EUROPAPARLAMENTET

1999 *2004*

Tillfälligt utskott för avlyssningssystemet Echelon

DEFINITIVT FÖRSLAG

Den 18 maj 2001

FÖRSLAG TILL BETÄNKANDE

om förekomsten av ett globalt avlyssningssystem för kommunikation från privatpersoner och företag (avlyssningssystemet ECHELON)

Tillfälligt utskott för avlyssningssystemet Echelon

Föredragande Gerhard Schmid

INNEHÅLL

Sida

7. Förenligheten av ett kommunikationsavlyssningssystem av typen "ECHELON" med unionsrätt 61

BESKRIVNING AV ÄRENDETS GÅNG

Vid sitt sammanträde den 5 juli 2000 beslutade Europaparlamentet tillsätta ett tillfälligt utskott för avlyssningssystemet Echelon. För att uppfylla sitt mandat utsåg det tillfälliga utskottet vid sitt konstituerande sammanträde den 5 juli 2000 Gerhard Schmid till föredragande.

Utskottet granskade förslaget till betänkande vid sitt/sina sammanträde/n den ….

Vid detta sammanträde/det sista av dessa sammanträden antog utskottet förslaget till beslutstext med röstsiffrorna …. för och … mot, samt … nedlagda röster/enhälligt.

Vid röstningen deltog följande: …, ordförande/tjänstgörande ordförande; … och … vice ordföranden; … föredragande; …, … (som ersättare för …), … (som ersättare för … enligt artikel 153 punkt 2 i stadgarna), … samt ….

Betänkandet ingavs den ….

Fristen för inlämnande av ändringsförslag anges i utkastet till föredragningslista för den session när betänkandet skall prövas/prövades till …. klockan ….

FÖRSLAG TILL BESLUT

Beslut i Europaparlamentet i frågan om förekomsten av ett globalt avlyssningssystem för kommunikation från privatpersoner och företag (avlyssningssystemet ECHELON)

Europaparlamentet (EP) har beaktat följande:

– Europaparlamentets beslut den 5 juli 2000 att tillsätta ett tillfälligt utskott för avlyssningssystemet Echelon och fastställa dettas mandat;

– EG-fördraget, som syftar till bildandet av en gemensam marknad med hög konkurrensförmåga;

– EU-fördraget, särskilt dess artikel 6, punkt 2, som fastlägger EU:s skyldighet att skydda de grundläggande rättigheterna, och dess del V, som gäller bestämmelser om en gemensam utrikes- och säkerhetspolitik;

– EU:s stadga om de grundläggande rättigheterna, där artikel 7 föreskriver skydd för privat- och familjelivet, och uttryckligen föreskriver rätten till skydd för kommunikation;

– den europeiska konventionen om mänskliga rättigheter, särskilt dess artikel 8, som skyddar den privata sfären, samt de många andra internationella fördrag som föreskriver skydd för den privata sfären;

– innehållet i betänkandet om förekomsten av ett globalt avlyssningssystem för kommunikation från privatpersoner och företag (avlyssningssystemet Echelon), som avgivits av det tillfälliga utskottet för avlyssningssystemet Echelon (A5-…/2001);

i fråga om förekomsten av ett globalt avlyssningssystem för kommunikation från privatpersoner och företag (avlyssningssystemet ECHELON)

A. det kan inte längre betvivlas att det finns ett världsomspännande system för avlyssning av kommunikation, som bedrivs i samverkan mellan USA, Storbritannien, Kanada, Australien och Nya Zeeland, inom ramen för UKUSA-avtalet;det förefaller enligt de indicier som föreligger sannolikt att systemets kodnamn verkligen är ECHELON, vilket dock har mindre betydelse;

B. systemet tjänar inte syftet att avlyssna militär trafik utan trafik från privatpersoner och företag, medan den analys som genomförts enligt betänkandet har visat att systemets möjligheter inte alls är så stora som delvis antagits i massmedia;

i fråga om avlyssningssystemets begränsningar

C. avlyssningssystemet baseras på global avlyssning av trafik via kommunikationssatelliter; kommunikation inom områden med hög kommunikationstäthet förmedlas dock endast av satelliter i mycket liten utsträckning, varför alltså en dominerande del av kommunikationen inte kan avlyssninas i satellitföljarstationer, utan bara genom inkoppling på kablar respektive uppfångning av radiosignaler. vilket – så som visats genom de analyser som redovisas i betänkandet – bara kan ske inom mycket snäva gränser; tillgången på personal för den slutliga analysen av avlyssnad kommunikation utgör ytterligare en begränsning, varför

ECHELON-staterna bara har tillgång till en liten del av den kabel- och radioburna trafiken och bara kan analysera en liten del av trafiken;

i fråga om förekomsten av andra avlyssningssystem

D. avlyssning av kommunikation är en vanlig metod för underrättelsetjänsternas verksamhet och ett sådant system skulle kunna drivas också av andra stater, om de har ekonomiska resurser och geografiska förutsättningar för detta; Frankrike – åtminstone vad gäller geografiska förutsättningar – skulle tack vare sina territorier på andra sidan havet som enda EU-stat ensam kunna upprätta ett globalt avlyssningssystem, och det finns därutöver indikationer på att även Ryssland skulle kunna driva ett sådant system;

i fråga om förenligheten med EU:s lagstiftning

E. i fråga om hur ett system av typ ECHELON kan förenas med EU:s lagstiftning måste man skilja på två olika fall: Om systemet endast används i underrättelsesyfte, så är systemet inte oförenligt med EU:s lagstiftning, eftersom EG-fördraget inte berör verksamhet inom staternas säkerhetstjänster, vilken verksamhet faller under del V i EU-fördraget (GASP), där det för närvarande dock inte finns några motsvarande bestämmelser och inga beröringspunkter. Om systemet däremot missbrukas för företagsspionage så står det i motsatsställning till kravet på lojalitet mellan medlemsstaterna och till tanken med en gemensam marknad med fri konkurrens, vilket skulle innebära att en medlemsstat som bedriver sådan verksamhet skulle bryta mot EU-rätten.

i fråga om förenlighet med de grundläggande rättigheterna gällande den privata sfären (artikel 8 i Europakonventionen)

F. varje avlyssning av kommunikation är ett starkt intrång på den enskilda människans privata sfär; artikel 8 i Europakonventionen, som föreskriver skydd för den privata sfären, medger bara intrång för att skydda den nationella säkerheten, förutsatt att bestämmelser finns fastlagda i nationell lagstiftning och är allmänt tillgängliga, och föreskriver under vilka förhållanden och villkor som staten får göra sådana intrång; intrång därutöver måste vara rimliga och en sammanvägning av olika intressen alltså ske, och det är enligt rättspraxis i Europadomstolen inte tillräckligt att verksamheten är ”nyttig eller önskvärd”.

G. ett underrättelsesystem, som utan beaktande av principen om rimlighet skulle avlyssna all kommunikation, skulle inte vara förenlig med Europakonventionen, och det skulle likaledes vara ett brott mot Europakonventionen om den bestämmelse, enligt vilken kommunikationsavlyssningen bedrivs, inte har någon rättslig grund, om bestämmelsen inte allmänt tillgänglig eller är så formulerad att dess följder för den enskilde inte är förutsebara; de bestämmelser enligt vilka den amerikanska underrättelsetjänsten är verksam utomlands i är stor utsträckning sekretessbelagda och tillämpningen av rimlighetsprincipen kan sålunda åtminstone ifrågasättas och är ett brott mot de av Europadomstolen fastlagda principerna om lagstiftningens allmänna tillgänglighet och förutsebarhet;

H. medlemsstaterna kan inte undandra sig de skyldigheter som baseras på Europakonventionen genom att de låter andra länders underrättelsetjänster vara verksamma på sitt territorium, vilka är underkastade mindre stränga bestämmelser, eftersom detta skulle undergräva innehållet i Europadomstolens tidigare rättspraxis och beröva legalitetsprincipen med dess båda komponenter om tillgänglighet och förutsebarhet dess effekt;

I. en underrättelsetjänst måste för att vara rättsligt legitim i relation till de grundläggande

rättigheterna också vara underställd ett fungerande kontrollsystem, för att kompensera för den risk som uppkommer när en del av en förvaltning arbetar i hemlighet; Europadomstolen har uttryckligen framhävt vikten av ett fungerande kontrollsystem för underrättelsetjänsternas verksamhet och det synes därför betänkligt att några medlemsstater inte har några egna parlamentariska kontrollorgan för säkerhetstjänsten;

i fråga om huruvida EU-medborgarna är tillräckligt skyddade mot underrättelsetjänsterna

J. skyddet för EU-medborgarna är avhängigt den nationella lagstiftningen i medlemsstaterna, som är mycket varierande inom EU och det delvis helt saknas parlamentariska kontrollorgan och därmed knappast kan vara tal om ett tillräckligt skydd; de europeiska medborgarna har ett grundläggande intersse av att deras respektive nationella parlament är utrustat med ett formellt strukturerat särskilt kontrollorgan, som övervakar och kontrollerar underrättelsetjänstens verksamhet; i de fall när kontrollorgan finns föreligger också en stark tendens till att mer bekymra sig om den nationella säkerhetstjänstens verksamhet än om den internationellt riktade underrättelsetjänstens, eftersom det i regel endast är den förstnämnda som berör de egna medborgarna;

