhedsområder

Spionagens angrebspunkter ligger selvfølgelig i områderne forskning og udvikling, indkøb, personale, produktion og distribution, salg, marketing, produktionslinjer og finansielle forhold. Betydningen og værdien af disse data bliver ofte undervurderet (jf. punkt 10.1.4).

10.1.2. Konkurrencespionage

En virksomheds strategiske position på markedet er afhængig af dens situation med hensyn til forskning og udvikling, produktionsprocesser, produktlinier, finansiering, markedsføring,

[1] Informationen für geheimschutzbetreute Unternehmen, BMWI 1997

salg, distribution, indkøb og arbejdsstyrken[1]. Oplysninger herom er af stor interesse for enhver konkurrent på markedet, da man derved får indblik i planer og svagheder og kan træffe strategiske modforanstaltninger.

En del af disse oplysninger er offentligt tilgængelig. Der findes specialiserede konsulentfirmaer, som fuldt lovligt kan udarbejde en konkurrenceanalyse, heriblandt ansete firmaer som f.eks. Roland & Berger i Tyskland. „Competitive Intelligence" er i USA blevet et fast værktøj for virksomhedsledelsen.[2]. Ved professionel bearbejdelse af mange enkeltinformationer skabes et klart situationsbillede.

Overgangen fra lovlig til strafbar konkurrencespionage sker ved valget af de midler, som bruges til at indhente informationerne. Først når de anvendte midler er ulovlige i den pågældende retsorden, overskrider man grænsen til det kriminelle - udarbejdelse af analyser er i sig selv ikke strafbar. De oplysninger, som er af særlig interesse for konkurrenten, bliver selvfølgelig beskyttet mod indgreb og kan kun fås ved at overtræde loven. De teknikker, der anvendes i den sammenhæng, er ikke forskellige fra de almindelige spionagemetoder, som er omhandlet i kapitel 2.

Der foreligger ingen præcise tal for omfanget af konkurrencespionage. Usikkerheden er - ligesom ved den klassiske spionage - meget stor. De involverede parter (den spionerende part og offeret) er ikke interesseret i offentlighed. For de skadelidte virksomheder er det ensbetydende med et tab af image, og den spionerende virksomhed er selvfølgelig heller ikke interesseret i, at dens aktiviteter bliver offentliggjort. Derfor kommer kun få tilfælde for retten.

Alligevel er der igen og igen forlydender om konkurrencespionage i pressen. Ordføreren har desuden drøftet dette spørgsmål med sikkerhedsscheferne i et par store tyske virksomheder[3] og med ledelsen i amerikanske og europæiske virksomheder. Konklusionen er den, at konkurrencespionage afsløres regelmæssigt, men at den ikke bestemmer den daglige forretningsgang.

10.2. Skaden som følge af økonomisk spionage

På grund af den store usikkerhed er det ikke muligt at foretage nøjagtige beregninger af omfanget af skaden som følge af konkurrencespionage/økonomisk spionage. Dertil kommer, at en del af de anførte tal bevidst er sat højt. Sikkerhedsfirmaer og sikkerhedstjenester har en forståelig interesse i, at placere skadens omfang i den høje ende af skalaen af det realistisk mulige. Ikke desto mindre gør tallene et vist indtryk.

Allerede i 1998 anslog Max Planck Instituttet skaden som følge af økonomisk spionage i Tyskland til mindst 8 mia. DM[4]. Formanden for sammenslutningen af sikkerhedskonsulentfirmaer i Tyskland nævner under henvisning til sagkyndige et beløb på 15 mia. DM om .året. Formanden for de europæiske politiorganisationer, Hermann Lutz anslår skaden til 20 mia. DM om året. FBI[5] nævner for årene 1992/1993 en skade på 1,7 mia. US-

[1] M.F.Porter, Competitive Strategy
[2] Hummelt, Roman, Wirtschaftsspionage auf dem Datenhighway, Hanserverlag, München 1997
[3] Enkeltheder og navne beskyttet.
[4] IMPULSE,3/97,S.13 ff.
[5] Erklæring i Kongressen, L.J.Freech, direktør i FBI, 9.5.1996

dollar, som påføres den amerikanske økonomi som følge af konkurrencespionage og økonomisk spionage. Den forhenværende formand for udvalget om tilsyn med efterretningstjenester i Repræsentanternes Hus, USA taler om 100 mia. US-dollar i tab som følge af mistede kontrakter og yderligere forsknings- og udviklingsomkostninger. Mellem 1990 og 1996 har dette ført til tab af 6 mio. arbejdspladser.[1]

Det er i grunden ikke nødvendigt at kende den nøjagtige skade. Staten er forpligtet til via politi- og efterretningsinstanser at gribe ind mod konkurrencespionage og økonomisk spionage uanset omfanget af den skade, der påføres nationaløkonomien. Tallet for den samlede skade danner heller ikke et brugbart grundlag for virksomhedens beslutninger om beskyttelse af oplysninger og interne foranstaltninger for at beskytte sig mod spionage. Den enkelte virksomhed må selv beregne den største, potentielle skade som følge af tyveri af oplysninger, foretage en vurdering af sandsynligheden for, at spionage finder sted, og afveje de således beregnede beløb mod sikkerhedsomkostningerne. Problemet ligger egentlig ikke i, at der mangler nøjagtige tal for den samlede skade. Det er snarere det, at der bortset fra meget store virksomheder næppe foretages sådanne cost-benefit-beregninger og sikkerheden derfor forsømmes.

10.3. Hvem spionerer?

Ifølge en undersøgelse af firmaet Ernest Young LLP[2] er de vigtigste bagmænd for spionage mod virksomheder konkurrenter (39%), kunder (19%), leverandører (9%) og efterretningstjenester (7%). Det er egne medarbejdere, private spionagefirmaer, betalte hackere og fagfolk fra efterretningstjenester, der udfører spionage.[3]

10.3.1. Egne medarbejdere (insiderdelikt)

Den anvendte litteratur, oplysningerne fremsat af sagkyndige i udvalget, og resultaterne fra ordførerens samtaler med sikkerhedschefer og -myndigheder viser enslydende, at skuffede og utilfredse medarbejdere udgør den største risiko for spionage. Som ansatte har de direkte adgang til oplysninger, de lader sig hyre for penge og spejder efter virksomhedshemmeligheder for deres bagmænd.

Store risici opstår også ved jobskifte. Nu om stunder behøver man ikke længere at kopiere enorme mængder papir for at kunne fjerne vigtige oplysninger fra virksomheden. De indlæses upåagtet på disketter og kan ved skiftet til en ny arbejdsplads tages med til den nye arbejdsgiver.

10.3.2. Private spionagefirmaer

Antallet af private firmaer, som har specialiseret sig i at spejde efter data, er i stadig vækst. Sådanne firmaer beskæftiger til dels tidligere medarbejdere i efterretningstjenester. Disse firmaer arbejder ofte som sikkerhedskonsulenter og som detektivbureauer, som på bestilling skaffer oplysninger. Som regel anvendes lovlige metoder, men der findes også firmaer, der benytter ulovlige metoder.

[1] Robert Lyle, Radio Liberty/Radio free Europe, 10.februar 1999
[2] Computerzeitung, 30.11.1995, S.2
[3] R.Hummelt, Spionage auf dem Datenhighway, München 1997, S.49ff

10.3.3. Hackere

Hackere er computerspecialister, som i kraft af deres viden kan skaffe sig adgang til edb-net. I hackertidsalderens første år var det computernørder, som morede sig ved at knække edb-systemers sikkerhedskoder. Nu om stunder findes der hackere, der arbejder på bestilling såvel inden for tjenesterne som på markedet.

10.3.4. Efterretningstjenester

Efter Den Kolde Krigs slutning har efterretningstjenesternes opgaver forrykket sig. International organiseret kriminalitet og økonomiske forhold er nye opgaver.(Jf. kapitel 10.10.5).

10.4. Hvordan spioneres der?

Ifølge oplysningerne fra sikkerhedsmyndighederne og sikkerhedscheferne i store virksomheder anvender man i økonomisk spionage alle afprøvede efterretningsmetoder og -midler (jf. kapitel 2.2.4.). Virksomheder har dog en mere åben struktur end militæret og efterretningstjenester eller regeringsinstanser. Der er derfor betydelige ekstra risici ved økonomisk spionage:

- det er lettere at rekruttere medarbejdere, og en virksomhedskoncerns muligheder med hensyn til sikkerhed kan ikke sammenlignes med sikkerhedsmyndighedernes;
- arbejdspladsens mobilitet bevirker, at vigtige oplysninger kan medtages på en bærbar computer. Tyveri af laptops eller hemmelig kopiering af en harddisk efter indbrud i et hotelværelse er en af standardteknikker for økonomisk spionage;
- indbrud i et edb-net gennemføres lettere end ved sikkerhedsfølsomme statslige anlæg, mens sikkerhedsbevidstheden og -foranstaltninger netop hos små og mellemstore virksomheder er langt mindre;
- aflytning på stedet (jf. kapitel 3.3.2) er af samme grunde simplere.

Det fremgår af de indhentede oplysninger, at økonomisk spionage hovedsageligt gennemføres på stedet eller ved den mobile arbejdsplads og at de ønskede oplysninger med få undtagelser (jf. punkt 10.6) ikke kan fås gennem aflytning af de internationale telekommunikationsnet.

10.5. Staters økonomiske spionage

10.5.1. Efterretningstjenesters strategiske økonomiske spionage

Efter Den Kolde Krigs slutning er der i efterretningstjenester opstået ledig kapacitet, som nu indsættes på andre områder. USA erklærer offentligt, at en del af dens efterretningsvirksomhed også beskæftiger sig med erhvervslivet. Det omfatter f.eks. overvågning af overholdelse af økonomiske sanktioner, overvågning af overholdelse af våbenleveringsregler og produkter med dobbelt anvendelse (dual-use), udviklingerne på råstofmarkederne og situationen på de internationale finansmarkeder. Så vidt det er ordføreren bekendt, er det ikke kun de amerikanske efterretningstjenester, der beskæftiger sig med dette område, og der er heller ingen omfattende kritik heraf.

10.5.2. Efterretningstjenesters deltagelse i konkurrencespionage

Kritik ytres i de tilfælde, hvor nationale efterretningstjenester misbruges til gennem spionage at skaffe landets egne virksomheder internationale konkurrencefordele. I den sammenhæng kan der skelnes mellem to former:[1].

10.5.2.1. Hightech-stater

Højtudviklede industrilande kan have stort gavn af industrispionage. Ved at udspionere udviklingstilstanden i en bestemt sektor kan der træffes foranstaltninger i forbindelse med landets egen udenrigsøkonomi og støttepolitik, som enten styrker konkurrenceevnen for landets egen industri eller er støttebesparende. Et andet tyngdepunkt kan ligge i udformningen af enkeltheder ved meget store kontrakter (jf. 10.6).

