BETÆNKNING

om eksistensen af et globalt system til aflytning af privat og økonomisk kommunikation (Echelon-aflytningssystemet) (2001/2098 (INI)

Det Midlertidige Udvalg om Echelon-aflytningssystemet

Ordfører: Gerhard Schmid
"Sed quis custodiet ipsos custodes"
Juvenal (ca. 60-130 e.K.), 6. Satire, 347
## INDHOLD

<table>
<thead>
<tr>
<th>Side</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROTOKOLSIDE</td>
</tr>
<tr>
<td>FORSLAG TIL BESLUTNING</td>
</tr>
<tr>
<td>BEGRUNDELSE</td>
</tr>
</tbody>
</table>

### 1. Indledning

1.1. Nedsættelse af udvalget | 22 |
1.2. Påstandene i de to STOA-undersøgelser om et globalt aflytningssystem med dæknavnet Echelon | 22 |
1.2.1. Den første STOA-rapport fra 1997 | 22 |
1.2.2. STOA-rapporterne fra 1999 | 22 |
1.3. Udvalgets mandat | 23 |
1.4. Hvorfor ikke et undersøgelsesudvalg? | 23 |
1.5. Arbejdsmetode og arbejdsplan | 24 |
1.6. Echelon-systemets tilskrevne egenskaber | 24 |

### 2. Efterretningstjenester og deres virksomhed

2.1. Indledning | 26 |
2.2. Hvad er spionage | 26 |
2.3. Spionagemål | 26 |
2.4. Spionagemetoder
   2.4.1. Menneskets rolle i spionagen | 27 |
   2.4.2. Analysering af elektromagnetiske signaler | 27 |
2.5. Bestemte efterretningstjenesters virksomhed | 28 |

### 3. Tekniske forudsætninger for at aflytte telekommunikation

3.1. Forskellige kommunikationsmediers eksponering for aflytning | 30 |
3.2. Muligheder for at aflytte på stedet | 30 |
3.3. Muligheder forbundet med et globalt arbejdende aflytningssystem | 31 |
   3.3.1. Adgang til kommunikationsmedierne | 31 |
   3.3.2. Muligheder for automatisk analyse af opfanget kommunikation: anvendelse af filtre | 35 |
   3.3.3. Den tyske efterretningstjeneste som eksempel | 36 |

### 4. Den tilgrundliggende teknologi for satellitkommunikation

4.1. Kommunikationssatelliters betydning | 37 |
4.2. Hvordan en satellitforbindelse fungerer | 38 |
   4.2.1. Geostationære satellitter | 38 |
   4.2.2. En satellitkommunikationsforbindelses signalvej | 38 |
   4.2.3. De vigtigste eksisterende satellitkommunikationssystemer | 39 |
5. Indiciebevis på eksistensen af mindst ét globalt aflytningssystem

5.1 Hvorfor indiciebevis?
5.1.1. Påvisning af efterretningstjenesternes aflytningsaktiviteter
5.1.2. Påvisning af eksistensen af stationer i de geografisk nødvendige områder
5.1.3. Bevis for et snævert efterretningssamarbejde
5.2. Hvorledes identificerer man en station til aflytning af satellitkommunikation?
5.2.1. Kriterium 1: Adgang til anlæggene
5.2.2. Kriterium 2: Antennernes art
5.2.3. Kriterium 3: Antennestørrelsen
5.2.4. Kriterium 4: Dokumentation fra officiel side
5.3. Offentligt tilgængelige oplysninger om kendte lyttestationer
5.3.1. Metode
5.3.2. Præcis analyse
5.3.3. Sammenfatning af resultaterne
5.4. UKUSA-aftalen
5.4.1. UKUSA-aftalens historiske udvikling
5.4.2. Belæg for aftalens eksistens
5.5 Evaluering af deklassificeret amerikansk materiale
5.5.1. Dokumenternes art
5.5.2. Dokumenternes indhold
5.5.3. Sammenfatning
5.6. Oplysninger fra forfattere og journalister
5.6.1. Nicky Hager
5.6.2. Duncan Campbell
5.6.3. Jeff Richelson
5.6.4. James Bamford
5.6.5. Bo Elkjær og Kenan Seeberg
5.7. Udtalelser af tidligere efterretningsmedarbejdere
5.7.1 Margaret Newsham (tidligere medarbejder i NSA)
5.7.2. Wayne Madsen (tidligere NSA-medarbejder)
5.7.3. Mike Frost (tidligere medarbejder i den canadiske efterretningstjeneste)
5.7.4. Fred Stock (tidligere medarbejder i den canadiske efterretningstjeneste)
5.8 Regeringsoplysninger
5.8.1. Udtalelser fra americansk side
5.8.2. Udtalelser fra engelsk side
5.8.3. Udtalelser fra australsk side
5.8.4. Udtalelser fra newzealandsk side
5.8.5. Udtalelser fra nederlandsk side
5.8.6. Udtalelser fra italiensk side
5.9. Forespørgsler til Rådet og Kommissionen .................................................................73
5.10. Parlamentsrapporter ..................................................................................................74
5.10.1. Rapporter fra det belgiske kontroludvalg Comité Permanent R.............................74
5.10.2. Rapport fra den franske Nationalforsamlings Udvalg for Nationalt .........................74
5.10.3. Rapport fra det italienske parlamentariske udvalg om informations- og sikkerhedstjenester og statssikkerhed ...................................................................................75
6. Kan der findes andre globale aflytningssystemer? ...........................................................76
   6.1. Forudsætninger for et sådant system .........................................................................76
   6.1.1. Teknisk-geografiske forudsætninger ........................................................................76
   6.1.2. Politisk-økonomiske forudsætninger ........................................................................76
   6.2. Frankrig ........................................................................................................................76
   6.3. Rusland .......................................................................................................................77
   6.4. De øvrige G-8 stater og Kina .........................................................................................78
7. Foreneligheden af kommunikationsaflytningssystemer af "Echelon"-typen med EU-retten .................................................................79
   7.1. Bemærkninger ..............................................................................................................79
   7.2. Det efterretningstjenestelige systems forenelighed med EU-retten .........................79
   7.2.1. Forenelighed med EF-retten ....................................................................................79
   7.2.2. Forenelighed med anden EU-ret ..............................................................................80
   7.3. Spørsmålet om foreneligheden, hvis et aflytningssystem misbruges til konkurrencespionage .................................................................81
   7.4. Resultat .......................................................................................................................81
8. Efterretningstjenesters kommunikationsovervågning og foreneligheden heraf med den grundlæggende ret til privatsfæren .................................................................................83
   8.1. Kommunikationsovervågning som et indgreb i den grundlæggende ret til privatsfæren ................................................................................................................83
   8.2. Beskyttelse af privatsfæren gennem internationale aftaler ...........................................83
   8.3. Den europæiske menneskerettighedskonvention (EMK) .............................................84
   8.3.1. EMK's betydning for EU .........................................................................................84
   8.3.2. Rækkevidden af EMK's rumlige og personlige beskyttelse ........................................84
   8.3.3. Telekommunikationsovervågning og artikel 8 i EMK .............................................85
   8.3.4. Betydningen af artikel 8 i EMK for efterretningstjenesvendighed ..........................86
   8.4. Pligten til at være på vagt over for udenlandske efterretningstjenester .................87
   8.4.1. Omgåelse af artikel 8 i EMK ved at inddragelse af udenlandske efterretningstjenester .................................................................................................................87
   8.4.2. Konsekvenserne af at tåle ikke-europæiske efterretningstjenesters virke på EMK- staternes territorium ........................................................................................................88
9. Er EU's borgere tilstrækkeligt beskyttede over for efterretningstjenesvendighed? ..........91
   9.1. Beskyttelse over for efterretningstjenesvendighed: en opgave for de nationale parlamerter ..................................................................................................................91
   9.2. De nationale myndigheders beføjelser til gennemførelsen af overvågningsforanstaltninger ................................................................................................................91
   9.3. Kontrol med efterretningstjenesterne ..........................................................................92
9.4. Vurdering af situationen for de europæiske borgere ..................................................... 95

10. Beskyttelse mod økonomisk spionage................................................................................. 97

10.1. Spionagens mål: erhvervslivet....................................................................................... 97

10.1.1. De enkelte spionagemål......................................................................................... 97

10.1.2. Konkurrencespionage ............................................................................................ 97

10.2. Skaden som følge af økonomisk spionage .................................................................. 98

10.3. Hvem spionerer?.......................................................................................................... 99

10.3.1. Egne medarbejdere (insiderdelikt).......................................................................... 99

10.3.2. Private spionagefirmaer....................................................................................... 99

10.3.3. Hackere................................................................................................................ 100

10.3.4. Efterretningstjenester ........................................................................................ 100

10.4. Hvordan spioneres der?................................................................................................ 100

10.5. Staters økonomiske spionage..................................................................................... 100

10.5.1. Efterretningstjenesters strategiske økonomiske spionage ..................................... 100

10.5.2. Efterretningstjenesters deltagelse i konkurrencespionage ..................................... 101

10.6. Egner Echelon sig til industrihugspionage? ................................................................ 101

10.7. Offentliggjorte tilfælde............................................................................................... 102

10.8. Beskyttelse mod økonomisk spionage........................................................................ 107

10.8.1. Retlig beskyttelse.................................................................................................. 107

10.8.2. Andre forhindringer for økonomisk spionage ....................................................... 107

10.9. USA og økonomi efter Den Kolde Krig .................................................................... 108

10.9.1. Udfordringen for den amerikanske regering: Økonomisk spionage mod amerikanske

virksomheder ...................................................................................................................... 108

10.9.2. Den amerikanske regerings holdning til aktiv økonomisk spionage ....................... 110

10.9.3. Retssituationen ved bestikkelse af embedsmænd................................................... 111

10.9.4. Advocacy Center og dets rolle i USA's eksportfremme ......................................... 112

10.10. Sikkerhed i forbindelse med edb-net ....................................................................... 114

10.10.1. Betydningen af dette kapitel ............................................................................... 114

10.10.2. Risikoen ved brugen af moderne informationsteknologier i erhvervslivet .......... 114

10.10.3. Hyppigheden af angreb på net ............................................................................ 116

10.10.4. Gerningsmænd og metoder ................................................................................ 116

10.10.5. Hackerangreb udefra .......................................................................................... 117

10.11. Undervurdering af risici ............................................................................................ 117

10.11.1. Risikobevidsthed i erhvervslivet ........................................................................ 117

10.11.2. Risikobevidsthed i erhvervslivet ........................................................................ 117

11. Selvbeskyttelse ved kryptografi........................................................................................ 120

11.1. Formål og virkning af kryptering (kodning)................................................................ 120

11.1.1. Krypteringens/kodningens formål ....................................................................... 120

11.1.2. Kodningens/krypteringens funktion ................................................................... 120

11.2. Sikkerhed ved kryptering........................................................................................... 121

11.2.1. Generelt .............................................................................................................. 121

11.2.2. Absolut sikkerhed : det såkaldte one-time pad .................................................. 121

11.2.3. Relativ sikkerhed i forhold til den tekniske udvikling ........................................ 122

11.2.4. Standardisering og forsættlig begrænsning af sikkerheden .................................. 123

11.3. Problemerne i forbindelse med en sikker nøgleadministration/- udveksling ............ 124
11.3.1. Asymmetrisk kryptering: public key-systemet
11.3.2. Public key-kryptering for privatpersoner
11.3.3. Fremtidige metoder
11.4. Sikkerheden ved krypterede produkter
11.5. Kryptering i konflikt med statsinteresser
11.5.1. Forsøg på at begrænse kryptering
11.5.2. Betydningen af en sikker kryptering for den elektroniske handel
11.5.3. Problemer for forretningsrejsende
11.6. Praktiske problemer i forbindelse med kryptering

12. EU's eksterne forbindelser og indsamling af efterretningsoplysninger
12.1. Indledning
12.2. Muligheder for samarbejde inden for EU
12.2.1. Eksisterende samarbejde
12.2.2. Fordele ved en fælles europæisk efterretningspolitik
12.2.3. Afsluttende bemærkninger
12.3. Samarbejde uden for Den Europæiske Union
12.4. Afsluttende bemærkninger

13. Konklusioner og henstillinger
13.1. Konklusioner
13.2. Henstillinger

MINDRETLAUSUDTALELSER OG BILAG OFFENTLIGGJORT SÆRSKILT I DEL 2
PROTOKOLSIDE


På sidstnævnte møde vedtog det forslag til beslutning (for: 27; imod: 5; hverken/eller: 2).

Til stede under afstemningen var: Carlos Coelho (formand), Elly Plooij-van Gorsel, Neil MacCormick og Giuseppe Di Lello Finuoli (næstformænd), Gerhard Schmid (ordfører), Mary Elizabeth Banotti, Bastiaan Belder, Maria Berger, Charlotte Cederschiöld, Gérard Deprez, Giorgios Dimitrakopoulos, Robert Evans, Colette Flesch, Pernille Frahm, Anna Karamanou, Eva Klamt, Alain Krivoules, Torben Lund, Erika Mann, Jean-Charles Marchiani, Hughes Martin, Patricia McKenna, William Francis Newton Dunn (for Jorge Salvador Hernández Mollar, jf. forretningsordenens artikel 153, stk. 2), Reino Paasilinna, Bernd Posselt (for Hubert Pirker), Jacques Santkin (for Catherine Lalumière), Ilka Schröder, Gary Titley (for Ozan Ceyhun), Maurizio Turco, Gianni Vattimo, W.G. van Velzen, Christian von Bötticher, Jan Marinus Wiersma og Christos Zacharakis (for Enrico Ferri)

Mindretalsudtalelserne og bilagene er offentliggjort særskilt (A5-0264/2001- Del 2).


Fristen for ændringsforslag til denne betænkning vil fremgå af forslaget til dagsorden for den mødeperiode, hvor den skal behandles.
FORSLAG TIL BESLUTNING

Europa-Parlamentets beslutning om eksistensen af et globalt system til aflytning af privat og økonomisk kommunikation (Echelon-aflytningssystemet) (2001/2098 (INI))

Europa-Parlamentet,

– der henviser til sin afgørelse af 5. juli 2000 om nedsættelse af et midlertidigt udvalg om Echelon-aflytningssystemet og om dettes mandat¹,

– der henviser til EF-traktaten, der bl.a. tilsiget etablering af et fælles marked med en høj grad af konkurrenceevne,

– der henviser til EU-traktatens artikel 11 og 12, som forpligter medlemsstaterne til at styrke og udvikle deres gensidige politiske solidaritet,

– der henviser til traktaten om Den Europæiske Union, særlig artikel 6, stk. 2, der fastlægger EU's forpligtelse til at respektere menneskerettighederne, og afsnit V med bestemmelser om en fælles udenrigs- og sikkerheds-politik,

– der henviser til artikel 12 i verdenserklæringen om menneskerettighederne,

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

– der henviser til forretningsordenens artikel 150, stk. 2,

– der henviser til betænkning fra Det Midlertidige Udvalg om Echelon-aflytningssystemet (A5-0264/2001),

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

¹ EFT C 121 af 24.4.2001, s. 36.
verdensomspændende kommunikationsaflytningssystem, som fungerer gennem et samarbejde mellem USA, Det Forenede Kongerige, Canada, Australien og New Zealand inden for rammerne af UKUSA-aftalen, og at det på grundlag af de foreliggende indicier og samstemmende erklæringer fra meget forskellige kredse - herunder amerikanske kilder - kan antages, at systemet eller dele deraf i det mindste i en vis periode gik under dæknavnet "Echelon",

B. der henviser til, at der ikke kan være tvivl om, at systemet i det mindste benyttes til aflytning af privat og erhvervsmæssig kommunikation og ikke til aflytning af militær kommunikation, idet undersøgelsen dog har vist, at systemet sandsynligvis langtfra har den tekniske kapacitet, som visse dele af medierne har antaget,

C. der henviser til, at det derfor er forbavsende, for ikke at sige foruroligende, at mange af de ansvarlige inden for EU, navnlig medlemmer af Kommissionen, i forbindelse med høringer herom har erklæret, at de ikke havde kendskab til dette fænomen,

Aflytningssystemets grænser

D. der henviser til, at aflytningssystemet navnlig 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 nævnte grænser; der tillige henviser til, at personaleressourcerne til den endelige analyse af opfanget kommunikation medfører yderligere begrænsninger, og at UKUSA-staterne derfor kun har adgang til en meget begrænsset del af den kabel- og radiobaserede kommunikation og kun kan analysere en endnu mere begrænset del af kommunikationen; der endvidere henviser til, at selv om de forhåndenværende midler og muligheder for aflytning af kommunikation er meget store, er det i praksis umuligt at foretage en udtømmende og detaljeret kontrol af al kommunikation på grund af selve kommunikationsmængdens enorme omfang,

Den mulige eksistens af andre aflytningssystemer

E. der henviser til, at aflytning af kommunikation er en almindelig anvendt spionageform blandt efterretningsstjenester, og at et sådant system også vil kunne anvendes af andre stater, hvis de råder over de nødvendige finansielle midler og har de geografiske forudsætninger herfor; der tillige henviser til, at Frankrig - i kraft af sine oversøiske territorier- er den eneste EU-medlemsstat, der geografisk og teknisk er i stand til selvstændig drift af et globalt aflytningssystem og også råder over den dertil fornødne tekniske og organisatoriske infrastruktur; der henviser til, at der er udførlige beviser for, at Rusland sandsynligvis opererer med et sådant system,

Forenelighed med EU-retten

F. 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, er det ikke i strid med EU-retten, da aktiviteter vedrørende statens sikkerhed 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 kriterier; der henviser til, at systemet, hvis det derimod anvendes til konkurrencespionage, er i strid med medlemsstaternes pligt til loyalt samarbejde og konceptet om et fælles marked med fri konkurrence, således at en medlemsstat, der deltager heri, overtræder EU-retten,

G. der henviser til, at Rådet på plenarmødet den 30. marts 2000 fremsatte følgende erklæring: "Rådet kan ikke acceptere, at der oprettes eller findes et system til aflytning af telekommunikation, som ikke respekterer medlemsstaternes lovgivning, og som overtræder de grundlæggende principper, som går ud på at beskytte den menneskelige værdighed",

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

H. der henviser til, at enhver aflytning af kommunikation er et alvorligt indgreb i den enkeltes privatsfære, og at menneskerettighedskonventionens artikel 8, der garanterer respekt for privatsfæren, kun tillader indgreb med henblik på beskyttelse af den nationale sikkerhed, og kun for så vidt som der er 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 ikke må gå længere, end hvad der er nødvendigt, 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",

I. der henviser til, at et efterretningssystem, som foretager en vilkårlig og vedvarende aflytning af enhver form for kommunikation, ville overtræde proportionalitetsprincippet og ikke være foreneligt med den europæiske menneskerettighedskonvention (EMK), og at der ligeledes ville foreligge en krænkelse av 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, eller indgrebet går videre, end nødvendigt er; der tillige henviser til, at de bestemmelser, som danner grundlag for den amerikanske efterretningstjenestes virke i udlandet, for det meste er fortrolige, og at der dermed kan sættes spørgsmålstegn ved, om proportionalitetsprincippet overholdes, hvormed der i så fald sandsynligvis er tale om en krænkelse af de af Menneskerettighedsdomstolen fastlagte principper om tilgængelighed til retsakter og forudsigelighed i anvendelsen heraf,

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

K. der henviser til, at efterretningstjeneres ved lov legitimerede virksomhed kun er i overensstemmelse med de grundlæggende rettigheder, hvis der findes et fyldestgørende kontrolsystem, som kan modvirke 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 efterretningsstjenester.

**Er EU-borgerne beskyttet tilstrækkeligt mod efterretningsvirksomhed?**

L. 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; de desuden henviser til, at EU-borgerne har en grundlæggende interesse i, at deres nationale parlementer har et særligt, formelt struktureret kontroludvalg, der overvåger og kontrollerer efterretningsstjenesternes aktiviteter; der henviser til, at disse selv der, hvor der findes kontrolorganer, i høj grad fristes til snarere at beskæftige sig med indenrigsefterretningsstjenesternes virke end med udenrigsefterretningsstjenesternes, da landets egne borgere som regel kun berøres af førstnævntes aktiviteter; der henviser til, at det ville tilskynde efterretningsstjenester til en aflytningspraksis, der er afpasset efter det, der er nødvendigt, hvis de var forpligtet til at give en borger, hvis kommunikation er blevet aflyttet, meddelelse herom på et senere tidspunkt, f.eks. fem år efter aflytningen har fundet sted,

M. der henviser til, at anlæg til satellitaftlytning i betragtning af deres størrelse ikke kan bygges på en stats område, uden at den pågældende stat er indforstået hermed,

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

**Økonomisk spionage**

O. der henviser til, at det er en del af udenrigsefterretningstjenesternes opgave at beskæftige sig med økonomiske data, herunder vedrørende 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,

P. der henviser til, at de amerikanske efterretningsstjenester ikke kun efterforsker generelle erhvervsmæssige fakta, men netop i forbindelse med udbud også aflytter virksomheders kommunikation i enkeltheder og som begrundelse anfører ønsket om at bekæmpe forsøg på bestikkelse; der henviser til, at der ved detaljeret aflytning er den risiko, at oplysningerne ikke benyttes til bekæmpelse af bestikkelse, men til konkurrencespionage, selv om USA og Det Forenede Kongerige hævder, at det ikke er tilfældet; der henviser til, at det fortsat ikke står fuldstændigt klart, hvilken rolle der spilles af det amerikanske handelsministeriums Advocacy Center, og at en planlagt samtale, som skulle have skabt klarhed herom, blev aflyst,

Q. der henviser til, at der inden for rammerne af OECD i 1997 blev indgået en aftale om bekæmpelse af bestikkelse af embedsmænd, der gør bestikkelse strafbar i henhold til folkeretten, og at bestikkelse i enkelte tilfælde derfor ud fra dette perspektiv heller ikke kan berettige aflytning af kommunikation,
R. der mener, at det under ingen omstændigheder er acceptabelt, at efterretningstjenester lader sig anvende til konkurrenceanlægning 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 hævdt.

S. der henviser til, at autoritative kilder under det besøg, som delegationen fra Det Midlertidige Udvalg om Echelon-aflytningssystemet aflagde i USA, har bekræftet Brown-rapporten fra den amerikanske Kongres, der antyder, at 5% af de efterretninger, der indsamles via non-open sources, anvendes til økonomisk spionage; der henviser til, at de samme kilder anslag, at denne overvågning kunne give den amerikanske industri mulighed for en kontraktmæssig forstørrelse på op til 7 mia. USD;

T. der henviser til, at følsomme virksomhedsoplysninger ofte holdes inden for selve virksomheden, og at konkurrenceanlægning derfor navnlig sker ved, at der gøres forsøg på at få oplysninger via medarbejdere eller indslusede personer og i stadig stigende grad ved at tænke ind i interne edb-net; der henviser til, at kommunikationsovervågningssystemer kun kan anvendes til konkurrenceanlægning, når følsomme data kommer ud via kabelkommunikation eller trådløs kommunikation (satellit), og at dette 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 videokonference via VSAT eller kabel;
- når der forhandles om vigtige kontrakter på stedet (f.eks. i bygge- og anlægssektoren, opbygning af telekommunikationsinfrastruktur, etablering af nye transportsystemer osv.), og der derfra skal føres samråd med virksomhedernes hovedkontor,

U. der henviser til, at risiko- og sikkerhedsbevidstheden hos de små og mellemstore virksomheder ofte er utilstrækkelig, og at faren for industrispionage og aflytning af kommunikation ikke erkendes,

V. der henviser til, at EU-institutionerne (med undtagelse af Den Europæiske Centralbank, Rådets generaldirektorat for eksterne forbindelser og Kommissionens generaldirektorat for eksterne forbindelser) ikke altid udviser en udpræget sikkerhedsbevidsthed, og at der derfor er behov for handling,

*Mulighederne for selv at beskytte sig*

W. 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 stærkt 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,
X. 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 forsvarspolitis, idet samarbejdet med andre partnere på dette område dog skal fortsættes,

Y. der henviser til, at Det Europæiske Råd i december 1999 i Helsinki besluttede at udvikle en mere effektiv europæisk militær kapacitet for fuldt ud at kunne løse samtlige Petersberg-opgaver til støtte for FUSP; der henviser til, at Det Europæiske Råd endvidere med henblik på at opnå dette mål besluttede, at EU senest i 2003 skal være i stand til hurtigt at udsende militære styrker på op til 50.000-60.000 mand, som skal opretholde sig selv, bl.a. med hensyn til den fornødne befallings-, kontrol- og efterretningsskapacitet; der henviser til, at de første skridt i retning af en sådan uafhængig efterretningsskapacitet allerede er taget inden for rammerne af WEU og den faste sikkerheds- og forsvars-politiske komité,

Z. der henviser til, at et samarbejde mellem efterretningstjenestene inden for EU også forekommer uomgængeligt, dels fordi det vil være ulogisk at tale om en fælles sikkerheds-politik uden inddragelse af sikkerheds-jenestene, og dels fordi dette vil indebære mange fordele af erhvervsmæssig, økonomisk og politisk art; der henviser til, at dette også vil 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 der må sikres passende kontrol af et sådant samarbejde fra Europa-Parlamentets side,

AA. der henviser til, at Europa-Parlamentet er i færd med at gennemføre forordningen om offentlig adgang til Europa-Parlamentets, Rådets og Kommissionens dokumenter ved at tilpasse sin forretningsordenen med hensyn til tilgængeligheden af følsomme dokumenter,

Indgåelse og ændring af internationale aftaler om beskyttelse af borgere og virksomheder

1. bekræfter på grundlag af oplysningerne fra Det Midlertidige Udvalg, at der ikke længere er tvivl om eksistensen af et verdensomspændende aflytningssystem for kommunikation, som anvendes inden for rammerne af UKUSA-aftalen med deltagelse fra USA, Det Forenede Kongerige, Canada, Australien og New Zealand;

2. opfordrer Europarådets generalsekretær til at forelægge Ministerudvalget et forslag til beskyttelse af privatsfæren som garanteret i artikel 8 i EMK og tilpasset til de moderne kommunikationsmetoder og aflytningsmuligheder, enten i en tillægsprotokol eller sammen med reglerne om databeskyttelse som led i en revision af databeskyttelseskonventionen, forudsat at der derved hverken sker en reduktion af det retsbeskyttelsesniveau,

Menneskerettighedsdomstolen har sikret, eller af den fleksibilitet, der er nødvendig for tilpasning til videre udviklinger;

3. opfordrer de medlemsstater - hvis lovgivning vedrørende efterretningstjenesternes aflytningskapacitet indeholder bestemmelser om beskyttelse af privatsfæren, som er diskriminerende - til at sikre alle europæiske borgere samme retsgarantier vedrørende beskyttelse af privatlivets fred og af kommunikationshemmeligheden;

4. opfordrer EU-medlemsstaterne til at oprette en europæisk platform bestående af repræsentanter for de nationale instanser, der er ansvarlige for overvågning af medlemsstaternes overholdelse af de grundlæggende rettigheder og borgernes rettigheder, for
at undersøge, hvorvidt de nationale lovgivninger om efterretningstjenester er i overensstemmelse med den europeiske menneskerettighedskonvention og Den Europæiske Unions charter om grundlæggende rettigheder, og vurdere de lovændige bestemmelser om sikring af brev- og telehemmeligheden samt vedtage en henstilling til medlemsstaterne om udarbejdelse af en adferds kodeks, der 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 denne betænkningss kapitel 8, særlig punkt 8.3.4., der er baseret på artikel 8 i EMK;

5. opfordrer medlemsstaterne til på den næste regeringskonference at vedtage, at Den Europæiske Unions charter om grundlæggende rettigheder er bindende ret, der kan indbringes for en domstol, for derved at forbedre beskyttelsesniveauet for de grundlæggende rettigheder, navnlig hvad angår beskyttelse af privatsfæren;

6. 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 Luxembourg;

7. opfordrer EU-institutionerne til inden for deres respektive kompetence- og virksomhedsområder at føre de grundlæggende rettigheder som fastlagt i chartret ud i livet;

8. 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 rettigheder, som sikrer beskyttelse af privatsfæren, til den nye teknologiske udvikling;

9. mener, at det er nødvendigt, at der forhandles om og indgås en aftale mellem EU og USA, hvori det fastlægges, at parterne gensidigt respekterer de bestemmelser om beskyttelse af borgernes privatsfære og hemmeligheden af virksomheders kommunikation, der er gældende for deres egne borgere og virksomheder;

10. opfordrer USA til at undertegne tillægsprotokollen til den internationale konvention om borgerlige og politiske rettigheder, således at enkeltpersoner kan indbringe sager mod USA for krænkelse af konventionen for konventionens Menneskerettighedskomité; 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;

_Nationale lovgivningsforanstaltninger til beskyttelse af borgere og virksomheder_

11. opfordrer medlemsstaterne til at revurdere og om nødvendigt vedtage deres nationale lovgivning om efterretningstjeners virksomhed for at sikre overensstemmelse med de grundlæggende rettigheder som omhandlet i den europeiske menneskerettigheds konvention og med Den Europæiske Menneskerettighedsdomstols retspraksis;

12. opfordrer medlemsstaterne til at tilvejebringe bindende instrumenter, der kan sikre fysiske
og juridiske personer effektiv beskyttelse mod enhver form for ulovlig aflytning af deres kommunikation;