K. om underrättelsetjänster skulle samarbeta inom ramen för GASP skulle av institutionerna krävas att de åstadkommer tillräckliga skyddsbestämmelser för de europeiska medborgarna;

i fråga om företagsspionage

L. det ingår i underrättelsetjänsternas uppgifter att intressera sig för underrättelser från näringslivet, såsom branschutveckling, utvecklingen på råvarumarknaderna, respekten för handelsembargon, respekten för leverantörsreglerna i fråga om Dual Use-varor mm, vilket ofta medför att företag som berörs av sådana frågor övervakas;

M. det kan åtminstone inte tolereras att underrättelsetjänsterna blir verktyg för konkurrensspionage, så att de spionerar på utländska företag för att ge inhemska företag en konkurrensfördel; det finns dock inte några fall belagda där det globala avlyssningssystemet används för detta, även om det har påstått s i flera fall;

N. känsliga företagsdata förekommer i stor utsträckning inom företagen själva, vilket innebär att konkurrensspionage i första hand bedrivs genom att man försöker få information från medarbetare i företagen eller insmugglade personer, eller försöker tränga in i företagens interna datanät; det bara är i de fall när känsliga data hamnar utanför företaget via ledningar eller radiosignaler (satelliter) som ett kommunikationsövervakningssystem kan användas för konkurrensspionage, och detta förekommer systematiskt bara i följande tre fall:
   - hos företag som arbetar i tre tidszoner, så att underhandsresultat i verksamheten skickas från Europa till Amerika och därifrån vidare till Asien;
   - när videokonferenser äger rum i multinationella koncerner, och förmedlas av VSAT eller kabel;
   - när viktiga beställningar diskuteras på platsen (som vid stora byggprojekt, uppbyggnad av teleinfrastruktur, nya transportsystem, osv) och kontakter därifrån måste tas med huvudkontoret;

i fråga om möjligheterna att skydda sig själv

O. säkerhet för företagen kan bara uppnås om hela arbetsmiljön säkras tillsammans med alla kommunikationsvägar som kan ifrågakomma för överföring av känslig information; det finns tillräckligt säkra krypteringssystem till överkomliga priser på den europeiska marknaden;

även privatpersoner bör uppmanas att kryptera sin e-postmeddelanden; ett okrypterat e-postmeddelande är som ett brev utan kuvert; det finns på Internet relativt användarvänliga system som rentav ställs till förfogande för privat bruk utan kostnad;

i fråga om samarbete mellan underrättelsetjänster inom EU

P. EU har kommit överens om att samordna underrättelsetjänsternas informationsinsamling inom ramen för den egna säkerhets- och försvarspolitiken, utan att detta innebär att samarbete med andra partners på detta område skall upphöra;

Q. ett samarbete mellan underrättelsetjänsterna inom EU förefaller också önskvärt med tanke på dels att det vore absurt att försöka bedriva en gemensam säkerhetspolitik utan att säkerhetstjänsterna medverkade, dels att det finns flera fördelar med ett sådant samarbete ur professionell, finansiell och politisk synvinkel; det skulle också i högre grad motsvara tanken på att vara en likaberättigad partner till USA och skulle medföra att samtliga medlemsstater ingick i ett system som garanterar full konformitet med Europakonventionen; en motsvarande kontroll av samarbetet via Europaparlamentet måste naturligtvis säkerställas;

R. Europaparlamentet står i begrepp att etablera egna bestämmelser om tillgång till sekretessbelagda och känsliga upplysningar och handlingar;

varför Europaparlamentet

i fråga om avslutande och ändring av internationella avtal för skydd av medborgare och företag

1. uppmanar generalsekreteraren i Europarådet att föreslå ministerrådet genomföra en utredning av huruvida det vore meningsfullt att anpassa det skydd för privatsfären som garanteras i Europakonventionens artikel 8 till de moderna kommunikationsmetoderna och avlyssningsmöjligheterna i ett tilläggsprotokoll, eller i kombination med en reglering av dataskyddet i samband med en revidering av konventionen om dataskydd, under förutsättning att detta varken skulle innebära en minskning av den rättsliga skyddsnivå som domstolen etablerat eller en inskränkning av den flexibilitet som krävs för anpassning till den fortsatta utvecklingen;

2. uppmanar medlemsstaterna att upprätta en europeisk plattform för att granska den lagstiftning som skyddar brev- och telefonhemligheten, att i detta syfte komma överens om en gemensam text som skyddar den privata sfären, så som denna definieras i artikel 7 i EU:s stadga om de grundläggande rättigheterna, för alla europeiska medborgare inom medlemsstaternas territorier och därutanför, samtidigt som underrättelsetjänsternas verksamhet sker i enlighet med dessa rättigheter och uppfyller de villkor som härletts ur Europakonventionens artikel 8 och som presenteras i kapitel 8 i betänkandet, särskilt punkt 8.3.4;

3. uppmanar medlemsstaterna i Europarådet att fatta beslut om ett tilläggsprotokoll som gör det möjligt för de europeiska gemenskaperna att ansluta sig till Europakonventionen, eller överväga andra åtgärder för att komma till rätta med konflikten mellan den rättspraxis som tillämpas i domstolen i Strassbourg och den som tillämpas i domstolen i Luxembourg.

4. uppmanar FN:s generalsekreterare att ge det ansvariga utskottet i uppdrag att lägga fram förslag till beslut som syftar till att anpassa artikel 17 i det internationella fördraget om medborgerliga och politiska rättigheter till de tekniska förändringarna, så att den privata sfären garanteras ett skydd;

5. uppmanar USA att underteckna tilläggsprotokollet till det internationella fördraget om medborgerliga och politiska rättigheter, så att det skulle bli möjligt för enskilda personer att anföra besvär mot USA under hänvisning till brott mot fördraget inför det konventionella utskottet för mänskliga rättigheter; berörda amerikanska icke-statliga organisationer, särskilt ACLU (American Civil Liberties Union) och EPIC (Electronic Privacy Information Center), uppmanas att utöva tryck i denna riktning på den amerikanska regeringen;

i fråga om nationella lagstiftningsåtgärder till skydd för medborgare och företag

6. uppmanar medlemsstaterna att kontrollera sin egen lagstiftning i fråga om underrättelsetjänstens verksamhet med avseende på dess överensstämmelse med de grundläggande rättigheterna;

7. uppmanar medlemsstaterna att sträva mot en gemensam skyddsnivå gentemot underrättelsetjänsternas verksamhet, med en orientering mot det starkaste skydd som förekommer bland medlemsstaterna, eftersom de medborgare som berörs av en underrättelsetjänsts verksamhet i regel tillhör någon annan stat och därmed de övriga medlemsstaterna;

8. uppmanar EU:s institutioner att åstadkomma tillräckliga skyddsbestämmelser för de europeiska medborgarna för det fall att underrättelsetjänster skulle samarbeta inom ramen för GASP; Europaparlamentet som logiskt kontrollorgan måste i sin tur åstadkomma de nödvändiga förutsättningarna för övervakning på detta mycket känsliga område, så att det blir realistiskt och också ansvarsfullt att begära att få den nödvändiga kontrollrätten;

i fråga om särskilda lagstiftningsåtgärder för att bekämpa företagsspionage

9. uppmanar medlemsstater att genomföra diskussioner om i vilken utsträckning företagsspionage och korruption för att vinna beställningar kan bekämpas med bestämmelser i europeisk och internationell lag, särskilt om det vore möjligt att införa bestämmelser inom ramen för WTO, som skulle ta hänsyn till den konkurrensstörande effekten av sådan verksamhet, exempelvis genom att föreskriva att sådana kontrakt bleve ogiltiga;

10. uppmanar medlemsstaterna att i ett gemensamt entydigt uttalande själva förbinda sig att inte bedriva företagsspionage riktat mot varandra, och därmed ge uttryck för sin samstämmighet med EU-fördragets anda och bestämmelser;

i fråga om lagstiftningsåtgärder och kontroll av dessa

11. uppmanar de nationella parlament som inte har egna parlamentariska kontrollorgan för övervakning av underrättelsetjänsten att upprätta sådana;

12. uppmanar de nationella kontrollorgan som övervakar säkerhetstjänsterna att vid utövandet av sina kontrollbefogenheter lägga stor vikt vid skyddet av den privata sfären, oberoende av om det är de egna medborgarna, andra EU-medborgare eller medborgare utanför EU som berörs;

13. uppmanar Tyskland och Storbritannien att ställa som villkor för fortsatt medgivande till USA:s underrättelsetjänst att avlyssna kommunikation på sitt territorium kräva att denna avlyssning sker i samstämmighet med Europakonventionen, dvs att de uppfyller principen om rimlighet, att lagstiftningen är tillgänglig och dess effekter är förutsebar för den enskilde, samt att en motsvarande fungerande kontroll finns, eftersom de är ansvariga för att den underrättelseverksamhet som bedrivs på deras territorium med deras godkännande eller