10.5.2.2. Teknisk mindre avancerede stater

For en del af disse stater drejer det sig om at fremskaffe teknisk know-how for at kunne indhente et efterslæb hos landets egen industri uden udviklingsomkostninger og licensgebyr. Desuden drejer det sig om fremskaffelse af originale produkter og fremstillingsteknikker med henblik på at opnå konkurrenceevne på verdensmarkedet med billigere (lavere lønsomkostninger) kopiprodukter. Det er dokumenteret, at den russiske efterretningstjeneste har fået tildelt denne opgave. I Den Russiske Føderations lov nr. 5 om efterretningsvirksomhed i udlandet nævnes eksplicit fremskaffelse af økonomiske og forskningstenkiske oplysninger som en opgave for efterretningstjenesten.
For en anden gruppe stater (herunder Iran, Irak, Syrien, Lybien, Nordkorea, Indien og Pakistan) drejer det sig om fremskaffelse af oplysninger til deres nationale oprustning, fremfor alt på det nukleare område og til fremstilling af biologiske og kemiske våben. En anden aktivitet for efterretningstjenesterne i disse stater er drift af kamuflagefirmaer med henblik på at undgå mistanke i forbindelse med indkøb af dual use-varer.

10.6. Egner Echelon sig til industrispionage?

Afsløring af oplysninger af betydning for konkurrencespionage beror ved den strategiske kontrol af international telekommunikation kun på et tilfælde. Følsomme virksomhedsoplysninger befinder sig jo først og fremmest i selve virksomheden, og det betyder, at der med henblik på konkurrencespionage først og fremmest gøres forsøg på at få oplysninger via medarbejdere eller indslusede personer eller ved at trænge ind i det interne edb-net. Kun når følsomme data kommer ud via nettet eller radio (satellit), kan et kommunikationsovervågningssystem anvendes til konkurrencespionage. Det sker systematisk:

- ved virksomheder, der arbejder inden for tre tidszoner, således at mellemresultater sendes fra Europa til Amerika og videre til Asien.
- ved multinationale selskabers videokonferencer via V-Sat eller kabel;
- når der forhandles om vigtige kontrakter på stedet (f.eks. i bygge- og anlægssektoren, telekommunikationsinfrastruktur, nyoprettelse af transportsystemer osv.) og der derfra skal føres samråd med hovedkontoret.

Hvis virksomheder i disse tilfælde ikke beskytter deres kommunikation, giver tapning af denne kommunikation værdifulde oplysninger til konkurrencespionage.

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

10.7. Offentliggjorte tilfælde

Der findes et antal tilfælde af økonomisk spionage hhv. konkurrencespionage, som er offentliggjort i medierne og i relevant litteratur. En del af disse kilder er undersøgt og har dannet grundlaget for nedenstående tabeller. Det anføres kort, hvem der var involveret, hvornår det skete, hvad det drejede sig om, hvad der var målet og konsekvenserne.
Det er påfaldende, at indberetningerne om et og samme tilfælde for en del er meget forskellige. F.eks. i Enercon-sagen nævnes NSA eller det amerikanske handelsministerium eller den fotograferende konkurrent som gerningsmand.

Sag	Hvem	Hvornår	Hvad	Hvordan	Mål	Følger	Kilde
Air France	DGSE	Til 1994	Samtaler mellem rejsende forretningsfolk	I Air France's kabiner på 1. klasse afsløres skjulte mikrofoner - flyselskabet fremsatte en offentlig undskyldning	Fremskaffelse af informationer	Ikke nævnt	"Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?" af Arno Schütze, 1/
Airbus	NSA	1994	Informationer om en flyvemaskinehandel mellem Airbus og saudi-arabisk flyselskab	Aflytning af faxmeddelelser og telefonsamtaler mellem forhandlingsparterne	Videreformidling af information til de amerikanske konkurrenter Boeing og Mc-Donnell-Douglas	Amerikanerne afslutter 6-million-dollar-forretningen	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9. November 2000
Airbus	NSA	1994	Kontrakt på 6 mia. dollar med Saudi-Arabien Afsløring af bestikkelse af det europæiske Airbus-konsortium	Aflytning af faxmeddelelser og telefonsamtaler mellem: det europæiske Airbus-konsortium og det saudiske luftfartsselskab/regeringen om kommunikationssatellitter	Afsløring af bestikkelse	McDonnell-Douglas, den amerikanske konkurrent til Airbus, afslutter handelen	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, af Duncan Campbell
BASF	Sælger	Ikke nævnt	Beskrivelse af fremgangsmåden for produktion af hudcremeråstof i BASF (kosmetiksektion)	Ikke nævnt	Ikke nævnt	Ingen, fordi afsløret	„Nicht gerade zimperlich“, Wirtschaftswoche Nr.43 / 16. Oktober 1992
Bundeswirtschaftsministerium DE	CIA	1997	Information om hightech-produkter i Bundeswirtschafts-ministerium (det tyske økonomiministerium)	Benyttelse af agent	Fremskaffelse af informationer	Agenten afsløres ved forsøg og udvises	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ af Arno Schütze, 1/98
Bundeswirtschaftsministerium DE	CIA	1997	Baggrunden for Mykonos-processen i Berlin, Hermeslån vedr. Iran-eksport, fortegnelse over tyske virksomheder, der leverer hightech-produkter til Iran	CIA-agent under dække af US-ambassadør fører venskabelige samtaler med lederen af den for det arabiske område (hovedvægt Iran) ansvarlige sektion i det tyske økonomiminsterium	Fremskaffelse af informationer	Ikke nævnt. Embedsmanden henvender sig til tyske sikkerhedsmyndigheder, der signaliserer over for de amerikanske organer, at en CIA-operation er uønsket. CIA-agenten bliver derefter "trukket tilbage"	„Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste“, Landesamt für Verfassungsschutz Baden-Württemberg, Stuttgart, Situation: 1998
Dasa	Russisk efterretnings-tjeneste	1996 – 1999	Salg og videregivelse af oprustningsteknologiske dokumenter fra en virksomhed for forsvarsteknik i München (ifølge SZ af 30.5.2000: rustningsvirksomheden Dasa i Ottobrunn)	2 tyskere handler efter ordre	Fremskaffelse af informationer om styrede missiler, våbensystemer (panser- og luftforsvar)	SZ af 30.5.2000: "(..) Ud fra militære synspunkter er forrædderiet "ikke særligt tungtvejende". Dette gælder også for den økonomiske skade, konstaterede domstolen"	„Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Bonn, April 2001 „Haftstrafe wegen Spionage für Russland“, SDZ / 30. Mai 2000
Embargo	BND Den tyske	ca. 1990	Fornyet eksport af embargo-beskyttet teknologi til Libyen	Aflytning af telefonvæsenet	Afsløring af illegal våben- og teknologitransfer	Ingen særlige konsekvenser, leveringer forhindres ikke	"Maulwürfe in Nadelstreifen", Andreas Förster, S. 110

Sag	Hvem	Hvornår	Hvad	Hvordan	Mål	Følger	Kilde
	efterretnings-tjeneste		(bl.a. ved Siemens)				
Enercon	Ekspert i vindenergi fra Oldenburg og en kvindelig medarbejder fra Kenetech	Ikke nævnt	Vindkraftanlægget, ejet af firmaet Enercon i Aurich	Ikke nævnt	Ikke nævnt	Ikke nævnt	„Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Bonn, April 2001
Enercon	NSA	Ikke nævnt	Vindmølle til elfremstilling, udviklet af den østfriesiske ingeniør Aloys Wobben	Ikke nævnt	Videregivelse af Wobbens tekniske retningslinjer til amerikansk firma	Amerikansk firma anmelder inden Wobben vindmøllen til patentmyndigheden; Wobben anklages af et amerikansk sagførerfirma (overtrædelse af patentrettigheder)	„Aktenkrieger“, SZ, 29. März 2001
Enercon	US-virksomhed	1994	Vigtige detaljer i et hightech-vindkraftanlæg (fra omstillingsanlæg til elektroniske kredsløbskort)	Fotografier	Vellykket patentsag i USA	Enercon GmbH lægger planer om åbning af det amerikanske marked på is	„Sicherheit muss künftig zur Chefsache werden“, HB / 29. August 1996
Enercon	Oldenburgsk ingeniør W. og US-firmaet Kenetech	Marts 1994	Vindgenerator type E-40 fra Enercon	Ingeniør W. videregiver oplysninger, medarbejder ved Kenetech fotograferer anlæg plus elektriske detaljer	Kenetech: undersøger beviser med henblik på senere (1995) klage på grund af overtrædelse af patentrettigheder over for Enercon Enercon: illegal fremskaffelse af oplysninger fra forretningshemmeligheder TV-journalist skal af en tidligere NSA-medarbejder have fået at vide, at detaljerede oplysninger fra Enercon om Echelon af amerikanerne blev givet videre til Kenetech	Ikke nævnt	„Klettern für die Konkurrenz“, SZ 13. Oktober 2000
Enercon	Kenetech Windpower	Inden 1996	Oplysninger til vindenergianlæg fra Enercon	Kenetech-ingeniører fotograferer anlæg	Kopiering af anlægget hos Kenetech	Enercon får ret: mod spioner anlægges sag; anslået tab: flere hundrede millioner DM	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ af Arno Schütze, 1/98
Japans handels-ministerium	CIA	1996	Forhandlinger om importkvoter for amerikanske biler på det japanske marked	Hacker i det amerikanske handelsministeriums computersystem	Den amerikanske forhandlinger Mickey Kantor skal indvillige ved laveste tilbud	Kantor accepterer laveste tilbud	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ af Arno Schütze, 1/98

Sag	Hvem	Hvornår	Hvad	Hvordan	Mål	Følger	Kilde
Japanske biler	Den amerikanske regering	Ikke nævnt	Forhandlinger om import af japanske luksusbiler Oplysninger om japanske bilers emissionsnormer	COMINT, ikke nøjere beskrevet	Fremskaffelse af informationer	Ingen oplysninger	"Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, af Duncan Campbell
López	NSA	Ikke nævnt	Videokonference fra VW og López	Aflytning fra Bad Aibling	Videregivelse af oplysninger til General Motors og Opel	Gennem aflytnings-foranstaltninger ville statsadvokaten have fået meget nøje oplysninger med henblik på afsløring	Kaptajn i det tyske Bundeswehr, Erich Schmidt-Eenboom, citerer i „Wenn Freunde spionieren" www.zdf.msnbc.de/news/54637.asp?cp1=1
López	López og tre af hans med-arbejdere	1992 - 1993	Dokumenter og oplysninger fra områderne forskning, planlægning, fabrikation og indkøb (dokumenter til fabrik i Spanien, udgiftsoplysninger om forskellige modelserier, projektstudier, indkøb og sparestrategier)	Indsamling af materiale	VW's benyttelse af dokumenter fra General Motors	Efter strafferetligt opgør enedes koncernerne uden om domstolen. López træder tilbage i 1996 som manager for VW, VW skiller sig i 1997 af med tre andre medarbejdere i López-teamet, betaler 100 mio. dollars til GM/Opel (angiveligt sagførerudgifter) og erhverver i 7 år reservedele for i alt 1 mia. dollar fra GM/Opel	„Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste", Landesamt für Verfassungsschutz Baden-Württemberg, Stuttgart, Stand: 1998
López	NSA	1993	Videokonference mellem José Ignacio López og VW's chef Ferdinand Piëch	Båndoptagelse af videokonferencen og dennes videregivelse til General Motors	Beskyttelse af forretningshemmeligheder i den amerikanske General Motors, som López tilsigtede at give videre til VW (prislister, hemmelige planer om ny bilfabrik og nye små biler)	López afsløres, retssag indstilles i 1998 mod betaling af bøder Vedrørende NSA intet	„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?" af Arno Schütze, 1/98
Los Alamos	Israel	1988	To medarbejdere i Israels atomforskningsprogram bryder koden for centralcomputeren i atomvåbenlaboratoriet Los Alamos	Hackere	Fremskaffelse af informationer om nye amerikanske atomvåbentændere	Ingen særlige konsekvenser, da hackerne flygter til Israel, én bliver dér foreløbig sat fast, ingen officiel forbindelse til Israels efterretningstjeneste	"Maulwürfe in Nadelstreifen", Andreas Förster, S. 137
Smugling	BND	70'erne	Smugling af computeranlæg til DDR	Ikke nævnt	Afsløring af teknologitransfer til Østblokken	Ingen særlige konsekvenser, leveringer blev ikke forhindret	"Maulwürfe in Nadelstreifen", Andreas Förster, S. 113