13. opfordrer medlemsstaterne til at tilstræbe et fælles beskyttelsesniveau over for efterretningsaktiviteter og med henblik herpå udarbejde en adfærdskodeks (som nævnt i punkt 4), som er baseret på det højeste nationale beskyttelsesniveau, da de borgere, der er berørt af en udenrigsefterretningsstjenestes virke, som regel er statsborgere i andre stater og dermed også i andre medlemsstater;

14. opfordrer medlemsstaterne til sammen med USA at vedtage en adfærdskodeks af samme art som EU's adfærdskodeks;

15. opfordrer de medlemsstater, der endnu ikke har gjort det, til at sikre en parlamentarisk og retlig kontrol med deres eftetretningstjenester;

16. opfordrer Rådet og medlemsstaterne til snarest muligt at indføre et system for demokratisk overvågning og kontrol af den autonome europeiske efterretningsvirksomheds kapacitet og andre fælles og koordinerede efterretningsaktiviteter på europæisk plan; mener, at Europa-Parlamentet bør spille en vigtig rolle inden for dette overvågnings- og kontrolsystem;

17. opfordrer medlemsstaterne til at gå sammen om deres kommunikationsaflytningsmidler for at gøre den europeiske sikkerheds- og forsvars-politik mere effektiv med hensyn til efterretningsvirksomhed, bekæmpelse af terrorisme, spredning af atomvåben eller international narkotikahandel under overholdelse af bestemmelserne om beskyttelse af privatlivets fred og kommunikationshemmelighed og under kontrol fra Europa-Parlamentets, Rådets og Kommissionens side;

18. opfordrer medlemsstaterne til med henblik på øget beskyttelse af EU-borgernes privatsfære at indgå en aftale med tredjelande, som forpligter alle de kontraherende parter til i tilfælde af aflytning på en anden kontraherende parts territorium at underrette denne om de planlagte foranstaltninger;

Særlige foranstaltninger til bekæmpelse af økonomisk spionage

19. opfordrer medlemsstaterne til at overveje, i hvilken udstrækning økonomisk spionage og bestikkelse med henblik på skaffe kontrakter kan bekæmpes gennem europeisk 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, f.eks. ved at annullere sådanne kontrakter; opfordrer USA, Australien, New Zealand og Canada til at tilslutte sig disse initiativer;

20. opfordrer medlemsstaterne til i EF-traktaten at indføje en bestemmelse om forbud mod økonomisk spionage og til ikke at drive økonomisk spionage mod hinanden, enten direkte eller under dække af en fremmed magt, der eventuelt kan intervenere på deres territorium, eller lade en fremmed magt drive spionage fra en EU-medlemsstats territorium, for at respektere EF-traktatens ånd og bogstav;

21. opfordrer medlemsstaterne til gennem et fælles entydigt og bindende instrument at forpligte sig til ikke at udøve økonomisk spionage og derved at bekræfte deres forpligtelser over for
EF-traktatens ånd og bogstav; opfordrer endvidere medlemsstaterne til at gennemføre dette bindende principl i deres nationale lovgivning om efterretningstjenester;

22. opfordrer medlemsstaterne og den amerikanske regering til at indlede en åben dialog mellem USA og EU om økonomisk spionage;

Foranstaltninger vedrørende anvendelsen af gældende ret og kontrollen hermed

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

24. anmoder de nationale kontroludvalg for efterretningstjenesterne om under udvøvelsen 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;

25. opfordrer medlemsstaterne til at sikre, at deres efterretningssystemer ikke misbruges til at opsætte konkurrencerelaterede oplysninger i strid med medlemsstaternes loyalitetspligt og konceptet om et fælles marked baseret på fri konkurrence;

26. opfordrer Tyskland og Det Forenede Kongerige til at gøre de amerikanske efterretningstjenester fortsat tilgængelige, at kommunikation på deres territorium betinget af, at denne sker i overensstemmelse med EMK, dvs., at proportionalitetsprincippet overholdes, at retsgrundlaget er tilgængeligt og konsekvenser forudsigelige for den enkelte, og at der gennemføres en effektiv kontrol, da de selv bærer ansvaret for, at efterretningstjeneste på deres territorium, hvad enten den er tilladt eller blot tålt, sker i overensstemmelse med menneskerettighederne;

Fremme af borgernes og virksomhedernes selvbeskyttelse

27. opfordrer Kommissionen og medlemsstaterne til at informere deres borgere og virksomheder om, at deres internationale kommunikation under visse omstændIGHeder kan blive aflyttet; understreger, at denne oplysningaktion må ledsages af praktisk bistand ved udarbejdelse og gennemførelse af omfattende beskyttelsesforanstaltninger, herunder vedrørende informationsteknologisikkerhed;

28. opfordrer Kommissionen, Rådet og medlemsstaterne til at udvikle og gennemføre en effektiv og aktiv politik for sikkerhed i informationssamfundet; understreger, at denne politik må lægge særlig vægt på at øge bevidstheden hos alle brugere af moderne kommunikationssystemer om nødvendigheden af at beskytte fortrolige oplysninger; understreger endvidere, at der bør oprettes et europæisk, koordineret net af organer, som kan yde praktisk bistand ved opstilling og implementering af omfattende beskyttelsesstrategier;

29. 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 brugervenlig krypteringssoftware med offentlig kildetekst;
30. 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";

31. 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"; opfordrer Kommissionen til at fastlægge en standard for sikkerhedsgraden af software bestemt til brug ved elektronisk kommunikation og placere software, hvis kildetekst ikke er offentlig, i den mindst pålidelige kategori;

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

33. opfordrer EU-institutionerne og medlemsstaternes offentlige forvaltninger til at sørge for, at deres personale uddannes og gøres fortrøligt med de nye krypteringsteknologier og -teknikker ved indførelse af en relevant praksis og afholdelse af de nødvendige uddannelseskurser;

34. opfordrer til særlig opmærksomhed omkring ansøgerlandenes stilling; anmoder om, at der ydes støtte, hvis de på grund af manglende teknologisk uafhængighed ikke kan træffe de fornødne sikkerhedsforanstaltninger;

Andre foranstaltninger

35. opfordrer virksomhederne til at samarbejde mere intensivt med kontraspionageorganer og især at informere disse om angreb udefra med henblik på økonomisk spionage for derved at øge disse organers effektivitet;

36. opfordrer Kommissionen til at lade foretage en sikkerhedsundersøgelse af, hvad der skal beskyttes, og få udviklet et sikkerhedskoncept;

37. opfordrer på baggrund af den stærkt tiltrængte modernisering Kommissionen til at opdatere sit krypteringssystem og anmoder indtrængende budgetmyndigheden (Rådet og Parlamentet) om at stille de nødvendige midler til rådighed;

38. anmoder det kompetente udvalg om at udarbejde en initiativbetænkning om sikkerheden og beskyttelsen af hemmeligheder i EU-institutionerne;

39. opfordrer Kommissionen til at sikre databeskyttelse i forbindelse med dens egen databehandling og øge beskyttelsen af den fortrøelige art af dokumenter, der ikke er offentligt tilgængelige;

40. anmoder Kommissionen og medlemsstaterne om som led i det 6. rammeprogram for forskning at investere i nye teknologier inden for krypterings- og dekrypteringsteknik;

41. opfordrer til, at stater, der udsættes for konkurrenceforvridning som følge af statsstøtte eller økonomisk misbrug af spionage, giver meddelelse herom til myndighederne og kontrolorganerne i den stat, hvorfra disse aktiviteter er udført, for at disse konkurrenceforvridende aktiviteter kan bringes til ophør;
42. opfordrer Kommissionen til at forelægge et forslag med henblik på i tæt samarbejde med erhvervslivet og medlemsstaterne at etablere et europæisk, koordineret net af rådgivningsinstanser - navnlig i de medlemsstater, hvor der endnu ikke findes sådanne - for informationssikkerhed i erhvervslivet, som ud over at skærpe bevidstheden om problemet også skal yde praktisk hjælp;

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

44. pålægger sin formand at sende denne beslutning til Rådet, Kommissionen, Europarådets generalsekretær og Parlamentariske Forsamling, medlemsstaternes og ansøgerlandenes regeringer og parlamentter samt USA, Australien, New Zealand og Canada.
BEGRUNDELSE

1. Indledning

1.1. Nedsættelse af udvalget


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

1.2.1. Den første STOA-rapport fra 1997


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.

---

1 Duncan Campbell, Teknikens stade inden for kommunikationsefterretninger (Comint) i forbindelse med den automatiserede behandling i efterretningsøjenmed af aflyttede faste eller fælles bredbåndforbindelser på flere sprog og dens anvendelse på indhentning og udvælgelse af Comint, herunder talegenkendelse, Bind 2/5 i: STOA (red.), Udviklingen i overvågningsteknologien og risikoen for misbrug af kommercielle oplysninger (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 efter anmodning fra udvalgene lader udføre forskningsprojekter. Arbejderne underkastes dog ikke nogen videnskabelig kontrol.

3 Steve Wright, An appraisal of technologies for political control (1998), STOA interim study, PE 166.499/INT.ST., s. 20.

4 Duncan Campbell, Teknikens stade inden for kommunikationsefterretninger (Comint) i forbindelse med den automatiserede behandling i efterretningsøjenmed af aflyttede faste eller fælles bredbåndforbindelser på flere sprog og dens anvendelse på indhentning og udvælgelse af Comint, herunder talegenkendelse, Bind 2/5 i: STOA (red.), Udviklingen i overvågningsteknologien og risikoen for misbrug af kommercielle oplysninger (oktober 1999), PE 168.184.
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 Thomson CFS skal have lidt skade som følge heraf. Campbell refererer her til beretninger i den amerikanske presse.1

STOA-undersøgelsen resulterede i, at Echelon blev drøftet i næsten alle medlemsstaternes parlamerter, 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.2 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 "Overvågningssteknologiens 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 tavshedsplicit 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 overtræde fællesskabsretsretten. Var der blevet tale om et undersøgelsesudvalg, ville det således have været ensbetydende med en indholdsmaessig begrænsning uden yderligere rettigheder, hvorfor et flertal af Europa-Parlamentets medlemmer afviste at nedsætte et sådant udvalg.

1.5. Arbejdsmetode og arbejdsplan


1.6. Echelon-systemets tilskrevne egenskaber

Echelon-aflytningssystemet adskiller sig fra andre aflytningssystemer som følge af den ganske særlige karakter, som to egenskaber efter sigende 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

---
\(^1\) 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.
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 (UKUSA-staterne¹), 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.


¹ Se kapitel 5, 5.4.
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

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 industri spionage. 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 industri spionage 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.

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 herves 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 grænses tilfælde er ufrivilligt samarbejde, hvorved der "udfrittes" oplysninger: Ved angiveligt harmlose 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 registrere og tyde sådanne satellitters signaler.


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 i almindelighed kun borgere og andre personer, som opholder sig på eget statsterritorium (se kapitel 8).

2.5. Bestemte efterretningstjenesters virksomhed

<table>
<thead>
<tr>
<th>Land</th>
<th>Udlandskommunikation</th>
<th>Statslig kommunikation</th>
<th>Civil kommunikation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Belgien</td>
<td>+</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Danmark</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Finland</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Frankrig</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Tyskland</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Grækenland</td>
<td>+</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Irland</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Italien</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Nederlandene</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Land</td>
<td>Spalte 1</td>
<td>Spalte 2</td>
<td>Spalte 3</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>----------</td>
<td>----------</td>
</tr>
<tr>
<td>Østrig</td>
<td>+</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Portugal</td>
<td>+</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Sverige</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Spanien</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>UK</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>USA</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Canada</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Australien</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>New Zealand</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

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

De enkelte spalter angiver:

Spalte 1: Det pågældende land

Spalte 2: Udlandskommunikation omfatter kommunikation til og fra udlandet, idet der både kan være tale om civil, militær eller diplomatisk kommunikation.\(^1\)

Spalte 3: Statslig kommunikation (militær, ambassader osv.)

Spalte 4: Civil kommunikation.

"+" = kommunikation aflyttes
"-" = kommunikation aflyttes ikke

\(^1\) Hvis efterretningstjenesten har adgang til kabel, kan den aflytte kommunikation til og fra udlandet. Aflytter efterretningstjenesten satellitkommunikation, har den ganske vist kun adgang til downlink, men kan aflytte hele den transporterede kommunikation, dvs. også kommunikation, der ikke er bestemt til det pågældende territorium. Da satelliternes dækningsområde som regel omfatter hele Europa eller endnu større områder (se kapitel 4, 4.2.5.) kan man aflytte satellitkommunikationen i hele Europa ved hjælp af en modtagerstation.
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).


3.2. Muligheder for at aflytte på stedet

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, selv om det rent teknisk er besværligt, aflyttes, såfremt lytteposten befinder sig i samme celle (diameter i byområder 300 m på landet 30 km).

- **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 afgrenses 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.

---

3.3. Muligheder forbundet med et globalt arbejdende aflytningssystem

Til interkontinentale 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) overfores 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 tape 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 indsette 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 **UKUSA-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 afdække 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.


- 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 dør 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.¹

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

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

3.3.1.2. Radiokommunikation ²


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 (mobiletelefoner 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.

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 UKUSA-staterne med jordbaserede lyttestationer kun har adgang til en meget begrænset del af radiokommunikationen.

3.3.1.3. Kommunikation via geostationære telekommunikationssatellitter


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 maskinens radar suppleres med et system til identifikation af bestemte mål, som kan lokaliseres og klassificere elektronisk stråling og korrele den med radarkontakter. Der eksisterer ingen særskilt SIGNINT-kapacitet.

Derimod har de amerikanske flådeds 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.

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

3.3.1.5. Muligheder for at foretage aflytning fra spionagesatellitter

Så længe radiobølger ikke bundtes ved hjælp af brugbare antenner, forplanter de sig i alle retninger, altså også i verdensrummet. Signal intelligence satellitter i lavt kredsløb kan kun

---

1 Hans Dodel, Satellitenkommunikation, Hüthig Verlag (1999).
3 Süddeutsche Zeitung nr. 80, af 5.4.2001, s. 6.
4 Jeffrey T. Richelson, The U.S. Intelligence Community, Ballinger, (1989), s. 188 og s. 190.
opfange den sender, der skal aflyttes, i få minutter ad gangen. I tætbefolkede industriområder vanskelliggøres aflytningen af de mange sendere på samme frekvens i en sådan grad, at det næsten er umuligt at skelne enkelte signaler.\(^1\) 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).\(^2\) 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 - 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 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 efterretningsstjenesterne; selv afslutningen på den kolde krig var ikke nok til at tage et sådant skridt.\(^4\)

---

\(^1\) Skrivelse af 14.2.2001 fra statssekreter i det tyske forsvarsministerium, Walter Kolbow, til ordføreren.

\(^2\) Major A. Andronov, Zarubezhnoye voyennoye voyennoye obozreniye, nr. 12, 1993, s. 37-43.

\(^3\) Privat meddelelse til ordføreren, kilde beskyttet.

\(^4\) Privat meddelelse til ordføreren, kilde beskyttet.
3.3.3. Den tyske efterretningstjeneste som eksempel


Andre efterretningstjenesters muligheder kan være større på bestemte områder som følge af forskellige retsrammer eller grundet et større antal analytikere. Især en analyse af de kabelbaserede kommunikationsstrømme øger den statistiske sandsynlighed for en fuldrykkelse, 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 omfanger satellitkommunikation ved hjælp af en række søgetermer (som i Tyskland skal godkendes forinden af den såkaldte G10-kommission2). De relevante tal er som følger (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 rødt i loven (teoretisk ville 100% have været tilladt - i det mindste for sagen ved forfatningsdomstolen), men er teknisk begrundet, f.eks. begrænset analysekapacitet.

Også antallet af anvendelige søgetermer er begrænset af tekniske årsager og kravet om tiladelse. I præmisserne til forfatningsdomstolens dom tales ved siden af de rent formelle søgetermer (forbindelser, der anvendes af udlandets 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.


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 af den internationale kommunikation i Centraleuropa aftaget stærkt de senere år; den ligger mellem 0,4 og 5%.1 Dette hænger sammen med fordelene ved optiske glasfibrekabler, 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 glasfibrekabel 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 glasfibrekabler. Som følge af signalernes lange transmissionstid på flere hundrede millisekunder spiller kvalitetsmangel ikke den store rolle ved normal taletranmission - selv om man kan høre tidsforskydningen. 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 vil 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 Oplysninger fra telekommunikationsudbydere i europæiske medlemsstater som svar på spørgsmål fra udvalget.
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 parallel med økvator, følger den nøjagtigt jordens omdrejning. Set fra jordens overflade vil satellitten da i ca. 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:


Ved mobilkommunikation (satellitmobiltelefoni) 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) satellitssystemer.

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 over halvdelen af deres kredsløb er synlige for brugeren i denne del af verden. Med to satellitter kan der i princippet således opnås en komplet regional dækning², som ikke er mulig fra en geostationær position over ækvator. For så vidt angår de russiske molnyia-satellitter, der har været anvendt som kommunikationssatellitter siden 1974 (prototype allerede i 1964), kredser tre satellitter med

---

en omløbstid på 12 timer og en indbyrdes afstand på 120° om Jorden og sikrer således kontinuerlig kommunikationstransmission.

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.

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

INTELSAT

INTELSAT har i øjeblikket 20 geostationære satellitter, der forbinder over 200 lande, og hvis ydelser udeles til medlemmerne af INTELSAT. Medlemmerne driver deres egne jordstationer. Gennem INTELSAT Business Service (IBS) har også ikke-medlemmer (f.eks. telefonselskaber, store firmaer, internationale koncerter) siden 1984 kunnet benytte satellitterne. INTELSAT tilbyder globale tjenester på områder som kommunikation, fjernsyn etc. Transmissionen af telekommunikation sker på C- og Ku-båndet (se nedenfor).

INTELSAT-satellitterne er de vigtigste internationale kommunikationssatellitter. Over disse afvikles størstedelen af den satellitbaserede internationale kommunikation. Satellitterne dækker det atlantiske, indiske og pacifiske område (se tabel, kapitel 5, 5.3).

Over Atlantihavet befinder der sig mellem 304°E og 359°E 10 Satellitter, det indiske område

2 Hans Dodel, privat meddelelse.
dækkes af 6 Satellitter mellem 62°E og 110,5°E, Stillehavsområdet af 3 satellitter mellem 174°E og 180°E. Via flere enkeltsatellitter i Atlanterhavsområdet dækkes behovet her.

**INTERSPUTNIK**


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

Med satellitterne (Horizont, Express, Express A under Den Russiske Føderation og LMI-1 under Lockheed-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, 5.3).

**INMARSAT**


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

**PANAMSAT**

PanAmSat blev oprettet i 1988 som kommerciel udbyder af et globalt satellitssystem og har hjemsted i USA. PanAmSat råder i øjeblikket over 21 satellitter, der på verdensplan, men hovedsagelig i USA, udbyder forskellige tjenesteydelser som tv-, Internet- og telekommunikation.

Telekommunikationstransmissionen sker på C- og Ku-båndet.

Af de 21 satellitter dækker 7 det atlantiske område, 2 Stillehavsområdet og 2 det indiske område. De øvrige satelliters dækningssområde omfatter Amerika (Nord- und Syd-). PanAmSatellite spiller kun en underordnet rolle for kommunikationen i Europa.

---

4.2.3.2. Regionale Satellitsystemer

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

EUTELSAT¹


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.

ARABSAT²


Telekommunikationstransmissionen sker hovedsagelig på C-båndet.

PALAPA³

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 satellitsystemer⁴

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 departementer 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 israelsk satellit, der dækker 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

ITU (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 satellitter 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 og andre civile kommunikationssatellitter
- Ku-båndet (10 – 20 GHz) til sendestationer, f.eks. INTELSAT-Ku-Spot og EUTELSAT
- Ka-båndet (20 - 46 GHz) til sendestationer, f.eks. militære kommunikationssatellitter (se kapitel 4, 4.3.)
- V-båndet (46 – 56 GHz) til små jordbaserede sendestationer (VSATs)

### 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 begrænse dem til små, regionalt begrænsede spots.


For så vidt angår INTELSAT-satellitterne\(^1\) forholder dette sig mere præcist 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-området. 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).


4.2.6 De nødvendige antennestørrelser til radiostationer

Som modtageantener på jorden anvendes parabolantenner med en diameter mellem 0,5 og 30 m. Parabolspejlet reflekterer alle indgående bølger og koncentrerer dem i sit brændpunkt. I brændpunktet befinder sig det egentlige modtagesystem. Jo større signalets energi er på modtagedestedet, desto mindre kan parabolantennens diameter være.

Med henblik på den undersøgelse, der udføres med denne betænkaning, er det afgørende, at en del af den interkontinentale kommunikation går over C-båndet i INTELSAT-satellitternes og andre satelliters (f.eks. INTERSPUTNIK's) Global Beam, til modtagelse af hvilken der til dels kræves satellitantenner med en diameter på over 30 m (se kapitel 5). 30m-antenners var også nødvendige for de første lyttestationer for kommunikationssatellitter, 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 (se også kapitel 5, 5.2.3.). De typiske antenner, der i dag kræves til INTELSAT-kommunikation på C-båndet, har en diameter på mellem 13 og 20 m.

Til INTELSAT-satellitternes Ku-Spots og til andre satellitter (EUTELSAT-Ku-bånd, AMOS Ku-bånd etc.) kræves antenner med et gennemsnit på 2 til 15 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 0,5-3,7 m (f.eks. VSATs under EUTELSAT eller INMARSAT) tilstrækkelige.

4.3. Satellitkommunikation til militære formål

4.3.1. Generelt
Også på det militære område spiller kommunikationssatellitter en vigtig rolle. Mange lande - deriblandt USA, Det Forenede Kongerige, Frankrig og Rusland - har egne geostationære militære kommunikationssatellitter, der muliggør global kommunikation uafhængigt af andre kommunikationsmidler. USA har med ca. 32 orbitalpositioner på verdensplan gennemsnitligt placeret en satellit for hver 10°. Til militær kommunikation griber man dog delvis også tilbage til kommersielle, geostationære satellitter.

4.3.2. Militært anvendte frekvenser
De frekvensbånd, der anvendes til militær kommunikation, ligger i frekvensområdet mellem GHz og 81 GHz. Typisk anvendte bånd til militære kommunikationssatellitter er X-båndet (SHF) ved 3-30 GHz og Ka-båndet (EHF) ved 20-46 GHz.

4.3.3. Modtagestationernes størrelse
I forbindelse med modtagestationerne sondrer man mellem mobile stationer, der kan have en diameter helt ned til få decimeter, og stationære stationer, der som regel ikke overskrider en diameter på 11 m. Der findes dog to antennetyper (til modtagelse af DSCS-satellitter) med en diameter på 18 m.

4.3.4 Eksempler på militære kommunikationssatellitter
Det amerikanske MILSTAR-program (Military Strategy, Tactical and Relay Satellite System), der globalt råder over 6 geostationære satellitter, gør det muligt for USA ved hjælp af små jordstationer globalt at sikre kommunikation mellem, fly, skibe og Man-Packs indbyrdes og mellem disse og kommandocentralen. Gennem indbyrdes forbindelse af satellitterne bevarer denne mulighed, også når samtlige jordstationer uden for USA er ude af drift.

DSCS (Defense Satellite Communications System) sikrer med 5 geostationære satellitter ligeledes global kommunikation. Kommunikationssystemet anvendes af USA's militære tjenester og af visse regeringsmyndigheder.

Det britiske militære satellitsystem SKYNET kan ligeledes anvendes globalt.

Det franske system, SYRACUSE, det italienske system, SICRAL, og det spanske system indgår som "passagerer" på de nationale, civile kommunikationssatellitter og muliggør militær kommunikation på X-båndet; denne er dog regionalt begrænset.

Russerne sikrer deres militære kommunikation via en transponder på Molnya-satellitternes X-bånd.

NATO har egne kommunikationssatellitter (NATO IIID, NATO IVA og IVB). Satellitterne
transmitterer tale, telex og data mellem de forskellige militære enheder.
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 i det minste ingen officiel erklæring fra UKUSA-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 UKUSA-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 UKUSA-stat.

- påvisning af, at der findes en efterretningssmæssig 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 lett bevises, at der i mange af disse stater findes efterretningstjenester, der aflytter civil kommunikation. Dette gælder også for de fem såkaldte UKUSA-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 UKUSA-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 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

1 Ordføreren råder over oplysninger, der bekræfter, at dette er korrekt. Kilden er beskyttet.
er intet sted, hvorfra **al** satellitkommunikation i verden kan aflyttes (se kapitel 4, 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 efterretningssammestigt samarbejde mellem stater og driver systemer i de nødvendige dele af verden.

Ingen af UKUSA-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.

5.1.3. Bevis for et snævert efterretningssamarbejde

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

5.2.1. Kriterium 1: Adgang til anlæggene

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), i Yakima (USA) eller 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 fra militære kommunikationssatellitter,
- modtagelse fra spionagesatellitter (billeder, radar),
- modtagelse fra SIGINT-satellitter,
- aflytning af civile kommunikationssatellitter.

Udefra kan man ikke på antennerne/radomerne se, hvilken opgave de tjener. Man kan imidlertid på grundlag af antennernes diameter til dels foretage konklusioner om deres funktion. For civile kommunikationssatellitter, der skal modtage den såkaldte "Global Beam" på C-båndet af den på satellitter baserede civile internationale kommunikation, er der teknisk betingede minimumsstørrelser. I forbindelse med første generation af disse satellitter krævedes antenner med en diameter på 25-30 m, i dag er en diameter på 15-20 m tilstrækkelig. Den automatiske computerfiltrering af de opfangede signaler kræver en så god signalkvalitet som muligt, derfor vælger man til efterretningssbrug antennestørrelser, der ligger i overkanten.

Også til militær kommunikation er der ved kommandocentraler to antennetyper med en diameter på ca. 18 m (AN/FSC-78 und AN/FSC-79). De fleste antenner til militær kommunikation har dog en meget mindre diameter, da de skal være mobile (taktiske stationer).

På jordstationerne til modtagelse fra SIGINT-satellitter er der på grund af karakteren af det signal, der sendes til stationen (høj koncentration og høj frekvens), kun behov for små antenner. Dette gælder også for antenner til modtagelse fra spionsatellitter.

Er der i et anlæg mindst 2 satellitantenner med en diameter over 18 m, aflyttes der med sikkerhed civil kommunikation. På stationer, der drives af USA's militær, kan én af antennerne også anvendes til militær kommunikation.

5.2.4. Kriterium 4: Dokumentation fra officiel side
For så vidt angår nogle stationer, foreligger der fra officiel side en nøje definition af opgaverne. Som officielle kilder regnes her oplysninger fra regeringer og fra militære enheder.

Er dette kriterium opfyldt, er de øvrige kriterier ikke nødvendige for at identificere en station som aflytningsstation for civil kommunikation.
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 (Hager1, Richelson2, Campbell3), deklassificerede dokumenter4, Federation of American Scientists hjemmeside5 samt operatørernes6 (NSA, AIA, m.fl.) hjemmesider og andre Internet-oplysninger. For så vidt angår den New Zealandske station i Waihopai, foreligger der en nøje definition af dennes opgaver, formuleret af New Zealands regering7. Derudover er kommunikationssatelliternes 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 satellitannende kan kun opfange det, der befinder sig inden for det respektive dækningsområde, den står i. For at kunne opfange kommunikation, der hovedsagelig transmitters 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 satellitannende, også når to satelliters Beams overlapper hinanden.
– Har en satellit flere dækningsområder end blot Global-Beam, hvilket er karakteristisk for vore dages generation af satellit, kan en enkelt satellitannende ikke længere opfange den samlede kommunikation, der transmitteres over denne, da en enkelt satellitannende ikke kan stå i alle satellitens dækningsområder. Til modtage Hemi-Beams og Global-Beams fra en satellit kræves altså to satellitannender i forskellige områder (sml. redegørelsen for

6 Military.com; *.mil-Homepages
dækningsområder i kapitel 4). Kommer der yderligere Beams til (Zone- og Spot-Beams), kreves der yderligere satellitantenner. Forskellige Beams fra en satellit, der overlapper hinanden, kan i principippet modtages med én satellitantenne, da det er teknisk muligt at adskille de forskellige frekvensbånd ved modtagelsen, men dette medfører dog en forringelse af signal/støjforholdet.

Derudover gælder de i kapitel 5.2. anførte forudsætninger: manglende adgang til anlæggene, da de drives af militærer, at der kræves en parabolantenne til modtagelse af satellitsignaler, og at kravene til størrelsen af satellitantennerne til modtagelse af C-båndet i Global-Beam for første generation af INTELSAT var mindst 30 m, for senere generationer 15-18 m. De officielle beskrivelser af en del af stationernes opgaver er anvendt som belæg for disse stationers funktion som aflytningsstationer.

5.3.2.1. INTELSAT-udviklingens parallelitet med bygningen af stationer
Et globalt aflytningssystem må vokse med fremskridtene inden for kommunikation. Indledningen af satellitkommunikation 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 opstår nye dækningsområder, bygges nye stationer og nye satellitantenner, er dette inter tilfælde, men kan tages som indici um for tilstedeværelsen af en aflytningsstation for kommunikation.

Da INTELSAT-satellitterne 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 globale 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.