åtminstone utan deras fördömande inte inskränker de grundläggande rättigheterna;

i fråga om åtgärder för att främja medborgarnas och företagens egenskydd

14. uppmanar kommissionen och medlemsstaterna att utveckla program som främjar medborgarnas och företagens medvetenhet om säkerhetsproblematiken, samtidigt som de ger praktisk hjälp för att ta fram och tillämpa omfattande skyddskoncept;

15. uppmanar kommissionen och medlemsstaterna att vidta lämpliga åtgärder för att främja, utveckla och tillskapa europeisk krypteringsteknologi och krypteringsprogramvara, och framför allt att stödja projekt som syftar till att utveckla användarvänliga krypteringsprogram med öppen källkod;

16. uppmanar kommissionen och medlemsstaterna att främja sådana programvaruprojekt som arbetar med öppen källkod, eftersom detta är enda garantin för att programvaran inte har några inbyggda ”back doors” (s k ”open-source software);

17. uppmanar de europeiska institutionerna och medlemsstaternas offentliga förvaltningsorgan att systematiskt använda sig av kryptering av e-postmeddelanden, för att på lång sikt nå därhän att kryptering blir det normala förfarandet;

i fråga om övriga åtgärder

18. uppmanar företagen att samarbeta närmare med kontraspionaget, särskilt att meddela dess organ om attacker utifrån i syfte att bedriva företagsspionage, för att därmed höja dessa organs effektivitet;

19. uppmanar kommissionen att lägga fram ett förslag till inrättandet av ett europeiskt rådgivande organ i frågor om företagsinformationssäkerhet, som utöver en ökning av medvetenheten om problemet också kan ge praktisk hjälp;

20. bedömer det som meningsfullt att organisera en alleuropeisk kongress för skydd för den privata sfären mot telekomavlyssning, i syfte att bereda en plattform för icke-statliga organisationer i Europa, USA och i andra länder, där gränsöverskridande och internationella aspekter diskuteras och verksamhetsområden och metoder kan samordnas;

21. uppdrar åt sin ordförande att lägga fram detta beslut inför rådet, kommissionen, medlemsstaternas regeringar och parlament, de stater som ansökt om medlemskap samt Europarådet.

MOTIVERING

1. Inledning:

1.1. Bakgrund till tillsättandet av utskottet

Den 5 juli 2000 beslutade Europaparlamentet att tillsätta ett tillfälligt utskott för ECHELON-systemet. Den utlösande faktorn var debatten med anledning av den studie STOA [1] beställt om det så kallade ECHELON-systemet [2], som författaren Duncan Campbell presenterat i samband med en utfrågning i utskottet för medborgerliga fri- och rättigheter, rättsväsen och inre angelägenheter, under temat "EU och datasäkerhet".

1.2. Utsagor i de båda STOA-studierna om ett globalt avlyssningssystem med täcknamnet ECHELON

1.2.1. Den första STOA-rapporten från 1997

I en rapport[3] som STOA beställt för Europaparlamentet 1997 under rubriken "Analys av teknik för politisk kontroll" från Omega Foundation, beskrevs ECHELON i kapitlet "Nationella och internationella nätverk för kommunikationsövervakning". Den person som skrivit rapporten hävdade att samtliga kommunikationer inom Europa via e-mail, telefon och fax rutinmässigt avlyssnades av NSA (den amerikanska underrättelsetjänsten) [4] Genom denna rapport blev ECHELON känt i Europa som ett heltäckande globalt avlyssningssystem.

1.2.2. STOA-rapporterna från 1999

För att få höra mer om detta temaområde utlämnade STOA 1999 ett uppdrag om en femdelad studie, som skulle gälla "Övervakningsteknikens utveckling och riskerna för missbruk av företagsinformation". Band 2/5, som författats av Duncan Campbell, gällde de dåvarande underrättelsemässiga kapaciteterna, särskilt hur systemet ECHELON fungerade [5]

Särskild uppmärksamhet väckte utsagan i rapporten att ECHELON övergått från att utnyttjas för sitt ursprungliga ändamål, alltså försvar mot östländerna, till att användas för företagsspionage. Denna tes stöds i rapporten av exempel på uppgifter om företagsspionage; bland andra Airbus och Thomson CFS skall ha lidit uttalad skada av detta.

---

[1] STOA (Scientific and Technological Options Assessment) är en avdelning under generaldirektionen för vetenskap inom Europaparlamentet, som lämnar ut forskningsuppdrag.
[2] Lägesrapport gällande fjärravlyssning (COMINT) vid automatisk bearbetning i underrättelsesyfte av övervakade flerspråkiga kommersiella bredbandssystem och offentliga nät, samt användbarheten i fråga målbestämning för COMINT, inklusive språkigenkänning (oktober 1999).
[3] Scientific and Technological Options Assessment.
[4] Steve Wright, An appraisal of technologies for political control (1998), 20.
[5] Lägesrapport gällande avlyssning av kommunikation (COMINT) vid automatisk bearbetning i underrättelsesyfte av övervakade flerspråkiga kommersiella bredbandssystem och offentliga nät, samt användbarheten i fråga om målbestämning för COMINT, inklusive språkigenkänning (oktober 1999), PE 168.184.

STOA-studien ledde till att ECHELON diskuterades i nästan alla parlament i medlemsstaterna, och i Frankrike och Belgien skrevs till och med rapporter därom.

1.3. Utskottets mandat

Vid samma tidpunkt som Europaparlamentet beslutade tillsätta ett utskott med tidsbegränsat uppdrag fastställde man också dess mandat. Mandatet för det tillfälliga utskottet är följande:

"- att kontrollera huruvida systemet med beteckningen ECHELON för avlyssning av kommunikationer finns, enligt den verksamhetsbeskrivning av detta som återfinns i STOA-rapporten om utvecklingen av övervakningstekniken och riskerna för missbruk av företagsinformation;
- att analysera i vilken utsträckning ett sådant system är förenligt med gemenskapslagstiftningen, särskilt med artikel 286 i EU-fördraget och direktiven 94/56/EEG och 97/66/EEG, och med artikel 6, punkt 2 i EU-fördraget, med beaktande av följande frågeställningar:
  - Är unionsmedborgarnas rättigheter skyddade mot underrättelsetjänsters verksamhet?
  - Är kryptering ett rimligt och tillräckligt skydd för att garantera medborgarens privatsfär, eller bör ytterligare åtgärder vidtas, och i så fall vilka?
  - Hur kan EU:s organ tydligare göras uppmärksamma på riskerna med de aktuella verksamheterna, och vilka åtgärder kan vidtas?
- att fastställa huruvida näringslivet i Europa är utsatt för en risk genom den globala avlyssningen av information;
- att eventuellt lägga fram förslag till politiska och lagstiftningsmässiga initiativ."

1.4. Varför tillsätts inte ett utskott för utredning?

Europaparlamentet valde att tillsätta ett tillfälligt utskott därför att tillsättandet av ett utredningsutskott med den enda uppgiften att kontrollera om brott begås mot gemenskapslagstiftningen inom ramen för EG-fördraget (art. 193 EGF) skulle inskränka utskottets verksamhet till att endast behandla frågor som regleras i detta. Frågor som sorterar under delarna V (GASP) och VI i EUF (polisiärt och juridiskt samarbete om brottslighet) kan då inte behandlas. Dessutom omfattar enligt det interinstitutionella beslutet [1] de särskilda befogenheterna hos ett utredningsutskott endast krav på vittnesmål och tillgång till handlingar i de fall när inte detta strider mot krav på sekretess eller offentlig eller nationell säkerhet, vilket åtminstone utesluter instämning av säkerhetstjänster för vittnesmål. Ett utredningsutskott kan inte heller utvidga sin verksamhet till stater utanför EU, eftersom dessa definitionsmässigt inte kan bryta mot EU:s lagstiftning. Tillsättandet av ett utredningsutskott skulle sålunda bara inneburit en begränsning i fråga om innehåll utan någon utvidgning av befogenheter, varför detta alternativ avvisades av en majoritet av Europaparlamentets ledamöter.

1.5. Arbetsmetoder och arbetsplan

Utskottet har valt följande arbetssätt för att kunna utföra sitt mandat till fullo: I ett arbetsprogram, som föreslagits av rapportförfattaren och antagits av utskottet, upptogs följande relevanta ämnesområden: 1. Styrkta uppgifter om ECHELON. 2. Diskussion på nationell parlaments- och regeringsnivå. 3. Underrättelsetjänster och deras verksamhet. 4. Kommunikationssystem och möjligheten att avlyssna dessa. 5. Kryptering. 6. Företagsspionage.

[1] Beslut av Europaparlamentet, rådet och kommissionen av den 19 april 1995 gällande detaljerna i fråga om tillämpningen av Europaparlamentets undersökningsrätt (95/167/EEG), artikel 3, punkt 3 - 5.