Sag	Hvem	Hvornår	Hvad	Hvordan	Mål	Følger	Kilde
TGV	DGSE	1993	Siemens-udgiftsberegning Ordre til levering af højhastighedstog til Sydkorea	Ikke nævnt	Dumpingpris	ICE-producenten går glip af ordren til fordel for Alcatel-Alsthom	„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ af Arno Schütze, 1/98
TGV	Ukendt	1993	Udgiftsberegning fra AEG og Siemens med hensyn til offentligt udbud i Sydkorea til levering af højhastighedstog	Siemens påstår, at dets telefon- og faxforbindelser er blevet aflyttet i filialen i Seoul	Forhandlingsfordel for den britisk-franske medansøger GEC Alsthom	Ordregiverne vælger GEC Alsthom, selv om det tyske tilbud først var bedre	„Abgehört“, Berliner Zeitung, 22. Januar1996
Thomson-Alcatel vs. Raytheon	CIA/ NSA	1994	Tildeling af en brasiliansk milliardkontrakt vedr. satellitovervågning af Amazonas til det franske Thomson-Alcatel (1,4 mia. dollars)	Aflytning af kommunikationsforbindelserne hos vinderen af udbuddet (Thomson-Alcatel, FR)	Afsløring af korruption (udbetaling af bestikkelsespenge)	Clinton indgiver klage hos den brasilianske regering; efter den amerikanske regerings insisteren ny tildeling af kontrakten til det amerikanske firma "Raytheon"	"Maulwürfe in Nadelstreifen", Andreas Förster, S. 91
Thomson-Alcatel vs. Raytheon	Det amerikanske økonomiministerium har gjort en indsats	1994	Forhandlinger om milliardprojekt til radarovervågning af den brasilianske regnskov	Ikke nævnt	Overtagelse af kontrakten	De franske koncerner Thomson CSF og Alcatel mister kontrakten til fordel for det amerikanske firma Raytheon	„Antennen gedreht“, Wirtschaftswoche Nr.46 / 9. November 2000
Thomson-Alcatel vs. Raytheon	NSA Department of Commerce	Department of Commerce	Forhandlinger om milliardprojekt (1,4 mia. dollars) til overvågning af Amazonas (SIVA) Afsløring af bestikkelse af det brasilianske Selection Panels. Anmærkning fra Campbell: Rayethon udruster aflytningsstation i Sugar Grove	Aflytning af forhandlingen mellem Thomson-CSF og Brasilien og videregivelse af resultaterne til Raytheon Corp.	Afsløring af bestikkelse Overtagelse af kontrakten	Raytheon får kontrakten	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, af Duncan Campbell http://www:rayethon:com/sivam/contract:html
Thyssen	BP	1990	Millionkontrakt om gas- og olieudvinding i Nordsøen	Aflytning af faxmeddelelser fra den udvalgte bydende (Thyssen)	Afsløring af korruption	BP sagsøger Thyssen for at få skadeserstatning	"Maulwürfe in Nadelstreifen", Andreas Förster, S. 92
VW	Ukendt	Forløbne år	Ikke nævnt	Bl.a. i jordhøje nedgravet infrarød kamera, som via radiosignaler formidler billeder	Fremskaffelse af informationer om nye udviklinger	VW meddeler tab i trecifret omfang	„Sicherheit muss künftig zur Chefsache werden“, HB / 29. August 1996
VW	Ukendt	1996	VW's teststrækning i Ehra-Lessien	Skjult kamera	Oplysninger om nye modeller fra VW	Ikke nævnt	„Auf Schritt und Tritt“ Wirtschaftswoche Nr. 25, 11. Juni 1998

10.8. Beskyttelse mod økonomisk spionage

10.8.1. Retlig beskyttelse

I alle industrilande er tyveri af produktionshemmeligheder strafbart. Som det er tilfældet med andre aspekter af strafferetsplejen er der også forskelle med hensyn til det nationale beskyttelsesniveauer. Som regel er straffen dog betydelig lavere end for spionage, der skader den militære sikkerhed. I mange tilfælde er det kun konkurrencespionage mod virksomheder i eget land, der er forbudt, men ikke mod virksomheder i udlandet. Det gælder også for USA.

De relevante love forbyder i grunden kun spionage mellem virksomheder indbyrdes. Det er tvivlsomt om de også begrænser statslige efterretningstjenesters virksomhed. Disse har jo i kraft af loven om deres oprettelse tilladelse til at stjæle oplysninger.

Der er tale om grænsetilfælde, når efterretningstjenester stiller oplysninger, erhvervet ved spionage, til rådighed for den enkelte virksomhed. Normalt ville en sådan handling ikke være omfattet af de love, der tildeler efterretningstjenester særlige beføjelser. Navnlig indenfor EU ville det være ensbetydende med en krænkelse af traktaten (jf. kapitel...).

I praksis vil det imidlertid være meget vanskeligt for en virksomhed at påberåbe sig retlig beskyttelse ved at henvende sig til en domstol. Aflytning efterlader ingen spor og giver intet i retten holdbart bevismateriale.

10.8.2. Andre forhindringer for økonomisk spionage

Det er accepteret blandt staterne, at efterretningstjenester i forbindelse med fremskaffelse af generelle strategiske oplysninger også beskæftiger sig med det økonomisk område. Dette "gentlemen's agreement" bliver imidlertid ved konkurrencespionage til fordel for egen industri krænket i vid udstrækning. Har en stat beviseligt gjort sig skyldig deri, får den store politiske problemer. Det gælder også og navnlig en verdensmagt som USA, hvis krav på den politiske føring på verdensplan i så fald ville lide alvorlig skade. Mellemstore stater ville snarere kunne tillade sig at blive anklaget, men ikke en verdensmagt.

Bortset fra de politiske problemer er der også et praktisk spørgsmål. Hvilken virksomhed skal resultaterne fra konkurrencespionage stilles til rådighed for? Inden for luftfartsindustrien er det let at besvare, da der her på verdensplan kun er tale om to store leverandører. I alle andre tilfælde, hvor der er tale om flere leverandører, som til og med ikke er statsejede, er det yderst vanskeligt at begunstige en bestemt virksomhed. Ved videregivelse til individuelle virksomheder af detaljerede oplysninger om konkurrenters bud i forbindelse med internationale udbud ville man måske kunne forestille sig , at disse spionageoplysninger blev videregivet til alle konkurrenter i eget land. Det gælder især, hvis der er statsstøtteordninger, som de nationale konkurrenter har ligelig adgang til, som det er tilfældet i USA ved det såkaldte Advocacy Center. Ved tyveri af teknologi, som nødvendigvis må udmunde i en patentering, ville ligebehandling af virksomheder selvfølgelig ikke længere være muligt.

Det ville navnlig i det amerikanske politiske system være et stort problem. Amerikanske politikere er i forbindelse med finansiering af deres valgkampagne i høj grad afhængige af bidrag fra virksomhederne i deres valgkreds. Hvis det blev det offentligt kendt, at efterretningstjenesterne havde forfordelt en bestemt virksomhed, ville det, selv om der kun

var tale om et enkelt tilfælde, skabe enorme dønninger i det politiske system. Som den forhenværende direktør for CIA, Woolsey udtrykte det i en samtale med repræsentanter for udvalget: "In this case the hill (i.e. the US-Congress) would go mad!". Det er så sandt som det er sagt.

10.9. USA og økonomisk spionage

10.9.1 Det officielle amerikanske standpunkt med hensyn til økonomisk spionage

CIA's forhenværende direktør, Woolsey og formanden for tilsynsudvalget for efterretningstjenester i Repræsentanternes Hus, Porter Goss har i samtaler kort sammenfattet indtaget følgende standpunkt:

1. USA overvåger international telekommunikation for at få generelle oplysninger om økonomiske udviklinger, leveringer af dual use-varer og overholdelsen af embargoregler.

2. USA foretager målrettet overvågning af kommunikation fra bestemte virksomheder i forbindelse med udbud for at forhindre konkurrenceforvridning som følge af bestikkelse til skade for amerikanske virksomheder.

Det er forbudt for amerikanske virksomheder at benytte sig af bestikkelse og revisorer er pligtige til at melde det, hvis de opdager udbetaling af bestikkelsesbeløb. Hvis der ved kommunikationsovervågning konstateres bestikkelse i forbindelse med offentlige udbud, vil den amerikanske ambassadør rette henvendelse herom til regeringen i det pågældende land. De amerikanske virksomheder, der deltager i udbuddet bliver derimod ikke direkte orienteret.

10.9.2. Advocacy Center og dets rolle i USA's eksportfremme

10.9.2.1. Advocacy Center og dets opgave

Advocacy Center, som henhører under det amerikanske handelsministerium, er kernen i den nationale eksportstrategi, som blev fulgt af præsident Clinton og nu videreføres af præsident Bush. Centret blev oprettet i 1993 og har siden da bistået flere hundrede amerikanske virksomheder i forbindelse med offentlige kontrakter i udlandet. I centret forenes den amerikanske regerings relevante ressourcer, som omfatter alt fra eksperter inden for de enkelte områder til erhvervsattacheer ved ambassaderne og selve Det Hvide Hus.

10.9.2.2. Centrets arbejdsmåde

Personalet selv består kun af 12 personer (pr. 6.2.2001). Centret fungerer som kontaktpunkt mellem virksomhederne og de forskellige instanser i USA, som beskæftiger sig med eksportfremme. Det arbejder for alle firmaer uden forskelsbehandling, men støtter i henhold til klare regler kun projekter som er af national interesse for USA. Således må de leverede produkter (beregnet efter deres værdi) for 50% være af amerikansk oprindelse.

10.9.2.3. Åbne spørgsmål i forbindelse med centret

Den amerikanske regering har ikke givet tilladelse til det planlagte møde mellem udvalgets medlemmer og centret. Derfor må to spørgsmål, som der hersker tvivl om, stå uløste hen.

a) udvalget ligger inde med dokumenter, som synes at bevise, at CIA er involveret i centrets arbejde.

b) centret oplyser på Internettet, at det samler ressourcerne fra 19 "US government agencies". Andetsteds nævnes kun 14 af disse "agencies". Hvorfor er navnene på de sidste fem ikke offentliggjort?