I de tidlige 1970'ere 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 antennen (en mod Atlanterhavet, en mod Det Indiske Ocean). På grund af de to stationers beliggenhed var modtagelse af den samlede kommunikation mulig.

**Den anden globale generation**

Den anden generation af INTELSAT-satellitter (IV og IVA) blev udviklet i 70erne og bragt i geostationær kredsloeb (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.
I de sene 70'ere byggedes **Sugar Grove** det østlige USA (stationen fandtes allerede til aflytning af russisk kommunikation); den blev sat i drift i 1980. Ligeledes i de sene 70'ere 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 med de indtil nu kendte oplysninger vanskeligt at dokumentere en sammenhæng mellem bygning af yderligere stationer og etablering 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 lytestationer karakteristiske kriterier:

**Satellitter over Det indiske Ocean:**

<table>
<thead>
<tr>
<th>Satellitter</th>
<th>Dækningsområde</th>
<th>Stationer</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTELSAT 604 (60°E), 602 (62°E), 804 (64°E), 704 (66°E)</td>
<td>INTELSAT Atlantic Ocean</td>
<td>Geraldton, Australien</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pine Gap, Australien</td>
</tr>
</tbody>
</table>

RR\445698DA.doc 53/190 PE 305.391
EXPRESS 6A (80°E)
INMARSAT indisk område

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
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.


5.3.2.3. Stationerne i detaljer

I den detaljerede beskrivelse af stationer sondres mellem stationer, der entydigt aflytter kommunikationssatellitter (kriterier jf. kapitel 5, 5.2) og stationer, hvis opgaver ikke med sikkerhed kan dokumenteres med ovenanførte kriterier.

5.3.2.3.1. Stationer til aflytning af kommunikationssatellitter

De i kapitel 5, 5.2. anførte kriterier, der kan betragtes som indicer på stationer til aflytning af kommunikationssatellitter passer på følgende stationer:

Yakima, USA (120°W, 46°N)

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 almindelig 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 kommunikationssatellitter gennem Navy-stationer.¹ Derudover ligger Sugar Grove i nærheden af (60 miles fra) den almindelige satellitmodtagelsesstation i Etam.

**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 kommunikationssatellitter gennem Navy-stationer.¹ Derudover ligger Sugar Grove i nærheden af (60 miles fra) den almindelige satellitmodtagelsesstation i Etam.

**Sabana Seca, Puerto Rico (66°W, 18°N)**

**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. 21 satellitantenner, hvoraf to med en diameter på 30 m; der findes ingen oplysninger om de øvrige antenner.

Om stationens opgaver oplyses intet officielt, størrelsen og antallet af satellitantennerne og desses placering kun 110 km fra Telekom-stationen i Goonhilly lever 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 ca.12 har en diameter på over 20 m. Mindst én af de store antenner, men næppe alle, er modtagelsesantenne for militær kommunikation (AN/FSC-78). I Menwith Hill arbejder briter og amerikanere sammen. US-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

¹ „It provides enhanced intelligence support to Air Force operational commanders and other consumers of communications satellite information collected by Navy-commanded filed stations.“ aus der Homepage der 544th Intelligence Group http://www.aia.af.mil.
Men with Hill såvel jordstation for spionagesatellitter som aflytningsstation 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. Fire satellitantenner af samme størrelse (diameter ca. 20 m), 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 civile 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 dør stationerede ca. 900 personer er amerikanere fra CIA og NAVSECGRU.²


**Misawa, Japan (141°O, 40°N)**

**Waihopai, Neuseeland (173°O, 41°S)³**
Waihopai har eksisteret siden 1989. Siden da har der været en stor antenne med en diameter på 18 m, en anden er kommet til senere. Ifølge Hager er de store antenner rettet mod Intelsat 701 over Stillehavet. Waihopais opgave er ifølge officielle oplysninger fra GCSB (General Communications Security Bureau) aflytning af kommunikationssatellitter samt evaluering og bearbejdning af signalerne⁴.

---

⁴ Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet: "Securing our Nations Safety", Dezember 2000, http://www.dpmc.govt.nz/dess/securingoursafety/index.html; "In 1989, [...] the GCSB opened its satellite communications interception station at Waihopai, near Blenheim. [...] The signals
Da stationen kun råder over to satellitantenner, kan den new zealdanske efterretningstjeneste kun aflytte en lille del af kommunikationen i Stillehavsområdet. Stationen er altså kun hensigtsmæssig i sammenhæng med en anden station i samme område. Hager nævner ofte Geraldtown i Australien som "søsterstation" til Waihopai.

**Hongkong (22°N, 114°O)**
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 US-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)**

**Ayios Nikolaos, Cypern (32°O, 35°N)**
Ayios Nikolaos på Cypern er en britisk station. Stationen har 14 satellitantenner, hvis størrelse er ukendt, dens opgaver er fordelt på to enheder, „Signals Regiment Radio" og "Signals Unit (RAF)".

---

intelligence is obtained from a variety of foreign communications and other non-communications signals, such as radar. The GCSB not only intercepts the signals, it also processes, decrypts or decodes and/or translates the information the signals contain before passing it on as a report to the appropriate Minister or government department."


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 efterretningsstjeneste. 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 fire satellitantenner, hvoraf to har en diameter på ca. 15 m.

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

**Buckley Field, USA, Denver Colorado (104°W, 40°N)**
Stationen blev oprettet i 1972. Her er stationeret 544th IG (Det. 45). På området findes mindst 6 satellitantenner, hvoraf 4 har en diameter på ca. 20 m. Ifølge officielle oplysninger er det stationens opgave at indsamle, evaluere og analysere data om nukleare hændelser, der er opnået via SIGINT-satellitter.

**Medina Annex, USA Texas (98°W, 29°N)**

**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 Meade, USA (76°W, 39°N)**
Fort Meade er Headquarters 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 20 m, der drives af amerikanere eller briter, hhv. hvor amerikanere eller briter udfører efterretningsstjenestelige aktiviteter.
2. Udviklingen i INTELSAT-kommunikationen og den samtidige bygning af aflytningsstationer dokumenterer systemets globale sigte.
3. Nogle af disse stationer har ifølge officielle oplysninger til opgave at aflytte kommunikationssatellitter.
4. Oplysningerne i de deklassificerede dokumenter kan tages som belæg for de der anførte stationer.
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 kommunikationssatellitter.

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

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. I februar 1941 leverede de amerikanske kryptoanalytiker en krypteringsmaskine (PURPLE) til Storbritannien. I foråret 1941 indledtes det kryptoanalytiske samarbejde. Det efterretningstjenestelige samarbejde styrkedes gennem flådernes fælles indsats i det nordlige Atlanterhav i sommeren 1941. I juni 1941 kunne briterne bryde den tyske flådes kode, ENIGMA.


2 Christopher Andrew, “The making of the Anglo-American SIGINT Alliance”, s. 99: „At a meeting 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”. (citeret efter COS (40)289, CAB 79/6, PRO. Smith, The Ultra Magic Deals, 38, 43f. Sir F.H. Hinsley, et al., British Intelligence in the Second World War, Vol. I, 312f.)
3 Christopher Andrew, “The making of the Anglo-American SIGINT Alliance”, s. 100: „In the spring of 1941, Steward Menzies, the Chief of SIS, appointed an SIS liaison officer to the British Joint Services Mission in Washington, Tim O’Connor, …, to advice him on cryptologic collaboration”.
organisation.¹

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 Italien².


5.4.2. Belæg for aftalens eksistens

5.4.2.1 Den engelske Intelligence and Security Committee's årsberetning for 1999/2000

I lang tid var der fra de kontraherende staters side ikke blevet sket nogen officiel anerkendelse af UKUSA-aftalen. I årsberetningen fra den engelske Intelligence and Security Committee, Det Forenede Kongeriges parlamentariske kontrolorgan, nævnes UKUSA-aftalen imidlertid udtrykkeligt: "Den samlede informations kvalitet viser klart værdien af det nævnte samarbejde

---

³ Harry S. 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 to 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.“ (citeret efter Bradley F. Smith, The Ultra-Magic Deals and the Most Secret Special Relationship (Presidio (1993)).
⁴ Christopher Andrew, “The making of the Anglo-American SIGINT Alliance” in Hayden, Peake and Samuel Halpern (Eds), In the Name of Intelligence. Essays in Honor of Walter Pforzheimer (NIBC Press 1995) 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.

5.4.2.2. Det new zealandske statsministeriums offentliggørelser

Derudover er der andre belæg for dennes eksistens.

5.4.2.3 US-Navy's akronymfortegnelse
UKUSA står ifølge US-Navy3 for „United Kingdom – USA“ betegner en „5-nation SIGINT agreement“.

5.4.2.4. 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

5.4.2.5. 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.

5.4.2.6. 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 bekræftet den tidligere vicedirektør for NSA, Dr. Louis Torella, der var til stede

---

1 Intelligence and Security Committee Annual Report 1999-2000. Presented to Parliament by the Prime Minister by Command of Her Majesty, November 2000, 8 Rz 14. Originaltekst: "The quality of intelligence gathered clearly reflects the value of the close co-operation under the UKUSA agreement. A recent illustration of this occurred when the US National Security Agency's (NSA) equipment accidentally failed and for some three days US customers, as well as GCHQ's normal UK customers, were served directly from GCHQ."

2 Domestic and External Secretariat des Department of the Prime Minister and Cabinet i New Zealand, Securing our Nation's Safety. How New Zealand manages its security and intelligence agencies (2000).

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.

ved undertegnelsen, aftalens eksistens.¹

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

5.4.2.8. 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

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, 2b, 4, 10 og 16)
I National Security Council Intelligence Directive 9 (NSCID 9) af 10. marts 1950⁴ defineres udlændingekommunikation med henblik på COMINT; ifølge denne definition omfatter udlændingskommunikation enhver regeringskommunikation i bredeste forstand (ikke kun militært) samt al anden kommunikation, der kan rumme oplysninger af militær, politisk, videnskabelig eller økonomisk værdi.

¹ Andrew, Christopher „The growth of the Australian Intelligence Community and the Anglo-American Connection“, 223-4.
Direktivet (NSCID 9 ændr. af 29.12.1952) fastlægger udtrykkeligt, at FBI er eneansvarlig for indre sikkerhed.¹

Direktivet fra Department of Defense (DoD) af 23. december 1971² 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 1971 strukturen i NSA, hhv. CSS.

I sin redegørelse til „House Permanent Select Committee on Intelligence“ den 12. April 2000³ definerede NSA-direktør 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 1992⁴, henvises til NSA's voksende globale opgave (access) ud over støtte til militære operationer.

5.5.2.2. Intelligence Agencies' beføjelser (dokument 7)⁵
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.⁶

---

⁶ Document 2a. Memorandum from President Harry S. Truman to the Secretary of State, the Secretary of Defense, Subject: Communications Intelligence Activities, October 24, 1952.
5.5.2.4. Enheder, der er aktive på „Echelon-Sites“ (dokument 9, 12)
I NAVSECGRU INSTRUCTIONs C5450.48A1 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 19942 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, nye dokumenter)
- Sugar Grove, West Virginia udpeges som SIGINT-station i NAVSECGRU INSTRUCTIONs C5450.48A3
- Misawa Air Base, Japan, udpeges som SIGINT-station i History of the Air Intelligence Agency - January to 31 December 19944 og i beskrivelsen af aktiviteterne i Naval Security Group i dokumenter fra marineministeriet5
- Sabana Seca i Puerto Rico udpeges som SIGINT-station, samme og i beskrivelsen af aktiviteterne i Naval Security Group i dokumenter fra marineministeriet6
- Guam, udpeges som SIGINT-station, samme
- Yakima, Washington, udpeges som SIGINT-station, samme
- Menwith-Hill, Storbritannien, beskrivelse af aktiviteterne i Naval Security Group i dokumenter fra marineministeriet8
- Bad Aibling, Tyskland, beskrivelse af aktiviteterne i Naval Security Group i dokumenter fra marineministeriet9
- Medina, Texas, beskrivelse af aktiviteterne i Naval Security Group i dokumenter fra


5 Department of the Navy, Naval Security Group Instruction C5450.32E af 9.5.1996.
6 Naval Security Group Instruction C5450.33B af 8.8.1996
7 COMINT Report der NSA aus Fort George G. Meade, Maryland af 31. August 1972

PE 305.391 64/190 RR\445698DA.doc
marineministeriet¹
- Kunia, Hawaii, beskrivelse af aktiviteterne i Naval Security Group i Naval Security Group Instructions²

5.5.2.6. Beskyttelse af USA-borgeres privatliv (dokument 7, 7a -f, 9, 11,16)
I NAVSECGRU INSTRUCTIONs C5450.48A hedder det, at borgernes privatliv skal garanteres.³


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

Ifølge disse dokumenter betyder COMINT indsamling og bearbejdning af udlændisk kommunikation (passed by electromagnetic means), inklusive aflytning og bearbejdning af ukodet skrevet 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.
5. 544th Intelligence Group og Detachment 2 og 3 under Air Intelligence Agency deltager i indsamlingen af efterretningmæssige oplysninger.

¹ Department of the Navy, Naval Security Group Instruction C5450.60A af 8.4.1996.
7. Sugar Grove i West Virginia, Misawa Air Base i Japan, Puerto Rico (dvs. Sabana Seca), Guam, Yakima i staten Washington nævnes som SIGINT-stationer.

8. Der nævnes yderligere stationer, hvor Naval Security Group er aktiv, uden at disse dog betegnes som SIGINT-stationer.

9. 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. Nicky Hager


Ifølge Hager går efterretningssamarbejdet inden for UKUSA-aftalen 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. 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, 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.

I et foredrag i udvalget den 24. april 2001 understregede Hager, at aflytningssystemet ikke var

---


PE 305.391 66/190 RR\445698DA.doc
almægtigt. Da de begrænsede ressourcer skulle anvendes så effektivt som muligt, var det ikke muligt at aflytte alt, men kun det, der kunne give vigtige oplysninger. Målene var derfor snarere af politisk eller diplomatisk interesse. Hvis der blev foretaget aflytning med henblik på økonomiske oplysninger, drejede det sig snarere om makro- end om mikroøkonomiske interesser.

Hvad angik aflytningssystemernes funktion, så førte hver partner egne lister over søgeord, hvorefter kommunikation blev aflyttet. Endvidere blev kommunikation også gennemgået efter nøgleord, som USA indgiver i systemet via såkaldte "dictionary manager". Englænderne skulle derfor f.eks. ikke have kontrol med og vidste heller ikke, hvilke informationer der samles i Morwenstow, fordi disse videresendes direkte til USA.


5.6.2. Duncan Campbell

Den engelske journalist Duncan Campbell baserer sig i sine mange udgivelser på Hagers og Richelons arbejde, samt på samtaler med tidligere efterretningstjenestearbejdere og andre forskningsarbejdere. Ifølge ham er ECHELON del af et globalt aflytningssystem, der aflytter og forarbejder internationale satellitkommunikation. Hver medlemsstat råder over "Dictionary" Computer, der gennemgår den aflyttede kommunikation efter nøgleord.

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 falso, "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." 1

I en tale for udvalget den 22. januar 2001 var Capbell af den opfattelse, at USA anvendte efterretningstjenesten til at støtte amerikanske virksomheder med at få kontrakter. Relevante oplysninger skulle via CIA og med bistand fra Advocacy Center og Office of Executive Support i Handelsministeriet blive videregivet til virksomhederne. Til støtte for denne teori forelagde han dokumenter, der dokumenterede, at Advocacy Center griber ind til fordel for amerikanske virksomheder. Det drejer sig om oplysninger, der befinder sig på centrets hjemmeside. 2 At Advocacy Centers resultater skyldes aflytning er ren spekulation og

Campbell understregede i sit indlæg, at flere europæiske landes aflytningskapacitet var vokset betydeligt inden for de seneste år, f.eks. i Schweiz, Danmark og Frankrig. Der var også en stigning i det bilaterale og multilaterale samarbejde inden for efterretningssektoren.

5.6.3. Jeff Richelson

Den amerikanske forfatter Jeffrey Richelson, tidligere medlem af National Security Archives, har pr. Internet gjort 16 tidligere klassificerede dokumenter tilgængelige; disse giver et indblik i NSA's (National Security Agency)\(^1\) opståelse, udvikling, management og mandat.


I sin bog fra 1985 „The Ties That Bind“\(^2\) beskriver han udførligt UKUSA-aftalens tilblivelse og de aktiviteter, de hemmelige tjenester i USA, Det Forenede Kongerige, 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 metoder 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.

I artiklen „Desperately Seeking Signals“\(^4\), der udkom i 2000, gengiver han i kortført UKUSA-aftalens indhold, nævner satellitaflyningsanlæg til kommunikationsatellite og beskriver muligheder og grænser for aflytning af civil kommunikation.

5.6.4. James Bamford

Den amerikanske forfatter James Bamford, der baserer sit arbejde på lige dele undersøgelser i arkiver og interviews med medarbejdere i efterretningstjenesten, var en af de første, der beskæftigede sig med NSA's SIGNIT-virksomhed. Allerede i 1982 offentliggjorde han bogen "The Puzzle Palace“\(^5\), hvis kapitel 8 "Partners" udførligt beskriver UKUSA-aftalen. Ifølge

Ordforeren ville give Advocacy Center mulighed for at tage stilling til disse anklager i forbindelse med en rejse til Washington DC. Det aftale møde blev imidlertid aflyst med kort varsel af Commerce Department Center.


hans seneste bog "Body of Secrets"\(^1\), der bygger på resultaterne i "Puzzle Palace", kaldes computernetværket, der forbindes efterretningstjenesten, "Platform". ECHELON skulle derimod være betegnelsen for det software, der blev anvendt på samtlige stationer, og som muliggør en ensartet bearbejdning og direkte adgang til andres data. \(^2\) I senere kapitler bruger han imidlertid betegnelsen ECHELON for aflytningssystemet inden for rammerne af UKUSA-aftalen.

I "Body of Secrets" og det i denne sammenhæng interessante kapitel "Muscle" giver Bamford en oversigt over den historiske udvikling inden for NSA's kommunikationsovervågning, samt en beskrivelse af systemets omfang, UKUSA-partnerskabets funktion og mål. Han understreger, at interviews med dusinvis af nuværende og tidligere NSA-ansatte har vist, at NSA ikke beskæftiger sig med konkurrencespionage for øjeblikket.


Ifølge Bamford er det største problem for Europa ikke spørgsmålet om, hvorvidt ECHELON-systemet stjæler forretningshemmeligheder og videregiver dem til konkurrenter, men krænkelsen af den grundlæggende ret til en privatsfære. I "Body of Secrets" beskriver han udforligt, hvordan beskyttelsen af "US persons" (det er US-statsborgere og personer, der opholder sig lovligt i USA) har udviklet sig, og at der også er interne begrænsninger for andre "UKUSA-residents". Samtidig påpeger han, at der ikke er nogen beskyttelse for andre personer, heller ingen pligt til at slette data, og at NSA's lagerkapacitet var uudtømmelig.

Bamford understreger imidlertid også systemets begrænsninger, der dels skyldes, at det kun er en ringe del af den internationale kommunikation, der går via satellit, og at det er langt vanskeligere at aflytte fiberoptiske kabler, og dels, at NSA kun råder over begrænset kapacitet til en endelig analyse, hvortil kommer en konstant voksende kommunikationsstrøm frem for alt via Internet.

5.6.5. Bo Elkjær og Kenan Seeberg

De to danske journalist, Bo Elkjær og Kenan Seeberg oplyste den 22. januar 2001 over for udvalget, at Echelon allerede var stærkt udviklet i 80'erne. Danmark, der havde udvidet aflytningskapaciteten væsentligt inden for de sidste 10 år, arbejdede sammen med USA siden 1984.

Som det fremgår af en artikel i Ekstra Bladet\(^3\), hvor de henviser til et lysbilledforedrag (25


\(^3\) Bo Elkjær, Kenan Seeberg, ECHELON singles out the Red Cross, A bombshell in the surveillance scandal: The organization is a possible surveillance target, Ekstra Bladet, Denmark, 8.3.2000, http://cryptome.org/echelon-red.htm.
lys billeder) af en ukendt officer fra 544. Intelligence Group under Air Intelligence Agency, påpegede de, at også forskellige ngo'er (bl.a. Røde Kors) var ECHELON-mål.

5.7. Udtalelser af tidligere efterretningsmedarbejdere

5.7.1 Margaret Newsham (tidligere medarbejder i NSA)¹

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 netværket.

5.7.2. Wayne Madsen (tidligere NSA-medarbejder)
Wayne Madsen², 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 navnlidt 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.

Under mødet med udvalgsdelegationen i Washington D.C. var han særlig bekymret for den fare, det globale spionagesystem indebar for europæiske borgeres privatsfære.

5.7.3. Mike Frost (tidligere medarbejder i den canadiske efterretningstjeneste
Mike Frost var i over 20 år beskæftiget i den canadiske efterretningstjeneste, CSE³. Aflytningsstationen i Ottawa er kun en del af et verdensomspændende netværk af spionagestationer.⁴ I et interview med CBS oplyste han, at der "overalt i verden, hver dag sker aflytning af telefonsamtaler, e-mails og telefax'er via ECHELON, et hemmeligt overvågningsnetværk under regeringen".⁵ Dette omfatter også civil kommunikation. Som eksempel anførte han i et interview med en australisk 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 gennemsmøgning af kommunikationen fundet et stikord og gengivet samtalen; den for analyse ansvarlige person

¹ Bo Elkjær, Kenan Seeberg, Echelon was my baby – Interview with Margaret Newsham, Ekstra Bladet, 17.1.1999.
² NBC-fjernsynsinterviev "60 Minutes" af 27.2.2000; http://cryptome.org/Echelon-60min.htm.
³ Communication Security Establishment, under det canadiske forsvarsministerium, driver Sigint.
⁴ NBC-fjernsynsinterviev "60 Minutes" af 27.2.2000; http://cryptome.org/Echelon-60min.htm.
⁵ Florian Rötzer, Die NSA geht wegen Echelon an die Öffentlichkeit; http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_order=special
var ikke sikker og havde derfor registreret hendes personlige data.\footnote{NBC-fjernsynsinterview "60 Minutes" af 27.2.2000; http://cryptome.org/Echelon-60min.htm.}

UKUSA-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.\footnote{James Woolsey, Remarks at the Foreign Press Center, Transcript, 7.3.2000, http://cryptome.org/Echelon-cia.htm.}

\section*{5.7.4. Fred Stock (tidligere medarbejder i den canadiske efterretningstjeneste)}


\section*{5.8 Regeringsoplysninger}

\subsection*{5.8.1. Udtalelser fra amerikansk side}


\subsection*{5.8.2. Udtalelser fra engelsk side}

Det fremgår af forskellige forespørgsler i House of Commons\footnote{Commons Written Answers, House of Commons Hansard Debates.}, at RAF-stationen Menwith Hill henhører under det engelske forsvarsministerium, men som kommunikationsinstallation stilles til rådighed for NSA\footnote{12.7.1995.}, der udpeger stationslederen\footnote{25.10.1994.}. I midten af 2000 var der i RAF

\footnote{1 NBC-fjernsynsinterview "60 Minutes" af 27.2.2000; http://cryptome.org/Echelon-60min.htm.\footnote{Interview i den australske sender Channel 9 af 23.3.1999; \url{http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm}.}


5.8.3. Udtalelser fra australisk side

5.8.4. Udtalelser fra newzealandsk side
Som anført under 5.4.2.2. henvises der i en publikation fra det newzealandske statsministerium fra sidste år om de nationale efterretnings- og sikkerhedstjenester udtrykkeligt til partnerskabet mellem efterretningstjenesterne i USA, Det Forenede Kongerige, Canada, Australien og New Zealand og fordelene for New Zealand.

5.8.5. 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. 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.

5.8.6. Udtalelser fra italiensk side


5.9. Forespørgsler til Rådet og Kommissionen


De tilsvarende forespørgsler til Kommissionen blev besvaret med, at den var bekendt med

1 Skrivelse til det nederlandske Andetkammer om ”Het grootschalig afluisteren van moderne telecommunicatiesystemen” af 19.01.01.
rapporten, men at der hverken forelå beleg eller klager over, at en medlemsstat skulle overtræde EF-traktaten i så henseende⁴. Den forsvarer dog altid ihærdigt Fællesskabets interesser og bestræber sig bestandig på at forbedre sikkerheden for sit datanetværk.⁵ På plenarmødet den 18. september erklærede Bangemann, at Kommissionen har ikke, hverken fra medlemsstaterne eller fra nogen anden, hvis rettigheder kunne være krænket, en borger, en virksomhed, hvem som helst, nogen som helst indikation af, at dette system eksisterer i den form, som er blevet skildret. "For hvis systemet eksisterede i den form, så ville det naturligvis være en himmelrørende krænkelse af rettigheder, af borgernes individuelle rettigheder og naturligvis også et angreb på medlemslandenes sikkerhed. Det er fuldstændigt klart. I det øjeblik, hvor noget sådant blev officielt bekræftet, ville Rådet og naturligvis også Kommissionen og Parlamentet måtte reagere på det. I så fald ville Kommissionen kæmpe imod det med alle til rådighed stående midler for at bevæge medlemslandene til ikke at indhente informationer illegalt på denne måde".³

5.10. Parlamentsrapporter

5.10.1. 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 det 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.

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 transmitterses via satellit (ca. 1% af alle internationale telefonsamtaler), hvis der anvendes søgeord, og at dets kapacitet med hensyn til kryptring er betydeligt større end angivet fra amerikansk side. Der er fortsat tvivl om udsagnene om, at der ikke finder industriopionage sted i Menwith Hill. Det understreges udtrykkeligt, at det er umuligt at konstatere med sikkerhed, hvilke aktiviteter Echelon driver.

5.10.2. Rapport fra den franske Nationalforsamlings Udvalg for Nationalt

Lone Dybkjær til Kommissionen (17.12.1999) m.fl.

**Forsvar**


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 frihedsretigheder, 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 indicer 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.

**5.10.3. Rapport fra det italienske parlamentariske udvalg om informations- og sikkerhedstjenester og statssikkerhed**


Konklusionerne vedrørende eksistensen af et system ved navn ECHELON er vague. Ifølge rapporten kunne man på grundlag af høringerne i udvalget i overvejende grad udelukke, at der kunne eksistere et integreret aflytningssystem af dette navn, som blev anvendt af de fem UKUSA-stater (USA, Det Forenede Kongerige, Australien, New Zealand og Canada) med det formål at aflytte kommunikation globalt. Det var klart, at der fandtes et snævrere samarbejde mellem de angelsaksiske lande, men udvalgets undersøgelser gav ikke grundlag for at påstå, at dette samarbejde var stillet mod etablering af et integreret aflytningssystem eller endog et globalt aflytningsnet. Efter udvalgets opfattelse var det sandsynligt, at betegnelsen ECHELON stod for et stadium i den teknologiske udvikling inden for satellitaflytning. Der henvises udtrykkeligt til, at det italienske efterretningsvæsen SISMI havde udelukket, at der for øjeblikket findes en proces for automatisk talegenkendelse, således at det heller ikke er muligt målrettet at foretage en aflytning af samtaler, der indeholder disse nøgleord.

---

\(^1\) 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 sécurité nationale, N° 2623 Assemblé nationale, enregistré 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 global aflytning af international kommunikation, der transmíttieres 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 transmíttieres via satellit, skal aflyttes.

Et yderligere globalt arbejdende aflytningssystem vil være tvunget til at oprette stationer uden for UKUSA-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 begrænser kredsen i princippet til Kina og G8-staterne uden USA og Det Forenede Kongerige.

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° Ø / 12° S) og La Réunion (55° Ø / 20° S) og helt sydpå Terres Australes og Antarctiques Francaises. I Stillehavsområdet ligger Ny Kaledonien (165° Ø / 20° S), Wallis og Futana (176° V / 12° S) samt Fransk Polynesien (150° V / 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\textsuperscript{1} findes der stationer i Kourou i Fransk Guyana og i Mayotte. Der foreligger intet om stationernes størrelse, antallet af satellitantenner og desses størrelse. Andre stationer hævdes at ligge i Frankrig i Domme i nærheden af Bordeaux og i Alluets-le-Roi i nærheden af Paris. Antallet af satellitantenner anslår Jauvert til i alt 30. Forfatteren Erich Schmidt-Eenboom\textsuperscript{2} hævder, at der også drives en station i Ny Kaledonien, og at den også benyttes af den tyske efterretningstjeneste.

Teoretisk set vil Frankrig også kunne drive et globalt aflytningssystem, da landet ud over de geografiske forudsætninger også har de nødvendige tekniske og økonomiske forudsætninger. Ordføreren disponerer imidlertid ikke over tilstrækkelige offentligt tilgængelige oplysninger til at kunne fremsætte seriøse påstande.

\subsection*{6.3. Rusland}

Den russiske efterretningstjeneste FAPSI (Federalnoye Agentstvo Pravitelstvennoy Svyazi), der er ansværlig for kommunikationssikkerhed og SIGINT, driver sammen med den russiske militære efterretningstjeneste GRU aflytningsstationer i Letland, Vietnam og Cuba.

Ifølge retsgrundlaget har FAPSI til formål at indsamle oplysninger inden for det politiske, økonomiske, militære og forskningstekniske område til understøttelse af den økonomiske udvikling og det forskningstekniske og militære fremskridt\textsuperscript{3}. Desuden nævner FAPSI's direktør tapning af krypteret kommunikation med udlandet og global aflytning som de primære opgaver\textsuperscript{4}.