7. Mål för spionage och skydd mot spionage. 8. Rättsliga ramvillkor och skydd för den privata sfären. Dessa ämnesområden behandlades i tur och ordning vid de enskilda sammanträdena. Ordningsföljden mellan ämnena har valts av praktiska skäl och avspeglar inte någon värdering av deras relativa vikt. Som förberedelse inför varje sammanträde gick rapportförfattaren systematiskt igenom och analyserade tillgängligt material. Till sammanträdena inbjöds sedan beroende på ämnet företrädare för de nationella förvaltningarna (särskilt säkerhetstjänsterna) och parlamenten i deras funktion som kontrollorgan för säkerhetstjänsterna, samt jurister och experter från högskolor och näringsliv inom kommunikations- och avlyssningsteknik, företagssäkerhet och krypteringsteknik. Vidare utfrågades journalister som arbetat med respektive ämne. Mestadels var sammanträdena offentliga, men i enstaka fall hölls slutna sammanträden, om detta bedömdes lämpligt för att gynna inhämtandet av information. Vidare har utskottets ordförande och rapportförfattaren gemensamt farit till London och Paris för att där träffa personer som av olika skäl inte kunnat medverka vid sammanträdena men vilkas medverkan i utskottsarbetet bedömts som värdefullt. Av samma skäl har utskottspresidiet, samordnarna och rapportförfattaren rest till USA. Dessutom har rapportförfattaren fört många enskilda samtal, delvis i förtroende.

1.6. Egenskaper som tillskrivs ECHELON-systemet

Det avlyssningssystem som betecknas ECHELON skiljer sig från annan underrättelseverksamhet däri att det har två egenskaper som gör det särpräglat:
För det första har systemet uppgetts kunna erbjuda samtidig heltäckande övervakning. Med hjälp av framför allt satellitföljande stationer och spionsatelliter skulle systemet kunna avlyssna varje meddelande som överfördes via telefon, telefax, Internet eller e-post, oavsett avsändare, och därmed ge kännedom om meddelandets innehåll.

För det andra hävdas att ECHELON blir ett kraftfullare system genom att flera länder runt om i världen samverkar om systemet (Storbritannien, USA, Kanada, Australien och Nya Zeeland). De stater som medverkar i ECHELON (ECHELON-staterna) kan ställa sina avlyssningsresurser till varandras förfogande och dela den ökade kostnaden och den utvunna informationen. Denna internationella samverkan är nödvändig, särskilt för en världsomspännande övervakning via satelliter, eftersom detta är enda möjligheten att för en internationell förbindelse kunna avlyssna båda parterna i ett samtal. Det är uppenbart att satellitföljande stationer är så stora att de inte kan upprättas på en stats territorium utan att den staten givit sitt medgivande till detta. Här krävs ömsesidiga överenskommelser och samverkan mellan flera länder fördelade över jordklotet.

De tänkbara riskerna för den privata sfären och näringslivet med ett system av typ ECHELON baseras emellertid inte enbart på att det är ett särskilt kraftfullt övervakningssystem. En viktig annan faktor är att dess användning sker inom en i stor utsträckning rättsligt oreglerad zon. Ett avlyssningssamtal för internationell kommunikation inriktas normalt inte på det egna landets invånare. Den som avlyssnas har därmed såsom varande utlänning inget inomstatligt rättsskydd. Med detta system är sålunda den enskilda individen helt utlämnad. Den parlamentariska kontrollen är också otillräcklig på detta område, eftersom väljarna utgår från att det inte är de själva som berörs, utan "bara" utlänningar, varför de inte fäster så stort avseende vid verksamheten, samtidigt som de förtroendevalda i första hand ser till sina väljares intressen. Det bör därför inte betraktas som märkligt att de förhör som hållits i den amerikanska kongressen om NSA:s verksamhet främst berört frågan om huruvida amerikanska medborgare omfattats av verksamheten, medan själva förekomsten av ett system av detta slag inte väckt någon anstöt. Desto viktigare förefaller det att ta itu med frågan på europeisk nivå.

2. Underrättelsetjänsternas verksamhet

2.1. Inledning

De flesta regeringar förfogar utöver polisen också över en underrättelsetjänst med syftet att skydda landets säkerhet. Verksamheten inom underrättelsetjänsten är oftast hemlig och sorterar ofta under säkerhetspolisen. Underrättelsetjänstens uppdrag är

- att inhämta information för att bekämpa hot mot statens säkerhet
- att bedriva kontraspionage i allmänhet
- att skapa skydd mot risker som kan hota försvarsmakten
- att inhämta information om utländska sakförhållanden.

2.2. Vad är spionage?

Regeringar har behov av att systematiskt samla in och bedöma information om vissa sakförhållanden i andra länder. Det är fråga underlag för beslut när det gäller försvaret, utrikespolitiken osv. I detta syfte bedriver staten underrättelseverksamhet. Underrättelsetjänsten utvärderar först systematiskt den information som är offentlig, så kallade öppna källor. Rapportförfattaren har uppgift om att i genomsnitt minst 80 procent av underrättelsetjänstens verksamhet gäller öppna källor. [1] Särskilt viktig information på de nämnda områdena hålls emellertid hemlig av regeringarna respektive företagen, och finns därmed inte tillgänglig offentligt. Den som vill komma över sådan information måste stjäla den. Spionage är helt enkelt organiserad stöld av information.

2.3. Mål för spionage

De klassiska målen för spionage är militära hemligheter, andra regeringars hemligheter och information om regeringars stabilitet eller hot mot denna. Hit hör exempelvis nya vapensystem, militära strategier, eller information om lokalisering av truppförband. Inte mindre viktig är information om kommande beslut inom utrikespolitiken, valutapolitik, eller insiderinformation om spänningar inom en regering. Därutöver finns intresse för ekonomiskt viktig information. Hit kan branschinformation höra, men även detaljer om ny teknik eller utlandsaffärer.

2.4. Medel för spionage

Spionage är att skaffa sig tillgång till information som innehavaren egentligen vill skydda mot åtkomst av främlingar. Skyddet måste alltså övervinnas och brytas igenom. Detta gäller både politiskt spionage och företagsspionage. Spionage erbjuder samma svårigheter inom båda områdena, och samma metoder används inom båda områdena. Det finns ingen skillnad logiskt sett, men skyddsnivån inom näringslivet är normalt lägre och företagsspionage är därför ofta lättare att genomföra. Särskilt är medvetenheten om risken för avlyssning av kommunikation lägre inom näringslivet än inom de statliga säkerhetsområdena.

2.4.1. Användning av människor vid spionage

Skyddet av hemlig information är alltid organiserat på samma sätt:

- endast ett fåtal väl kontrollerade personer har tillgång till den hemliga informationen

[1] I en rapport, "Preparing for the 21st Century; An Appraisal of U.S. Intelligence", från "Commission on the Roles and Capabilities of the US Intelligence Community" konstateras att 9% av alla ekonomiska underrättelser härrör från offentliga källor (kapitel 2: "The Role of Intelligence").

- det finns fasta regler för hur denna information skall hanteras
- informationen lämnar normalt inte det skyddade området och om så sker är den skyddad, exempelvis genom kryptering. Organiserat spionage inriktar sig därför i första hand på att skaffa sig tillgång till den önskade informationen direkt och utan omvägar via **personer** (så kallad *human intelligence*). Det kan röra sig om
  - insmugglade personer (agenter) från den egna underrättelsetjänsten
  - personer från målsektorn som värvats.

Personer värvas oftast till arbete för främmande underrättelsetjänst på följande grunder:
- sexuell förförelse;
- mutor i form av kontanter eller ekonomiska vinster;
- utpressning;
- ideologier;
- belöning i form av särskild uppmärksamhet eller ära (missnöjdhet, mindervärdeskomplex).

Ett gränsfall är ofrivillig medverkan i form av "skumning". Detta innebär att medarbetare vid myndighet eller i företag under i övrigt harmlösa omständigheter (samtal vid konferenser, kongresser, i baren till ett hotell) lockas till avslöjanden genom vädjan till vederbörandes fåfänga osv.

När man utnyttjar personer har detta fördelen att den önskade informationen blir tillgänglig direkt. Det finns emellertid nackdelar med detta:
- kontraspionaget inriktas alltid på personer eller agenter;
- de svagheter som ligger till grund för värvning av personer är också en riskfaktor för den som spionerar;
- människor är aldrig ofelbara och fångas därför förr eller senare upp genom kontraspionagets insatser.

Där så är möjligt försöker man därför ersätta användning av agenter eller värvade personer med spionage som är anonymt och personoberoende. Enklast sker detta vid analys av radiotrafik från militärt intressanta anläggningar eller fordon.

2.4.2. Analys av elektromagnetiska signaler

Den form av spionage med tekniska medel som är bäst känd för allmänheten är satellitfotografering. Därutöver fångas emellertid alla typer av elektromagnetiska signaler upp och utvärderas (så kallad *signal intelligence* , SIGINT).

2.4.2.1. Elektromagnetiska signaler som inte används för kommunikation

Vissa elektromagnetiska signaler, t ex strålning från radarstationer, kan på det militära området ge värdefull information om hur en fiendes luftförsvar är organiserat (så kallad *electronic intelligence*, ELINT). Elektromagnetisk strålning som kan ge information om var trupp, flygplan, fartyg eller ubåtar befinner sig är en värdefull informationskälla för underrättelsetjänsten. Även satellitföljning av fotograferande spionsatelliter från andra stater, och registrering och avkodning av signalerna från dessa, har betydelse.