10.10. Sikkerhed af edb-net

(*under udarbejdelse*)

10.11. Undervurdering af risici

Ordføreren ønsker på dette punkt endnu at føre nogle samtaler og undersøge skriftligt materiale. Følgende punkter vil blive behandlet:

10.11.1. Store virksomheder

10.11.2. Små og mellemstore virksomheder

10.11.3. Europæiske institutioner

10.11.4. Forskningsinstitutioner

11. Selvbeskyttelse ved kryptografi

11.1. Formål og virkning af kryptering (kodning)

11.1.1. Krypteringens/kodningens formål

Ved enhver overførelse af data er der en risiko for, at meddelelsen havner i forkerte hænder. Hvis man i et sådant tilfælde vil forhindre, at udenforstående får kendskab til indholdet, må budskabet gøres ulæseligt og uaflytbar, dvs. at det må kodes. Inden for militæret og diplomatiet har man siden tidernes morgen i den sammenhæng anvendt koder.[1]
I de sidste to årtier har kodning fået tiltagende betydning, eftersom en stadig voksende del af kommunikationen går til udlandet og ens egen stat ikke længere kan beskytte brev- og telefonhemmeligheden. Desuden har de øgede tekniske muligheder for legal aflytning/opsnapning af kommunikation i eget land fremkaldt et skærpet behov for beskyttelse hos foruroligede borgere. Og til sidst har forbryderes stigende interesse i illegal adgang til oplysninger og forfalskning deraf fremkaldt beskyttelsesforanstaltninger (f.eks. inden for banksektoren).

Ved opfindelsen af den elektriske og elektroniske kommunikation (telegraf, telefon radio, fjernskriver, faks og internet) blev det meget enklere og umådeligt hurtigere at sende meddelelser. Ulempen var, at der ikke fandtes teknisk beskyttelse mod aflytning/tapning, og at enhver med et tilsvarende apparat kunne aflytte kommunikationen, når han fik adgang til kommunikationsmidlet. Gennemført professionelt efterlader aflytning få eller slet ingen spor. Derved har kodning fået en hel ny betydning. Banksektoren begyndte som den første med fremkomsten af den elektroniske pengetrafik regelmæssigt at beskytte den derved forbundne kommunikation gennem kryptering. Med den tiltagende globalisering af økonomien blev kommunikationen også inden for dette område i det mindste for en del beskyttet ved kryptering. Med den omfattende indførelse af den helt ubeskyttede kommunikation via Internet voksede også den private borgers behov for at beskytte kommunikationen mod aflytning.

Spørgsmålet er om der findes billige, lovlige, tilstrækkelig sikre og let anvendelige metoder til kryptering af kommunikation, som gør det muligt for den enkelte at beskytte sig mod aflytning.

11.1.2. Kodningens/krypteringens funktion

Krypteringens princip er at forvandle en læselig tekst til kodesprog på en sådan måde, at den ikke længere giver mening eller giver en anden mening. Indviede kan forvandle teksten tilbage til originalversionen. Ved kryptering eller kodning laves en betydningsbærende række bogstaver f.eks. om til en meningsløs række, som ingen udenforstående forstår.

Hertil anvendes en bestemt metode (kodens algoritme), som bygger på bytning af bogstaver (transposition) og/eller erstatning af bogstaver (substitution). **Kodningsmetoden (algoritmen)** hemmeligholdes nu om stunder ikke. Tværtimod, var der for nylig et offentligt verdensomspændende udbud for den nye globale krypteringsstandard til anvendelse i erhverslivet. Det gælder også gennemførelse af en bestemt algoritme som hardware i et apparat, f.eks. en kryptofaks.

[1] Dokumenteret så langt tilbage som til antikken.

Selve **det hemmelige** er den såkaldte nøgle. Det lader sig bedst forklare med et eksempel fra et beslægtet område. Det er som regel bekendt, hvordan en dørlås fungerer, eftersom den er omfattet af et patent. Den individuelle beskyttelse af en dør følger deraf, at der for en bestemt type lås kan findes mange forskellige nøgler. Det samme gælder for kodning af oplysninger: med **en almen kendt kodningsmetode** (algoritme) kan man ved hjælp af forskellige og af de involverede hemmeligholdte individuelle nøgler **hemmeligholde mange forskellige meddelelser**.

For at skabe klarhed om disse begreb henvises til eksemplet fra den såkaldte "Cæsarkode". Den romerske feltherre Cæsar kodede meddelelser, idet han simpelthen udskiftede hvert bogstav med det tredjefølgende i alfabetet, dvs. A med D, B med E osv. Ordet **Echelon** bliver således **HFKHORQ**. Selve **algoritmen** er en **forskydning af bogstaverne** inden for alfabetet, den konkrete nøgle er den anvisning, at det er **det tredjefølgende bogstav i alfabetet**. Både kodning og dechifrering følger samme regler: bogstaverne flyttes tre pladser. Der er tale om en symmetrisk metode. Nu til dags kan en sådan kode brydes på mindre end et sekund.

Ved en god kodning kan metoden være offentlig kendt, og alligevel kan kodningen betegnes som sikkert. Dertil kræves imidlertid, at der er mange forskellige nøgler, at en efterprøvning af alle nøgler (et såkaldt **brute force attack**) også ved anvendelse af computere ikke er muligt inden for en rimelig tidsfrist. På den anden side er et stort udvalg af nøgler i sig selv ikke et tegn på kryptologisk sikkerhed, hvis algoritmen frembringer en kodet tekst, som indeholder angrebspunkter for dechifrering (f.eks. koncentration af bestemte bogstaver).[1] Cæsars kode er ud fra begge synsvinkler ingen sikker kode. Ved simpel substitution kan den hurtigt brydes om ikke andet, så på grund af bogstavernes forskellige hyppighed inden for et sprog. Der findes kun 25 forskydningsmuligheder, d.v.s. kun 25 nøgler, eftersom det latinske alfabet kun består af 26 bogstaver. Modstanderen kan her simpelthen forsøge sig frem til den passende nøgle og dechiffrere teksten.

Hvordan skal et sikkert system være?.

11.2. Sikkerhed ved kryptering

11.2.1. Generelt

Hvis man forlanger, at et kodningssystem skal være sikkert, er der to muligheder. Man kan forlange, at det er absolut sikkert, at det er umuligt at dechifrere meddelelsen uden kendskab til nøglen og at denne umulighed kan bevises matematisk. Man kan også nøjes med, at koden med den nuværende teknik ikke kan brydes og dermed synes at give sikkerhed for en periode, som langt overstiger den "kritiske" periode, hvori meddelelsen skal holdes hemmeligt.

11.2.2. Absolut sikkerhed : det såkaldte one-time pad

En absolut sikker metode er indtil videre kun det såkaldte one-time pad. Dette system blev udviklet mod slutningen af Første Verdenskrig,[2] .men senere benyttet til den røde fjernskriver

[1] Jf. også Leiberich, Vom diplomatischen Code zur Falltürfunktion - Hundert Jahre Kryptographie in Deutschland, Spektrum der Wissenschaft, Juni 1999, 26 ff.

[2] Indført af Major Joseph Mauborgne, leder af den amerikanske hærs afdeling for kryptografisk forskning. Jf.

mellem Moskva og Washington. Der er tale om en nøgle, som består af bogstaver i en fuldstændig tilfældig rækkefølge, og denne rækkefølge gentages ikke. Sender og modtager bruger disse bogstavsrækker kun en gang til kodningen og sletter nøglen omgående efter anvendelsen. Da der ikke findes en indre orden i nøglen er det for en kryptoanalytiker umuligt at bryde koden. Det er der matematisk bevis for.[1]

En ulempe ved denne fremgangsmåde er, at det ikke er let at skabe et stort antal af disse tilfældige nøgler [2]og at sikker fordeling af nøgler er vanskelig og upraktisk. Denne metode anvendes derfor ikke i almindelig erhvervskommunikation.

11.2.3. Relativ sikkerhed i forhold til den tekniske udvikling

11.2.3.1. Brug af kodnings- og dechifreringsmaskiner

Allerede inden opfindelsen af one-time pad blev der udviklet krypteringsmetoder, som gav et stort antal nøgler og kodede tekster, som indeholdt færrest mulige regelmæssigheder og derfor næsten ingen angrebspunkter for en kryptoanalyse. Med henblik på en hurtig praktisk anvendelse af disse metoder, blev der udviklet kodnings-og dechifreringsmaskiner. Den mest opsigtsvækkende af sin art var vel ENIGMA,[3] som under Anden Verdenskrig blev brugt i Tyskland. Det lykkedes en hær af kodningseksperter i Bletchley Park at bryde ENIGMAs kode ved hjælp af særlige maskiner, de såkaldte "bomber". Både ENIGMA og "bomben" var mekaniske maskiner.

11.2.3.2. Anvendelsen af computere inden for kryptologi

Opfindelsen af computeren var banebrydende for kryptologividenskaben, da dens kapacitet gjorde det muligt at anvende stadig mere komplicerede systemer. Selv om krypteringsgrundprincipperne ikke derved blev ændret, så var der dog tale om visse fornyelser. For det første blev mulighederne for endnu mere komplicerede krypteringssystemer mangedoblede, da der ikke længere var mekaniske grænser herfor, og for det andet blev krypteringsprocessen markant hurtigere.

Informationerne forarbejdes digitalt af computere med binærtal. Det betyder, at disse informationer udtrykkes i en rækkefølge af to signaler nemlig 0 og1. 1 svarer fysisk til en elektrisk spænding hhv. en magnetisering (lys), 0 til bortfald af spænding hhv. magnetisering (ingen lys). I den forbindelse er ASCII-standarderne[165] blevet indført, hvor hvert bogstav er repræsenteret af en syvcifret kombination af 0 og 1[166]. En tekst udformes således som en række 0- og 1-taller; i stedet for med bogstaver krypteres ved hjælp af tal.

I den forbindelse kan der både anvendes transposition (ombytning) og substitution

---

Singh, Geheime Botschaften (1999), 151

[1] Jf. Singh, Geheime Botschaften (1999), 151 ff.

[2] Jf. Wobst, Abenteuer Kryptologie[2] (1998), 60.

[3] Enigma blev udviklet af Arthur Scherbius og patenteret i 1928. Den har en vis lighed med en skrivemaskine, da den er forsynet med et tastatur til skrivning af en tekst, som skal kodes. Ved en tekniske anordning og roterende valse kodes teksten og den dechifreres med den samme maskine d ved hjælp af kodebøger.

[165] American Standard Code for Information Interchange

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

(udskiftning). Substitution kan f.eks. ske ved at tilføje en nøgle i form af en tilfældig talrække. Ifølge den binære matematiks regler adderes ens tal til nul (altså 0 + 0 = 0 og 1+ 1 = 0), mens to forskellige tal adderes til 1 (0 + 1 = 1). Den nye krypterede talrække, som er opstået ved addition, er således en binær talrække, der enten kan videreforarbejdes digitalt eller kan gøres læselig igen ved at fjerne den tilføjede nøgle.

Anvendelsen af computere gør det muligt at producere hemmelige tekster ved hjælp af stærke krypteringsalgoritmer, der praktisk talt ikke længere frembyder angrebspunkter for en kryptoanalyse. Dekryptering kan i så fald kun finde sted ved gennemprøvning af alle mulige nøgler. Jo længere nøglen er, desto større er muligheden for at dette ikke lykkes, også selv om der anvendes de allerkraftigste computere, på grund af den tid, det vil tage. Der findes altså brugbare metoder, som på det nuværende tekniske stade må regnes for at være sikre.