I Atlanterhavsområdet ligger en station i Lourdes på Cuba (82°V, 23°N), som drives sammen med den cubanske efterretningstjeneste. Fra denne station samler Rusland både strategiske

\textsuperscript{1} Jean Guisnel, L'espionage n'est plus un secret, The Tocqueville Connection, 10.7.1998.

\textsuperscript{2} Vincent Jauvert, Espionnage comment la France écoute le monde, Le Nouvel Observateur, 5.4.2001, Nr. 1900, s. 14.

\textsuperscript{3} Erich Schmidt-Eenboom: Streng Geheim, Museumsstiftung Post und Telekommunikation, Heidelberg 1999, s. 180.


oplysninger og militær og kommerciel kommunikation.¹ I Det Indiske Ocean ligger stationer i Rusland, som der ikke foreligger nærmere oplysninger om. En anden station i Skrunda i Letland blev nedlagt i 1998.² 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 foreligger der imidlertid tilstrækkelige oplysninger til, at der kan fremsættes sikre 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.

---


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, australiske 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 europeiske 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 oplysninger4 og direktiv 97/66/EF om behandling af personoplysninger og beskyttelse af privatlivets fred inden for telesektoren5

1 Jf. ovenstående kapitel 1, 1.3.
2 Jf. ovenstående kapitel 2.
3 Jf. 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," 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, Parlamentet i øjeblikket har til behandling. En medlemsstats deltagelse i et aflytningssystem, der tjener statens sikkerhed, kan dermed ikke stride mod EU's databeskyttelsesdirektiver.

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. Også denne forordning kan kun anvendes, for så vidt som organerne handler inden for rammerne af EF-traktaten. 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 herfor.

7.2.2. Foreenlighed 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.

Beskyttelsen af personers grundlæggende rettigheder og frihedsrettigheder sikres på disse områder kun gennem EU-traktatens artikel 6 og 7, navnlig art. 6, stk. 2, hvor Unionen forpligter sig til at respektere de grundlæggende rettigheder, således som disse garanteres ved den europæiske menneskerettskonvention og som de følger af medlemsstaternes fælles forfatningsmæssige traditioner. I tilknytning til medlemsstaternes forpligtelse til at respektere de grundlæggende rettigheder og navnlig den europæiske menneskerettskonvention (jf. nedenstående 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 efterretningstjenestelige formål, er spørgsmålet om overtrædelse af EU-traktatens art. 6, stk. 2, i øjeblikket ikke

---

1 Art. 3, stk. 2, i direktiv 95/46.
2 Art. 1, stk. 3, i direktiv 97/66.
5 Art. 3, stk. 1; jf. også betragtning 15: Når denne behandling finder sted i fællesskabsinstitutioner og -organer som led i udøvelsen af aktiviteter, som ikke hører under denne forordning, kan disse personers grundlæggende rettigheder sikres under overholdelse af artikel 6 i traktaten om Den Europæiske Union.
7 For så vidt angår overvågning af telekommunikation, findes der på EU-plan omfattet af artikel 6 i traktaten om Den Europæiske Union.
relevant.

7.3. Spørgsmålet om foreneligheden, hvis et aflytningssystem misbruges til konkurrencespionage

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 fordøjelser 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 fordøjelser 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 forvirring af konkurrencen.

En sådan adfærd vil i øvrigt efter ordførerens mening udgøre en krænkelse af databeskyttelsesdirektivet for telekommunikationsområdet1, 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 konkurrencespionage, gennemfører 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 medlemsstatene 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 undtagelser, når dette er nødvendigt af hensyn til statens sikkerhed, forsvar og retsforsøg. 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 principielt ikke kan stride mod EU-retten, da det ikke udviser de berøringspunkter med EU-retten, der kræves for at der er tale om uførenelighed. Dette gælder ganske vist kun, så længe systemet virkelig udelukkende anvendes med sigte på statens sikkerhed i bred betydning. Anvendes det derimod til andet formål og til

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 overvågningsforanstaltninger 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 197 af 12.7.2000, s.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.

1 Direktiv 97/66/EF, EFT L 24 af 30.1.1998, s. 1.
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 dermed også efterretningstjenester ubetinget respektere retten til privatlivets fred, der 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 UKUSA-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 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 UKUSA-stater 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 2226/94 vom 14.7.1999, Abs. Nr. 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."


\(^{3}\) Art. 12 verdenserklæringen 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 enkelte menneske i forbindelse med elektronisk databehandling; jf. STOA-rapporten om 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.

dog ikke underskrevet tillægsprotokollen\(^1\), som udvider Menneskerettighedskomiteens befojelser 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 de grundlæggende rettigheder ved indførelse af et EU-charter om grundlæggende rettigheder. I charterets artikel 7 under overskriften "Respekt for privativet og familielivet" nævnes retten til respekten for den enkeltes kommunikation sågar eksplicit\(^2\). Desuden fastlægges i artikel 8 den grundlæggende ret til "Beskyttelse af personoplysninger". Det kunne beskytte den enkelte borger i de tilfælde, hvor vedkommendes personoplysninger behandles (elektronisk eller på anden vis), hvilket som regel er tilfældet ved aflytning og altid ved anden opsnapning.

Charteret er indtil videre ikke indarbejdet i traktaten. Det har derfor kun bindende virkning for de tre institutioner, som ved den højtidelige proklamation i Nice den 7. december 2000 underkastede sig dets bestemmelser: Rådet, Kommissionen og Europa-Parlamentet. De er, så vidt det er ordføreren bekendt, ikke involveret i efterretningsvirksomhed. Også hvis charteret derved have relevans for forbuddet mod konkurrenceforvridende statsstøtte (jf. kapitel 7, 7.3.)

Den europeiske 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 afgives af Menneskerettighedshjemmet i Strasbourg. Nationale bestemmelser for at overensstemmes med EMK kan derfor efterprøves af Menneskerettighedshjemmet og signatarstaterne kan i tilfælde af en krænkelse af menneskerettighederne dømmes og forpligtes til at udbetale en erstatning. Desuden har EMK vundet i betydning ved, at De Europæiske Fællesskabers Domstol i sine afgørelser i forbindelse med efterprøvning af love gentagne gange har henvist til den sammen med medlemsstaternes retsprincipper. 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

De rettigheder, der garanteres i EMK, er universelle menneskerettigheder og er derfor ikke bundet til et statsborgerskab. De garanteres enhver person under signatarstaternes jurisdiktion.


\(^2\) "Enhver har ret til privatliv og familieliv, sit hjem og sin kommunikation.”
Det betyder, at menneskerettighederne skal garanteres på en stats territorium som helhed, og at lokale undtagelser er en overtrædelse af konventionen. Desuden gælder de også uden for en signatarstats territorium i det omfang, 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 privatsfæreren.1

Det sidste er navnlig vigtigt, fordi der er det særlige aspekt ved spørgsmålet om de grundlæggende rettigheder 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 efterretningstjenesters 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 begreberne "privatliv" og "korrespondance" omfattet af den beskyttelse, som ydes ved artikel 8 i EMK.2 Beskyttelsen af denne grundlæggende ret 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 registrerer data, såsom forbindelsens tidspunkt og varighed og de valgte numre.3

Den grundlæggende ret i henhold til artikel 8, stk. 2, i EMK er ikke uindskrænket. Indgreb i denne ret kan være tilladt, hvis der er et retsgrundlag i den nationale lovgivning.4 Bestemmelsen skal være almen tilgængelig og dens konsekvenser skal være forudsigtelige.5

Medlemsstaterne er ikke frit stillet med hensyn til gennemførelsen af disse indgreb. I henhold til 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, forebygelse af forbrydelser, men også landets økonomiske velfærd6, hvilket imidlertid ikke berettiger økonomisk spionage, da


2 Menneskerettighedsdomstolen, Klass u.a., 6.9.1978, Z 41.


5 Silver u.a., 25.3.1983, Z 87 f.

6 Menneskerettighedsdomstolen har i et tilfælde accepteret "den økonomiske velfærd" som berettiget grund. Det
artiklen kun omfatter indgreb, som "er nødvendigt i et demokratisk samfund". Til hvert indgreb vælges det mest lemporlige 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 efterretningsvirksomhed

Hvis efterretningstjenesterne i deres virke skal respektere de grundlæggende rettigheder, skal følgende generelle principper overholdes: 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 alment tilgengeligt, 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. Domstolen har også krævet, at det altid skal fremgå af loven, under hvilke omstændigheder og på hvilke betingelser den offentlige anklager kan indledte et hemmeligt og derved potentielt farligt indgreb i privatsfæren.¹

Hvis efterretningsvirksomhed skal være i overensstemmelse med menneskerettighederne, må man være opmærksom på, at hensynet til den nationale sikkerhed ganske vist kan gøre den berettiget, men at det i henhold til artikel 8, stk. 2, i EMK er underlagt proportionalitetsprincippet. Selv den nationale sikkerhed kan kun bruges som berettigelse for indgreb, når de er nødvendige i et demokratisk samfund. Menneskerettighedsdomstolen har entydig fastslået, at en stats interesse i at beskytte den nationale sikkerhed må afvejes mod indgrebets omfang og borgerens interesse i respekten for privatsfæren.² Indgrebene er ikke begrænset til det strengt nødvendige, men det er ikke tilstrækkeligt, at de blot er nyttige eller ønskværdige.³ Den opfattelse, at aflytning af al telekommunikation er den bedste beskyttelse mod organisert kriminalitet, ville være i strid med artikel 8 i EMK, selv om den skulle være tilladt i henhold til national lovgivning.

På grund af efterretningstjenesternes 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 til beskyttelse af den nationale sikkerhed rummer den fare, at det under foregivende af at forsvarer demokratiet undergraver eller sågar ødelegger det. Derfor er det nødvendigt med adækvate og effektive garantier mod sådant misbrug.⁴ En efterretningstjenestes legitime virksomhed er kun i overensstemmelse med de grundlæggende rettigheder, hvis den pågældende EMK-stat har


¹ Menneskerettighedsdomstolen, Leander, 26.3.1987, Z 51.
⁴ Menneskerettighedsdomstolen, Silver m.fl., 24.10.1983, Z 97.
⁵ Menneskerettighedsdomstolen, Leander, 26.3.1987, Z 60.
etableret fyldestgørende kontrolsystemer og andre garantier mod misbrug. Domstolen lagde i forbindelse med Sveriges efterretningsvirksomhed stor vægt på tilstedevidærlensen af parlamentarikere i politiets kontrolorgan, og overvågningen ved justitsministeren, parlamentets ombudsmænd og retsudvalget. Ud fra denne betragtning forekommer det betænkeligt, at Frankrig, Grækenland, Irland, Luxemburg og Spanien ikke har et tilsynsudvalg for efterretningsstjenester og at de heller ikke har et kontrolsystem, som kan sidestilles med den parlamentariske ombudsmænd i de nordiske lande. Det er derfor glædeligt, at forsvarsudvalget i den franske Assemblée Nationale bestræber sig på nedsættelse af et kontroludvalg, 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 efterretningsstjenester

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

Som det allerede er udførligt belyst, skal signatarstaterne opfylde en række forudsætninger for at sikre, at deres efterretningsstjenester opfylder forpligtelserne i henhold til artikel 8 i EMK. Det siger sig selv, at disse efterretningsstjenester ikke kan frigøre sig for disse forpligtelser ved at gribe tilbage til andre efterretningsstjenester, 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 efterretningsstjenester er underkastet begrænsninger. En efterretningsstjeneste kan kun få oplysninger fra en anden efterretningsstjeneste, hvis videregivelsen er i overensstemmelse med landets egen lovgivning. Den ved lov fastsatte rækkevidde af efterretningsstjenesternes aksioner må ikke udvides ved aftaler med andre tjenester. Ligeledes må den kun udføre efterretningsvirksomhed for en anden efterretningsstjeneste 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 grundlæggende ret.

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

1 Ordføreren er bekendt med, at hverken Luxembourg eller Irland har en udenlandsk efterretningsstjeneste, og at de ikke driver Sigint. Kravet om en særlig kontrolinstans vedrører her kun efterretningsstjenester inden for landets grænser.

2 For kontrollen med efterretningsstjenester i medlemsstaterne jf. kapitel 9.

3 Det franske lovforslag ("Proposition de loi tendant à la création de délégations parlementaires pour le renseignement") og betænkningen herom af Arthur Paecht, medlem af det franske parlament, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusiers de ses collègues tendant à la création d'une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de l'assemblée nationale le 23. november 1999.

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 uøvelsen af deres suverænitet underkaste en kontrol med respekten for de grundlæggende rettigheder. De kan ikke tilsidesætte denne forpligtelse ved at afstå fra deres suverænitet. Disse stater er fortsat ansvarlige for deres territorium og derved forpligtet over for EU-borgere, også i det tilfælde, hvor uøvelse af suveræniten 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 de grundlæggende rettigheder i henhold til artikel 8 i EMK ikke krænkes af private (!), dvs. også på horisontalt plan, hvor den enkelte ikke står over for myndighederne, men en anden person. 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, at den efterretningsvirksomhed, der udøves på dens territorium, er i overensstemmelse med menneskerettighederne.

8.4.2.2. Konsekvenser for aflytningsanlæg

I Tyskland har man i Bad Aibling stillet et eget territorium til rådighed for USA 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, udøver der 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 Morwenstow i Storbritannien gennemføres efter oplysningerne fra GCHQ aflytning af civil kommunikation i samarbejde med USA 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 det krav 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 gendsigt påtale, at den anden stat også opfylder sine forpligtelser i henhold til konventionen. Det gælder i hvert fald, indtil det er bevis, at en EMK-stat systematisk og vedvarende overtræder EMK. USA har imidlertid ikke undertegnet EMK og har heller ikke underkastet sig et tilsvarende kontrolsystem. De amerikanske efterretningstjenesters aktiviteter er underlagt meget nøje regler, for så vidt angår

---

amerikanske borgere hhv. personer, som har legit nat ophold i USA. Der gælder imidlertid andre regler for NSA's virksomhed i udlandet, og mange af disse regler er tilsyneladende fortrolige og derved utilgængelige. Det forekommer endnu mere forurlopende, at den amerikanske efterretningstjeneste ganske vist 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 Det Forenede Kongerige om at tage de forpligtelser, der udspringer af EMK, alvorligt og gøre NSA's udføjelse af yderligere efterretningstjenester 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 alment 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 nødvendigt. Derfor må man vælge det lempeligst muligt omfang, der gennemføres fra amerikansk side, skønnes at være mindre alvorligt end et indgreb fra amerikansk side, da borgeren i første tilfælde kan påberåde sig sin grundlæggende ret hos nationale instanser. 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 påvirkning af strafferetsplejen fra amerikansk side til at motvide det europæiske tilladsel lighedsreglementet. For EU-borgeren må et indgreb, der gennemføres fra amerikansk side, kunne vare ganske vist mindre alvorligt end et indgreb fra europæisk side, da borgeren i ændret tilfælde kan påberåde sig sine grundlæggende rettigheder. For EMK er det vigtigt at gennemføre disse indgreb, det er et omfattende indgreb, det betyder, at det er vigtigt at gennemføre dette indgreb, det er et omfattende indgreb, det betyder, at det er vigtigt at "..."...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

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

ved EMK garanterede ensartede beskyttelsesniveau i Europa opretholdes.
9. Er EU's borgere tilstrækkeligt beskyttede over for efterretningsvirksomhed?

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

Om end efterretningsstjenesternes aktiviteter i fremtiden kan henføres under FUSP (den fælles udenrigs- og sikkerhedspolitik), er der endnu ikke udarbejdet bestemmelser herom på EU-plan1, og ordninger om beskyttelse af borgere over for efterretningsstjenesternes aktiviteter afhænger alene fra de nationale retssystemer.

De nationale parlamenter har her en dobbelt funktion: som lovgiver træffer de afgørelser om efterretningsstjenesternes 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 begrensninger, der er fastsat i artikel 8 i den europæiske menneskerettighedskonvention, dvs. relevante bestemmelser skal være nødvendige og forholdsmappe og deres konsekvenser for den enkelte skal være forudsigelige. Desuden skal der fastlægges tilstrækkelige og effektive kontrolforanstaltninger vedrørende kontrolmyndighedernes beføjelser.

Desuden spiller de nationale parlamenters rolle i de fleste lande en aktiv rolle som kontrolmyndighed, da kontrol med den udøvende myndighed (og dermed også med efterretningsstjenesterne) 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 sikkerhed2 (over for udlandet).

I alle medlemsstater kan principippet om hemmelig telekommunikation brydes, når formålet er at håndhæve loven, forudsat der er tilstrækkelig bevis for, at en person har begået en forbrejelse (eventuelt under særlige alvorlige omstændigheder). Da indgreb i udøvelsen af retten til privatsfæren er alvorlig, kræves generelt en dommerkendelse til en sådan aktion3. Kendelsen indeholder præcise oplysninger om kontrollens tilladte varighed, de relevante kontrolforanstaltninger og tilintetgørelse af insamlede 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 indenrigsministre 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 undergrundsbefæl og terrorisme og organiseeret kriminalitet. Indsamlingen af relevante data samt analyse heraf foretages af særlige indenrigsefterretningstjenester.


9.3. Kontrol med efterretningstjenesterne

Det er derfor særlig vigtigt 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 erfærer, 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 probleem, at det på grund af efterretningstjenesterne særlige karakter, ofte er yderst vanskeligt at fastslå, om alle oplysninger er forelagt, eller om en del tilbageholdes. Derfor må bestemmelserne herom

---

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.
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).
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, 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 forfatningssaglige hensyn ønskeligt, at efterretningstjenestens arbejde som helhed underlægges kontrol af et parlamentarisk organ i overensstemmelse med principippet om magtfordeling.


Derudover findes der et parlamentarisk kontrolorgan (PKGr), som består af ni medlemmer af Forbundsagen 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 døftelser er hemmelige og medlemmerne er forpliget til at udvise fuld fortrolighed – også efter at de har nedlagt deres hvert. Halvvejs og ved udløbet af valgperioden forelægger PKGr den tyske Forbundsstat en beretning om sin kontrolaktivitet.

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

I Frankrig 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 parlementet 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

---

1 En udtømmende redegørelse findes i: Parlamentarisk kontrol med efterretningstjenesten i Tyskland (9.9.2000, udgivet af Den Tyske Forbundsag, den parlamentariske kontrolgroupes sekretariat).
2 Lov om kontrol med Forbundsstatens efterretningstjenestes aktiviteter (PKGrG) af 17. juni 1999, BGB1 I 1334, idgF.
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
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. Nationalforsamlings forsvarsudvalg
har allerede godkendt et sådant forslag1, men forslaget er endnu ikke behandlet i plenum.

I Det Forenede Kongerige kræver enhver overvågning af telekommunikation på britisk jord
een 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 sikkerhedsstjenesternes 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
etfterretningstjenesters (M15, M16 og GCHQ) aktiviteter, står for den parlamentariske kontrol.
Dette udvalg er navnlig ansvarlig for gennemgang af udgifter og administration samt kontrol
af sikkerhedsstjenestens, 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
etterretningstjenesterne, da deres medlemmer er bundet af reglen om fortrolighed og moderne
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.

1 Jf. lovforslag "Proposition de loi tendant à la création de déléguations parlementaires pour le renseignement" og
betænkning herom af Arthur Paecht, Rapport fait au nom de la Commission de la défense nationale et des forces
armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création
d'une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de L'Assemblée
nationale le 23 novembre 1999.

2 Intelligence Services Act 1994, Section 10.
Det er glædeligt, at de fleste af EU's medlemsstater har nedsat et særligt parlamentarisk kontroludvalg, der skal gennemgå efterretningstjenesternes aktiviteter. I Belgien\(^1\), Danmark\(^2\), Tyskland\(^3\), Italien\(^4\), Nederlandene\(^5\) og Portugal\(^6\) findes der et parlamentarisk kontroludvalg, som både er ansvarlig for kontrol med militære og civile efterretningstjenester. I Det Forenede Kongerige\(^7\) overvåger det særlige kontroludvalg kun (om end væsentlig mere omfattende) civile efterretningstjenester, mens den militære efterretningstjeneste overvåges af det normale forsvarsudvalg. I Østrig\(^8\) henhører de to grene af efterretningstjenesten under to separate kontroludvalg, mens de 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.

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 beskyttelsesniveaet gennem deres stemme ved valg. Den uheldige virkning rammer først og

---

1 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.
2 Udvælgel vedrørende efterretningstjenesterne, Lov om etablering af et udvalg om forsvarsrets og politiets efterretningstjenester, lov 378 af 6/7/88.
3 Das parlamentarische Kontrollgremium (PKGr), Gesetz über die Kontrolle Nachrichtendienstlicher Tätigkeit des Bundes (PKGrG) af 17. juni 1999 BGBI I 1334 idgF.
4 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.
7 Intelligence and Security Committee (ESC), intelligence services act 1994, Section 10.
8 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 anlæggere, der er ansvarlig for kontrolforanstaltninger for at beskytte forfattningsorganer og deres handlekraft (Art. 52a B-VG, §§ 32b ff forretningsordenen 1975.
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.

Desuden vil spørgsmålet om beskyttelse af europeiske borgere blive placeret i en fuldstændig ny sammenhæng, når de første skridt som led i en fælles sikkerhedsropolitik 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


10.1.1. De enkelte spionagemål

Strategiske oplysninger, som er vigtige for økonomisk spionage, kan opdeles efter 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, billede- 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. kapitel 10, 10.1.4).

10.1.2. Konkurrencespionage

En virksomheds strategiske position på markedet er afhængig af dens situation med hensyn til

¹ Informationen for geheimschutzbetreute Unternehmen, Bundesministerium für Wirtschaft, 1997.
forskning og udvikling, produktionsprocesser, produktlinjer, finansiering, markedsføring, salg, distribution, indkøb og arbejdsstyrken. 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.


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 sikkerhedscheferne i et par store tyske virksomheder 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. Sikkerhedskonsulenter 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. Formanden for sammenslutningen af sikkerhedskonsulentfirmaer i Tyskland, Klaus-Dieter Matschke, nævner under henvisning til

---

3 Enkeltheder og navne beskyttet.
4 IMPULSE,3/97,S.13 ff.


**10.3. Hvem spionerer?**

Ifølge en undersøgelse af firmaet Ernest Young LLP\(^3\) er de vigtigste bagmænd for spionage mod virksomheder konkurrenter (39%), kunder (19%), leverandører (9%) og efterretningsstjenester (7%). Det er egne medarbejdere, private spionagefirmaer, betalte hackeré og fagfolk fra efterretningsstjenester, der udfører spionage.\(^4\)

**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.


**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 efterretningsstjenester. Disse

---


\(^3\) Computerzeitung, 30.11.1995, s. 2

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.

10.3.3. Hackere
Hackere er computerspecialister, som i kraft af deres viden kan skaffe sig adgang til edb-net. I hackertidssalerens 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 organisert 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 efterretningsteknikker 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 virksomhedsconcerns 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 standardteknikkerne for økonomisk spionage;
- indbrud i 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 simplicer.

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. kapitel 10, 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 i højere grad end tidligere indføres på andre områder. USA erklærer offentligt, at en del af dem efterretningstjenester 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), udviklinger 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 konkurrencefordelere. I den sammenhæng kan der skelnes mellem to former:¹.

10.5.2.1. Hightech-stater

Højudviklede industrielande kan have stort gavn af industrispionage. Ved at udspionere udviklingsstilstanden 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. kapitel 10, 10.6).

10.5.2.2. Teknisk mindre avancerede stater

For en del af disse stater drejer det sig om at fremskaffe teknisk knowhow for at kunne indhente et efterslæb hos landets egen industri uden udviklingsomkostninger og licensgebyr. Desuden drejer det sig om fremskaffelse af originale produkter og fremstillingsmekanikker med henblik på at opnå konkurrenceevne på verdensmarkedet med billigere (lavere lønomkostninger) kopiprodukter. Det er dokumenteret, at den russiske efterretningstjeneste har fået tildelt denne opgave. I Den Russiske Foderations lov nr. 5 om efterretningstjenester til udlandet nævnes eksplicit fremskaffelse af økonomiske og forskningstekniske oplysninger som en opgave for efterretningstjenesten. For en anden gruppe stater (herunder Iran, Irak, Syrien, Libyen, 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 efterretningstjenestene 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 nettag eller radio (satellit), kan et kommunikationsovervågningsystem 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 VSAT eller kabel;
- når der forhandles om vigtige kontrakter på stedet (f.eks. i bygge- og anlægssektoren, telekommunikationsinfrastrukture, nyoprettelse af transportsystemer osv.) og der derfra skal føres samråd med hovedkontoret.

¹ Private oplysninger fra en efterretningstjeneste til ordføreren. Kilde beskyttet.
Hvis virksomheder i disse tilfælde ikke beskytter deres kommunikation, giver tapning af denne kommunikation værdifulde oplysninger til konkurrencespionage.

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.
<table>
<thead>
<tr>
<th>Sag</th>
<th>Hvem</th>
<th>Hvornår</th>
<th>Hvad</th>
<th>Hvordan</th>
<th>Mål</th>
<th>Følger</th>
<th>Kilde</th>
</tr>
</thead>
<tbody>
<tr>
<td>BASF</td>
<td>Sälger</td>
<td>Ikke nævnt</td>
<td>Beskrivelse af fremgangsmåden for produktion af hudcremeråstof i BASF (kosmetiksektion)</td>
<td>Ikke nævnt</td>
<td>Ikke nævnt</td>
<td>Ingen, fordi afsløret</td>
<td>„Nicht gerade zimperlich&quot;, Wirtschaftswoche Nr.43 / 16. oktober 1992</td>
</tr>
<tr>
<td>Forbunds-økonomiministeriet, DE</td>
<td>CIA</td>
<td>1997</td>
<td>Information om hightech-produkter i Forbundsøkonomiministeriet</td>
<td>Benyttelse af agent</td>
<td>Fremskaffelse af informationer</td>
<td>Agenten afsløres ved forsøg og udvises</td>
<td>„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?&quot; af Arno Schütze, 1/98</td>
</tr>
</tbody>
</table>
"(...) Ud fra militære synspunkter er forræderiet "ikke særligt tungtvejende". Dette gælder også for den økonomiske skade, konstaterede domstolen" | „Anmerkungen zur Sicherheitslage der deutschen Wirtschaft", ASW; Bonn, 2001 |

"Hafstrafe wegen Spionage für Russland", SZ / 30. mai
<table>
<thead>
<tr>
<th>Sag</th>
<th>Hvem</th>
<th>Hvornår</th>
<th>Hvad</th>
<th>hvordan</th>
<th>Mål</th>
<th>Følger</th>
<th>Kilde</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embargo</td>
<td>BND Den tyske efterretningstjeneste</td>
<td>ca. 1990</td>
<td>Formyet eksport af embargo-beskyttet teknologi til Libyen (bl.a. ved Siemens)</td>
<td>Aflytning af telefonvæsenet</td>
<td>Afsløring af illegal våben- og teknologitransfer</td>
<td>Ingen særlige konsekvenser, leveringer forhindres ikke</td>
<td>&quot;Maulwürfe in Nadelstreifen&quot;, Andreas Förster, s. 110</td>
</tr>
<tr>
<td>Enercon</td>
<td>Eksperter i vindenergi fra Oldenburg, en kvindelig medarbejder fra Kenetech</td>
<td>Ikke nævnt</td>
<td>Vindkraftanlægget, ejet af firmaet Enercon i Aurich</td>
<td>Ikke nævnt</td>
<td>Ikke nævnt</td>
<td>Ikke nævnt</td>
<td>„Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Bonn, April 2001</td>
</tr>
<tr>
<td>Japanske handelsministerium</td>
<td>CIA</td>
<td>1996</td>
<td>Forhandlinger om importkvoter for amerikanske biler på det japanske marked</td>
<td>Hacker i det amerikanske handelsministeriums computersystem</td>
<td>Den amerikanske forhandlinger Mickey Kantor skal indvillige ved laveste tilbud</td>
<td>Kantor accepterer laveste tilbud</td>
<td>„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ af Arno Schütze, 1/98</td>
</tr>
<tr>
<td>Sag</td>
<td>Hvem</td>
<td>Hvornår</td>
<td>Hvad</td>
<td>Hvordan</td>
<td>Mål</td>
<td>Felger</td>
<td>Kilde</td>
</tr>
<tr>
<td>------------------</td>
<td>-------</td>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>----------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>López</td>
<td>NSA</td>
<td>Ikke nævnt</td>
<td>Videokonference fra VW og López</td>
<td>Aflytning fra Bad Aibling</td>
<td>Videregivelse af oplysninger til General Motors og Opel</td>
<td>Gennem aflytningsforanstaltninger ville statsadvokaten have fået meget nøje oplysninger med henblik på afsløring</td>
<td>Kaptajn i det tyske Bundeswehr, Erich Schmidt-Eenboom, citerer i „Wenn Freunde spionieren“ <a href="http://www.zdf.msnbc.de/news/54637.asp?cp1=1">www.zdf.msnbc.de/news/54637.asp?cp1=1</a></td>
</tr>
<tr>
<td>Los Alamos</td>
<td>Israel</td>
<td>1988</td>
<td>To medarbejdere i Israels atomforskningsprogram bryder koden for centralcomputeren i atomvåbenlaboratoriet Los Alamos</td>
<td>Hackere</td>
<td>Fremskaffelse af informationer om nye amerikanske atomvåbentændere</td>
<td>Ingen særlige konsekvenser, da hackerne flygter til Israel, én bliver derefter be脂肪 sat fast, ingen officiel forbindelse til Israel er efterretningsdieneste</td>
<td>&quot;Maulwürfe in Nadelstreifen&quot;, Andreas Förster, s. 137</td>
</tr>
<tr>
<td>Smuggling</td>
<td>BND</td>
<td>70'erne</td>
<td>Smuggling af computeranlæg til DDR</td>
<td>Ikke nævnt</td>
<td>Afsløring af teknologistransfer til Østblokken</td>
<td>Ingen særlige konsekvenser, leveringer blev ikke forhindret</td>
<td>&quot;Maulwürfe in Nadelstreifen&quot;, Andreas Förster, s. 113</td>
</tr>
<tr>
<td>TGV</td>
<td>DGSE</td>
<td>1993</td>
<td>Siemens-udgiftsberegning Ordre til levering af højhastighedstog til Sydkorea</td>
<td>Ikke nævnt</td>
<td>Dumpingpris</td>
<td>ICE-producenten går glip af orden til fordel for Alcatel-Alsthom</td>
<td>„Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ af Arno Schütze, 1/98</td>
</tr>
<tr>
<td>Sag</td>
<td>Hvem</td>
<td>Hvornår</td>
<td>Hvad</td>
<td>Hvordan</td>
<td>Mål</td>
<td>Følger</td>
<td>Kilde</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>---------</td>
<td>------</td>
<td>---------</td>
<td>-----</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>TGV</td>
<td>Ukendt</td>
<td>1993</td>
<td>Udgiftsregning fra AEG og Siemens med hensyn til offentligt udbud i Sydkorea til levering af højhastighedstog</td>
<td>Siemens påstår, at dets telefon- og faxforbindelser er blevet aflyttet i filialen i Seoul</td>
<td>Forhandlingsfordel for den britisk-franske medansøger GEC Alsthom</td>
<td>Ordregiverne vælger GEC Alsthom, selv om det tyske tilbud først var bedre</td>
<td>„Abgehört“, Berliner Zeitung, 22. januar 1996</td>
</tr>
<tr>
<td>Thomson-Alcatel vs. Raytheon</td>
<td>CIA/ NSA</td>
<td>1994</td>
<td>Tildeling af en brasiliansk milliardkontrakt vedr. satellitovervågning af Amazonas til det franske Thomson-Alcatel (1,4 mia. dollars)</td>
<td>Aflytning af kommunikationsforbindelserne hos vinderen af udbuddet (Thomson-Alcatel, FR)</td>
<td>Afsløring af korruption (udbetaling af bestikkelsespenge)</td>
<td>Clinton indgiver klage hos den brasilianske regering; efter den amerikanske regering insisterer ny tildeling af kontrakten til det amerikanske firma <em>Raytheon</em></td>
<td>&quot;Maulwürfe in Nadelstreifen&quot;, Andreas Förster, s. 91</td>
</tr>
<tr>
<td>Thyssen</td>
<td>BP</td>
<td>1990</td>
<td>Millionkontrakt om gas- og olieudvinding i Nordsøen</td>
<td>Aflytning af faxmeddelelser fra den udvalgte bydende (Thyssen)</td>
<td>Afsløring af korruption</td>
<td>BP sagsager Thyssen for at få skadesersatning</td>
<td>&quot;Maulwürfe in Nadelstreifen&quot;, Andreas Förster, s. 92</td>
</tr>
</tbody>
</table>
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 de 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.