Signalerna uppfångas av markstationer, lågflygande satelliter eller kvasigeostationära SIGINT-satelliter. Denna del av den elektromagnetiskt anknutna underrättelseverksamheten tar i anspråk en kvantitativt viktig andel av underrättelsetjänstens avlyssningskapacitet. Det finns emellertid ytterligare områden för insats av teknik.

2.4.2.2. Analys av avlyssnad kommunikation

Underrättelsetjänsterna i många länder avlyssnar andra länders militära och diplomatiska meddelandetrafik. Många underrättelsetjänster övervakar också andra länders civila meddelandetrafik i den mån denna är tillgänglig. I några länder har underrättelsetjänsten också rätt att övervaka den trafik som når det egna landet eller som lämnar det. I demokratier är den egna underrättelsetjänstens möjligheter att övervaka de **egna** medborgarnas meddelandetrafik reglerad och kontrollerad. De nationella lagstiftningarna skyddar emellertid bara medborgare som befinner sig i sitt eget land (se kapitel 8).

2.5. Vissa underrättelsetjänsters verksamhet

Den offentliga debatten har främst inriktat sig på den avlyssningsverksamhet som bedrivs av de amerikanska och brittiska underrättelsetjänsterna. Kritiken gäller avlyssning och analys av kommunikation (tal, fax, e-post). För en **politisk** analys krävs en måttstock som kan användas för att bedöma sådan verksamhet. Som jämförelsemåttstock kan man ta den avlyssningsverksamhet som EU-ländernas underrättelsetjänster bedriver. Följande tabell 1 ger en översikt. Av tabellen framgår att avlyssning av privat kommunikation i underrättelsesyfte inte är specifikt för den amerikanska eller den brittiska underrättelsetjänsten.

Land	Utrikes-kommunikation	Statlig kommunikation	Civil kommunikation
Belgien	+	+	-
Danmark	+	+	+
Finland	+	+	+
Frankrike	+	+	+
Tyskland	+	+	+
Grekland	+	+	-
Irland	-	-	-
Italien	+	+	+
Luxemburg	-	-	-
Nederländerna	+	+	+
Österrike	+	+	-
Portugal	+	+	-
Sverige	+	+	+
Spanien	+	+	+
Storbritannien	+	+	+
USA	+	+	+
Kanada	+	+	+
Australien	+	+	+
Nya Zeeland	+	+	+

Tabell 1: Avlyssningsverksamhet som bedrivs av underrättelsetjänsterna inom EU och i ECHELON-staterna

Spalterna har följande betydelse:
spalt 1: det egna landet
spalt 2: utrikesommunikation avlyssnas
spalt 3: statlig kommunikation (militär, ambassader osv) avlyssnas
spalt 4: civil kommunikation avlyssnas.

3. Tekniska randvillkor för avlyssning av telekommunikation

3.1. Olika kommunikationsmediers avlyssbarhet

När människor på ett visst avstånd från varandra vill kommunicera krävs ett medium för denna kommunikation. Detta medium kan vara:

- luften (ljudvågor);
- ljus (morseblink, optofiber);
- elektrisk ström (telegraf, telefon);
- elektromagnetiska vågor (radiotrafik av alla slag).

Om en tredje part skaffar sig tillträde till kommunikationsmediet kan kommunikationen avlyssnas. Sådant tillträde kan vara lätt eller svårt, kan vara möjligt från många platser eller bara från vissa platser. I det följande kommer två extremfall att diskuteras: dels en spions tekniska möjligheter när vederbörande befinner sig på plats, dels möjligheterna till ett världsomspännande avlyssningssystem.

3.2. Avlyssningsmöjligheter på platsen [1]

På platsen kan varje kommunikation avlyssnas om den avlyssnande är beredd att bryta mot lagen och den avlyssnade inte vidtar skyddsåtgärder.

- **Samtal** i ett rum kan avlyssnas med hjälp av utplacerade mikrofoner (buggning) eller genom att en fönsterrutas svängningar avläses med en laserstråle.

- **Bildskärmar** utsänder strålning som kan uppfångas på upp till 30 m håll och som kan avläsas och avslöja vad som visas på skärmen.

- **Telefon, telefax och e-post** kan avlyssnas genom att den lyssnande ansluter till den kabel som lämnar byggnaden.

- **Bärbar kommunikationsradio** kan avlyssnas på upp till …. kilometers håll.

- **Företagsintern kommunikationsradio** kan avlyssnas inom den räckvidd som UKV-bandet har.

Villkoren för användning av tekniska medel för spionage på platsen är idealiska, eftersom avlyssningsåtgärderna kan inriktas på en viss person eller ett visst objekt och praktiskt taget alla former av kommunikation kan avlyssnas. Det är bara buggning och anslutning till en kabel som medför nackdelen av en viss upptäcktsrisk.

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

3.3. Möjligheten till ett världsomspännande avlyssningssystem

Nu för tiden finns flera kommunikationsmedier för internationell kommunikation oavsett meddelandenas form (tal, fax, data). Möjligheterna att anordna ett världsomspännande avlyssningssystem begränsas av två faktorer:

- kommunikationsmediets tillgänglighet;
- nödvändigheten att filtrera fram intressant kommunikation ur en enorm reservoar av pågående kommunikation.

3.3.1. Kommunikationsmediets tillgänglighet

3.3.1.1. Kabelburen kommunikation

Alla typer av kommunikation kan ske via kabel (tal, fax, e-post, data). Kabelburen kommunikation kan bara avlyssnas om kabeln själv är åtkomlig. Sådan åtkomst är alltid möjligt i ändpunkten av en kabelförbindelse, om ändpunkten ligger innanför gränsen till det land som utför avlyssningen. Inomstatligt kan alltså **tekniskt sett** alla kablar avlyssnas, om avlyssningen är tillåten enligt lag. Utländska underrättelsetjänster har dock sällan laglig tillgång till kabeln inom en annan stats jurisdiktion. Illegalt kan dock tillgång till kabeln beredas, om än med hög risk för upptäckt.

Interkontinentala kabelförbindelser har sedan telegraferingens tidsålder förverkligats med undervattenskablar. Tillgång till dessa kablar kan beredas där kablarna kommer upp ur vattnet. Om flera länder samarbetar om avlyssning blir kabelförbindelserna åtkomliga i alla de ändpunkter som befinner sig i de samverkande länderna. Detta har haft historisk betydelse, eftersom såväl undervattenskablarna för telegrafi som de första undervattenskoaxialkablarna för telefoni mellan Europa och Amerika lämnade havet i Newfoundland (kanadensiskt territorium) och förbindelserna till Asien löpte via Australien, eftersom det krävdes signalförstärkare på vägen. Idag dras optofiberkablarna raka vägen utan hänsyn till berglandskapet under vattnet och utan behov av signalförstärkare, utan mellanlandning i Australien eller Nya Zeeland. Elektriska kablar kan också avlyssnas mellan ändpunkter, med hjälp av induktion (dvs elektromagnetiskt via en spole som läggs intill kabeln), utan att någon direkt elektrisk förbindelse behövs. Detta kan åstadkommas av ubåtar vid elektriska undervattenskablar, låt vara till höga kostnader. Denna teknik utnyttjades av USA för att avlyssna en viss undervattenskabel till Sovjetunionen, vilken överförde okrypterad trafik till de ryska atomubåtarna. En heltäckande tillämpning av denna teknik är omöjlig av rena kostnadsskäl.

Hos de optofiberkablar av den äldre generationen som används idag är induktiv avlyssning bara möjlig vid signalförstärkarna. I dessa signalförstärkare omvandlas den optiska signalen till en elektrisk signal, som förstärks och sedan åter omvandlas till en optisk signal. Här uppstår frågan hur de gigantiska datamängder som transporteras i en sådan kabel skulle transporteras från avlyssningspunkten till den plats där analys av trafiken sker, utan att man behöver dra en särskild optofiberkabel för detta. Användning av en ubåt med analysteknik ombord kan av ekonomiska skäl bara ske i enstaka fall, exempelvis under i krig i syfte att fånga upp strategiskt viktig militär kommunikation. För rutinövervakning av internationell kommunikation kan enligt rapportförfattarens bedömning ingen utbåtsinsats vara aktuell. Optofiberkablar av den senaste generationen bygger på erbiumlasrar som signalförstärkare, varför dessa förbindelser inte kan avlyssnas elektromagnetiskt. Sådana optofiberkablar kan sålunda endast avlyssnas i förbindelsens ändpunkter.

I praktiken innebär detta för avlyssningssamarbetet mellan de så kallade **ECHELON-staterna** att de inte till rimliga kostnader kan avlyssna undervattenskablar på annan plats än vid de ändpunkter som ligger på deras eget territorium. I princip kan de alltså endast komma åt kabelburen kommunikation som kommer till eller lämnar deras egna länder. Med andra ord har de för **Europas** del endast tillgång till den kabelkommunikation som kommer till och lämnar **Storbritannien.** För inhemsk kommunikation används för närvarande framför allt det inhemska kabelnätet. Undantag kan förekomma i samband med privatiseringen av telekommunikationen, men dessa är partiella och inte förutsägbara.