11.2.4. Standardisering og forsætlig begrænsning af sikkerheden

Som følge af udbredelsen af computere i 70'erne blev det stadig mere presserende at få standardiseret krypteringssystemerne, da det var den eneste måde, hvorpå virksomheder kunne kommunikere sikkert med deres forretningsforbindelser uden alt for store udgifter. De første bestræbelser herpå fandt sted i USA.

En stærk kryptering kan også anvendes til illegale formål eller af en eventuel militær modstander og kan også vanskeliggøre eller forhindre elektronisk spionage. Derfor har NSA krævet, at der blev valgt en krypteringsstandard, der var tilstrækkelig sikker for erhvervslivet, men som Sikkerhedstjenesten selv var i stand til at dekryptere ved hjælp af sit særlige tekniske udstyr. Derfor blev nøglens længde begrænset til 56-bit. Det mindsker antallet af mulige nøgler til 100 000 000 000 000 000 stk.[167] . Den 23. november 1976 overtog man officielt Horst Feistels såkaldte luciferkryptografering i **56-bit udgaven** Data Encryption Standard (DES) (datakryptograferingsstandard), som i et kvart århundrede var den officielle amerikanske krypteringsstandard[168]. Også Europa og Japan overtog den amerikanske krypteringsstandard, især inden for bankverdenen. DES-algoritmen har i modstrid med forlydender i diverse medier hidtil været ubrydelig; dog findes der i mellemtiden hardware, der er stærk nok til at gennemprøve alle nøgler ("brute force attack"). Triple-DES, som har en 112 bit-nøgle, regnes derimod fortsat for at være sikker. Afløseren for DES, AES (Advanced Encryption Standard - avanceret krypteringsstandard) er en europæisk metode[169], som blev udviklet under navnet Rijndael i Leuven i Belgien. **Den er hurtig og regnes for at være sikker, da man her ikke ville indføre nogen begrænsning af nøglens længde.** Dette beror på en ændret amerikansk krypteringspolitik (jf. 11.1.4. ovenfor).

Standardiseringen betød en væsentlig forenkling af krypteringen for virksomhederne. Dog er der fortsat problemer med nøgleadministrationen.

11.3. Problemerne i forbindelse med en sikker nøgleadministration/-

[167] Dette binærtal består af 56 nuller og ettaller, jf. Singh: Geheime Botschaften (1999), 03.
[168] Jf. Singh: Geheime Botschaften (1999), s. 302ff.
[169] Systemet er udviklet af to belgiske kryptografer ved Det Katolske Universitet i Leuven, Joan Daemen og Vincent Rijmen.

udveksling

11.3.1. Assymmetrisk kryptering: public key-systemet

Så længe et system arbejder med en nøgle, som bruges til både kryptering og dekryptering (symmetrisk kryptering) er det uhåndterligt, når der er tale om **mange** kommunikationspartnere. Nøglen skal nemlig **forinden** udleveres til hver ny kommunikationspartner på en sådan måde, at ingen tredjepart har fået kendskab hertil. For erhvervslivet er det besværligt i praksis, for privatpersoner kun muligt i enkelttilfælde.

Asymmetrisk kryptering kan løse dette problem: der anvendes ikke samme nøgle til kryptering og dekryptering. Meddelelsen krypteres med en nøgle, som gerne må være kendt af alle, den såkaldte **offentlige nøgle**. Der er dog tale om en envejsmetode; den giver ikke mulighed for at føre en krypteret tekst tilbage til klartekst. Derfor kan enhver, der vil have en krypteret meddelelse, også uden særlige sikkerhedsforanstaltninger sende sin kommunikationspartner sin offentlige nøgle til kryptering af meddelelsen. Dekrypteringen af den således modtagne meddelelse sker ved hjælp af en anden nøgle, **den private nøgle**, der er hemmelig og ikke sendes[170]. For at forstå metoden kan man bruge billedet med en hængelås: enhver kan få en sådan lås til at snappe i og dermed lukke en dragkiste forsvarligt, men det er kun den, der har den rigtige nøgle, der kan åbne den[171]. Den offentlige og den private nøgle udgør et sammenhængende par, men det er ikke beregningsmæssigt muligt at bestemme den private nøgle ud fra den offentlige nøgle.

Ron Rivest, Adi Shamir og Leonard Adleman har opfundet et assymetrisk krypteringssystem ved hjælp af RSA-metoden, som er opkaldt efter dem. Ved en envejsfunktion (en såkaldt faldlemsfunktion) anvendes det resultat, der opnås ved multiplikation af to meget store primtal som en del af den offentlige nøgle. Dermed krypteres klarteksten. Dekryptering kan kun ske ved hjælp af værdierne af de to anvendte primtal, men der findes ingen matematisk metode, der kan opløse multiplikationen af to primtal, så det bliver muligt at beregne de to basisprimtal af resultatet af multiplikationen. Hidtil er dette kun muligt ved systematisk afprøvning. Derfor er denne metode med den nuværende viden sikker, såfremt der vælges tilstrækkeligt høje primtal. Den eneste risiko ligger i, at en brillant matematiker på et eller andet tidspunkt finder en hurtigere metode til at opløse resultatet i faktorer. Hidtil er dette dog ikke lykkedes for nogen trods en ihærdig indsats.[172] Fra mange sider hævdes det oven i købet, at problemet er uløseligt, men et eksakt bevis herpå foreligger ikke.[173]

Public key-krypteringssystemet kræver ganske vist meget længere computertid eller anvendelse af hurtige og store computere end symmetriske systemer (f.eks. DES).

---

[170] Ideen med asymmetrisk kryptering i form af et public key-krypteringssystem stammer fra Whitfield Diffie og Martin Hellmann.
[171] Singh: Geheime Botschaften (1999), s. 327.
[172] Jf. Buchman: Faktorisierung grosser Zahlen, Spektrum der Wissenschaft 2, 199, s. 6 ff.
[173] Jf. Singh: Geheime Botschaften (1999), s. 335 f.

11.3.2. Public key-kryptering for privatpersoner

For at sikre en bredere adgang til public key-kryptering kom Phil Zimmermann på den idé at forene public key-metoden, som kræver stor computerkapacitet, med en hurtigere symmestrisk metode. Selve meddelelsen skulle krypteres ved en symmetrisk metode, den i Zürich udviklede IDEA-metode, mens nøglen for den symmetriske kryptering samtidig skulle sendes efter public key-metoden. Zimmermann udviklede et brugervenligt program kaldet PGP-programmet ("Pretty Good Privacy"), som ved et tryk på en tast (hhv. museklik) skabte de nødvendige nøgler og foretog en kryptering. Programmet blev overført til Internettet, hvor enhver kunne downloade det til sin computer. PGP blev endelig købt af den amerikanske virksomhed NAI, men står stadig til gratis rådighed for privatpersoner.[174] Kildeteksten fra de tidligere versioner blev offentliggjort, så det må formodes, at der ikke er nogen skjult bagdør indbygget. Kildeteksten til den nyeste version PGP 7, der udmærker sig ved en særlig brugervenlig grafisk overflade, offentliggøres desværre ikke længere. Der findes ganske vist stadigvæk en anden implementering af Open PGP Standards: GnuPG, som indeholder de samme krypteringsmetoder som PGP og også er kompatibel med PGP. Der er dog tale om fri software, kildekoden er kendt, og enhver kan anvende og videregive den. Det tyske Forbundsministerium for Økonomi og Teknologi har støttet overførselen af GnuPG til Windows og udviklingen af en grafisk overflade, som dog endnu ikke er helt afsluttet. Så vidt ordføreren ved, arbejdes der dog på sagen.

Samtidig findes der konkurrerende standarder til OpenPGP som f.eks. S/MIME, som støttes af mange e-mail-programmer. Ordføreren har dog ingen oplysninger om frie implementeringer heraf.

11.3.3. Fremtidige metoder

Kvantekryptografien kunne i fremtiden åbne helt nye aspekter for en sikker nøgleudveksling. Den sikrer, at aflytning ved nøgleudveksling bemærkes. Sendes fotoner med en polarisering, kan denne ikke konstateres, uden at den ændres. Dermed kan det med sikkerhed konstateres, hvis der har været andre på linjen. Kun en nøgle, der ikke er blevet aflyttet, vil så kunne anvendes. Under forsøg er det allerede lykkedes at overføre data via 48 km lyslederkabler og over 500 m i luften.[175]

11.4. Sikkerheden ved krypterede produkter

Under drøftelserne om den effektive sikkerhed ved krypteringer er det gang på gang blevet hævdet, at amerikanske produkter altid har indbygget en skjult bagdør. I medierne har f.eks. Excel sørget for store overskrifter, idet det hævdes, at halvdelen af nøglen i den europæiske version er åbent registreret på edb-registerets titelside. Microsoft har også vakt opmærksomhed i pressen, idet en hacker har fundet en "NSA-nøgle" skjult i programmet, hvilket naturligvis er blevet kraftigt dementeret af Microsoft. Da Microsoft ikke har offentliggjort sin kildekode, er dette dog ren spekulation. Hvad angår de tidligere versioner af PGP og GnuPG, kan det i hvert fald med stor sikkerhed udelukkes, at der er indbygget en skjult bagdør, da kildeteksten i

[174] Informationer om software, se www.pgpi.com
[175] Med hensyn til kvantekryptografi se Wobst: Abenteuer Kryptographie[2] (1998), 234ff.

disse tilfælde er offentliggjort.

11.5.Kryptering i konflikt med statsinteresser

11.5.1. Forsøg på at begrænse kryptering

Visse stater har i første omgang forbudt brugen af krypteringssoftware eller krypteringsmaskiner og kræver tilladelse, hvis der ønskes undtagelser fra dette forbud. I den forbindelse skal det nævnes, at der ikke kun er tale om diktaturer som Kina, Iran eller Irak. Også demokratiske stater har ved lov indskrænket brugen eller salget af krypteringsprogrammer eller -maskiner. Ganske vist skulle kommunikationen beskyttes mod at blive læst af uvedkommende privatpersoner, men staten skulle nu som før i givet fald fortsat have ret til aflytning. Myndighedernes manglende tekniske overlegenhed skulle udlignes ved lovforbud. F.eks. har Frankrig indtil for nylig haft et generelt forbud mod brug af kryptering og har krævet tilladelse hertil. I Tyskland var der for nogle år siden ligeledes en debat om begrænsning af kryptering og obligatorisk deponering af nøgler. USA har i stedet tidligere begrænset nøglelængden.

11.5.2. Betydningen af en sikker kryptering for den elektroniske handel

I mellemtiden har disse forsøg en gang for alle vist sig at være omsonst. Det er ikke kun retten til beskyttelse af privatlivets fred, men også håndfaste økonomiske interesser, der står i vejen for statens interesse i at have adgang til dekryptering og dermed til klartekster. For elektronisk handel og elektronisk bankvirksomhed står og falder med sikker kommunikation på Internettet. Kan denne ikke garanteres, vil disse handelsformer bukke under, fordi kunderne så ikke længere vil have tillid hertil. Denne sammenhæng forklarer ændringen af den amerikanske eller franske krypteringspolitik.