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


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 konkurrender 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 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 økonomi efter Den Kolde Krig**

Siden 1990 har den amerikanske regering i stigende grad sat lighedstegn mellem økonomisk sikkerhed og national sikkerhed. Årsberetningen fra Det Hvide Hus "National Security Strategy"\(^1\) understreger igen og igen, *"at økonomisk sikkerhed er et integrerende element ikke kun i nationens interesser, men også i nationens sikkerhed"*. Denne udvikling har flere årsager. Der er faktisk tale om tre faktorer, der har spillet sammen:

- efterretningstjenesternes interesse i opgaver også efter Den Kolde Krig,
- udenrigsministeriets enkle erkendelse af, at USA's førende rolle i verden efter Den Kolde Krig ikke kun må bygge på militær styrke, men også på økonomisk styrke,
- president Clintons indenrigspolitiske interesser i en styrkelse af den amerikanske økonomi og skabelse af arbejdspladser.

Denne sammenlægning af regeringsinteresser har haft følger i praksis.


Som en konsekvens, i det mindste set ud fra en amerikansk synsvinkel, har regeringen givet CIA og dernæst NSA til opgave at hindre konkurrencefordrejninger, der skyldes bestikkelse. Tidligere CIA-direktør James Woolsey gjorde dette helt klart på en pressekonference, som han holdt den 7. marts 2000 efter udenrigsministeriets ønske\(^2\).

Som en konsekvens har handelsministeriet koncentreret sine eksportfremmeaktiviteter på en sådan måde, at amerikanske firmaer kun har kontakt med en enkelt partner, når de ønsker at eksportere. I den forbindelse sker der ikke kun en passiv, men også en aktiv koncentration af alle regeringens muligheder (se nærmere herom i kapitel 10, 10.9.4).

**10.9.1 Udfordringen for den amerikanske regering: Økonomisk spionage mod amerikanske virksomheder**

Det er hverken usædvanligt eller nyt, at den amerikanske økonomi udsættes for efterretningsoperationer. Både USA og andre vigtige industristater har i årtier været mål for økonomisk spionage. Under Den Kolde Krig kom tilvejebringelsen af økonomiske og

---

\(^1\) National sikkerhedsstrategi.

\(^2\) State Department Foreign Press Center Briefing, Subject: Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage, Washington DC, 7.3.2000.
teknologiske informationer imidlertid først i anden række efter den klassiske spionage. Efter afslutningen af Den Kolde Krig har økonomisk spionage etableret sig som et selvstændigt mål.


10.9.1.1. Aktørerne


10.9.1.2. Målene for økonomisk spionage

De mål for økonomisk spionage, der nævnes af FBI, adskiller sig ikke fra dem, der er omtalt i kapitel 10, 10.1.1. Men som prioriterede mål nævnes højteknologi og forsvarsindustrien.

Derudover nævnes, hvilket er ganske interessant, informationer om tilbud, kontrakter, kunder og strategiske oplysninger på disse områder som mål for økonomisk spionage, der forfølges aggressivt.

---

2 "Consequently, foreign governments, through a variety of means, actively target U.S. persons, firms, industries and the U.S. government itself, to steal or wrongfully obtain critical technologies, data, and information in order to provide their own industrial sectors with a competitive advantage".
4 Ordførerens udlægning af Louis J. Freeh's kryptiske udtalelser under høringen.
5 På disse områder er kommunikationsaflytning en særdeles lovende metode!
10.9.1.3. Metoder

FBIU har som led i Economic Counterintelligence Program konstateret en række forskellige spionagemetoder. For det meste anvendes en kombination af metoder og kun sjældent en enkelt metode. Ifølge FBI er den bedste kilde en person i en virksomhed eller en organisation, hvilket gælder generelt og ikke kun i USA (se kapitel 10, 10.3. og 4.). Under høringen udtalte FBI sig om, hvordan personer anvendes til spionage, men mærkeligt nok ikke om elektroniske metoder.

10.9.2 Den amerikanske regerings holdning til aktiv økonomisk spionage

CIA's forhenværende direktør, Woolsey, sammenfattede på en pressekonference1 og under en samtale med medlemmer af udvalget i Washington kort det amerikanske efterretningstjenestes aflytningsvirksomhed således:

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. Woolsey gav imidlertid ingen konkrete eksempler på et spørgsmål herom.

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 deltaget i udbuddet bliver derimod ikke direkte orienteret. Ren konkurrencespionage udelukkede han kategorisk

Den fungerende direktør for CIA, George J. Tenet, udtalte sig tilsvarende under en høring i udvalget om tilsyn med efterretningstjenester i Repræsentanternes Hus den 12. april 20002:

"Det er hverken USA's politik eller praksis at drive spionage, som ville give amerikanske virksomheder en unfair fordel". Under den samme høring sagde Tenet endvidere, at eventuelle oplysninger om bestikkelse ville blive givet videre til andre regeringsmyndigheder, som så måske kunne hjælpe amerikanske virksomheder.3 På et spørgsmål af medlem af Repræsentanternes Hus Gibbons indrømmede Tenet, at der ikke fandtes noget lovforbud mod konkurrencespionage, og at han heller ikke anså det for nødvendigt, da tjenesterne ikke ville udføre den slags aktiviteter.

1 James Woolsey, Remarks at the Foreign Press Center, Transskript, 7.3.2000, http://cryptome.org/echelon-cia.htm
2 "It is not the policy nor the practice of the U.S. to engage in espionage that would provide an unfair advantage to U.S. Companies".
3 "As I indicated also in my testimony, there are instances where we learn, that foreign companies or their governments bribe, lie, cheat or steal their way to disenfranchise American companies. When we generate this information, we take it to other appropriate agencies, make them aware of it. They use that information through other means and channels to see if they can assist an American company. But we play defense, we never play offense.”.
Formanden for udvalget om tilsyn med efterretningstjenester i Repræsentanternes Hus, Porter Goss, tegnede under en samtale i Washington et tilsvarende billede af aflytningsaktiviteterne.

10.9.3. Retssituationen ved bestikkelse af embedsmænd

Bestikkelse som middel til at opnå kontrakter er ikke noget europæisk, men et internationalt fænomen. Transparency International opstillede i Bribe Payers Index (BPI), som offentliggjordes i 1999, en liste over de 19 førende eksportlande baseret på, hvor hyppigt de tilbød bestikkelse, og her delte Tyskland og USA 9. pladsen. Sverige, Østrig, Nederlandene, Det Forenede Kongerige og Belgien havde en lavere bestikkelsesrate, og kun Spanien, Frankrig og Italien rangerede højere.2

Den amerikanske begrundelse for økonomisk spionage bygger på europæiske virksomheders korruptionspraksis i enkeltstående tilfælde. Dette er tvivlsomt, og ikke kun fordi fejlagtig adfærd ikke kan udgøre nogen begrundelse for omfattende spionage. Tværtimod ville en sådan praksis uden lov og ret kun kunne tolereres i et område, hvor der hersker lovløse tilstande.

I Europa gribes der til lige så hårde retsmidler over for korruption som i USA. De overensstemmende interesser førte i 1997 til vedtagelsen af OECD-konventionen fra 1997 om bekæmpelse af bestikkelse af udenlandske embedsmænd i internationale erhvervstransaktioner.3 Den forpligter signatarstaterne til at gøre bestikkelse af en udenlandsk embedsmænd strafbart og indeholder ud over en beskrivelse af, hvori den strafbare handling består, også bestemmelser om sanktioner, jurisdiktion og håndhævelse.

Konventionen, som trådte i kraft den 15.2.1999 er med undtagelse af Irland gennemført og ratificeret af alle EU-medlemsstaterne. USA gennemførte konventionen ved en tilpasning af Foreign Corrupt Practices Act (FCPA) fra 1977, som pålægger virksomheder bogføringspligt og forbryder bestikkelse af udenlandske embedsmænd, på grundlag af International Anti-Bribery and Fair Competition Act fra 1998.4 Hverken i USA eller EU er bestikkelse af udenlandske embedsmænd fradragsberettiget.5

Medens OECD-konventionen kun er rettet mod bekæmpelse af bestikkelse af udenlandske

2 Graden af bestikkelse bevæger sig mellem 10 (laveste) og 0 (højeste): Sverige (8,3), Australien (8,1), Canada (8,1), Østrig (7,8), Schweiz (7,7), Nederlandene (7,4), Det Forenede Kongerige (7,2) Belgien (6,8), Tyskland (6,2), USA (6,2), Singapore (5,7), Spanien (5,3), Frankrig (5,2), Japan (5,1), Malaysia (3,9), Italien (3,7), Taiwan (3,5), Sydkorea (3,4), Kina (3,1).
embedsmænd, vedtog Europarådet i 1999 to mere vidtgående konventioner, som imidlertid endnu ikke er trådt i kraft. Den strafferetlige konvention om korruption\(^1\) omhandler også bestikkelse i den private sektor. Den er undertegnet af alle EU-medlemsstater undtagen Spanien og også af USA, men dog kun ratificeret af Danmark.

Den civilretlige konvention om korruption\(^2\) indeholder bestemmelser om ansvar og skadeserstatning og særlig om kontrakters og kontraktbestemmelsers ugyldighed, hvis de indeholder en forpligtelse til at betale bestikkelse. Den er undertegnet af alle EU-medlemsstater, bortset fra Nederlandene, Portugal og Spanien, men heller ikke af USA.

Der er også blevet vedtaget to EU-retsakter om bekæmpelse af bestikkelse: konventionen om bestikkelse af tjenestemænd og den fælles aktion om bestikkelse i den private sektor.

Konventionen om bekæmpelse af bestikkelse, som involverer tjenestemænd ved De Europæiske Fællesskaber eller i EU's medlemsstater\(^3\), har til formål at sikre, at passiv og aktiv bestikkelse er en strafbar adfærd overalt i EU. Medlemsstaterne forpligter sig til at gøre såvel aktiv som passiv bestikkelse, der involverer tjenestemænd, til en strafbar adfærd, uanset om det drejer sig om en af medlemsstatens egne statsborgere en tjenestemand i en anden medlemsstat eller en EU-tjenestemand.

Den fælles aktion om bestikkelse i den private sektor\(^4\) skal sikre, at aktiv og passiv bestikkelse, der involverer virksomheder, gøres til en strafbar adfærd, og den indeholder bestemmelser om strafferetlige sanktioner ikke kun for fysiske personer, men også for juridiske personer. Den fælles aktions anvendelsesområde er imidlertid begrænset i forhold til konventionen om bestikkelse, der involverer tjenestemænd, idet den kun forpligter medlemsstaterne til at pålægge sanktioner for lovovertrædelser, der i det mindste delvis er begået på dens område. Medlemsstaterne er derimod frit stillet med hensyn til, om de vil udvide den strafbare adfærd til at omfatte lovovertrædelser, der begås af landets egne statsborgere i udlandet eller til fordel for indenlandske juridiske personer. I Tyskland og Østrig anses bestikkelse begået i udlandet for at være en strafbar adfærd, hvis den også er en strafbar adfærd dér, hvor den blev begået.

**10.9.4. Advocacy Center og dets rolle i USA’s eksportfremme**

Med Executive Order 12870 oprettede præsident Clinton i 1993 den såkaldte Trade Promotion Coordinating Committee (TPCC)\(^5\), som skal samordne udviklingen af regeringens handelsfremmepolitik og udarbejde en strategi på området. Ifølge den nævnte Executive Order har også en repræsentant for National Security Council (NSC)\(^6\) sæde i TPCC.

---


\(^6\) Homepage des National Security Councils (NSC), [http://www.whitehouse.gov/nsa](http://www.whitehouse.gov/nsa)

10.9.4.1. Advocacy Center og dets opgave

"The Advocacy Center helps U.S. Businesses by:"

- Marshalling the resources of the U.S. Government - from the various financing, regulatory, country and sector experts, through the world-wide network of commercial officers, to the White House;
- Fighting to level the playing field and promote open competition in the international bidding arena – from the multibillion dollar infrastructure project to the strategic contract for a small business;
- Pursuing deals on behalf of U.S. companies from start to finish, through “hands-on” support;
- Supporting U.S. jobs and boosting U.S. exports through the successes of U.S. companies who successfully bid for overseas projects and contracts;
- Assisting U.S. firms with stalled negotiations due to foreign government inaction or “red tape”.

10.9.4.2. Centrets arbejdsmåde
Personalet selv består kun af direktøren og12 personer (pr. 6.2.2001). Projektledernes arbejdsmråder er: Rusland og de nye uafhængige stater, Afrika, Østasien og Stillehavsområdet; Mellemosten og Nordafrika; Sydasien, Bangladesh, Indien, Pakistan, Sri Lanka; Europa og Tyrkiet; Kina, Hongkong og Taiwan; Canada, Vestindien og Latinamerika; fly-, automobil- og forsvarsindustri i hele verden samt telekommunikation, informationsteknologi og computerindustri i hele verden.

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 skal mindst 50% af de leverede produkter (beregnet efter værdi) være af amerikansk oprindelse.

10.9.4.3. CIA's deltagelse i TPCC's arbejde
Duncan Campbell har forelagt udvalgsmedlemmerne forskellige deklassificerede dokumenter,

---

1 TPCC-brochure om Advocacy Center, oktober 1996.
som dokumenterer CIA's deltagelse i Advocacy Center's arbejde. De indeholder protokoller fra møder i TPCC's Indonesia Working Group i juli og august 1994.¹ Denne gruppe, som skulle udarbejde en handelsstrategi for Indonesien, havde ifølge dokumenterne deltagelse af indtil flere CIA-medarbejdere, som nævnes ved navn i protokollerne. Derudover fremgår det af protokollerne, at en af CIA-medarbejderne definerede det som et af gruppens mål at finde frem til hovedkonkurrenterne og fremlægge disse oplysninger som baggrundsinformation.²

10.9.4.4. Åbne spørgsmål i forbindelse med centret
Den amerikanske regering gav ikke tilladelse til det planlagte møde mellem udvalgets medlemmer og centret, som dette havde givet tilsagn om. Derfor må to spørgsmål, som der hersker tvivl om, stå uløste hen, hvilket ordføreren beklager:

a) udvalget ligger inde med dokumenter (se kapitel 10, 10.9.4.3.) som beviser, at CIA er involveret i TPCC's arbejde.

b) Advocacy Center oplyser i den tidligere citerede informationsbrochure, som det selv har udarbejdet, at det samler ressourcerne fra 19 "US government agencies". Andetsteds i brochuren nævnes kun 18 af disse "agencies". Hvorfor er navnet på det 19. ikke offentliggjort?

Ordføreren forstår aflysningen af det planlagte møde med Advocacy Center på den måde, at der foregår aktiviteter, som den amerikanske regering ikke ønsker at drøfte.

10.10. Sikkerhed i forbindelse med edb-net

10.10.1. Betydningen af dette kapitel
Som allerede forklaret i kapitel 10, 10.4. er den næstbedste metode til økonomisk spionage i dag - ud over anvendelsen af spioner - indbrud i edb-net eller datatyveri fra bærbare computere. Redegørelserne i dette kapitel har ikke direkte noget med et globalt organiseret aflytningssystem for international kommunikation at gøre. Men udvalgets målsætning taget i betragtning kommer man i kapitlet om økonomisk spionage ikke uden om en kort fremstilling af et af de mest betydningsfulde værktojer i den forbindelse. Den vil sikkert være en hjælp til at vurdere betydningen af et aflytningssystem for international kommunikation i forbindelse med økonomisk spionage.

10.10.2. Risikoen ved brugen af moderne informationsteknologier i erhvervslivet
Den moderne elektroniske databehandling har for længst holdt sit indtog i erhvervslivet. Den samlede mangfoldighed af data opbevares særdeles tæt på lagermedier. Edb-lagrede data er nu en af de vigtigste faktorer i virksomhedernes knowhow. Denne forvandling fra et industriamfund til et informationssamfund åbner op for chancer, men indebærer også

² ibidem: “Bob Beamer suggested that any primary competitors known to the group for these projects should be included as background information”. Bob Beamer er en af CIA-repræsentanterne.
betydelige sikkerhedsmæssige risici.¹

10.10.2.1. Risikoen vokser

Den voksende risiko kan sammenfattes som følger:²


10.10.2.2. Nogle risici i enkeltheder

Komprimering af informationer på kompakte datamedier

Forretningshemmeligheder optager i dag yderst lidt fysisk plads på komprimerede datamedier. Dermed er det muligt at opbevare de komplette planer til en ny fabrik på flytbare medier af størrelse som en pakke cigaretter og smugle dem ud fra en virksomhed, eller bryde ind i et edb-net og hurtigt "støvsuge" dem elektronisk uden at efterlade spor.

Decentralisering af hemmelige informationer

På de store datamaters tid var det let at kontrollere adgangen til hemmelige informationer, da der kun var tale om at forvalte en datamat. I dag har brugeren på nettet på hans eller hendes arbejdsplads adgang til betydelig computerkapacitet. Dette er naturligvis en stor fordel for brugeren, men set ud fra et sikkerhedsmæssigt synspunkt er det en katastrofe.

Forenklet mulighed for at kopiere informationer


Beslutningstagernes mobilitet

Virksomhedernes beslutningstagere medbrører strategisk vigtige informationer om virksomheden på deres laptops, ofte uden at have gjort sig dette tilstrækkeligt klart. Hurtig kopiering af en harddisk ved en "toldkontrol" eller ved ransagning af et hotelværelse åbner store muligheder for efterretningsstjenester. Eller en notebook bliver simpelthen stjålet. I øvrigt er det på grund af decentraliseringen vanskeligt at ind passe indholdet af harddiske i laptops tilhørende en virksomheds beslutningstagere i en central sikkerhedsstyring.

Outsourcing af vedligehold til eksterne tjenesteydere

Outsourcing kan i teorien føre til en driftsøkonomisk reducering af udgifter. I forbindelse med informationsteknologi og vedligehold af telefonanlæg har teknikere udefra adgang til næsten

¹ Computerspionage, Dokumentation Nr. 44, Forbundsøkonomiministeriet, juli 1998.
alle informationer. Der kan ikke i tilstrækkelig høj grad gøres opmærksom på de dermed forbundne risici.

**Utilstrækkelig netadministration**

Ud over sikkerhedsmangler ved selve softwaren, som hackere normalt opdager, udgår den største fare fra netadministratører, der ikke i tilstrækkelig grad er sig de forskellige risici bevidst. Grundindstillingen af Windows NT er konfigureret på en sådan måde, at stort set alle informationer om afslores, som der er brug for til et vellykket angreb. Hvis disse indstillinger og standardpasswords ikke ændres, er det let at trænge ind på nettet. En udbredt fejl består også i at ofre meget på sikkerheden i form af firewall-beskyttelse, men at glemme at beskytte nettet ordentligt mod angreb indefra.

1.0.10.3. **Hyppigheden af angreb på net**


1.0.10.4. **Gerningsmænd og metoder**

Fremmede efterretningsstjenester, der angriber IT-systemer, forsøger at skaffe sig de ønskede informationer så ubemærket som muligt. Der kan i princippet skelnes mellem tre grupper af gerningsmænd med tre forskellige modi operandi.

**Interne gerningsmænd med uindskrænkede adgangsrettigheder**

En indsluset eller hvervet spion, der er avanceret til sikkerhedsadministrator i et datacenter, behøver med henblik på sin efterretningsvirksomhed blot at varetage de beføjelser ekstensivt, som han officielt har fået overdraget, for at stjæle næsten hele sin arbejdsgivers knowhow. Det samme gælder for en ledende udviklingsingeniør med uindskrænkede adgangsrettigheder til alle virksomhedens teknikdatabaser.

En sådan spion er så effektiv, som tænkes kan. Han løber imidlertid en stor risiko for at blive opdaget, hvis der opstår mistanke, fordi undersøgelselserne straks koncentreres om den lille personkreds, der har uindskrænket adgang til informationer. Derudover er det et rent lykketæt, som hverken kan planlægges eller styres, hvis en spion får omfattende adgangsrettigheder.

---

Interne gerningsmænd med adgangsrettigheder fra en enkelt arbejdsplads

En spion, der opererer internt i en virksomhed, har en klar fordel i forhold til hackeren, der angriber udefra: han skal blot overvinde netsikkerhedssystemet og ikke også gennemtrænge en firewall. Fra en enkelt arbejdsplads kan han med den fornødne viden få indblik i netarkitekturen, og med de teknikker, der også benyttes ved hacking udefra, og andre internt anvendelige teknikker, kan man indsamle betydelige informationsmængder. Hertil kommer, at spionen uden at vække mistanke kan kommunikere med andre ansatte og gennem såkaldt "social engineering" kan skaffe sig oplysninger om passwords.

Sådanne spioner kan være meget effektive, men effektiviteten er ikke så let at beregne som i det første tilfælde. Risikoen for opdagelse er mindre, især inden for net, hvis administrator ikke er så opmærksom på risikoen for angreb indefra. Det er betydeligt lettere at indsluse en spion, der er teknisk uddannet til at trænge ind i computernet (praktikanter, gæsteforskere osv.).

10.10.5. Hackerangreb udefra

At hackere gang på gang trænger ind i computernet udefra er almindeligt kendt og veldokumenteret. Det er efterhånden blevet almindeligt, at også efterretningsstjener uddanner specialister til at trænge ind i computernet. Hvor effektivt et hackerangreb vil være, kan ikke forudses eller planlægges, da det i høj grad afhænger af, hvor godt organiseret "forsvaret" er, og f.eks. om forskningsafdelingens net overhovedet er forbundet med Internettet. Risikoen er for den professionelle spion er næsten lig nul, selv om angrebet som sådant opdages, for han behøver ikke være til stede for at kunne foretage det.

10.11. Undervurdering af risici

10.11.1. Risikobevidsthed i erhvervslivet

Risikobevidstheden omkring økonomisk spionage er endnu ikke særlig udpræget i erhvervslivet. Det kommer bl.a. til udtryk ved, at sikkerhedschefer ofte er placeret på mellemlederniveau og ikke sidder i virksomhedernes direktioner. Men sikkerhed koster penge, og direktionsmedlemmerne beskæftiger sig som regel først med sikkerhedspørgsmål, når det er for sent.

Store virksomheder har imidlertid deres egne sikkerhedsafdelinger og beskæftiger også de nødvendige fagfolk på IT-området. Små og mellemstore virksomheder råder derimod kun sjældent over sikkerheds ekspert er og er for det meste glade, når bare edb-systemet fungerer. Imidlertid kan også disse virksomheder blive udsat for økonomisk spionage, fordi en del af dem er meget nyskabende. Desuden er mellemstore underleverandørvirksomheder egnede operationsbaser for angreb på store virksomheder, fordi de er integreret i produktionsprocessen.

10.11.2. Risikobevidsthed i erhvervslivet

Forskere interesserer sig som regel kun for deres eget fagområde. Derfor er de undertiden et let bytte for efterretningsstjenerne. Ordføreren har med nogen undren konstateret, at også meget anvendelsesorienterede forskningsinstitutter udveksler ukrypterede oplysninger over e-

1 Anonymous, Hacker’s guide, Markt &Technik-Verlag (1999).
mail og over forskningsnettet. Det er groft letsindigt.

10.11.3. Risikobevidsthed i fællesskabsinstitutionerne

10.11.3.1. Den Europæiske Centralbank
Oplysninger om forberedelse af Den Europæiske Centralbanks beslutninger kan have stor værdi for efterretningstjenester. At der desuden er stor interesse for dem på markederne, siger sig selv. Udvalget har på lukkede møder også hørt repræsentanter for Den Europæiske Centralbank om sikkerhedsforanstaltninger til beskyttelse af oplysninger. Ordføreren er på baggrund heraf nået til den konklusion, at man er bevidst om risikoen, og at man efter evne sørger for sikkerhed. MEN ifølge nogle oplysninger er risikobevidstheden ikke særlig udpræget i nogle af de nationale centralbanker.

10.11.3.2. Rådet for Den Europæiske Union
Før udnævnelsen af den høje repræsentant for den fælles udenrigs- og sikkerhedspolitik, koncentrerede Rådet først og fremmest sine hemmeligholdelsesbestræbelser om at holde beslutningstagen og holdningerne i medlemsstaternes regeringer skjult for offentligheden og Europa-Parlamentet. Det ville aldrig have kunnet modstå en professionelt organiseret efterretningsooperation. F.eks. skal vedligeholdelsen af de tekniske installationer i tolkekabinerne være blevet varetaget af et israelsk firma. Rådet har nu vedtaget sikkerhedsforskrifter, der er i overensstemmelse med den norm, der anvendes inden for NATO.

10.11.3.3. Europa-Parlamentet
Europa-Parlamentet har hidtil ikke haft med klassificerede dokumenter at gøre og har derfor ingen erfaring med beskyttelse af fortrolige dokumenter og ingen sikkerhedskultur. Behovet vil først opstå, når Parlamentet får adgang til klassificerede dokumenter. I øvrigt kan et parlament, der skal være så åbent som muligt, ikke føre en generel hemmeligholdelsespolitik. Dog bør det være muligt om nødvendigt at kryptere e-mail-korrespondancen mellem de forskellige medlemmers kontorer for at beskytte informanter og andragere.

10.11.3.4. Europa-Kommissionen
I Europa-Kommissionen er der generaldirektorater, der på grund af arten af de oplysninger, de har med at gøre, ikke har noget behov for hemmeligholdelse eller beskyttelse. Derimod bør der herske absolut gennemskuelighed inden for alle områder, der har med lovgivning at gøre. Europa-Parlamentet må være på vagt for at forhindre, at interesserede firmaers indflydelse på lovgivningsforløb ikke igennem upassende fortrolighedsbestemmelser unødigt tilsløres mere, end det allerede er tilfældet inden for disse områder.