Detta gäller åtminstone telefon och telefax. I fråga om kommunikation via Internet och kabel gäller andra randvillkor. Sammanfattningsvis kan följande läggas fast:

- Kommunikation på Internet sker i form av datapaket, där de paket som adresseras till en viss mottagare kan vandra olika väger genom nätet.
- I början av Internet-epoken utnyttjade man lågbelastningsperioder i det offentliga forskningsnätet för överföring av e-post. Ett meddelandes väg var därmed helt oförutsägbart; de enskilda paketen transporterades på kaotiska, icke förutsägbara, vägar. Den viktigaste internationella förbindelsen vid denna tidpunkt det "academic backbone" som dragits mellan Europa och Amerika.
- När Internet kommersialiserades och Internet-leverantörer etablerades skedde en kommersialisering av hela nätverket. Internet-leverantörerna drev eller hyrde egna nät. De försökte också i allt större utsträckning hålla kommunikationen inom det egna nätet, för att undvika kostnaden för att utnyttja andra nätaktörer. Datapaketens väg genom nätet är därför idag inte bara en funktion av nätets belastning, utan också av kostnadsresonemang.
- Ett e-postmeddelande som skickas från en kund hos en Internet-leverantör till en kund hos en annan, skickas normalt inom avsändarens nät, även om detta inte är den snabbaste vägen. De datorer (routrar) som befinner sig i nätets knutpunkter och avgör paketens transportvägar organiserar överföringen till andra nät via särskilda kopplingspunkter (switchar).
- Vid tiden för academic backbone fanns switcharna för den globala Internet-trafiken i USA. Där hade underrättelsetjänsten vid den tidpunkten alltså tillgång till en stor del av den europeiska Internet-kommunikationen. Idag är det bara en mycket liten del av den inomeuropeiska kommunikationen på Internet som sker via USA.
- En liten del av den inomeuropeiska kommunikationen sker via en switch i London, som den brittiska underrättelsetjänsten GCHQ har tillgång till. Huvuddelen av kommunikationen håller sig på det europeiska fastlandet. Till exempel går över 95 procent av den tyska Internet-kommunikationen via en switch i Frankfurt.

I praktiken innebär detta att ECHELON-staterna bara har tillgång till en **mycket begränsad del** av den kabelburna Internet-kommunikationen.

3.3.1.2. Radiosignalburen kommunikation[1]

Avlyssbarheten hos radiokommunikation sammanhänger med räckvidden hos de radiovågor som används. Om radiovågorna följer jordytan (så kallade **markvågor**), så har de en begränsad

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

räckvidd, som sammanhänger med terrängen, bebyggelsen och växtligheten. Om radiovågorna skickas ut i rymden (så kallade **rymdvågor**), så kan de ha betydande räckvidd genom att de reflekteras mot olika skikt i jonosfären. Upprepade reflektioner ökar räckvidden avsevärt.

Räckvidden sammanhänger med våglängden:

- Långvåg (3 kHz – 300 kHz) kan bara tas emot som markvågor, därför att rymdvågorna inte reflekteras av jonosfären. Räckvidden är liten.
- Mellanvåg (300 kHz – 3 MHz) är markvågor, men nattetid kan rymdvågor bildas. Räckvidden är måttlig.
- Kortvåg (3 MHz – 30 MHz) tas främst emot som rymdvågor och har räckvidd **runt hela jorden**, tack vare upprepad reflexion.
- Ultrakortvåg (30 MHZ – 300 MHz) tas bara emot som markvågor, därför att rymdvågorna inte reflekteras av jonosfären. Radiovågorna går relativt rakt, ungefär som ljus. Räckvidden blir därmed på grund av jordytans krökning beroende av antennhöjden hos sändare och mottagare. Beroende på sändareffekten kan de nå upp till 100 km (för en bärbar kommunikationsradio ca 30 km).
- Decimeter- och centimetervågor (30 MHz – 30 GHz) har i ännu högre grad än UKV kvasioptiska egenskaper. De är lätta att samla och medger riktad sändning med låg effekt (markbundna radiolänkar). Sådana sändningar kan bara tas emot med en antenn som är nära parallell med den riktade vågen och befinner sig nära radiolänksträckan.

Lång- och mellanvåg används bara för radiosändare, radiofyrar och liknande. Militär och civil radiokommunikation sker på kortvåg och framför allt på ultrakortvåg och decimeter/centimetervågor.

Av ovanstående kan man härleda att ett globalt avlyssningssystem för kommunikation bara kan använda sig av kortvågstrafik. För alla andra typer av radiotrafik måste den avlyssnande stationen befinna sig inom 100 km från sändaren (t ex på ett fartyg, på en ambassad).

I praktiken innebär detta att ECHELON-staterna bara har tillgång till en **mycket begränsad del** av den radioburna kommunikationen.

3.3.1.3. Kommunikation via geostationära satelliter [1]

Som nämndes ovan kan decimeter- och centimetervågor lätt samlas och riktas. Om man riktar en radiolänk mot en stationär kommunikationssatellit på hög höjd som tar emot radiolänksignalen, omsätter den och skickar den tillbaka till jorden, så kan man utan användning av kabel täcka mycket stora avstånd. Räckvidden för en sådan förbindelse begränsas egentligen bara av att satelliten inte kan ta emot och sända bortanför sin jordhorisont. För att få global täckning sätter man därför in flera satelliter (närmare om detta i kapitel 4). Om ECHELON-staterna har avlyssningsstationer i de regioner som behövs kan de i princip avlyssna all telefon-, telefax- och datatrafik som sker via sådana satelliter.

3.3.1.4. Avlyssningsmöjligheter via flygplan och fartyg

Det är känt sedan länge att specialflygplan av typ AWACS används för att på långa avstånd upptäcka andra flygplan. Radarn i dessa maskiner används som ett avläsningssystem som

[1] Hans Dodel, Satellitenkommunikation, Hüthig Verlag 1999.

identifierar kända mål, lokaliserar elektroniska signaler, klassificerar källan och korrelerar denna med radarkontakter. Däremot har de inte separat SIGINT-förmåga. [1] Det långsamflygande spionflygplanet EP-3 som tillhör US Navy har däremot resurser för avlyssning av mikrovågor, ultrakortvåg och kortvåg. Signalerna analyseras direkt ombord på flygplanet, som används för rent militära ändamål. [2]

Därutöver finns också övervattensfartyg, och för insatser nära land ubåtar, som kan avlyssna militär radiotrafik. [3]

3.3.1.5. Avlyssningsmöjligheter via spionsatelliter

Radiovågor strålar, om de inte har fokuserats med hjälp av lämpliga antenner, åt alla håll, alltså även ut i rymden. Lågflygande *Signal Intelligence Satellites* kan bara lyssna på den sändare som skall avlyssnas under några få minuter. I högindustrialiserade områden med hög befolkningstäthet försvåras avlyssningen så kraftigt av samtidiga sändningar från flera källor med samma frekvens att det är svårt att filtrera fram enskilda signaler. [4] Dessa satelliter lämpar sig inte för kontinuerlig övervakning av civil radiotrafik.
Därutöver finns det högt uppskjutna (42 000 km) så kallade kvasistationära SIGINT-satelliter som tillhör USA[5] Till skillnad från de geostationära kommunikationssatelliterna har dessa satelliter en baninklination på 3 - 10°, ett apogeum på 39 000 - 42 000 km och ett perigeum på 30 000 - 33 000 km. Satelliterna står därför inte stilla över jordytan utan rör sig efter en komplicerad elliptisk bana. Under loppet av en dag täcker de därför in en större region och ger möjlighet till inpejling av radiokällor. Dessa egenskaper och de övriga kännetecken på dessa satelliter som är offentligt tillgängliga tyder på att de har rent militära uppgifter.
De mottagna signalerna skickas starkt fokuserade med frekvensen 24 GHz ned till en satellitföljarstation.

3.3.2. Möjligheter till automatisk analys av avlyssnad kommunikation: användning av filter

Vid avlyssning av kommunikation utomlands övervakar man inte någon speciell telefonförbindelse. Istället uppfångas all eller en del av den kommunikation som passerar den övervakade satelliten eller kabeln, och filtreras sedan med hjälp av en dator och särskilda filtreringsnycklar. Det är helt uteslutet att kunna analysera all uppfångad kommunikation.

Att filtrera fram kommunikation på en viss linje är enkelt. Med filtreringsnycklar kan även telefax och e-post sökas fram. Om analyssystemet får särskild träning kan till och med en viss röst filtreras fram. [6] Automatisk igenkänning av enstaka ord, som uttalas av olika röster, är dock enligt de uppgifter rapportförfattaren har tillgång till ännu så länge omöjligt. Det finns också andra faktorer som begränsar möjligheterna till filtrering: datorns ändliga kapacitet; språkproblemen; samt framför allt det begränsade antal personer som kan läsa och analysera de framfiltrerade meddelandena.