Det skal her bemærkes, at elektronisk handel kræver sikrere krypteringsmetoder i to henseender: ikke kun for at kunne kryptere meddelelser, men også for problemfrit at kunne fastslå forretningspartneres identitet. Den elektroniske underskrift kan nemlig foregå ved en omvendt anvendelse af public key-metoden: den private nøgle anvendes til kryptering, den offentlige nøgle til dekryptering. Denne form for kryptering bekræfter underskriftens ejermand. Enhver kan overbevise sig om en underskrifts ægthed ved at bruge en persons offentlige nøgle, men kan ikke selv efterligne underskriften. Også denne funktion er brugervenligt indarbejdet i PGP.

11.5.3. Problemer for forretningsrejsende

I mange lande er det forbudt for forretningsrejsende at bruge krypterede programmer på deres medbragte laptops. Dette gør det umuligt at beskytte kommunikation med den rejsendes firma eller sikre medførte data mod indgreb.

11.6. Praktiske problemer i forbindelse med kryptering

Hvis man skulle svare på spørgsmålet om, hvem der under hvilke omstændigheder

skulle rådes til kryptering, så bør man nok skelne mellem privatpersoner og virksomheder. Hvad privatpersoner angår, skal det siges åbent, at kryptering af fax og telefonsamtaler via kryptotelefon hhv. Cypherfax ikke er praktisk gennemførlig, ikke kun fordi anskaffelsesprisen for disse apparater er relativ høj, men også fordi anvendelsen heraf forudsætter, at samtalepartneren også har sådanne apparater, og at dette vel kun sjældent er tilfældet.

E-mails kan og bør enhver derimod kryptere. Der kan imod den ofte fremsatte påstand om, at man ikke har nogen hemmeligheder og derfor ikke behøver at kryptere, indvendes, at man jo heller ikke normalt sender skriftlige meddelelser på postkort. En ikke-krypteret mail er ikke andet end et brev uden kuvert. Kryptering af e-mails er sikker og relativ problemløs, og på Internettet findes der allerede brugervenlige systemer, som f.eks. PGP/GnuPG, der oven i købet stilles til fri rådighed for privatpersoner uden betaling. Dette er dog desværre ikke tilstrækkelig udbredt. På det punkt burde det offentlige gå foran med et godt eksempel og selv generelt foretage kryptering for at afmystificere dette.

Hvad virksomhederne angår, så bør det strengt overvåges, at følsomme informationer kun fremsendes ad sikre kommunikationsveje. Dette synes selvfølgeligt, og er det vel også for store virksomheder, men netop små og mellemstore virksomheder vil ofte videregive ukrypterede interne firmaoplysninger via e-mail, fordi de ikke er tilstrækkeligt opmærksomme på problemet. Her kan man håbe på, at industrisammenslutninger og handelskamre i stadig højere grad sørger for at orientere herom. Ganske vist er kryptering af e-mails kun et af mange sikkerhedsaspekter og har frem for alt ingen effekt, hvis informationen allerede inden krypteringen gøres tilgængelig for andre. Dette betyder, at hele arbejdsmiljøet skal sikres, så sikkerheden i de anvendte lokaler og den fysiske adgang til kontorer og computere kontrolleres. Der må også skabes hindringer for uautoriseret adgang til informationer via nettet ved hjælp af hensigtsmæssige fire-walls. Særlige risici frembyder sammenkoblingen af det interne net og Internettet. Hvis sikkerhed tages alvorligt, bør man også kun anvende driftssystemer, hvis kildekode er offentliggjort og kontrolleret, da man kun i så fald med sikkerhed kan sige, hvad der sker med oplysningerne. For virksomhederne er der således en række opgaver på sikkerhedsområdet. Der findes allerede mange firmaer på markedet, som tilbyder sikkerhedsrådgivning og -gennemførelse til acceptable priser, og udbuddet stiger konstant i takt med efterspørgslen. Desuden kan man håbe på, at industrisammenslutninger og handelskamre tager disse problemer op og især henleder de små virksomheders opmærksomhed på sikkerhedsproblemerne og hjælper dem med at udvikle og gennemføre et samlet beskyttelseskoncept.

12. EU's eksterne forbindelser og indsamling af efterretningsoplysninger

12.1. Indledning

Med vedtagelsen af Maastricht-traktaten i 1991 blev den fælles udenrigs- og sikkerhedspolitik (FUSP) etableret i sin mest grundlæggende form som Den Europæiske Unions nye politiske instrument. Seks år senere indførtes med Amsterdam-traktaten en styrket struktur til FUSP, og der blev skabt en mulighed for fælles initiativer på forsvarsområdet i EU, samtidig med at de eksisterende alliancer blev opretholdt. På grundlag af Amsterdam-traktaten og med erfaringerne fra Kosovo i erindring iværksatte Det Europæiske Råd i december 1999 i Helsinki det europæiske sikkerheds- og forsvarsinitiativ. Dette initiativ har til formål at oprette en multinational styrke på omkring 50.000-60.000 mand inden 2. halvår af 2003. Tilstedeværelsen af en sådan multinational styrke vil gøre nødvendigt at oprette en selvstændig efterretningskapacitet. En simpel integrering af WEU's eksisterende efterretningskapacitet vil ikke være tilstrækkelig til dette formål. Herudover kan det ikke undgås, at medlemsstaterne efterretningsorganer har et yderligere samarbejde, der går langt videre end de eksisterende former for samarbejde.

Den videre udvikling af FUSP er imidlertid ikke det eneste, der vil føre til et tættere samarbejde mellem EU's efterretningstjenester. Den fortsatte økonomiske integration i EU vil også gøre det nødvendigt med et mere intensivt samarbejde om indsamling af efterretningsoplysninger. En fælles europæisk økonomisk politik gør det også nødvendigt med en ensartet opfattelse af den økonomiske virkelighed uden for EU. Det er nødvendigt med en fælles beskyttelse af et fælles standpunkt under handelsforhandlinger i WTO eller med tredjelande. Stærke europæiske industrier har brug for fælles beskyttelse mod økonomisk spionage fra tredjelande.

Endelig må det understreges, at en fortsat udvikling af Unionens anden søjle og Unionens aktiviteter inden for indre og retlige anliggender også må føre til et styrket samarbejde mellem efterretningstjenesterne. Den fælles kamp mod terrorisme, ulovlig handel med våben, handel med mennesker og hvidvaskning af penge kan navnlig ikke finde sted uden et intensivt samarbejde mellem efterretningstjenester.

12.2. Muligheder for samarbejde inden for EU

12.2.1. Eksisterende samarbejde

Selv om der er en lang tradition hos efterretningstjenester for kun at overdrage de oplysninger, som de indsamler, til sig selv og måske endog en traditionel manglende tillid mellem de enkelte efterretningstjenester i EU, er samarbejdet mellem de enkelte tjenester allerede gradvist ved at blive øget. Hyppige kontakter eksisterer inden for NATO, WEU og Den Europæiske Union. Selv om efterretningstjenesterne inden for NATO stadig er betydeligt afhængige af de langt mere raffinerede bidrag fra De Forenede Stater, har oprettelsen af WEU's satellitcenter i Torrejon (Spanien) og efterretningsenheden i WEU's hovedkvarter bidraget til en mere selvstændig europæisk indsats på dette område.

12.2.2. Fordele ved en fælles europæisk efterretningspolitik

Ud over de tendenser som allerede finder sted, må det understreges, at der findes objektive fordele ved en fælles europæisk efterretningspolitik. De fordele kan beskriver på følgende måde.

12.2.2.1. Praktiske fordele

Først og fremmest findes der alt for meget klassificeret og uklassificeret materiale, som skal indsamles, analyseres og evalueres af et enkelt organ eller ved hjælp af en bilateral aftale i Vesteuropa. Kravene til efterretningstjenester spænder fra efterretningstjeneste på forsvarsområdet via efterretningsopgaver i forbindelse tredjelandes indenlandske og internationale økonomiske politik til efterretningsopgaver til fordel for bekæmpelse af organiseret kriminalitet og narkotikahandel. Selv om samarbejdet kun eksisterede i sin mest grundlæggende form, dvs. indsamling af frit tilgængelige oplysninger (OSINT), ville resultaterne fra dette samarbejde allerede være af stor betydning for EU's politikker.

12.2.2.2. Budgetmæssige fordele

På det seneste er midlerne til indsamling af efterretningsoplysninger blevet nedskåret og bliver i nogle tilfælde stadig nedskåret. Samtidig er behovet for oplysninger og dermed efterretningstjeneste steget. Disse budgetter, der er blevet nedskåret, muliggør ikke kun dette samarbejde, men gør det også lønsomt på lang sigt. Navnlig i forbindelse med opretholdelse og vedligeholdelse af tekniske faciliteter er det hensigtsmæssigt med fælles aktiviteter, når der er begrænsede midler til rådighed, men også i forbindelse med evaluering af de indsamlede oplysninger. Et forøget samarbejde vil øge effektiviteten ved indsamling af efterretningsoplysninger.

12.2.2.3. Politiske fordele

De indsamlede efterretningsoplysninger anvendes i princippet til at gøre det muligt for regeringer at træffe beslutninger på et bedre og velfunderet grundlag. Yderligere politisk og økonomisk integration i EU forudsætter, at oplysninger er tilgængelige på europæisk plan og baseret på mere end en enkelt kilde.

12.2.3. Afsluttende bemærkninger

Disse objektive fordele er kun eksempler på den stigende betydning af samarbejdet i EU. Tidligere stod nationalstaterne selv for deres eksterne sikkerhed, den indre orden, den nationale velstand og kulturelle identitet. Den Europæiske Union er i dag på mange områder ved at påtage sig en rolle, som i det mindste supplerer nationalstatens rolle. Det er umuligt at forestille sig, at efterretningstjenester vil være det sidste og eneste område, som ikke påvirkes af den europæiske integrationsproces.

12.3. Samarbejde uden for Den Europæiske Union

Siden 2. verdenskrig foregik samarbejdet inden for indsamling efterretningsoplysninger ikke i første omgang på europæisk plan, men langt mere på det transatlantiske plan. Dette er allerede blevet beskrevet tidligere, at der blev etableret meget tætte forbindelser inden for indsamling af efterretningsoplysninger mellem Det Forenede Kongerige og De Forenede Stater. De Forenede Stater var og er imidlertid også inden for efterretningsvirksomhed på forsvarsområdet i og uden for NATO den absolut mest dominerende partner. Det vigtige spørgsmål er derfor, hvorvidt stigende europæisk samarbejde inden for indsamling af

efterretningsoplysninger i alvorlig grad vil genere forbindelserne med De Forenede Stater, eller om den kan føre til en styrkelse af disse forbindelser. Hvordan vil forbindelserne mellem EU og USA udvikle sig under den nye Bush-regering? Og navnlig hvordan vil det særlige forhold mellem De Forenede Stater og Det Forenede Kongerige kunne opretholdes inden for disse rammer?