Der er imidlertid også områder i Kommissionen, hvor man har med følsomme oplysninger at gøre. Bortset fra Euratom drejer det sig først og fremmest om områderne eksterne forbindelser og konkurrence. På grundlag af de informationer, som udvalget har fået på lukkede møder af de pågældende generaldirektorater, og først og fremmest andre informationer, som ordføreren

1 Private oplysninger, kilden beskyttet.
2 Meddelelse fra medlemmerne af Coreper og tjenestemænd i Rådet. Kilder er beskyttet.
råder over, hersker der alvorlig tvivl med hensyn til risikobevidstheden omkring spionage og den professionelle håndtering af sikkerheden i Europa-Kommissionen. Der er naturligvis ikke muligt at pege på mangler ved sikkerheden i en betænkning, der er offentligt tilgængelig. Ordføreren anser det imidlertid for særdeles nødvendigt, at Europa-Parlamentet hurtigt tager dette spørgsmål op i en passende sammenhæng.

Allerede i dag kan det konstateres, at de krypteringssystemer, Kommissionen anvender ved kommunikation med nogle af de eksterne kontorer, er forældede. Det betyder ikke, at sikkerhedsstandarden er dårlig, men de apparater, der anvendes, fremstilles ikke længere, og kun ca. halvdelen af de eksterne kontorer råder over krypteringsmuligheder. Det er presserende nødvendigt at indføre et nyt system, der arbejder på grundlag af krypteret e-mail.
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 århier 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 ilegal adgang til oplysninger og forfalskning deraf fremkaldt beskyttelsesforanstaltninger (f.eks. inden for banksektoren).


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


1 Dokumenteret så langt tilbage som til antikken.
f.eks. en kryptofaks.


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 tredje følgende 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 tredje følgende bogstav i alfabetet**. Både kodning og dechiffering 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.


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 dechiffrere 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, men senere benyttet til den røde fjernskriver

---

2. Indført af Major Joseph Mauborgne, leder af den amerikanske hærs afdeling for kryptografisk forskning. *Simon*
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 bogstavsætter 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 nøgler2 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

11.2.3.2. Anvendelsen af computere inden for kryptologi
Opfindelsen af computeren var banebrydende for kryptologivideneskab, 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 mangedobleta, da der ikke længere var mekaniske grænser herfor, og for det andet blev krypteringsprocessen markant hurtigere.

Informationerne forarbejdes digitalt af computere med binære tal. Det betyder, at disse informationer udtrykkes i en rækkefølge af to signaler nemlig 0 og 1. I svarer fysisk til en elektrisk spænding hhv. en magnetisering (lys), 0 til bortfald af spænding hhv. magnetisering (ingen lys). I den forbindelse er ASCII-standarderne4 blevet indført, hvor hvert bogstav er repræsenteret af en syvcifret kombination af 0 og 15. 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, Carl Hanser Verlag (1999), 151.

1 Simon Singh, Geheime Botschaften, Carl Hanser Verlag (1999), 151 ff.
4 American Standard Code for Information Interchange.
5 A = 1000001, B = 1000010, C = 1000011, D = 1000100, E = 1000101 osv.
(udskiftning). Substitution kan f.eks. ske ved at tilføje en nogle 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 nogle.

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 nogle. Jo længere nøglen er, desto større er muligheden for at dette ikke lykkedes, 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 forsættlig 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.\(^1\).

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\(^2\). 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\(^3\), 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 et ændret amerikansk krypteringspolitik.

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/-udveksling

11.3.1. Asymmetrisk 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 udelveres 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.


1 Ideen med asymmetrisk kryptering i form af et public key- krypteringssystem stammer fra Whitfield Diffie og Martin Hellmann.
2 Simon Singh, Geheime Botschaften, Carl Hanser Verlag (1999), s. 327.
3 Johannes. Buchman: Faktorisierung grosser Zahlen, Spektrum der Wissenschaft 2, 199, s. 6 ff.
4 Simon Singh, Geheime Botschaften, Carl Hanser Verlag (1999), s. 335 f.
Public key-krypteringssystemet kræver ganske vist meget længere computertid eller anvendelse af hurtige og store computere end symmetriske systemer (f.eks. DES).

11.3.2. Public key-kryptering for privatpersoner

Samtidig findes der konkurrierende 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

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

1 Informationer om software, se www.pgpi.com.
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 disse tilfælde er offentliggjort.

11.5. Kryptering i konflikt med statsinteresser

11.5.1. Forsøg på at begrænse kryptering

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 omsøst. 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 forretningspartners 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 forudsetter, at samtalepartneren også har sådanne apparater, og at dette vel kun sjældent er tilfældet.


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 ukryteterede 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 uautoriserede 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


12.2. Muligheder for samarbejde inden for EU

12.2.1. Eksisterende samarbejde

Selv om der er en lang tradition hos efterretningsstjenester for kun at overdrage de oplysninger, som de indsamler, til sig selv og måske endog en traditionel manglende tillid mellem de enkelte efterretningsstjenester 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 efterretningsstjenesterne inden for NATO stadig er betydeligt afhængige af de langt mere raffinerede bidrag fra De Forenede Stater, har oprettelsen af

---

1 Charles Grant, Intimate relations. Can Britain play a leading role in European defence - and keep its special links to US intelligence? 4.2000, Centre for European Reform.
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 beskrive på følgende måde.

12.2.2.1. Praktiske fordele


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 efterretningsstjeneste 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 stad 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 efterretningsstjenester 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 tæt forbindelser inden for indsamling af efterretningsoplysninger mellem Det Forenede Kongerige og De Forenede Stater. De


På den anden side bør en stigende europaesisk bevidsthed ledsages af et større ansvær fra europaesisk 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 europaesisk efterretningscapacitet 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 kapacitetsfylt 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

13. Konklusioner og henstillinger

13.1. 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 eller dele heraf – i det mindste i en vis periode – er gået under betegnelsen "Echelon" kan antages på baggrund af de forhåndenværende indicier og mange overensstemmende erklæringer fra forskellige kredse. 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 tekniske muligheder sandsynligvis ikke er så omfattende, som mange medier har antaget. Alligevel forekommer det foruroligende, at mange ansvarlige i EU, der er blevet hørt, herunder navnlig medlemmer af Kommissionen, har erklæret, at de ikke havde kendskab til systemet.

**Aflytningssystemets grænser**


**Den mulige eksistens af andre aflytningssystemer**

Da aflytning af kommunikation er en almindelig anvendt fremgangsmåde blandt efterretningstjenester, kan et sådant system også drives af andre stater, for så vidt som de råder over de nødvendige finansielle midler og har de geografiske forudsætninger herfor. Frankrig er i kraft af sine oversøiske territorier som eneste EU-medlemsstat geografisk og teknisk i stand til på egen hånd at oprette et globalt aflytningssystem. Der er mange oplysninger, der tyder på, at også Rusland driver et sådant system.

**Forenelighed med EU-retten**

Hvad angår foreneligheden af et system som Echelon med gældende EU-ret, må der sondres mellem forskellige anvendelser:

Anvendes systemet kun til efterretningsformål, er det ikke i strid med EU-retten, da statssikkerhedstjenester 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

**Forenelighed med den grundlæggende ret til privatsfæren (Artikel 8 i EMK)**


Et efterretningssystem, som vilkårligt og varigt aflytter kommunikation, er ikke foreneligt med proportionalitetsprincippet og dermed heller ikke foreneligt med den europæiske menneskerettighedskonvention (EMK). Ligeledes foreligger der en krænkelse af EMK, hvis de bestemmelser, 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, der danner grundlaget for den amerikanske efterretningstjenestes 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 dets virkning. Skønt USA ikke selv er kontraherende part i EMK, må medlemsstaterne opfylde deres forpligtelser i henhold til denne konvention.

De kan ikke undrage sig deres forpligtelser i henhold til EMK ved at lade andre landes sikkerhedsstjenester, som er underlagt mindre strenge 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 betydning.

Efterretningstjenesters ved lov legitimerede virksomhed er kun i overensstemmelse med de grundlæggende rettigheder, hvis der desuden findes fyldstgørende kontrolsystemer, der udligner den risiko, dele af forvaltningsapparatets hemmelige aktiviteter medfører. Da Menneskerettighedsdomstolen udtrykkelig har fremhævet betydningen af et effektivt kontrolsystem for efterretningstjenester, føre kommer det betænkeligt, at visse medlemsstater ikke har et selvstændigt parlamentarisk kontrolorgan for efterretningstjenester.

**Er EU-borgerne tilstrækkelig beskyttet mod efterretningsvirksomhed?**

Der kan næppe tales om tilstrækkelig beskyttelse, eftersom EU-borgernes beskyttelse afhænger af gældende ret i de enkelte medlemsstater, 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 parlementer har et officielt særligt kontroludvalg, som overvåger og fører kontrol over efterretningstjenesternes aktiviteter. Dér, hvor der findes kontrolorganer, fristes disse imidlertid i høj grad til snarere at beskaæftige sig med indenrigsefterretningstjenesternes virke end med udenrigsefterretningstjenesternes, da det som regel kun er den førstnævnte tjenestes aktiviteter, som berører landets egne borgere.

I forbindelse med et samarbejde mellem efterretningstjeneste inden for rammerne af FUSP og sikkerhedsmyndighederne inden for samarbejdet om retlige og indre anliggender, må
institutionerne vedtage regler, der yder EU-borgerne tilstrækkelig beskyttelse.

**Økonomisk spionage**

Det indgår i udenrigsefterretningstjenestens opgave at beskæftige sig med økonomiske data, herunder sektorudvikling, udviklingen på råstofmarkedere, overholdelse af embargoer og regler for levering af varer med dobbelt anvendelse (dual use) m.m. Derfor foretages der ofte overvågning af de relevante virksomheder. USA's efterretningstjeneste opklarer imidlertid ikke kun generelle økonomiske forhold. Med den begrundelse at ville bekæmpe korruption aflytter de også kommunikation fra virksomheder i forbindelse med licitation. I forbindelse med en så detaljeret aflytning er der imidlertid risiko for, at oplysningerne ikke anvendes til bekæmpelse af korruption, med til udspionering af konkurrenter, selv om USA og Det Forenede Kongerige erklærer, at dette ikke er tilfældet. I den forbindelse skal det bemærkes, at den rolle, som Advocacy Center under det amerikanske handelsministerium spiller, stadig ikke er helt klar, og at dette center aflyste en samtale, der skulle have afklaret sagen. Der henvises endvidere til, at der inden for rammerne af OECD i 1997 blev vedtaget en aftale om bekæmpelse af korruption af tjenermænd, hvorefter bestikkelse skal være strafbart på internationalt plan. Heller ikke ud fra aspektet bestikkelse i enkelttilfælde kan aflytning af kommunikation være berettiget. Under alle omstændigheder skal det understreges, at det er uaceptabelt, når efterretningstjenestene lader sig bruge til konkurrencespionage, idet de udspionerer udenlandske virksomheder for at skaffe virksomheder i eget land en konkurrencefordel. Der findes imidlertid intet dokumenteret tilfælde, hvor det her undersøgte aflytningssystem anvendes til dette formål, selv om det ofte påstås. 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 stadigt hyppigere ved at tænke ind i det interne edb-net. Kun når følsomme data kommer ud via fast eller trådløs kommunikation (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 VSAT eller kabel;
- når der forhandles om vigtige kontrakter på stedet (f.eks. i bygge- og anlægssektoren, ved opbygning af telekommunikationsinfrastruktur, nyoprettelse af transportsystemer osv.) og der derfra skal føres samråd med hovedkontoret.

Risiko- og sikkerhedsbevidstheden hos små og mellemstore virksomheder er beklageligvis ofte utilstrækkelig, og risikoen for økonomisk spionage og aflytning af kommunikation ses ikke. Da sikkerhedsbevidstheden i de europæiske institutioner (med undtagelse af EIB, Generaldirektoratet for Eksterne Anliggender i Rådet og i Kommissionen) heller ikke altid er særlig udpræget, er der behov for handling.

**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 Internettet relativt brugervenlige systemer, som sågar stilles gratis til rådighed til privat brug.
Et samarbejde mellem efterretningstjenester inden for EU

I december 1999 i Helsinki vedtog Det Europæiske Råd at udvikle mere effektive europeiske militære strukturer for at kunne leve op til hele spektrum af Petersberg-opgaver til støtte for FUSP. For at nå dette mål skal EU inden 2003 være i stand til hurtigt at montere tropper i størrelsesordenen 50.000-60.000 mand, som er militært autonome og råder over de nødvendige færdigheder, hvad angår ledelse og strategisk opklaring samt den relevante efterretningskapacitet. De første skridt i retning af opbygning af denne kapacitet er allerede blevet foretaget inden for WEU og den faste politiske og sikkerheds-politiske komité. Et samarbejde mellem efterretningstjenesterne inden for EU synes at være uomgængeligt, dels fordi det vil være ulogisk at tale om en fælles sikkerheds-politik uden inddragelse af sikkerhedstjenesterne, og dels fordi det ville indebære mange erhvervsmæssige, økonomiske og politiske fordele. Det vil også være mere i overensstemmelse med tanken om at opstå som ligeværdig partner over for USA og vil kunne samle alle medlemsstater om et system, som er i overensstemmelse med EMK. En kontrol fra Europa-Parlamentets side må i så fald selvfølgelig være sikret. Europa-Parlamentet er i færd med at gennemføre Europa-Parlamentets og Rådets forordning (EF) nr. 1049/2001 af 30. maj 2001 om aktindsigt i Europa-Parlamentets, Rådets og Kommissionens dokumenter og tilpasse sin forretningsorden i forbindelse med adgang til følsomme dokumenter.

13.2. Henstillinger

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

1. Europarådets generalsekretær opfordres til at forelægge Ministerudvalget et forslag om 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 der derved hverken sker en reduktion af det retsbeskyttelsesniveau, Menneskerettighedsdomstolen har sikret, eller af den fleksibilitet, der er nødvendig for tilpasning til videre udviklinger.

2. EU's medlemsstater opfordres til at skabe en europæisk platform bestående af repræsentanter for de nationale organisationer, der er ansvarlige for at overvåge, at medlemsstaterne overholder de grundlæggende og borgerlige frihedsrettigheder, og undersøge, hvorvidt de nationale forskrifter for efterretningstjenester er i overensstemmelse med EMK og EU's charter om grundlæggende rettigheder. Den skal endvidere have ansvaret for at vurdere de lovmæssige bestemmelser om sikring af brev- og telehemmeligheden. Endvidere skal medlemsstaterne have forelagt en henstilling om udarbejdelse af en adfærskodeks, der sikrer beskyttelsen af privatsfæren, som fastlagt i artikel 7 i Den Europæiske Unions charter om grundlæggende rettigheder, for alle EU-borgere på medlemsstaternes territorium i dets helhed og desuden garantere, at efterretningstjenesters virksomhed er i overensstemmelse med de grundlæggende rettigheder og opfylder betingelserne i beretningens kapitel 8, særlig 8.3.4. som afledt af artikel 8 i EMK.

3. Europarådets medlemsstater opfordres til 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. Medlemsstaterne opfordres til at vedtage det europæiske charter om grundlæggende frihedsrettigheder på den næste regeringskonference som bindende ret for derved at højne beskyttelsen af de grundlæggende rettigheder, navnlig med henblik på beskyttelsen af privatsfæren. EU-organerne opfordres til at anvende de grundlæggende rettigheder i chartret inden for deres eget kompetence- og virksomhedsområde.

5. EU og USA opfordres til at indgå en aftale om gensidig anvendelse af forskrifterne om beskyttelse af privatsfæren og kommercialt fortrolighed inden for virksomhedskommunikation, som gælder for egne borgere.

6. Medlemsstaterne opfordres til at indgå en aftale med tredjelande med henblik på en øget beskyttelse af EU-borgeries privatsfære, hvorved alle stater forpligter sig til gensidig underretning i tilfælde af aflytningsforanstaltninger i en anden kontraherende stat.

7. 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 rettigheder, som sikrer beskyttelse af privatsfæren, til den nye teknologiske udvikling.

8. USA opfordres til at underskrive tillægsprotokollen til den internationale konvention om borgerlige og politiske rettigheder, således at enkeltpersoner kan indbringe sager mod USA for krænkelse af konventionen for konventionens Menneskerettighedskomite; de relevante amerikanske ngo'er, herunder navnlig ACLU (American Civil Liberties Union) og EPIC (Electronic Privacy Information Center) opfordres til at lægge pres på den amerikanske regering for at opnå dette.


National lovgivning med henblik på beskyttelse af borgere og virksomheder

10. Medlemsstaterne opfordres udtrykkeligt til at vurdere, om deres nationale lovgivning om efterretningsvirksomhed er overensstemmende med de grundlæggende rettigheder i henhold til EMK samt Menneskerettighedsmotolens retspraksis, og i givet fald at vedtage relevante bestemmelser. De opfordres til at tilsikre alle europæiske borgere samme retssikkerhed, for så vidt angår beskyttelse af privatlivet og posthemmeligheden. Såfremt lovgivningen vedrørende hemmelige tjenesters overvågningsbeføjelser indeholder diskriminerende bestemmelser, skal disse ophæves.

11. Medlemsstaterne opfordres til at tilstræbe et fælles beskyttelsesniveau over for efterretningsaktiviteter og med henblik herpå at udarbejde en adfærdskodeks, som er baseret på det højeste nationale beskyttelsesniveau, da de borgere, der er berørt af en udenrigsefterretningsstjenestes virke, som regel er statsborgerne i andre stater og derfor også i andre medlemsstater. En tilsvarende adfærdskodeks skal også indgås med USA.

12. Medlemsstaterne opfordres til at integrere deres aflytningsfaciliteter for at øge FUSP's effektivitet inden for efterretningsvirksomhed, bekæmpelse af terrorisme, udbredelse af atomvåben og international narkotikahandel under overholdelse af bestemmelserne om
beskyttelse af borgerne privatsfære og fortrolighed omkring virksomhedskommunikation og under Europa-Parlamentets, Rådets og Kommissionens kontrol.

Særlige foranstaltninger til bekæmpelse af økonomisk spionage

13. Medlemsstaterne opfordres 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 en regulering, som tager højde for den konkurrenceforvridende virkning af sådanne fremgangsmåder, f.eks. ved at annullere sådanne kontrakter. USA, Canada, Australien og New Zealand opfordres til at tilslutte sig dette initiativ.

14. Medlemsstaterne opfordres til på bindende vis at forpligte sig til ikke at udsætte økonomisk spionage direkte eller under dække af en udenlandsk magt, der er aktiv på deres territorium, eller at tillade, at en udenlandsk magt gør noget sådant fra deres territorium, og derved handle i overensstemmelse med EF-traktatens ånd og bestemmelser.

15. Medlemsstaterne og USA's regering opfordres til at indlede en åben dialog mellem USA og EU om økonomisk spionage.


17. Medlemsstaterne opfordres til at sikre, at deres efterretningstjenester ikke misbruges til fremkaldelse af konkurrenceoplysninger, da dette strider mod medlemsstaternes pligt til loyalitet og principippet om et fælles marked baseret på fri konkurrence.

Foranstaltninger vedrørende anvendelsen af gældende ret og kontrollen hermed

18. Medlemsstaterne opfordres til at sikre en passende parlamentarisk og retslig kontrol med hemmelige tjenester. Såfremt de nationale parlaments ikke råder over selvstændige parlamentariske kontrolorganer til overvågning af efterretningstjenester, opfordres de til at oprette sådanne.

19. De nationale tilsynsudvalg for efterretningstjenesterne anmodes 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.

20. 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.

21. Tyskland og Det Forenede Kongerige opfordres til at gøre de amerikanske efterretningstjenesters fortsatte tilladelse til aflytning af kommunikation på deres territorium betinget af, at denne sker er 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 efterretningssvirkomhed på deres territorium, hvad enten den er tilladt eller blot tålt, sker i overensstemmelse med menneskerettighederne.

**Fremme af borgernes og virksomhedernes selvbeskyttelse**

22. Kommissionen og medlemsstaterne opfordres til at underrette borgere om muligheden for, at international kommunikation eventuelt aflyttes. Denne information skal ledsages af praktisk bistand i forbindelse med udvikling og omsætning af omfattende beskyttelsesforanstaltninger, også hvad angår IT-sikkerhed.

23. Kommissionen, Rådet og medlemsstaterne opfordres til at udvikle og gennemføre en effektiv politik vedrørende sikkerhed i informationssamfundet. I den forbindelse skal man være særlig opmærksom på større bevidstgørelse af alle brugere af moderne kommunikationssystemer, for så vidt angår nødvendigheden af og mulighederne for beskyttelse af fortrolige oplysninger. Der skal oprettes et fælles europæisk net af agenturer, der er i stand til at sikre praktisk bistand i forbindelse med planlægning og gennemførelse af omfattende beskyttelsessstrategier.

24. 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 sigter mod at udvikle brugervenlig krypteringssoftware med offentlig kildetekst (open source text).

25. Kommissionen og medlemsstaterne opfordres til at fremme softwareprojekter, hvis kildetekst er offentlig (såkaldt "open source software"), da det kun derved kan sikres, at der ikke er indbygget "backdoors". Kommissionen opfordres til at fastlægge en standard for softwaresikkerhed i forbindelse med udveksling af oplysninger ad elektronisk vej, således at software, hvis kildekode ikke er offentlig, placeres i kategorien "mindst troværdig".

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

**Foranstaltninger til forbedring af sikkerheden i institutionerne**

27. Fællesskabets organer og de offentlige forvaltninger i medlemsstaterne opfordres til at sørge for, at de ansatte uddannes og i praksis og ved uddannelse gøres fortrolige med de nye kryptingsteknikker.


29. Kommissionen opfordres til at ændre sit krypteringssystem efter den nyeste standard, da en modernisering er absolut nødvendig, og budgetmyndigheden (Rådet og Parlamentet) anmodes om, at stille de nødvendige bevillinger til rådighed.

30. Det kompetente udvalg anmodes om at udarbejde en initiativbetyndkning om sikkerhed og beskyttelsen af data i de europæiske institutioner.

31. Kommissionen opfordres til at sikre beskyttelsen af data, der behandles hos den, og øge beskyttelsen af ikke offentligt tilgængelige dokumenter.
32. Kommissionen og medlemsstaterne anmodes om inden for rammerne af det 6. forskningsrammemprogram at intensivere forskningen i nye krypteringsteknikker og sikkerhed mod krypteringsangreb.

Andre foranstaltninger

33. Virksomhederne opfordres til at samarbejde mere intensivt med kontraspionageorganer og gøre disse bekendt med angreb udefra med henblik på økonomisk spionage for derved at øge disse organers effektivitet.


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

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

Del 2: Mindretalsudtalelser
Bilag
Det Midlertidige Udvalg om Echelon-aflytningssystemet

Ordfører: Gerhard Schmid
**INDHOLD**

<table>
<thead>
<tr>
<th>Side</th>
<th>Titel</th>
</tr>
</thead>
<tbody>
<tr>
<td>143</td>
<td>Mindretalsudtalelse fra Giuseppe di Lello, Pernille Frahm og Alain Krivine</td>
</tr>
<tr>
<td>144</td>
<td>Mindretalsudtalelse fra Patricia McKenna og Ilka Schröder</td>
</tr>
<tr>
<td>145</td>
<td>Mindretalsudtalelse fra Jean-Charles Marchiani</td>
</tr>
<tr>
<td>146</td>
<td>Mindretalsudtalelse fra Maurizio Turco</td>
</tr>
<tr>
<td>147</td>
<td>Bilag I.: Liste over eksperti, der har givet oplysninger i udvalget</td>
</tr>
<tr>
<td>150</td>
<td>Bilag II.: Litteraturliste</td>
</tr>
<tr>
<td>156</td>
<td>Bilag III.: Definitioner og oplysninger vedrørende kommunikationsovervågning med henblik på strafforfølgning</td>
</tr>
<tr>
<td>156</td>
<td>1. Forord</td>
</tr>
<tr>
<td>156</td>
<td>2. To forskellige ting: kommunikationsovervågning i strafferetligt øjemed/til efterretningsformål</td>
</tr>
<tr>
<td>157</td>
<td>3. Arbejder inden for EU på området strafferetlig kommunikationsovervågning.</td>
</tr>
<tr>
<td>160</td>
<td>4. Definitioner og oplysninger vedrørende andre grænseoverskridende arbejder inden for aflytning af telekommunikation</td>
</tr>
<tr>
<td>163</td>
<td>Bilag IV.:</td>
</tr>
</tbody>
</table>
Mindretalsudtalelse fra Giuseppe di Lello, Pernille Frahm og Alain Krivine


Et sådant udifferentieret system til opfangning af kommunikation, oplysninger og dokumenter krænker den grundlæggende ret til privatlivets fred, der garanteres af artikel 8 i den europæiske menneskerettighedskonvention og artikel 6 i EU-traktaten.

Dette system udgør således en grov krænkelse af de europæiske borgeres grundlæggende frihedsrettigheder, ideen om det frie marked og Unionens sikkerhed. Uanset om man er for eller imod disse ideer og disse traktater, er en sådan krænkelse uacceptabel.

Konklusionerne i betænkningen burde indeholde en anmodning til Det Forenede Kongerige om at tage afstand fra Echelon-systemet og til Tyskland om at lukke den aflytningsstation, der er placeret på dets territorium. Man kan kun beklage, at Den Europæiske Union bekymrer sig mere om industrispionage end om aflytning af privatpersoner.
Mindretalsudtalelse fra Patricia McKenna og Ilka Schröder


I hele verden findes der ingen offentlige mekanismer til at kontrollere efterretningstjenester og deres udemokratiske metoder. Det ligger i efterretningstjenesters natur, at de ikke kan kontrolleres. De må derfor afskaffes. Denne betænkning tjener til at legitimere en europæisk efterretningstjeneste, der vil krænke de grundlæggende rettigheder - nøjagtig lige som Echelon gør det.

Flertallet i Parlamentet fokuserer på industrien, hvis profitinteresser menes at være truet af industrispionage. Det grundlæggende problem er imidlertid, at ingen længere kan kommunikere fortroligt over større afstande. Politisk spionage udgør en langt større trussel end økonomisk spionage.

I denne betænkning underspilles disse risici i forbindelse med Echelon gang på gang, mens der intet nævnes om planlægningen af ENFOPOL-aflytningen i EU. For ethvert samfund er det et grundlæggende valg, om man vil leve under permanent kontrol. Ved at vedtage denne betænkning viser Europa-Parlamentet, at det ikke bekymrer sig om beskyttelsen af menneskerettighederne og de borgerlige rettigheder.
Mindretalsudtalelse fra Jean-Charles Marchiani

UEN-Gruppen er ikke overrasket over resultaterne af afstemningen om Gerhard Schmids betænkning, der oprindeligt skulle omhandle det angelsaksiske spionagesystem Echelon.

Parlamentets flertal gav fra begyndelsen klart udtryk for sine planer ved at vælge dette ad hoc-udvalg frem for at nedsætte et rigtigt undersøgelsesudvalg. På den måde var der ikke mere noget at frygte, da ordførerens evne til systematisk at aflede opmærksomheden på ingen måde var truet af utilfredsheden hos gruppe, hvis motivationer var alt for forskellige.

Vort budskab er klart: Gerhard Schmids bestræbelser har ikke kunnet bortforsklare, at Echelon-systemet eksisterer, eller at flere EU-medlemsstater deltager aktivt eller passivt i det.

Der er således tale om en alvorlig krænkelse af traktatens principper, der burde have udløst sanktioner eller i det mindste foranstaltninger med henblik på at forhindre, at solidariteten EU-landene imellem underordnes den angelsaksiske solidaritet.

Gerhard Schmids omfangrige betænkning indeholder mange oplysninger, men skyder forbi målet. Det er os derfor magtpåliggende at tage afstand fra den og forkaste et system, der gør det muligt for Parlamentet at pålægge en demokratisk valgt regering "præventive" sanktioner eller i en tilsvarende situation at undlade at gøre det.
Mindretalsutalelse fra Maurizio Turco

A. Samtidig med at det er tydeligt, at der formentlig findes et engelsk-amerikansk system for "systematiske og omfattende aflytninger, som gennemgås ved hjælp af søgemaskiner", omtales det ikke, at denne tekniske mulighed sikkert benyttes af Tyskland og Nederlandene - og formentlig også af Frankrig. Det betyder, at nogle medlemsstater aflytter institutioners, borgeres og virksomheders aktiviteter i andre medlemslande, da efterretningsvæsenet af hensyn til den nationale sikkerhed og uden at have tilladelse hertil aflytter kommunikation, som stammer fra udlandet.

B. Mens den forbedrede kryptering øger beskyttelsen af privatlivets fred, indebærer den samtidig en styrkelse af de tekniske og legale metoder til dechiffrering, fordi udviklingen af de kryptografiske, kryptoanalytiske systemer er uløseligt forbundet med aflytningsteknikken.