---

[1] Brev från Walter Kolbow, statssekreterare i Tysklands försvarsministerium, av 2001-02-14.
[2] Süddeutsche Zeitung Nr.80, av 2001-04-05, s. 6.
[3] Jeffrey T. Richelson, The U.S. Intelligence Community, Ballinger, New York 1989, s.188 , 190.
[4] Brev från Walter Kolbow, statssekreterare i Tysklands försvarsministerium, av 2001-02-14.
[5] Major Andronov, Zarubezjnoje vojennoje obozrenie, Nr.12,1993, s.37-43.
[6] Privat information till rapportförfattaren, källan skyddad.

När man bedömer möjligheterna hos filtersystemen måste man också beakta att den tekniska användbarheten för sådana avlyssningssystem som arbetar enligt "dammsugarprincipen" har flera aspekter. Vissa nyckelord bygger på militär säkerhet, andra förekommer vid narkotikahandel och andra former av internationell brottslighet, en del hör hemma i handeln med objekt som har flera användningsområden, och ytterligare en förekommer i samband med embargosituationer. Vissa nyckelord sammanhänger också med näringslivsverksamhet. Följaktligen uppdelas systemens kapacitet på flera områden. En begränsning av nyckelorden till att endast gälla områden som är intressanta för näringslivet skulle stå i strid med kraven från underrättelsetjänstens politiska ledning, något sådant har inte skett ens sedan det kalla kriget slutade. [1]

3.3.3. Exemplet den tyska underrättelsetjänsten

Avdelning 2 inom den tyska underrättelsetjänsten tar fram information genom att avlyssna utrikeskommunikation. Verksamheten underställdes en prövning i den tyska författningsdomstolen. De detaljer som kom fram under processen [2] gav tillsammans med uppgifter från Ernst Uhrlau, regeringens samordnare för säkerhetstjänsterna, som lämnades till ECHELON-utskottet 2000-11-21, en bild av underrättelsetjänstens möjligheter att avlyssna satellitförmedlad kommunikation.

Möjligheterna för andra underrättelsetjänster kan på grund av deras lagstiftning i relation till tillgängligheten hos kabelburen kommunikation eller på grund av ett större antal personer som sysslar med analys vara större på andra ställen. När man drar in den kabelbundna trafiken ökar den statistiska sannolikheten för träff, men därav följer inte med säkerhet att den analyserbara trafiken ökar. Utgående från exemplet Tyskland framgår det för rapportförfattaren tydligt vilka möjligheter och strategier underrättelsetjänsterna har att följa utlandsanknuten trafik, även om detta inte avslöjas direkt.

Den tyska underrättelsetjänsten försöker genom **strategisk** kommunikationsövervakning skaffa sig information från utlandet om utlandet. I detta syfte arbetar man med en rad sökbegrepp (som i Tyskland tidigare måste godkännas av den så kallade G10-kommissionen [3]) för att avläsa satellittrafik. Volymmässigt gällde följande (år 2000): av de omkring 10 miljonerna internationella kommunikationsförbindelserna / dag som sker till och från Tyskland går omkring 800 000 via satellit. Av dessa filtreras knappt 10 procent (75 000) i en sökmaskin. Denna begränsning är enligt rapportförfattaren inte en följd av lagstiftningen (teoretiskt skulle åtminstone före processen i författningsdomstolen 100 procent ha varit tillåtet), utan av tekniska faktorer, t ex begränsad analyskapacitet.

Även antalet hanterbara sökbegrepp är begränsat, både tekniskt och genom kravet på godkännande. I domskälen från författningsdomstolen diskuteras utöver de rent formella sökbegreppen (förbindelser som upprättas av utlänningar eller utländska firmor i utlandet) 2 000 sökbegrepp i fråga om kärnvapenspridning, 1 000 i fråga om vapenhandel, 500 i fråga om terrorism och 400 i fråga om narkotikahandel. Ifråga om terrorism och narkotikahandel har metoden dock inte visat sig särskilt framgångsrik.

[1] Privat information till rapportförfattaren, källan skyddad.
[2] BverfG, 1 BvR 2226/94 av 1999-07-14, punkt 1.
[3] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10 GG) av 1968-08-13.

Sökmaskinen granskar om det godkända sökbegreppet förekommer i telefax- eller telexmeddelanden. För närvarande klarar inte systemet att känna igen sammansatta ord. Om sökbegreppet inte återfinns makuleras meddelandena automatiskt, de får inte analyseras, eftersom lagstiftningen inte medger detta. Dagligen påträffas omkring 5 meddelanden från deltagare i fjärrkommunikation, som faller under det tyska grundlagsskyddet. Den strategiska spaningen inom underrättelsetjänsten i Tyskland syftar till att hitta mosaikstenar som kan ligga till grund för vidare spaning. Målet är inte någon heltäckande övervakning av kommunikation med utlandet. Enligt de uppgifter som rapportförfattaren haft tillgång till gäller motsvarande för andra underrättelsetjänsters SIGINT-verksamhet.

4. Tekniken bakom satellitkommunikation

4.1. Kommunikationssatelliternas betydelse

Satelliterna utgör idag en oundgänglig del av det globala kommunikationsnätet och bidrar till överföringen av tv- och radioprogram liksom multimediatjänster. Trots detta har i Centraleuropa satelliternas andel av den internationella trafiken minskat kraftigt under de gångna åren. I många regioner ligger den idag så lågt som under 10 procent. [1] Detta sammanhänger med fördelarna hos optofiberkablarna, som kan transportera ofantligt mycket större trafikvolymer med högre förbindelsekvalitet.

Även när det gäller tal sker kommunikationen idag med digital teknik. Kapaciteten av satellitförmedlade digitala förbindelser inskränker sig per satellittransponder till **1 890** talkanaler med ISDN-standard (64 kbit/s). Mot detta kan ställas en enda optofiber, som klarar **241 920** talkanaler med samma standard. Alltså ett förhållande på **1.128!**

Därtill kommer att satellitförbindelsernas kvalitet är lägre än hos optofiberkabel under vattnet. Kvalitetsnedsättningar på grund av signalernas långa löptid, som kan uppgå till flera hundra millisekunder, är vid normala talförbindelser nätt och jämnt märkbara – men dock hörbara. Vid data- och telefaxförbindelser, som sker med hjälp av en komplicerad "handskakningsprocedur", har kabeln tydliga fördelar för förbindelsesäkerheten. Samtidigt måste man komma ihåg att endast 15 procent av jordens befolkning är anslutna till det globala kabelnätet. [2]

För specifika uppgifter kan ändå satelliterna på lång sikt vara bättre än kabel. Några exempel från det civila området:

- nationell, regional och internationell telefon- och datatrafik i områden med låga kommunikationsvolymer, dvs på platser där det inte skulle löna sig att lägga kabel på grund av lågt utnyttjande;
- tidsbegränsad kommunikation vid katastrofinsatser, arrangemang, stora byggprojekt osv;
- FN-insatser i regioner med svag kommunikationsinfrastruktur;
- flexibel/mobil kommunikation inom näringslivet med satellitterminaler (VSAT, se vidare nedan).

Dessa användningsområden för satelliterna vid kommunikation följer av deras specifika egenskaper: radiovågorna från en enda geostationär satellit kan täcka nästan 50 procent av jordytan; även besvärlig terräng kan täckas. I detta område nås 100 procent av användarna, oavsett om de befinner sig till lands, till sjöss eller i luften. Satelliter kan driftsättas på några få månader, oberoende av infrastrukturen på platsen. De är tillförlitligare än kabel och kan utan problem ersättas.

[1] Se underlaget för ändring av G10-lagen i Tyskland.
[2] Deutsche Telekoms hemsida: www.detesat.com/deutsch/

Följande negativa egenskaper hos satellitkommunikationen måste beaktas: de relativt långa löptiderna för signalerna; försvagningen av signalen på längre avstånd; den kortare livslängden jämfört med kabel (12 till 15 år); större sårbarhet, lätta att avlyssna.

4.2. En satellitförbindelses arbetssätt

Som nämndes ovan i kapitel 3 kan man med lämpliga antenner fokusera mikrovågor. Därför går det att ersätta en kabel med en radiolänkförbindelse. Om nu sändar- och mottagarantenner inte står på en plan yta utan som i fallet jorden på ytan av en sfär, så "försvinner" den motsatta antennen vid ett visst avstånd under horisonten, på grund av jordens krökning. Då "ser" de båda antennerna inte längre varandra. Detta skulle till exempel inträffa om man försökte upprätta en radiolänkförbindelse mellan Europa och Amerika. Antennerna skulle behöva sitta på master med höjden 1,8 km för att en förbindelse skulle kunna fungera. Redan detta gör att radiolänkar inte är möjliga för internationella förbindelser av detta slag, alldeles bortsett från att signalen skulle dämpas kraftigt av luft och vattenånga längs sträckan. Om man istället ett gott stycke upp i rymden i en "stationär position" kan skapa en sorts spegel för radiolänkförbindelsen, så kan man överbrygga stora avstånd trots jordens krökning, på samma sätt som en trafikspegel gör det möjligt att se runt hörn. Den just beskrivna principen tillämpas i samband med så kallade geostationära satelliter.