Nogle mener, at der ikke behøver at være en modsætning mellem det særlige britisk-amerikanske forhold og en yderligere udvikling af FUSP. Andre mener, at navnlig indsamling af efterretningsoplysninger kan være et anliggende, der kan tvinge Det Forenede Kongerige til at vælge, hvorvidt dets skæbne ligger i Europa eller på den anden side af Atlanten. Det Forenede Kongeriges tætte forbindelser til USA (og til andre partnere i UKUSA-alliancen) kan gøre det vanskeligere for andre EU-stater at udveksle efterretningsoplysninger indbyrdes – idet Det Forenede Kongerige ville være mindre interesseret i en udveksling internt i Europa, og fordi EU-partnerne kan tænkes at have mindre tillid til Det Forenede Kongerige. Hvis USA mener, at Det Forenede Kongerige har udviklet særlige forbindelser med dets EU-partnere, og at landet er en del europæisk særaftale, kan det ligeledes være, at USA vil være tilbageholdende med at udveksle sine efterretningsoplysninger med Det Forenede Kongerige. Yderligere EU-samarbejde inden for efterretningsvirksomhed kan derfor være en alvorlig prøve for Det Forenede Kongeriges europæiske ambitioner såvel som for EU's mulighed for integration.

Under de nuværende omstændigheder er det imidlertid ret usandsynligt, at De Forenede Staters teknologiske fordel kan erstattes af selv særdeles hurtige fremskridt inden for samarbejdet mellem de europæiske partnere på kort og selv på længere sigt. Den Europæiske Union vil ikke være i stand at etablere et sofistikeret net af SIGINT-satelitter, satellitter til billedteknik og jordstationer. Den Europæiske Union vil ikke på kort sigt kunne udvikle et højt sofistikeret computernet, der er nødvendig for udvælgelse og evaluering af det indsamlede materiale. Den Europæiske Union vil ikke være rede til at afsætte de nødvendige midler i budgettet for at blive et reelt alternativ til De Forenede Staters bestræbelser inden for efterretningsvirksomhed. Det vil derfor allerede ud fra en teknologisk og budgetmæssig synsvinkel være i EU's interesse at opretholde tætte forbindelser med De Forenede Stater inden for indsamling af efterretningsoplysninger. Det vil imidlertid også ud fra en mere politisk synsvinkel være vigtigt at opretholde og i givet fald at styrke forbindelserne med De Forenede Stater navnlig med hensyn til den fælles bekæmpelse af organiseret kriminalitet, terrorisme, handel med narkotika og våben samt hvidvaskning af penge. Fælles efterretningsoperationer er nødvendige for at kunne støtte de fælles bestræbelser. Fælles fredsbevarende aktioner såsom i det tidligere Jugoslavien stiller krav om et større europæisk bidrag inden for alle indsatsområder.

På den anden side bør en stigende europæisk bevidsthed ledsages af et større ansvar fra europæisk side. Den Europæiske Union bør blive en mere ligeværdig partner ikke kun på det økonomiske område, men også på forsvarsområdet og derfor også inden for indsamling af efterretningsoplysninger. En mere selvstændig europæisk efterretningskapacitet bør derfor ikke betragtes som en svækkelse af de transatlantiske forbindelser, men bør anvendes som en styrkelse ved at gøre Den Europæiske Union til en mere lige og kapacitetsfyldt partner. Samtidig bør Den Europæiske Union gøre en selvstændig indsats for at beskytte sin økonomi og sin industri mod ulovlige og uønskede trusler såsom økonomisk spionage, cyber-kriminalitet og terroristangreb. Det er derimod nødvendigt med forståelse på begge sider af

Atlanten inden for industrispionage. Den Europæiske Union og De Forenede Stater bør blive enige om et regelsæt for, hvad der er tilladt, og hvad der ikke er tilladt på dette område. For at styrke det transatlantiske samarbejde på dette område kunne man tage et fælles initiativ i WTO for at bruge mekanismerne i denne organisation til at beskytte en fair økonomisk udvikling på verdensplan.

12.4. Afsluttende bemærkninger

Selv om det grundlæggende, nemlig beskyttelse af europæiske borgeres privatlivs fred, stadig er gældende, bør en yderligere udvikling af en fælles europæisk efterretningskapacitet anses for nødvendig og uundgåelig. Samarbejde med tredjelande og navnlig De Forenede Stater bør opretholdes, og hvad der er meget sandsynligt, styrkes. Dette indebærer ikke nødvendigvis, at europæiske SIGINT-aktiviteter automatisk bør integreres i EU's uafhængige Echelon-system, eller at EU skulle blive fuldgyldig partner af den eksisterende UKUSA-alliancen. Det bør imidlertid aktivt overvejes, hvorvidt der bør udvikles et behørigt europæisk ansvar inden for indsamling af efterretningsoplysninger. En integreret europæisk efterretningskapacitet forudsætter samtidig, at der indføres en ordning for politisk kontrol med disse organers aktiviteter. Der bør træffes beslutninger om måden, hvorpå efterretningsoplysninger skal vurderes, og hvordan man træffer de politiske beslutninger, som er resultatet af en analyse af efterretningsrapporteringer. Hvis en sådan ordning for politisk kontrol og dermed politisk bevidsthed om og ansvar for processen for indsamling af efterretningsoplysninger ikke indføres, vil det være til skade for den europæiske integrationsproces.

13. Konklusioner og henstillinger

13.1 Indledende bemærkning

I dette kapitel sammenfattes erkendelser og mulige konklusioner. Det må ikke betragtes som endeligt. Det er ordførerens mening, at det skal bruges som arbejdsgrundlag for den politiske diskussion i udvalget. Teksten vil senere blive ændret, for at kunne medtage elementer fra denne drøftelse.

13.2 Konklusioner

Eksistensen af et globalt aflytningssystem til privat og økonomisk kommunikation (Echelon)
Eksistensen af et verdensomspændende kommunikationsaflytningssystem, som fungerer i kraft af et samarbejde mellem USA, Det Forenede Kongerige, Canada, Australien og New Zealand inden for rammerne af UKUSA-aftalen, kan ikke længere drages i tvivl. At systemet vitterligt hedder "Echelon" forekommer sandsynligt ud fra de forhåndenværende indicier, men er af sekundær betydning. Det vigtigste er, at systemet ikke har til formål at aflytte militær kommunikation, men de private borgeres og erhvervslivets kommunikation.

Analysen har vist, at systemets styrke er langt fra den, der til dels er tillagt den i medierne.

Aflytningssystemets grænser
Aflytningssystemet er baseret på verdensomspændende aflytning af satellitkommunikation. I områder med en stor kommunikationstæthed formidles kun en mindre del af kommunikationen via satelliter. Det betyder, at den overvejende del af kommunikationen ikke kan aflyttes af jordbaserede anlæg, men kun ved tapning af kabel og opsnapning af radiokommunikation. Undersøgelserne har imidlertid vist, at Echelon-staterne kun har greb om en meget lille del af kabel- og radiobaseret kommunikation, og kun kan analysere en begrænset del af kommunikationerne, eftersom det er en opgave, der kræver meget personale.

Den mulige eksistens af andre aflytningssystemer
Da aflytning af kommunikation er en almindelig anvendt fremgangsmåde blandt efterretningstjenester, kan et sådant system også bruges af andre stater, for så vidt de råder over de nødvendige finansielle midler og har de geografiske forudsætninger dertil. Frankrig , som i hvert fald opfylder de geografiske forudsætninger, ville i kraft af sine oversøiske territorier som eneste EU-medlemsstat være i stand til på egen hånd at oprette et globalt aflytningssystem. Der er oplysninger, der tyder på, at også Rusland ville kunne drive et sådant system.

Forenelighed med EU-retten
Hvad angår foreneligheden af et system som Echelon med gældende EU-ret, må man skelne mellem de forskellige anvendelser:
Anvendes systemet kun til efterretningsformål, er det ikke i strid med EU-ret, da statssikkerheds tjenester og deres aktiviteter ikke er omfattet af EF-traktaten, men henhører under EU-traktatens Afsnit V (FUSP). Der foreligger endnu ingen relevante bestemmelser og følgelig er der ingen berøringspunkter. Misbruges systemet derimod til konkurrencespionage,

er det i strid med medlemsstaternes pligt til loyalt samarbejde og tanken om et fælles marked med fri konkurrence. Hvis en medlemsstat deltager i en sådan aktivitet, er der tale om en krænkelse af EU-retten.

Forenelighed med den grundlæggende ret til privatsfæren (Artikel 8 i EMK)
Enhver aflytning af kommunikation er et alvorligt indgreb i den enkeltes privatsfære. I henhold til artikel 8, der beskytter privatsfæren, er indgreb kun tilladt med henblik på beskyttelse af den nationale sikkerhed, for så vidt der er fastlagt bestemmelser herom i den nationale lovgivning. Disse bestemmelser skal være almen tilgængelige og fastlægge, under hvilke omstændigheder og forhold myndighederne må gøre et sådant indgreb. Indgrebet skal være afpasset efter, hvad der er nødvendigt, og der skal derfor foretages en afvejning af interesser. Det er ikke tilstrækkeligt, at indgrebet er nyttigt eller ønskværdigt.
Et efterretningssystem, som aflytter kommunikation uden at sikre overholdelsen af proportionalitetsprincippet, er ikke forenelig med den europæiske menneskerettighedskonvention (EMK). Ligeledes foreligger der en krænkelse af EMK, hvis den ordning, som kommunikationsovervågningen er baseret på, savner et retsgrundlag, ikke er almen tilgængelig eller er formuleret på en sådan måde, at konsekvenserne ikke er forudsigelige for den enkelte borger. Da de bestemmelser, som danner grundlaget for den amerikanske efterretningstjeneste virke i udlandet, for det meste er fortrolige, er det i hvert fald tvivlsomt om proportionalitetsprincippet respekteres. Der er sandsynligvis tale om en krænkelse af de af Menneskerettighedsdomstolen fastlagte principper om en bestemmelses tilgængelighed og forudsigeligheden af dens virkning. Skønt USA ikke selv er kontraherende part i EMK, må medlemsstaterne opfylde deres forpligtelser i henhold til denne konvention. De kan ikke uddrage sig deres forpligtelser i henhold til EMK ved at lade andre landes sikkerhedstjenester, som er underlagt mindre stregne bestemmelser, udøve deres virke på deres territorium. Ellers ville legalitetsprincippet og dets to elementer - tilgængelighed og forudsigelighed - blive gjort virkningsløse og Menneskerettighedsdomstolens retspraksis miste sin betynding.
Efterretningstjenesters ved lov legitimerede virksomhed er kun komform med de grundlæggende rettigheder, hvis der desuden findes et fyldestgørende kontrolsystem, som skal forhindre, at den hemmelige aktivitet bliver en del af forvaltningsapparatet. I betragtning af , at Menneskerettighedsdomstolen udtrykkeligt har fremhævet betydningen af et effektivt kontrolsystem for efterretningsvirksomhed, forekommer det betænkeligt, at visse medlemsstater ikke har et selvstændigt parlamentarisk kontrolorgan for efterretningstjenester.

Er EU-borgeren tilstrækkelig beskyttet mod efterretningsvirksomhed?
Der kan næppe tales om tilstrækkelig beskyttelse, eftersom EU-borgernes beskyttelse afhænger af retsstillingen i den enkelte medlemsstat, som udviser meget store forskelle på dette punkt og for en del slet ikke råder over parlamentariske kontrolorganer. EU-borgerne har en grundlæggende interesse i, at de nationale parlamenter har et officielt særligt tilsynsudvalg, som overvåger og fører kontrol med efterretningstjenesternes aktiviteter. Der, hvor der findes kontrolorganer, fristes de imidlertid i høj grad til snarere at beskæftige sig med indenrigsefterretningstjenesternes virke end med udenrigsefterretningstjenesterne, da det som regel kun er den førstenævnte tjenestes aktivitet, som berører landets egne borgere.