C. Der skal derfor findes løsninger på politisk niveau:
   - gennem retslig og parlamentarisk kontrol af de aflytnings- og overvågningsaktiviteter, som udføres af politi, efterretningsvæsen og spionagetjenester
   - ved at undgå, at der bliver stadig flere kontrolmyndigheder, som benytter forskellige normer for databeskyttelse, og uden at der findes en egentlig demokratisk og retslig kontrol
   - ved at indføre bestemmelser - ud fra de optimale standarder og ved anvendelse af Den Europæiske Menneskerettighedsdomstols retspraksis - for at beskytte de europæiske borgere mod, at privatlivets fred krænkes af statens indblanding i forebyggende øjemed, og ved at den eksisterende forskelsbehandling af EU-borgerne i de forskellige medlemsstater afskaffes.
Bilag I.: Liste over eksperter, der har givet oplysninger i udvalget

1. Medlemmer af nationale parlamenter

Arthur PAECHT, den franske Nationalforsamling
Armand De DECKER, formand for det belgiske Senat
Anne-Marie LIZIN, det belgiske Senat
Hans VAN HEVELE, det belgiske Senats sekretariat
Guilherme SILVA, det portugisiske parlament
Ludwig STIEGLER, den tyske Forbundsdag
Dieter ANTONI, det østrigske parlament
Desmond O´MALLEY, det irske parlament

2. Repræsentanter fra efterretningssektoren

Ernst UHRLAU, efterretningskoordinator i Bundeskanzleramt, Tyskland
Harald WOLL, Landesamt für Verfassungsschutz, Baden-Württemberg, Tyskland

3. Eksperter i telekommunikation og netværks- und computersikkerhed

José Manuel MENDES ESTEVES SERRA VERA, teknisk direktør, Banco Espirito Santo, Portugal
Clive FEATHER, softwareudviklingschef, Demon Internet Ltd, Det Forenede Kongerige
Jacques VINCENT-CARREFOUR, tidl. leder af afdelingen for netværkssikkerhed, France Telecom
Bruno PELLERO, konsulent med speciale i aflytning af telekommunikation, Italien
Erhard MÖLLER, Lutz BERNSTEIN, Bernd SCHINKEN, Fachhochschule Aachen, Tyskland

4. Forfattere og journalister med Echelon som speciale

Duncan CAMPBELL, Det Forenede Kongerige
Bo ELKJÆR, Danmark
Kenan SEEBERG, Danmark
James BAMFORD, Washington D.C.
Nicky HAGER, New Zealand

5. Krypteringseksperter

Reinhard WOBST, Unix Software, Tyskland
Bernd ROELLGEN, Ciphers GmbH, Tyskland
Peter BAHR, Ciphers GmbH, Tyskland
Johan KEMPENAERS, KBC Bank, Belgien
Leo VERHOEVEN, KBC Bank, Belgien
Bart PRENEEL, professor i kryptologi, det katolske universitet i Louvain, Belgien
Danny de TEMMERMAN, Europa-Kommissionen
Desmond PERKINS, Europa-Kommissionen

6. Ekspert på økonomisk spionage og beslægtede spørgsmål

Sorbas VON COESTER, direktør i Salamandre (konsulentfirma), Frankrig
Christian HARBULOT, Ecole de guerre économique, Frankrig
Thierry LA FRAGETTE, Circé, Frankrig
Ralf NEMEYER, Articon-Integralis, Tyskland

7. Menneskerettigheder og beskyttelse af privatsfæren

Dimitri YERNAULT, det frie universitet i Bruxelles
Simon DAVIES, Privacy International, Det Forenede Kongerige
Jérôme THOREL, Privacy International, Frankrig
Yaman AKDENIZ, Cyber Rights and Cyber Liberties, Leeds UK
David NATAF, Alexandre COSTE, Millet-Sala-Nataf (advokatkontor), Paris
Rüdiger DOSSOW, Europarådet, Strasbourg

8. Repræsentanter for EU-institutionerne

Europa-Kommissionen
Kommissionsmedlem Christopher PATTEN (eksterne forbindelser)
Kommissionsmedlem António VITORINO (relige og indre anliggender)
Kommissionsmedlem Erki LIIKANEN (virksomheder og informationssamfundet)
Lodewijk BRIET, Generaldirektoratet for Eksterne Forbindelser
Jacques DE BAENST, chef for protokol og sikkerhed
Françoise DE BAIL, Generaldirektoratet for Handel
Susan BINNS, Generaldirektoratet for det Indre Marked

Rådet for Den Europæiske Union
Brian CROWE, generaldirektør for eksterne forbindelser
Roland GENSON, Luxembourgs faste repræsentation, ansvarlig for retlige og indre anliggender
Hervé MASUREL, repræsentant for det franske formandskab
Ambassadør Gunnar LUND, repræsentant for det svenske formandskab

Den Europæiske Centralbank
Christoph BOERSCH, Wolfgang SCHUSTER, Dominique DUBOIS, Den Europæiske Centralbank

9. Samtalepartnere under rejser

Formandens og ordførerens rejse til Paris, 18.-19. januar 2001
Jean-Claude MALLET, generalsekretær i SGDN
Bertrand DUMONT, general i det franske luftvåben, vicegeneralsekretær i SGDN

PE 305.391/Del 2 148/190 RR\445599DA.doc
Claude-France ARNOULD, direktør for internationale og strategiske anliggender, SGDN
Henri SERRES, direktør med ansvar for sikkerhed i forbindelse med informationssystemer, SGDN
Stéphane VERCLYTTE, konsulent for retlige og europæiske anliggender, SGDN
Philippe DULUC, konsulent for forskning og teknologi, SGDN
Gérard ARAUD, direktør for strategiske anliggender i det franske udenrigsministerium
Olivier MOREAU, direktør for sikkerhed i det franske udenrigsministerium
Eric PERRAUDAU, konsulent i det franske forsvarsministerium
Jean-Pierre MILLET, advokat

Tom KING, formand for udvalget om efterretningsvirksomhed og sikkerhed, Underhuset
Alistair CORBETT, leder af ISC-sekretariatet, Underhuset
Donald ANDERSON, formand for udenrigsudvalget, Underhuset
Bruce GEORGE, formand for forsvarsudvalget, Underhuset
Jack STRAW, statssekreter i det britiske indenrigsministerium
Michael GILLESPIE, sikkerhedskoordinator
Charles GRANT, direktør, Centre for European Reform
Casper BOWDEN, direktør, FIPR

Udvalgets formandskabs, koordinatorernes og ordførerens rejse til Washington D.C., 6.-12. maj 2001
H.E. Günter BURGHARDT, leder af Kommissionens delegation i Washington D.C.
James WOOLSEY, tidligere direktør i CIA
Jeffrey RICHELSON, direktør, National Security Archive, George Washington University
Marc ROTENBERG, Electronic Information Privacy Centre
Wayne MADSEN, Electronic Information Privacy Centre
David SOBEL, Electronic Information Privacy Centre
Barry STEINHARDT, underdirektør, American Civil Liberties Union
Porter J. GOSS, formand for efterretningsudvalget i Repræsentanternes Hus
Nancy PELOSI, næstformand for efterretningsudvalget i Repræsentanternes Hus
Robert DAVIS, vicekonsulent i direktoratet for efterretningspolitik i det amerikanske justitsministerium.
Bilag II.: Litteraturliste

CITERET LITTERATUR


Andronov, Major A., Zarubezhnoye voyennoye obozreniya, nr.12, 1993, 37-43

Anonymus, Hacker’s guide, Markt &Technik-Verlag (1999)


Berliner Zeitung, Abgehört, 22.1.1996

Bode, Britta, Heinacher, Peter, Sicherheit muß künftig zur Chefsache erklärt werden Handelsblatt, 29.8.1996

Brady, Martin, Direktor der DSD, Brief vom 16.3.1999 an Ross Coulthart, Sunday Program Channel 9; http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp


Buchmann, Johannes, Faktorisierung großer Zahlen, Spektrum der Wissenschaft 2, 1999

Bundesministerium für Wirtschaft und Technologie der Bundesrepublik Deutschland, Computersonionage, Dokumentation Nr. 44, juli 1998

Bundesministerium für Wirtschaft und Technologie der Bundesrepublik Deutschland, Informationen für geheimschutzbetreute Unternehmen (1997)

Bundesverfassungsgericht der Bundesrepublik Deutschland, BVerfG-Urteil, 1 BvR 2226/94 vom 14.7.1999 (zu Art. 10 GG, Gesetz zu Artikel 10 Grundgesetz)

Campbell, Duncan, Teknikkens stade inden for kommunikationsefterretninger (Comint) i forbindelse med den automatiserede behandling i efterretningsøjemed af aflyttede fæste eller fælles bredbåndsoforbindelser på flere sprog og dens anvendelse på indhentning og udvælgelse af Comint, herunder talegenkendelse, del 2/5, i: STOA (Ed), Overvågningsteknologiens udvikling samt risikoen for misbrug af økonomiske oplysninger (oktober 1999), PE 168.184
Campbell, Duncan, Inside Echelon, Heise Online, 24.7.2000,
http://www.heise.de/tp/deutsch/special/ech/6928/1.html

Comité permanent de contrôle des service de renseignement, Rapport d'enquête sur la manière
dont les services belges de renseignement reagissent face à l'éventualité d'un système
américain "echelon" d'interception des communications téléphoniques et fax en Belgique,

Commission on the Roles and Capabilities of the US Intelligence Community, Preparing for
http://www.gpo.gov/int/report.html

Deutscher Bundestag, Sekretariat des PKGr, Die Parlamentarische Kontrolle der
Nachrichtendienste in Tyskland (2000)

Domestic and External Security Secretariat, Department of the Prime Minister and Cabinet
(New Zealand), "Securing our Nation's Safety", december 2000,

Dodel, Hans, Satellitenkommunikation, Hüthig Verlag (1999)

Elkjær, Bo & Seeberg, Kenan, Echelon was my baby, Ekstra Bladet, 17.1.1999

Eser, Albin, Überhofer Michael, Huber Barbara (Eds), Korruptionsbekämpfung durch
Strafrecht. Ein rechtsvergleichendes Gutachten zu den Bestechungsdelikten im Auftrag des


Fink, Manfred, Lauschziel Wirtschaft - Abhörgefahren und -techniken, Vorbeugung und
Abwehr, Richard Boorberg Verlag, Stuttgart (1996)

Förster, Andreas, Maulwürfe in Nadelstreifen, Henschel Verlag (1997)

Frattini, Franco, Il ruolo dei servizi di informazione e sicurezza nel caso 'Echelon'. Relazione
del comitato parlamentare per i servizi di informazione e sicurezza e per il segreto di stato.
Approvata nella seduta del 29 novembre 2000, Trasmessa alle Presidenze il 19 dicembre 2000

Freeh, Louis J, Statement for the Record, Hearing on Economic Espionage, House Judiciary
Committee, Subcommittee on Crime, Washington DC, 9.5.1996


Frowein, Jochen Abr., Peukert, Wolfgang, Europäische Menschenrechtskonvention², N. P.
Engel Verlag (1996)

Frost, Mike i et fjernsynsinterview på NBC "60 Minutes" af 27.2.2000,
http://cryptome.org/echelon-60min.htm

Frost, Mike i et interview på den australske sender Channel 9 af 23.3.1999,
http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm

Grant, Charles, Intimate relations. Can Britain play a leading role in European defence - and
keep its special links to US intelligence? 4.2000, Centre for European Reform

Guinsel, Jean, L'espionnage n'est plus un secret, The Tocqueville Connection, 10.7.1998

Hager, Nicky, Secret Power. New Zealands’s Role in the international Spy Network, Craig
Potton Publishing (1996)
Hager, Nicky, Exposing the global surveillance system, http://www.ncoic.com/echelon1.htm
Hoffmann, Wolfgang, Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. (ASW), Aktuelle Anmerkungen zur Sicherheitslage der deutschen Wirtschaft, april 2001
Hummelt, Roman, Wirtschaftsspionage auf dem Datenhighway, Strategische Risiken und Spionageabwehr, Hanser Verlag (1997)
Intelligence and Security Committee (UK), Annual Report 1999-2000
Jauvert, Vincent, Espionnage - comment la France écoute le monde, Le Nouvel Observateur, 5.4.2001, nr. 1900, s. 14 ff.
Kreye, Andrian, Aktenkrieger, Süddeutsche Zeitung, 29.3.2001
Kuppingher, Martin, Internet- und Intranetsicherheit, Microsoft Press Deutschland (1998), 60
Kyas, Othmar, Sicherheit im Internet, International Thomson Publishing (1998), 23
Leiberich, Otto, Vom diplomatischen Code zur Falltürfunktion - Hundert Jahre Kryptographie in Deutschland, Spektrum der Wissenschaft, juni 1999
Lyle Robert, Radio Liberty/Radio free Europe, 10. februar 1999
Madsen, Wayne i fjernsynsinterview på NBC "60 Minutes" den 27.2.2000, http://encryptome.org/echelon-60min.htm
Paecht, Arthur, 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 sécurité nationale, N° 2623 Assemblée nationale, enregistré à la Présidence de l'Assemblée nationale le 11 octobre 2000
Paecht, Arthur, Rapport fait au nom de la Commission de la défense nationale et des forces armées sur la proposition de loi (N° 1497) de M. Paul Quilès et plusieurs de ses collègues tendant à la création d'une délégation parlementaire pour les affaires de renseignement, enregistré à la Présidence de l'assemblée nationale le 23. novembre 1999
Richelson, Jeffrey T., The U.S. Intelligence Community, Westview Press, 1999
http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html

Richelson, Jeffrey T., Ball, Desmond, The Ties That Bind, Boston Unwin Hyman (1985)

Richter, Nicolas, Klettern für die Konkurrenz, Süddeutsche Zeitung, 13.9.2000

Rötzler, Florian, Die NSA geht wegen Echelon an die Öffentlichkeit, Heise Online, 26.2.2000,
http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special

Schmidt-Eenboom, Erich, Streng Geheim, Museumsstiftung Post und Telekommunikation Heidelberg (1999)


Shane Scott, Bowman Tom, America's Fortress of Spies, Baltimore Sun, 3.12.1995

Simon Singh, Geheime Botschaften, Carl Hanser Verlag (1999)


State Department Foreign Press Center Briefing, Subject: Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage, Washington DC, 7.3.2000

Süddeutsche Zeitung, Haftstrafe wegen Spionage für Russland, 30.5.2000

TPCC, Broschüre über das Advocacy Center, oktober 1996


Det Hvide Hus, Archive,
http://govinfo.library.unt.edu/npr/library/direct/orders/tradepromotion.html


Wirtschaftswoche "Antennen gedreht", Nr. 46/9, november 1999

Wirtschaftswoche "Nicht gerade zimperlich", Nr. 43/16, oktober 1992

Wobst, Reinhard, Abenteuer Kryptologie, Adison-Wesley (1998)


Woolsey, James, Remarks at the Foreign Press Center, Transskript, 7.3.2000,
http://cryptome.org/echelon-cia.htm

Wright, Steve, An appraisal of technologies for political control, STOA interim study (1998)

VIDEREKÆNDE LITTERATUR

Air Intelligence Agency (AIA), homepage, http://www.aia.af.mil
America’s Military Community, homepage, http://www.military.com
Bundesnachrichtendienst, Die Nachrichtendienste der Bundesrepublik Deutschland, 2000, http://www.bundesnachrichtendienst.de/diensteb.htm
Central Intelligence Agency (CIA), homepage http://www.odci.gov/index.html
Frankfurter Allgemeine Zeitung, Niederländische Wirtschaftspionage, 19.4.2000
Frankfurter Allgemeine Zeitung, Wirtschaftspionage, 3.2.2001
Gralla, Preston, So funktioniert das Internet: ein virtueller Streifzug durch das Internet, Markt und Technik (1999)
Hayden, Michael, Statement for the record of House Permanent Select Committee on intelligence, 12.4.2000 http://www.nsa.gov/releases/DIR_HPSCI_12APR.HTML
Innenministerium Brandenburg, Abwehr von Wirtschaftspionage, 1999
Mass, Christian, Satelliten Signale anzapfen und auswerten, Satellitenspionage für Einsteiger, Franzis Verlag, Funkschau Telekom, Poing 1998


Matschke, Klaus Dieter, Geheimdienste im Auftrag des Wettbewerbs, 5.9.1998, Seku Media Verlag Ingelheim

National Security Agency (NSA), homepage http://www.nsa.gov/


Schönleber, Claus, Verschlüsselungsverfahren für PC-Daten, Franzis Verlag, Poing 1995

Secretary of State for the Home Department, Interception of communication in the UK, juni 1999

Sénat et Chambre des représentants de Belgique, 14.2.2000, Rapport d’activités 1999 du Comité permanent de contrôle des services de renseignements et de sécurité

Tenet, George, redegørelse ved direktøren for Central Intelligence til the House Permanent Select Committee on Intelligence, 12.4.2000, http://sun00781.dn.net/irp/congress/2000_hr/tenet.html


The US Army Intelligence and Security Command (INSCOM), homepage http://www.vulcan.belvoir.army.mil


Ulfkotte, Udo, Marktplatz der Diebe, Wie die Wirtschaftsspionage deutsche Unternehmen ausplündert und ruiniert. Bertelsmann Verlag, München (1999)


Wall, Stephen, Det Forenede Kongeriges faste repræsentant ved Den Europæiske Union, skrivelse til kommissionsmedlem Liikanen om GCHQ, 21.3.2000

Wojahn, Jörg, Die globalen High-Tech-Schnüffler, 1.9.2000, Der Standard
Bilag III.: Definitioner og oplysninger vedrørende kommunikationsovervågning med henblik på strafforfølgning

1. Forord

Under udvalgets arbejde blev der i diskussionerne om tilladelighed, konsekvenser og risici i forbindelse med globale aflytningssystemer gang på gang henvist til foranstaltninger og aktiviteter inden for EU, som nok har med kommunikationsovervågning at gøre, men som hører ind under det retlige samarbejde i straffesager.

Derfor har ordføreren i betænkningens hovedafsnit ikke henvist til disse foranstaltninger, da spørgsmålet om det legitime i at anvende kommunikationsovervågning i strafferetligt øjemed ikke bør sammenblandes med spørgsmålet om det legitime i at anvende kommunikationsovervågning til efterretningsformål. Selv om der i begge tilfælde er tale om indgreb i privatsfæren, som begrundes med sikkerhedshensyn (i ordets bredeste betydning), er der dog så store forskelle, hvad angår arbejdsmetoder og mål, at bestemmelser, der synes fornuftige og passende for det ene område, ikke nødvendigvis er det for det andet. Om strafferetlige foranstaltninger er hensigtsmæssige og står i et rimeligt forhold til den pågældende lovovertrædelse, bør således ikke diskuteres på baggrund af den politiske vurdering af efterretningsforanstaltninger.

For at afhjælpe eventuelle uklarheder skal der her tages stilling til nogle af de rejste spørgsmål og gives en definition på nogle begreber. I det følgende vil der for det første blive peget på forskellene mellem kommunikationsovervågning i strafferetligt øjemed og til efterretningsformål, for det andet vil der under hensyntagen til EU's kompetenceområder blive redegjort for de EU-retsakter, der berører den strafferetlige kommunikationsovervågning, og endelig vil der for det tredje blive givet en definition på andre begreber, der gentagne gange er blevet nævnt i udvalget i forbindelse med de tværnationale arbejder vedrørende kommunikationsovervågning.

2. To forskellige ting: kommunikationsovervågning i strafferetligt øjemed/til efterretningsformål

Kommunikationsovervågning foretaget af efterretningsstjenester (som det såkaldte Echelon-system) har ikke til formål at overvåge enkeltpersoner i hjemlandet, men at foretage en generel overvågning af aktiviteter i udlandet for på forhånd at sikre sig sikkerheds relevante oplysninger. Denne overvågning finder sted i hemmelighed, og det er heller ikke på lang sigt formålet at nå ud til offentligheden. Med det argument, at sikkerheden kun kan garantieres ved hemmeligholdelse, og at det ikke drejer sig om landets egne borgere, tillades det hyppigt, at efterretningsstjenester arbejder i en juridisk gråzone, hvor reglerne er uklare og kontrollen mangelfuld.

Strafferetlig kommunikationsovervågning tager derimod sigte på, såfremt mistanken
tilstrækkelig stor, at afholde den enkelte fra at fuldende sin handling eller at sanktionere strafbare handlinger. Overvågningsforanstaltningerne iværksættes af myndighederne i hjemlandet. Er det påkrævet med overvågningsforanstaltninger i udlandet, iværksættes de af myndighederne på stedet efter anmodning om retshjælp. Da indgrebene er rettet mod landets egne borgere, er der efter politistatens afskaffelse indført meget konkrete bestemmelser og effektive kontrolmekanismer, der er baseret på en afvejning af interesser. Overvågningsforanstaltningerne må derfor kun iværksættes i konkrete tilfælde, hvor mistanken er tilstrækkelig stor, og skal i mange medlemsstater godkendes af en dommer. Også når overvågningen finder sted i det skjulte, er formålet at anvende beviserne i offentlige straffesager, hvorfor myndighederne selv har interesse i, at de tilvejebringes på lovlig vis.

3. Arbejder inden for EU på området strafferetlig kommunikationsovervågning

3.1. Generelt

Med indføjelsen af et afsnit om den fælles udenrigs- og sikkerhedspolitis i EU-traktaten er der skabt en mulighed for et samarbejde mellem efterretningstjenestene på eurpæisk plan, som der imidlertid endnu ikke er gjort brug af.

De bestemmelser og arbejder på området kommunikationsovervågning, der måtte findes på EU-plan, vedrører udelukkende det strafferetlige aspekt, dvs. samarbejdet om retlige og indre anliggender.

3.2. Begrænsningen af EU's beføjelser til tekniske bestemmelser

Tilladeligheden af aflytningsforanstaltninger hører i øjeblikket udelukkende ind under medlemsstaterne. I overensstemmelse med principippet om begrænset bemyndigelse kan EU kun gribe ind på områder, hvor traktaterne giver den befojelse til det. Men en sådan befojelse findes vel ikke i EU-traktatens afsnit VI "Bestemmelser om politisamarbejde og retligt samarbejde i kriminalsager". På området politisamarbejde (EU-traktatens artikel 30, stk. 1) er fælles handling kun mulig i forbindelse med operative aspekter, dvs. i forbindelse med den måde, hvorpar politiarbejdet gennemføres. På området retligt samarbejde er der ganske vist i artikel 31, litra c) generelt hjemmel for fælles handling til "sikring af foreneligheden mellem medlemsstaternes gældende regler", men kun såfremt "det er nødvendigt for at forbedre samarbejdet". Bestemmelsen tager således sandsynligvis sigte på deciderede samarbejdsbestemmelser. Den "indbyrdes tilnærmelse of medlemsstaternes strafferetlige regler (artikel 29, sidste led) er begrænset til fastsættelse af mindsteregler for, hvad der udgør kriminelle handlinger (artikel 31, litra c). Sammenfattende kan det altså konstateres, at det fortsat er national ret, der afgør, på hvilke betingelser overvågningsforanstaltninger er tilladelige. Så vidt ordføreren ved, ønsker ingen medlemsstater at røre ved denne rent nationale befojelse.

Et samarbejde mellem medlemsstaterne på grundlag af EU-traktaten kan derfor først blive tale om i forbindelse med gennemførelsen af de overvågningsforanstaltninger, der er tilladelige i henhold til national ret, dvs. på et lavere niveau. I de tilfælde, hvor
telekommunikationsovervågning er tilladt i henhold til den nationale retsorden, skal den pågældende medlemsstat kunne anmode de øvrige medlemsstater om hjælp til den tekniske gennemførelse. Om man betragter den tilstræbte tekniske forenkling, der sikkert øger effektiviteten af den grænseoverskridende aflytning i forbindelse med straffefølgning især på området organiseret kriminalitet, som noget positivt eller negativt, afhænger nok i stor udstrekning af tilliden til ens egen retsstat. Det skal i hvert fald endnu en gang understreges, at betingelserne for aflytningens tilladelighed, som er et rent nationalt anliggende, ikke berøres, heller ikke selv om den grænseoverskridende overvågning bliver lettere på grund af den tekniske harmonisering, og det som altid er umuligt at forhindre misbrug i de konkrete tilfælde.

3.3. Arbejder og retsakter på området telekommunikationsaflytning

På området telekommunikationsaflytning er der hidtil kun vedtaget to EU-retsakter: Rådets resolution af 17. januar 1995 om lovlig aflytning af telekommunikation, som igennem et tilsvarende memorandum skulle udvides til at omfatte tredjelande, og som desuden efter planen skulle følges op af et "opdateringsforslag" (begge dokumenter blev forberedt i "ENFOPOL-dokumenter"), og konventionen om gensidig retshjælp i straffesager.

Rådets resolution af 17. januar 1995 om lovlig aflytning af telekommunikation

Rådets resolution af 17. januar 1995 om lovlig aflytning af telekommunikation synes at kunne føres tilbage til samarbejdet mellem ekspertene på ILET-seminarerne (se nedenstående punkt 4) og i hovedtrækene at være i overensstemmelse med de IUR (international user requirements), der blev udarbejdet der.

Denne resolution tager sigte på, at der i alle medlemsstater skabes de tekniske forudsætninger for, at myndighederne inden for rammerne af deres nationale bemyndigelse virkelig kan få adgang til oplysningerne, altså rent teknisk kan realisere de beføjelser, de har i henhold til national ret.

For at opnå dette medtages der i et bilag nogle meget detaljerede "specifikationer", som medlemsstaterne kan kræve opfyldt, og Rådet "tager til efterretning", at de "udgør en vigtig sammenfattning af de kompetente myndigheders behov, for så vidt angår den tekniske gennemførelse af lovlige aflytningsforanstaltninger i moderne telekommunikationssystemer". Til disse specifikationer hører bl.a. tidstro data i forbindelse med kommunikation eller mulighed for at overføre aflyttet kommunikation til aflytningsmyndighederne via netoperatørerne. Rådet går i resolutionen ind for, "at der bør tages hensyn til ovennævnte specifikationer ved afgrensningen og gennemførelsen af foranstaltningerne", og anmoder medlemsstaterne og de ansvarelige ministre om at samarbejde "med henblik på at gennemføre specifikationerne i relation til netoperatørerne og tjenesteudbyderne".

Det skal understreges, at den valgte retsakt, resolutionen, ikke har bindende karakter, og at den derfor ikke giver medlemsstaterne nogen rettigheder og pligter. Den opstandelse, som resolutonen og de dertil knyttede dokumenter gav anledning til, skyldes ikke så meget

---

1 EFT C 329 af 4.11.1996.
indholdet som omstændighederne ved dens udarbejdelse, især den manglende gennemskuelighed.

Aftalememorandum


Memorandummet blev den 23. november 1995 undertegnet af EU-medlemsstaterne og af Norge, men ikke af andre tredjelande. Fra USA, Australien og Canada kom der blot skriftlige meddelelser om, at de ville iværksætte den nationale gennemførelse i deres lande.\(^2\)

Beklageligvis er teksten endnu ikke blevet offentliggjort, og den har derfor givet anledning til mange spekulationer i pressen.

Udkast til Rådets resolution om lovlig aflytning af telekommunikation med særligt henblik på ny teknologi


Konventionen om gensidig retshjælp i straffesager\(^5\)

---

\(^1\) Nr 10.037/95 ENFOPOL 112, ikke offentliggjort.


\(^3\) A4-0243/99.

\(^4\) Lovgivningsmæssig beslutning med Europa-Parlamentets udtalelse af 7.5.1999, EFT C 279 af 11.10.1999, s. 498.

\(^5\) 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 197 af 12.7.2000, s. 1, art 17 ff.
Den anden retsakt er en konvention om retshjælp i straffesager. I art. 17 ff. fastsættes det, på hvilke betingelser hvilken retshjælp skal kunne ydes i straffesager i forbindelse med aflytning af telekommunikation. Uden at gå i detaljer skal det blot nævnes, at konventionen på ingen måde beskærer de aflyttedes rettigheder, da den medlemsstat, hvor den aflyttede befinder sig, altid kan nægte at yde retshjælpen, hvis den ikke er i overensstemmelse med denne stats nationale ret.

4. Definitioner og oplysninger vedrørende andre grænseoverskridende arbejder inden for aflytning af telekommunikation

Ud over de forskellige EU-retsakter har de forskellige eksisterende og tidligere arbejdsgrupper om sikkerheds politik gentagne gange skabt forvirring. Derfor gives der i det nedenstående definitioner på nogle af de relevante begreber.

ILETS (International Law Enforcement Telecommunications Seminar)

ILET-seminarerne udsprang af et initiativ fra FBI. I 1993 indbød FBI strafforfølgningsmyndigheder og efterretningstjenester fra stater, til hvilke man havde et venskabeligt forhold, til at deltage i et møde i Quantico om aflytning af telekommunikation. Størstedelen af de nuværende EU-stater deltog sammen med Australien og Canada.1 Siden har der regelmæssigt fundet møder sted til drøftelse af kravene til en effektiv international kommunikationsaflytning.

På et møde i Bonn i 1994 enedes ILET-deltagerne om et dokument med politiske retningslinjer, i hvis bilag der var en liste over "international user requirements" (IUR 1.0 eller IUR 95). Her var opført de specifikationer, som burde overholdes af de forskellige telekommunikationsoperatører for at lette aflytningsprocessen. IUR 1.0 tjente - omend ikke officielt - som grundlag for Rådets resolution af 17. januar 1995 om lovlig aflytning af telekommunikation. Efterfølgende blev der afholdt yderligere ekspertmøder om IUR og deres gennemførelse og tilpasning til den nye telekommunikation.