Ved samarbejde mellem efterretningstjenester inden for rammerne af FUSP må institutionerne vedtage regler, der yder EU-borgerne tilstrækkelig beskyttelse.

Økonomisk spionage

Det indgår i udenrigsefterretningstjenesters opgave at beskæftige sig med økonomiske data, herunder sektorudviklinger, udviklingen på råstofmarkederne, overholdelse af embargoer og regler for levering af varer med dobbelt anvendelse (dual use) mm. Af disse grunde foretages der ofte overvågning af de relevante virksomheder. Situationen bliver imidlertid uacceptabel, når efterretningstjenesterne lader sig bruge til konkurrencespionage, idet de udspionerer udenlandske virksomheder for at skaffe virksomheder i eget land en konkurrencefordel. Det hævdes ofte, at det globale aflytningssystem anvendes til dette formål, men der foreligger intet tilfælde, hvor dette er bevist. Følsomme virksomhedsoplysninger befinder sig jo først og fremmest i selve virksomheden, og det betyder, at der med henblik på konkurrencespionage først og fremmest gøres forsøg på at få oplysninger via medarbejdere eller indslusede personer eller ved at trænge ind i det interne edb-net. Kun når følsomme data kommer ud via nettet eller radio (satellit), kan et kommunikationsovervågningssystem anvendes til konkurrencespionage. Det sker systematisk i følgende tre tilfælde:

- ved virksomheder, der arbejder inden for tre tidszoner, således at mellemresultater sendes fra Europa til Amerika og videre til Asien;
- ved multinationale selskabers videokonferencer via V-Sat eller kabel;
- når der forhandles om vigtige kontrakter på stedet (f.eks. i bygge- og anlægssektoren, telekommunikationsinfrastruktur, nyoprettelse af transportsystemer osv.) og der derfra skal føres samråd med hovedkontoret.

Muligheder for selvbeskyttelse

Virksomheder skal sikre hele arbejdsmiljøet og alle kommunikationsmidler, som anvendes til overførsel af følsomme oplysninger. Der findes tilstrækkelig sikre krypteringssystemer til varierende priser på det europæiske marked. Også private må indtrængende opfordres til at kryptere deres e-mail, da en ikke-krypteret e-mail er som et brev uden konvolut. Der findes på Internet rimeligt brugervenlige systemer, som sågar stilles gratis til rådighed til privat brug.

Et samarbejde mellem efterretningstjenester inden for EU

EU er nået til enighed om at koordinere efterretningstjenesternes indsamling af oplysninger inden for rammerne af den gradvise udformning af en fælles sikkerheds- og forsvarspolitik, samtidigt med at samarbejdet på dette område med andre partnere fortsættes. Et samarbejde mellem efterretningstjenesterne inden for EU synes at være ønskeligt , dels fordi det ville være ulogisk at tale om en fælles sikkerhedspolitik uden inddragelse af sikkerhedstjenesterne, og dels fordi det ville indebære mange professionelle, økonomiske og politiske fordele. Det ville også være mere i overensstemmelse med tanken om at optræde som ligeværdig partner over for USA og ville kunne samle alle medlemsstater om et system, som udformes konform med EMK. En tilsvarende kontrol fra Europa-Parlamentets side må i så fald selvfølgelig være sikret. Europa-Parlamentet er i færd med at udarbejde sine egne regler for behandling af fortrolige og følsomme oplysninger og dokumenter.

13.3. Henstillinger

Om indgåelse og ændring af internationale aftaler om beskyttelse af borgerne og virksomhederne

1. Europarådets generalsekretær opfordres til at foreslå ministerudvalget at undersøge, hvorvidt det ville være hensigtsmæssigt at tilpasse den i artikel 8 i EMK garanterede

beskyttelse af privatsfæren til de moderne kommunikationsmetoder og aflytningsmuligheder enten i en tillægsprotokol eller sammen med reglerne for databeskyttelse inden for rammerne af en revision af databeskyttelseskonventionen, forudsat at hverken retsbeskyttelsesniveauet som udviklet i Menneskerettighedsdomstolens retspraksis eller den fleksibilitet, der er nødvendig for tilpasning til videre udviklinger, derved forringes.

2. Medlemsstaterne opfordres til at skabe et europæisk platform for at vurdere bestemmelserne vedrørende sikring af brev- og telefonhemmeligheden, at vedtage en fælles tekst herom, som sikrer beskyttelsen af privatsfæren, som fastlagt i artikel 7 i Det Europæiske Charter for Grundlæggende Rettigheder, for alle EU-borgere på medlemsstaternes territorium i dets helhed og desuden garanterer, at efterretningstjenesters virksomhed er konform med de grundlæggende rettigheder, og opfylder betingelserne i betænkningens kapitel 8, særlig 8.3.4. som afledt af artikel 8 i EMK.

3. Europarådets medlemsstater anmodes om at vedtage en tillægsprotokol, som gør det muligt for De Europæiske Fællesskaber at tiltræde EMK, eller at overveje andre foranstaltninger, som kan udelukke konflikter i retsplejen mellem Menneskerettighedsdomstolen i Strasbourg og Domstolen i Luxemburg.

4. FN's generalsekretær opfordres til at pålægge det kompetente udvalg at forelægge forslag om tilpasning af artikel 17 i Den Internationale Konvention om Borgerlige og Politiske Frihedsrettigheder, som sikrer beskyttelsen af privatsfæren, til den nye teknologiske udvikling.

5. USA opfordres til at underskrive tillægsprotokollen til Den Internationale Konvention om Borgerlige og Politiske Frihedsrettigheder, således at borgeres klager mod USA på grund af krænkelse af konventionen, kan forelægges konventionens menneskerettighedskomite; de relevante amerikanske ngo'er, herunder nanvlig ACLU (American Civil Liberties Union) og EPIC (Electronic Privacy Information Center) anmodes om at lægge et tilsvarende pres på den amerikanske regering.

National lovgivning med henblik på beskyttelse af borgere og virksomheder

6. Medlemsstaterne opfordres til at vurdere deres nationale lovgivning om efterretningsvirksomhed i forhold til de grundlæggende rettigheder.

7. Medlemsstaterne opfordres til at tilstræbe et fælles beskyttelsesniveau med hensyn til efterretningsvirksomhed, som retter sig efter det højeste nationale beskyttelsesniveau, eftersom de borgere, der er berørt af en udenrigsefterretningstjenestes virke generelt er statsborgerne i andre stater og derfor også i de andre medlemsstater.

8. EU-institutionerne opfordres til i tilfælde af et samarbejde af efterretningstjenesterne inden for rammerne af FUSP at vedtage tilstrækkelige beskyttelsesregler til fordel for EU-borgerne; Europa-Parlamentet må som det oplagte kontrolorgan fra sin side skabe de nødvendige forudsætninger for overvågning af dette yderst følsomme område, således at det er realistisk, men også forsvarligt at kræve de fornødne kontrolbeføjelser.

Særlige foranstaltninger til bekæmpelse af økonomisk spionage

9. Medlemsstaterne opfordres til at overveje, hvorvidt økonomisk spionage og bestikkelse med henblik på at skaffe kontrakter kan bekæmpes ved europæiske og folkeretlige bestemmelser, navnlig om der er mulighed for en ordning inden for rammerne af WTO, som tager højde for den konkurrenceforvridende virkning af en sådan fremgangsmåde, f.eks. ved at kræve annulering af sådanne kontrakter.

10. Medlemsstaterne opfordres til i en fælles entydig erklæring at forpligte sig til ikke at udøve økonomisk spionage mod hinanden, og derved at bekræfte deres forpligtelse til EF-traktatens ånd og bestemmelser.

Foranstaltninger i retsanvendelsen og kontrollen dermed

11. Der rettes en appel til de nationale parlamenter, som ikke råder over et selvstændigt parlamentarisk kontrolorgan med henblik på overvågning af efterretningstjenester, om at oprette et sådant.

12. De nationale tilsynsudvalg for efterretningstjenesterne anmodes om i udøvelsen af de kontrolbeføjelser, der er overdraget dem, at lægge stor vægt på beskyttelsen af privatsfæren, uanset om der er tale om overvågning af egne statsborgere, EU-statsborgere eller borgere fra tredelande.

13. Medlemsstaternes efterretningstjenester opfordres til kun at tage imod oplysninger fra andre efterretningstjenester, hvis disse kan formidles under forudsætninger, der opfylder kravene i landets egen lovgivning, eftersom medlemsstaterne ikke kan frigøre sig fra de forpligtelser, som udspringer af EMK, ved at rette henvendelse til andre efterretningstjenester.

14. Der rettes en appel til Tyskland og England om at gøre yderligere tilladelse til aflytning af kommunikation på deres territorium ved de amerikanske efterretningstjenester betinget af, at den er i overensstemmelse med EMK, dvs, at indgrebet respekterer proportionalitetsprincippet, at retsgrundlaget er tilgængeligt og og at der er en tilsvarende effektiv kontrol, da de bærer ansvaret for, at efterretningsvirksomhed på deres territorium, hvad enten den er tilladt eller tålt, er i overensstemmelse med menneskerettighederne.

Fremme af borgernes og virksomhedernes selvbeskyttelse

15. Kommissionen og medlemsstaterne opfordres til at udarbejde programmer, som skærper borgernes og virksomhedernes bevidsthed med hensyn til sikkerhedsproblematikken og samtidig at tilbyde praktisk hjælp til udarbejdelse og gennemførelse af omfattende beskyttelseskoncepter.

16. Kommissionen og medlemsstaterne opfordres til at udarbejde hensigtsmæssige foranstaltninger til fremme, udvikling og fremstilling af europæisk krypteringsteknologi og -software, og navnlig at støtte projekter, som skal udvikle brugervenligt krypteringssoftware med offentlig kildetekst (open source text).

17. Kommissionen og medlemsstaterne opfordres til at fremme softwareprojekter, hvis kildetekst er offentligt, eftersom man kun ad den vej kan sikre, at der ikke er indbygget

"backdoors" (såkaldt "open source software") .

18. EU-institutionerne og de offetnlige forvaltninger i medlemsstaterne opfordres til systematisk at anvende kryptering af e-mail for derved på længere sigt at lade kryptering blive normen.

Andre foranstaltninger

19. Virksomhederne opfordres til at samarbejde mere intensivt med sikkerhedsinstitutioner, at gøre dem bekendt med angreb udefra med henblik på økonomisk spionage for derved at øge disse insitutionernes effektivitet.

20. Kommisisonen opfordres til at forelægge et forslag om oprettelse af en rådgivningsinstans for spørgsmål om sikkerhed i forbindelse med virksomhedsinformationer, som har til opgave at skærpe bevidstheden og også skal yde praktisk hjælp.

21. Europa-Parlamentet opfordres til at arrangere en international kongres om privatsfærens beskyttelse mod telekommunikationsovervågning, for derved at skabe et platform, hvor ngo'er fra Europa, USA og andre stater kan drøfte de grænseoverskridende og internationale aspekter og koordinere aktivitetsområder og fremgangsmåder.