TREVI-Gruppen

Inden for rammerne af TREVI-Gruppen behandlede EU-staternes justits- og indenrigsministre før Maastricht-traktatens ikrafttræden (det var den, der med EU-traktaten indførte bestemmelser om samarbejde om retlige og indre anliggender) spørgsmål vedrørende indre sikkerhed. TREVI-Gruppen er ikke længere aktiv, da disse emner i mellemtiden er overtaget af Rådets særlige arbejdsgrupper.

Hvad angår det område, der behandles her, er især to særlige arbejdsgrupper interessante,

---

arbejdsgruppen om retshjælp i straffesager, der inden for rammerne af samarbejdet om retlige og indre anliggender har behandlet konventionen om retshjælp i straffesager, og arbejdsgruppen om politisamarbejde, der beskæftigede sig med spørgsmål i forbindelse med lovlig aflytning af telekommunikation, herunder aflytning af nye kommunikationssystemer (mobiltelefoner, Internettet, E-mail); den sidstnævnte arbejdsgruppe beskæftigede sig også med harmonisering af normerne for de lovlige aflytningsmyndigheders krav til netoperatører og tjenesteudbydere.

"ENFOPOL"

"ENFOPOL" er - i modsætning til, hvad mange forfattere mener - ikke en arbejdsgruppe eller organisation, men en forkortelse, der dækker over arbejdsdokumenter vedrørende strafforfølgning og politiarbejde, en opfattelse, der deles af den særlige arbejdsgruppe om politisamarbejde. ENFOPOL er ikke en del af disse dokumenters titel, men det klassifikationssystem, de er ordnet efter.

\[\text{\footnotesize\cite{1} Jf. den østrigske indenrigsminister Schlögels skriftlige svar på spørgsmål fra parlamentsmedlem Van der Bellen, 4739/AB.XX.GP \url{http://www.parlinkom.gv.at/pd/pm/XX/AB/texte/040/AB04014_.html}. \\
\hspace{1em} Jf. Campbell, ILETS, die geheime Hand hinter ENFOPOL 98, \url{http://heise.de/tp/deutsch/special/enfo/6396/1.html}.}\]
Bilag IV.:

OVERSIGT

OVER

EFTERRETNINGSTJENESTER OG PARLAMENTARISKE KONTROLORGANER

I

MEDLEMSSTATERNE OG UKUSA-STATERNE
<table>
<thead>
<tr>
<th>Land</th>
<th>Efterretningstjeneste</th>
<th>Retsgrundlag</th>
<th>Opgaver</th>
<th>SIGINT-kapacitet</th>
<th>Kontrolmyndighed</th>
</tr>
</thead>
<tbody>
<tr>
<td>ØSTRIG</td>
<td><em>Heeresnachrichtenamt (HnA)</em></td>
<td>§ 20 Abs 3 Militärbefugniggesetz (MBG) BGBl I 86/2000</td>
<td>Militær efterretningstjeneste, forsvar mod udefrakommende aktiviteter, der kan true sikkerheden.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>Abwehramt (AbwA)</em></td>
<td></td>
<td>Parlamentarisk underudvalg:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Militær efterretningstjeneste.</td>
<td></td>
<td>Ständiger Unterausschuss des Landesverteidigungsausschusses zur Überprüfung von nachrichtendienstlichen Maßnahmen zur Sicherung der militärischen Landesverteidigung (14 medlemmer, alle parter i parlamentet skal være repræsenteret)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sorterer under forsvarsministeren.</td>
<td></td>
<td>1 Rechtsschutzbeauftragter</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


PE 305.391 164/190 RR\445698DA.doc
<table>
<thead>
<tr>
<th>Land</th>
<th>Efterretnings-tjeneste</th>
<th>Retsgrundlag</th>
<th>Opgaver</th>
<th>SIGINT-kapacitet</th>
<th>Kontrolmyndighed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Parlamentarisk underudvalg: Ständiger Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit (14 medlemmer, alle partier i parlamentet skal være repræsenteret)</td>
<td>1 Rechtsschutzbeauftragter</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Land</td>
<td>Efterretnings-tjeneste</td>
<td>Retsgrundlag</td>
<td>Opgaver</td>
<td>SIGINT-kapacitet</td>
<td>Kontrolmyndighed</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------</td>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>BELGIEN</td>
<td><strong>Service Général du Renseignement et de la Sécurité des Forces armées (S.G.R.)</strong>&lt;br&gt;Militærførretnings- og sikkerhedsstjeneste.&lt;br&gt;Sorterer under forsvarsministeren.</td>
<td><strong>Loi du 30 novembre 1998 organique des services de renseignement et de sécurité</strong></td>
<td>Informations- og dataindsamling på det militære, politiske, økonomiske og teknologisk/videnskabelige område. Opretholdelse af sikkerheden for militære anlæg og militærpersonale.</td>
<td><strong>Comité permanent de contrôle des services de renseignements et de sécurité (Comité permanent R)</strong>&lt;br&gt;Består af 3 medlemmer, der udpeges af Senatet; de må ikke udeve af det mandat, som er opnået ved valg, og ingen andre aktiviteter, der kunne udgøre en risiko for deres uafhængighed.</td>
<td><strong>Sûreté de l’Etat (V.S.)</strong>&lt;br&gt;Civilførretnings- og sikkerhedsstjeneste.&lt;br&gt;Sorterer under justitsministeren.</td>
</tr>
<tr>
<td>Land</td>
<td>Efterretnings-tjeneste</td>
<td>Retsgrundlag</td>
<td>Opgaver</td>
<td>SIGINT-kapacitet</td>
<td>Kontrolmyndighed</td>
</tr>
<tr>
<td>------</td>
<td>------------------------</td>
<td>--------------</td>
<td>---------</td>
<td>-----------------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| DANMARK | Forsvarets Efterretningsstjeneste (FET), Militær efterretningsstjeneste. Sorterer under Forsvarsministeriet. | **Lov om forsvarrets formål, opgaver og organisation m.v.** **Lov 909 af 8.12.1993** ["Rammelov, hvor FET ikke nævnes] [en ny lov om FET og PET er på vej] | Indsamling og evaluering af fortrolige forsvarsrelevante oplysninger om GUS, Øst- og Centraleuropa på det militære, politiske, økonomiske og teknologisk/videnskabelige område, SIGINT; dekryptering. Medarbejdere og budget: fortroligt. | ja | 2 kontrolorganer:  
Kontroludvalget vedrørende Politiets og Forsvarets Efterretningsstjenester (Wamberg-udvalget) (består af embedsmænd og advokater)  
Udnævnes af justitsministeren. |
<table>
<thead>
<tr>
<th>Land</th>
<th>Efterretnings-tjeneste</th>
<th>Retsgrundlag</th>
<th>Opgaver</th>
<th>SIGINT-kapacitet</th>
<th>Kontrolmyndighed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Land</td>
<td>Efterretningstjeneste</td>
<td>Retsgrundlag</td>
<td>Opgaver</td>
<td>SIGINT-kapacitet</td>
<td>Kontrolmyndighed</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------------------------------</td>
<td>------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>Sorterer under Forsvarsministeriet.</td>
<td></td>
<td>Indsamling og bearbejdning af oplysninger vedrørende Frankrigs sikkerhed Kontraspionage (uden for landets grænser).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Personale: 4.100 medarbejdere; Budget: FF 1,7 mia.</td>
<td></td>
<td>Personale: 4.100 medarbejdere; Budget: FF 1,7 mia.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Kontraspionage (uden for landets grænser).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FRANKRIG</td>
<td>Direction du renseignement militaire (DRM)</td>
<td>Décret n°92-523 du 16 juin 1992</td>
<td>Giver militæret de nødvendige militære oplysninger</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sorterer under Forsvarsministeriet.</td>
<td></td>
<td>1.700 personer, FF 90 mio., intern militær sikkerhed, understøttelse af hæren.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Omfatter bl.a. 1 medlem af Nationalforsamlingen og 1 medlem af Senate.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Civil efterretningstjeneste.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sorterer under indenrigsministeren.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FRANKRIG</td>
<td>Direction de la surveillance du territoire (DST)</td>
<td>Décret n°82-1100 af 22. december 1982</td>
<td>Kontraspionage inden for landets grænser.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Civil efterretningstjeneste.</td>
<td></td>
<td>Personale: 1.500 medarbejdere; opholdelse af den offentlige sikkerhed, kontraspionage i indlandet.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sorterer under indenrigsministeren.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Land</td>
<td>Efterretnings-tjeneste</td>
<td>Retsgrundlag</td>
<td>Opgaver</td>
<td>SIGINT-kapacitet</td>
<td>Kontrolmyndighed</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>TYSKLAND</td>
<td>Bundesnachrichtendienst (BND)</td>
<td>Gesetz über den Bundesnachrichtendienst (BNDG), BGBl 1990 I 2954 idgF</td>
<td>Indsamling og bearbejdning af oplysninger om udlandet, som er af sikkerheds- og udenrigspolitisk betydning.</td>
<td>ja</td>
<td>Parlamentarisches Kontrollgremium (PKGR)</td>
</tr>
<tr>
<td></td>
<td>Sorterer under forbundskansleren.</td>
<td></td>
<td></td>
<td></td>
<td>Parlamentarisk kontrolmyndighed for alle tre efterretningsstjenester, består af 9 medlemmer af Forbunds dagen.</td>
</tr>
<tr>
<td>TYSKLAND</td>
<td>Bundesamt für Verfassungsschutz (BfV)</td>
<td>Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für den Verfassungsschutz (BVerfSchG, BGBl 1090 I 2954)</td>
<td>Indsamling og bearbejdning af oplysninger om aktiviteter, der truer sikkerheden, samt om fjendtlige efterretningsstjenesters aktiviteter på landets territorium.</td>
<td></td>
<td>G 10-Kommission</td>
</tr>
<tr>
<td></td>
<td>Sorterer under indenrigsministeren.</td>
<td></td>
<td></td>
<td></td>
<td>Ikke forpligtet til at udføre ordrer. Kan, men skal ikke bestå af parlamentsmedlemmer.</td>
</tr>
<tr>
<td>TYSKLAND</td>
<td>Militärischer Abschirmdienst (MAD)</td>
<td>Gesetz über den militärischen Abschirmdienst (MADG), BGBl 1990 I 2954 idgF</td>
<td>Sikring af forbundshærens effektivitet, overvågning af sikkerheden for militære anlæg og militærpersonale.</td>
<td></td>
<td>4 medlemmer udnævnt af PKGR.</td>
</tr>
<tr>
<td>Land</td>
<td>Efterretningstjeneste</td>
<td>Retsgrundlag</td>
<td>Opgaver</td>
<td>SIGINT-kapacitet</td>
<td>Kontrolmyndighed</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------</td>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>------------------</td>
<td>-------------------</td>
</tr>
</tbody>
</table>
| GRÆKEN-LAND     | Ethniki Ypiresia Pliroforion (EYP) | Lov 1645/86 om den nationale efterretningstjeneste (Ethniki Ypiresia Pliroforion) | - Indsamling og behandling af oplysninger om landets nationale sikkerhed (oplysninger om organiseret kriminalitet, terrorisme samt militære, økonomiske og politiske oplysninger); underretning af relevante myndigheder.  
- Kontraspionage; overvågning af udenlandske efterretningstjenesters aktiviteter mod landet. | Særligt parlamentsudvalg til beskyttelse af kommunikationen og privatsfæren. Ingen særlig kontroret. Sammensætning: 1 næstformand i parlamentet, 1 parlamentsmedlem pr. gruppe, 1 kommunikations-specialist. | Institution til beskyttelse af personlige data |

"National efterretningstjeneste"  
Sorterer under KYSEA (Det Nationale Sikkerhedsråd: premierministeren, udenrigsministeren og forsvarsministeren).
<table>
<thead>
<tr>
<th>Land</th>
<th>Efterretnings-tjeneste</th>
<th>Retsgrundlag</th>
<th>Opgaver</th>
<th>SIGINT-kapacitet</th>
<th>Kontrolmyndighed</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRLAND</td>
<td>Efterretningspersonale</td>
<td></td>
<td>Eirlands nationale sikkerhedsinteresser (især IRA), sikkerhed i forbindelse med det nationale militær, teknologisk udvikling i forbindelse med udenlandsk militær.</td>
<td></td>
<td>Ingen specifik kontrolmyndighed.</td>
</tr>
<tr>
<td>Land</td>
<td>Efterretnings-tjeneste</td>
<td>Retsgrundlag</td>
<td>Opgaver</td>
<td>SIGINT-kapacitet</td>
<td>Kontrolmyndighed</td>
</tr>
<tr>
<td>------</td>
<td>----------------------</td>
<td>--------------</td>
<td>---------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>ITALIEN</td>
<td>Servizio per le informazioni e la sicurezza democratica (SISDE) Direzione investigazioni anti-mafia (DIA)</td>
<td>L. 24 ottobre 1977, n. 801, art. 6 Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato</td>
<td>Efterretnings- og sikkerhedsopgaver til beskyttelse af den demokratiske stat og dens institutioner. Oplysninger om aktiviteter i indlandet, der kan bringe sikkerheden i fare, kontraspionage, foranstaltninger til bekæmpelse af terrorisme og organiseret kriminalitet.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Land</td>
<td>Efterretningstjeneste</td>
<td>Retsgrundlag</td>
<td>Opgaver</td>
<td>SIGINT-kapacitet</td>
<td>Kontrolmyndighed</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>LUXEMBOURG</td>
<td>Service de renseignement</td>
<td>Loi concernant la protection des secrets intéressant la sécurité extérieure de l'État af 30. juli 1960.</td>
<td>Sikring af fortroligheden som omhandlet i straffelovens art. 120, litra g* og indhentning af de oplysninger, som er nødvendige til bevarelse af den ydre sikkerhed, hvad angår Storhertugdømmet Luxembourg og de stater, med hvilke der er indgået en regional aftale om et fælles forsvar. * &quot;Anslag imod Storhertugdømmet Luxembourg&quot;</td>
<td>Ingen parlamentarisk kontrol. (Oversvægningen af alle former for kommunikation med henblik på at afsløre anslag imod statens sikkerhed skal godkendes af et udvalg sammensat af præsidenten for højesteret, formanden for Statsrådets retsudvalg og formanden for statsrevisionen)</td>
<td></td>
</tr>
<tr>
<td>Land</td>
<td>Efterretnings-tjeneste</td>
<td>Retsgrundlag</td>
<td>Opgaver</td>
<td>SIGINT-kapacitet</td>
<td>Kontrolmyndighed</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>------------------</td>
</tr>
<tr>
<td>HOLLAND</td>
<td>Binnenlandse Veiligheidsdienst (BVD eller efter de seneste ændringer: AIVD)</td>
<td>[I øjeblikket er en helt ny lov til behandling]</td>
<td>Intern sikkerhedsstjeneste, bekæmpelse af højre- og venstrekstremisme, kontraspionage.</td>
<td></td>
<td>Parlamentsudvalg (4 medlemmer: formændene for de 4 største partier)</td>
</tr>
</tbody>
</table>

17. oktober 2021, Kj. Ger. 1
"Andre etablering af efterretningsst..."
<table>
<thead>
<tr>
<th>Land</th>
<th>Efterretnings-tjeneste</th>
<th>Retsgrundlag</th>
<th>Opgaver</th>
<th>SIGINT-kapacitet</th>
<th>Kontrolmyndighed</th>
</tr>
</thead>
<tbody>
<tr>
<td>PORTUGAL</td>
<td>Serviço de Informações de Segurança (SIS)</td>
<td></td>
<td>Sikkerhedsstjeneste for indre anliggender, efterretningsstjeneste (ingen eksekutive beføjelser), indsamling og evaluering af oplysninger om kriminelle og statsfjendtlige aktiviteter.</td>
<td></td>
<td>Assembleia República kan indkalde direktørerne for både SIS og SIEDM for et parlamentsudvalg.</td>
</tr>
</tbody>
</table>

PE 305.391 176/190 RR\445698DA.doc
<table>
<thead>
<tr>
<th>Land</th>
<th>Efterretnings-tjeneste</th>
<th>Retsgrundlag</th>
<th>Opgaver</th>
<th>SIGINT-kapacitet</th>
<th>Kontrolmyndighed</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPANIEN</td>
<td>Dirección General de la Guardia Civil (GC)</td>
<td>L.Org. 2/1986 de 13.03.1986 (BOE 14.03.1986) de Fuerzas y cuerpos de seguridad</td>
<td>Central spansk paramilitær politimyndighed omfattende politiets efterretningsstjeneste; bekæmpelse af organisef kriminalitet på spansk territorium.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPANIEN</td>
<td>Dirección General de la Policia</td>
<td></td>
<td>Central spansk politimyndighed omfattende politiets efterretningsstjeneste; intern og ekstern sikkerhedsstjeneste, overvågning af terrorisme og islaisk fundamentalisme i Mellemøsten og Nordafrika.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Land</td>
<td>Efterretnings-tjeneste</td>
<td>Retsgrundlag</td>
<td>Opgaver</td>
<td>SIGINT-kapacitet</td>
<td>Kontrolmyndighed</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>SVERIGE</td>
<td>Försvarets Radioanstalt (FRA)</td>
<td>Uafhængig enhed</td>
<td>Militær og ikke-militær etterretningsvirksomhed, dekryptering af kommunikation,</td>
<td>ja</td>
<td></td>
</tr>
<tr>
<td>Land</td>
<td>Efterretningstjeneste</td>
<td>Retsgrundlag</td>
<td>Opgaver</td>
<td>SIGINT-kapacitet</td>
<td>Kontrolmyndighed</td>
</tr>
<tr>
<td>------</td>
<td>----------------------</td>
<td>--------------</td>
<td>---------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>(radiostation)</td>
<td></td>
<td>radarovervågning.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Land</td>
<td>Efterretnings-tjeneste</td>
<td>Retsgrundlag</td>
<td>Opgaver</td>
<td>SIGINT-kapacitet</td>
<td>Kontrolmyndighed</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DET FORENEDE KONGE-RIGE</td>
<td>Government’s Communication Headquarters (GCHQ)</td>
<td></td>
<td>Udlanadspionage/efterretningsvirksomhed i udlandet; SIGINT på det politiske, økonomisk/videnskabelige og militære område.</td>
<td>ja</td>
<td>The Security Service Commissioner udnævnes af premierministeren, nuværende eller tidligere højtstående dommer.</td>
</tr>
<tr>
<td></td>
<td>Sorterer under udenrigsministeren.</td>
<td></td>
<td></td>
<td></td>
<td>The Investigatory Powers Tribunal</td>
</tr>
<tr>
<td></td>
<td>Secret Intelligence Service (SIS) = MI6</td>
<td>Intelligence Services Act 1994</td>
<td>Indsamling af oplysninger om efterretningsvirksomhed og politiske forhold i udlandet.</td>
<td></td>
<td>The Intelligence and Security Committee (ISC) Udvælget består af 9 medlemmer (Underhuset + Overhuset, ingen ministre), der udnævnes af premierministeren.</td>
</tr>
<tr>
<td></td>
<td>Sorterer under udenrigsministeren.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sorterer under indenrigsministeren.</td>
<td></td>
<td></td>
<td></td>
<td>The Intelligence and Security Committee</td>
</tr>
</tbody>
</table>

PE 305.391  180/190  RR\445698DA.doc
<table>
<thead>
<tr>
<th>Land</th>
<th>Efterretningstjeneste</th>
<th>Retsgrundlag</th>
<th>Opgaver</th>
<th>SIGINT-kapacitet</th>
<th>Kontrolmyndighed</th>
</tr>
</thead>
<tbody>
<tr>
<td>DET FORENEDE KONGERIGE</td>
<td>Defense Intelligence Staff (DIS)</td>
<td>Sorterer under forsvarsministeren.</td>
<td>Understøttelse af den militære sikkerhed, evaluering og analyse af militære, politiske, teknisk/videnskabelige og udvalgte økonomiske oplysninger.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Land</td>
<td>Efterretnings-tjeneste</td>
<td>Retsgrundlag</td>
<td>Opgaver</td>
<td>SIGINT-kapacitet</td>
<td>Kontrolmyndighed</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------</td>
<td>--------------</td>
<td>---------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>USA</td>
<td>Central Intelligence Agency (CIA)</td>
<td>National Security Act 1947</td>
<td>International indsamling af efterretnings-informationer, kontraspionage i udlandet, centralt ansvar for al efterretningsvirksomhed i USA.</td>
<td>Senate: Senate Select Committee on Intelligence (SSCI)</td>
<td>House of Representatives: House Permanent Select Committee on Intelligence (HPSCI)</td>
</tr>
<tr>
<td>Land</td>
<td>Efterretnings-tjeneste</td>
<td>Retsgrundlag</td>
<td>Opgaver</td>
<td>SIGINT-kapacitet</td>
<td>Kontrolmyndighed</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>USA</td>
<td>National Security Agency (NSA)</td>
<td>Executive Order 12333 of 4 December 1981.</td>
<td>Ansvarlig for sikkerheden i forbindelse med USA's informationssystemer, særlig for kryptering. Ansvarlig for kommunikationsaflytning i udlandet.</td>
<td>ja</td>
<td>Senate Select Committee on Intelligence (SSCI)</td>
</tr>
<tr>
<td>USA</td>
<td>National Reconnaissance Office (NRO)</td>
<td></td>
<td>Ansvarlig for udvikling og anvendelse af spionagesatellit-systemer (SIGINT).</td>
<td></td>
<td>Senate Select Committee on Intelligence (SSCI)</td>
</tr>
<tr>
<td>Land</td>
<td>Efterretnings-tjeneste</td>
<td>Retsgrundlag</td>
<td>Opgaver</td>
<td>SIGINT-kapacitet</td>
<td>Kontrolmyndighed</td>
</tr>
<tr>
<td>------</td>
<td>------------------------</td>
<td>--------------</td>
<td>---------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>USA</td>
<td>US Army Intelligence (f. eks. Deputy Chief of Staff for Intelligence, Intelligence and Security Command (INSCOM))</td>
<td>Executive Order 12333 (4. december 1981)</td>
<td>Indsamling og analyse af oplysninger på det militære område, udvikling af koncepter og systemer for militær efterretnings-virksomhed og elektronisk krigsførelse.</td>
<td>ja</td>
<td>Senate Select Committee on Intelligence (SSCI) House Permanent Select Committee on Intelligence (HPSCI)</td>
</tr>
<tr>
<td>USA</td>
<td>Marine Corps Intelligence Activity (MCIA) National Maritime Intelligence Center (NMIC)</td>
<td>Executive Order 12333 (4. december 1981)</td>
<td>Efterretnings-virksomhed for flåden, militær efterretnings-virksomhed og udvikling af kryptering og elektroniske hjælpeudstyr til krigsførelse.</td>
<td>ja</td>
<td>Senate Select Committee on Intelligence (SSCI) House Permanent Select Committee on Intelligence (HPSCI)</td>
</tr>
<tr>
<td>USA</td>
<td>Office of Naval Intelligence (ONI)</td>
<td>Executive Order 12333 (4. december 1981)</td>
<td>Efterretnings-virksomhed for flådespørgsmål og maritime spørgsmål, analyse af fremmede flåder, system til indsamling og overvågning af data vedrørende havene, undervandsplatforme og -våbensystemer.</td>
<td>ja</td>
<td>Senate Select Committee on Intelligence (SSCI) House Permanent Select Committee on Intelligence (HPSCI)</td>
</tr>
<tr>
<td>Land</td>
<td>Efterretnings-tjeneste</td>
<td>Retsgrundlag</td>
<td>Opgaver</td>
<td>SIGINT-kapacitet</td>
<td>Kontrolmyndighed</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------</td>
<td>--------------</td>
<td>---------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>USA</td>
<td>Air Intelligence Agency (AIA)</td>
<td><em>Executive Order 12333</em> (4. december 1981)</td>
<td>Efterretnings-virksomhed for luftvåbenet, militær efterretnings-virksomhed.</td>
<td>ja</td>
<td>Senate Select Committee on Intelligence (SSCI) House Permanent Select Committee on Intelligence (HPSCI)</td>
</tr>
<tr>
<td>USA</td>
<td>Federal Bureau of Investigation (FBI)</td>
<td><em>Title 28, United States Code (U.S. Code), Section 533</em> Grundlagt 1908. Navn siden 1935.</td>
<td>Kontraspionage, Forbundspolitiet.</td>
<td></td>
<td>Senate Select Committee on Intelligence (SSCI) House Permanent Select Committee on Intelligence (HPSCI)</td>
</tr>
<tr>
<td>USA</td>
<td>Drug Enforcement Administration</td>
<td><em>Executive Order</em> (1. juli 1973)</td>
<td>Indsamling af oplysninger om narkotika og hvidvaskning af penge i ind- og udland.</td>
<td></td>
<td>Senate Select Committee on Intelligence (SSCI) House Permanent Select Committee on Intelligence (HPSCI)</td>
</tr>
<tr>
<td>Land</td>
<td>Efterretnings-tjeneste</td>
<td>Retsgrundlag</td>
<td>Opgaver</td>
<td>SIGINT-kapacitet</td>
<td>Kontrolmyndighed</td>
</tr>
<tr>
<td>------</td>
<td>------------------------</td>
<td>--------------</td>
<td>---------</td>
<td>------------------</td>
<td>-----------------</td>
</tr>
</tbody>
</table>
| CANADA | Communication Security Establishment (CSE)  
Støttet af Canadian Forces Supplementary Radio System (CFSRS) | Det formelle mandat er fortroligt, sandsynligvis godkendt af regeringen. | Rådgivning af regering og erhvervsliv i sikkerhedspørgsmål i forbindelse med datatransmission og – behandling (Infosec), udvikling af krypteringssystemer. | ja | Intet uafhængigt kontrolorgan (kun kontrol ved rigsdagesrevisor og forsvarsministeren, der er ansvarlig over for Parlamentet). |
| CANADA | Canadian Security Intelligence Service (CSIS)  
Sorterer under indenrigsministeren. | Canadian Security Intelligence Service Act (CSIS Act) fra 1984 | Kontraspionage, bekæmpelse af sabotage og international terrorisme på landets territorium. | | The Security Intelligence Review Committee (SIRC)  
Uafhængigt organ bestående af 5 medlemmer, som ikke er parlaments-medlemmer. |
| CANADA | Director General Intelligence Division  
(Under Deputy Chief of the Defence Staff)  
Sorterer under forsvarsministeren. | | Militær efterretnings-virksomhed. | | |
<table>
<thead>
<tr>
<th>Land</th>
<th>Efterretnings-tjeneste</th>
<th>Retsgrundlag</th>
<th>Opgaver</th>
<th>SIGINT-kapacitet</th>
<th>Kontrolmyndighed</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUSTRALIEN</td>
<td>Defence Signals Directorate (DSD)</td>
<td></td>
<td>Indsamling og udbredelse af signaloplysninger. Tilvejebringelse af produkter til bevarelse af informations-sikkerheden (Infosec) for regering og militær.</td>
<td>Inspector General of Intelligence and Security (IGIS) (Udnævnt af premierministeren)</td>
<td>Inspector General of Intelligence and Security (IGIS)</td>
</tr>
<tr>
<td></td>
<td>Sorterer under forsvarsministeren.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUSTRALIEN</td>
<td>Defence Intelligence Organisation (DIO)</td>
<td></td>
<td>Indsamling og evaluering af strategiske og militære oplysninger og efterretningsmateriale.</td>
<td>Inspector-General of Intelligence and Security (IGIS)</td>
<td>Inspector-General of Intelligence and Security (IGIS)</td>
</tr>
<tr>
<td></td>
<td>Sorterer under forsvarsministeren.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AUSTRALIEN</td>
<td>Australian Secret Intelligence Service (ASIS)</td>
<td></td>
<td>Indsamling af oplysninger om udlandet, særlig Sydøstasien, af interesse for den nationale sikkerhed, økonomien og de eksterne forbindelser.</td>
<td>Inspector-General of Intelligence and Security (IGIS)</td>
<td>Inspector-General of Intelligence and Security (IGIS)</td>
</tr>
<tr>
<td></td>
<td>Ekstern efterretningsstjeneste.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sorterer under udenrigsministeren.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

RR\445698DA.doc 187/190 PE 305.391 DA
<table>
<thead>
<tr>
<th>Land</th>
<th>Efterretningstjeneste</th>
<th>Retsgrundlag</th>
<th>Opgaver</th>
<th>SIGINT-kapacitet</th>
<th>Kontrolmyndighed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Land</td>
<td>Efterretnings-tjeneste</td>
<td>Retsgrundlag</td>
<td>Opgaver</td>
<td>SIGINT-kapacitet</td>
<td>Kontrolmyndighed</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>Sorterer under premierministeren.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indenlandsk efterretningsstjeneste</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sorterer under premierministeren.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NEW ZEALAND</td>
<td>External Assessments Bureau (EAB)</td>
<td></td>
<td>Analyse af den politiske udvikling og udarbejdelse af rapporter om politiske og økonomiske forhold og tendenser.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ekstern efterretningsstjeneste</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sorterer under premierministeren.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Militær efterretningsstjeneste</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Land</td>
<td>Efterretningstjeneste</td>
<td>Retsgrundlag</td>
<td>Opgaver</td>
<td>SIGINT-kapacitet</td>
<td>Kontrolmyndighed</td>
</tr>
<tr>
<td>------</td>
<td>---------------------</td>
<td>-------------</td>
<td>---------</td>
<td>------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td></td>
<td>Sorterer under forsvarsministeren.</td>
<td></td>
<td>strategiske oplysninger.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>