4.2.1. Geostationära satelliter

Om man låter en satellit kretsa kring jorden över ekvatorn med ett varv på 24 timmar så kommer den att exakt följa jordens rotation. Från jordytan sett står satelliten i så fall stilla på höjden 36 000 km – den är **geostationär.** De flesta kommunikations- och tv-satelliter är av denna typ.

4.2.2. Signalens väg i en satellitförbindelse

Överföringen av signaler via satelliter kan beskrivas så här:

Den signal som kommer från en ledning skickas upp till satelliten via en radiolänkstation med en parabolantenn, en så kallad **uplink**. Satelliten tar emot signalen, förstärker den och skickar ned den till jordytan, till en annan radiolänkstation, via en så kallad **downlink.** Därifrån vidarebefordras signalen ut i ett kabelnät.

Vid mobilkommunikation överförs signalen direkt från den mobila kommunikationsenheten till satelliten, och kan därifrån matas tillbaka in i en ledning via en radiolänkstation, eller tas emot direkt av en annan mobil enhet.

4.2.3. De viktigaste existerande satellitkommunikationssystemen

Den kommunikation som kommer från de **för allmänheten tillgängliga kabelnäten** (som inte behöver vara statliga) överförs via satellitsystem med olika täckning från och till stationära radiolänkstatoner, för återföring till kabelnätet. Man skiljer mellan:

- globala (t ex INTELSAT)

- regionala (kontinentala) (t ex EUTELSAT)

- nationella (t ex ITALSAT)

satellitsystem.

De flesta av dessa satelliter är geostationära. Över hela världen driver 120 privata företag omkring 1000 satelliter.[1]

För platser långt norrut finns det vidare satelliter i omlopp med elliptiska banor (ryska Molnija-banor) som gör att satelliten under halva sin omloppstid är synlig för användare långt norrut. Med två satelliter får man då en regional täckning som man inte kan få med en geostationär satellit över ekvatorn.

Vidare finns det globala INMARSAT-systemet, som från början var avsett för bruk till sjöss. Det är ett **mobilkommunikationssystem**, som gör att man överallt på jorden kan skapa förbindelser via satellit. Även den arbetar med geostationära satelliter.

Det mobiltelefonsystem som kallas IRIDIUM och bygger på flera tidsförskjutna omloppssatelliter på låg höjd har nyligen ställt in driften på grund av dålig ekonomi till följd av lågt utnyttjande.

Det finns också en snabbt växande marknad för så kallade VSAT-förbindelser (VSAT = Very Small Apterture Terminal). Här rör det sig om satellitterminaler med antenndiametrar på mellan 0,9 och 3,7 m, som drivs av företag för eget bruk (t ex videokonferenser) eller av mobiltjänsteleverantörer för kortvariga förbindelser (t ex konferenser). 1996 fanns 200 000 VSAT-terminaler i drift runt om i världen. Volkswagen AG har 3 000, Renault 4 000, General Motors 100 000, medan det största europeiska oljebolaget har 12 000 VSAT-terminaler. Kommunikationen sker öppet, om inte kunden själv krypterar trafiken. [2]

4.2.3.1. Globala satellitsystem

Dessa satellitsystem täcker hela jordklotet med hjälp av flera satelliter som är utplacerade över Atlanten, Indiska oceanen och Stilla Havet.

INTELSAT [3]

INTELSAT (International Telecomunications Satellite Organisation) upprättades 1964 som en myndighet, med en organisation som liknar FN:s, och med verksamhetsmålet att bedriva internationell kommunikationstrafik. Medlemmar i organisationen var nationella offentligt ägda postverk. Idag är 144 regeringar medlemmar i INTELSAT. INTELSAT kommer att privatiseras under 2001.

För närvarande har INTELSAT en flotta av 19 geostationära satelliter, som förbinder över 200 länder och vilkas tjänster hyrs ut av medlemmarna i INTELSAT. Medlemmarna driver sina egna markstationer. Sedan 1984 har även icke medlemmar (t ex telefonbolag, stora företag, internationella koncerner) genom INTELSAT Business Service (IBS) kunnat utnyttja dessa satelliter. INTELSAT erbjuder globala tjänster för olika syften som kommunikation, tv osv. Telekommunikationsöverföringen sker på C- och Ku-banden (se nedan).

[1] G. Thaller, Satelliten im Erdorbit, Franzisverlag, München 1999
[2] H. Dodel, personligt meddelande.
[3] INTELSAT:s hemsida http://www.intelsat.com

INTELSAT-satelliterna är de viktigaste internationella kommunikationssatelliterna. Merparten av den satellitburna internationella trafiken sker via dessa satelliter.
De täcker länderna kring Atlanten, Indiska Oceanen och Stilla Havet (se tabellen i punkt 5.3).

Över Atlanten befinner sig 10 satelliter, mellan 304°E och 359°E, över Indiska Oceanen svävar 6 satelliter, mellan 62°E och 100,5°E, medan Stillahavsområdet täcks av 3 satelliter mellan 174°E och 180°E. Den stora trafikvolymen över Atlanten täcks av flera fristående satelliter där.

INTERSPUTNIK [1]
1971 grundades av 9 länder den internationella satellitkommunikationsorganisationen INTERSPUTNIK, som verktyg för dåvarande Sovjetunionon, med ungefär samma syfte som INTELSAT. Idag är INTERSPUTNIK en mellanstatlig organisation, där regeringar från vilka länder som helst får vara medlemmar. Organisationen har nu 24 stater som medlemmar (bl a Tyskland) och ca 40 användare (bl a Frankrike och Storbritannien), som representeras av sina postverk eller telekomföretag. Organisationen har sitt säte i Moskva.

Telekommunikationsöverföringen sker på C- och Ku-banden (se nedan).

Även här täcks hela jordklotet av satelliterna (Gorizont, Express, Express A från Ryska Federationen och LMI-1 från Lockheed-Martin-projektet): över Atlanten finns 1 satellit, en andra planeras, över Indiska Oceanen 3 satelliter och över Stilla Havet 2 (se tabellen i punkt 5.3).

INMARSAT
Sedan 1979 erbjuder INMARSAT (Interim International Maritime Satellite) med sina satelliter **mobil** kommunikation till sjöss, i luften och på land, över hela världen. De erbjuder även ett system för nödkommunikation. INMARSAT bildades på initiativ av International Maritime Organisation, som ett mellanstatligt organ. Numera har INMARSAT privatiserats och har sitt säte i London.

INMARSAT-systemet består av nio satelliter i geostationär bana. Fyra av dessa – INMARSAT III-generationen – täcker hela jordklotet inklusive polarområdena. Varje enskild satellit täcker omkring 1/3 av jordytan. Genom sina placeringar över de fyra oceanområdena (Västatlanten, Ostatlanten, Stilla Havet, Indiska Oceanen) når man global täckning. Samtidigt har varje INMARSAT-satellit ett antal "Spot Beams", som gör det möjligt att samla upp sändningsenergin i områden med större trafikbelastning.

Telekommunikationsöverföringen sker på C- och Ku-banden (se 4.2.4 nedan).

4.2.3.2. Regionala satellitsystem

Regionala satellitsystem når med sina trafikzoner enskilda regioner/kontinenter. Den kommunikation de överför måste alltså tas emot inom dessa regioner.

EUTELSAT [2]
EUTELSAT grundades 1977 av 17 postverk i Europa, med målet att klara Europas specifika behov av satellitkommunikation och att stödja den europeiska rymdfartsindustrin. Den har sitt

[1] INTERSPUTNIK:s hemsida http://www.intersputnik.com
[2] EUTELSAT:s hemsida http://www.eutelsat.org

säte i Paris och har omkring 40 medlemsländer. EUTELSAT kommer att privatiseras under 2001.

EUTELSAT driver 18 geostationära satelliter, som täcker Europa, Afrika och stora delar av Asien. En förbindelse med Amerika drivs också. Satelliterna är placerade mellan 12,5°W och 48°E. EUTELSAT erbjuder främst tv (850 digitala och analoga kanaler) och radio (520 kanaler), men täcker också ett visst kommunikationsbehov, främst inom Europa (inklusive Ryssland): t ex för videokonferenser, för privata nät inom stora företag (bl a General Motors, Fiat), för nyhetsbyråer (Reuters, AFP), för börsdataförmedling och för mobil dataöverföring. Telekommunikationen sker på Ku-bandet.

ARABSAT [1]
ARABSAT är en pendang till EUTELSAT för den arabiska regionen, grundat 1976. I organisationen ingår 21 arabiska länder. ARABSAT-satelliterna används både för tv-sändningar och för kommunikation.

Telekommunikationen sker främst på C-bandet.

PALAPA [2]
Det indonesiska PALAPA-systemet är i drift sedan 1995 och är en sydasiatisk pendang till EUTELSAT. Det täcker med sina satelliter Malaysia, Kina, Japan, Indien, Pakistan och andra länder i regionen.

Telekommunikationsöverföringen sker på C- och Ku-banden.

4.2.3.3. Nationella satellitsystem[3]

Flera stater har egna satellitsystem för att tillgodose nationella krav. Dessa system har begränsad täckning.

Den franska kommunikationssatelliten **TELECOM** har bland annat till uppgift att förbinda de franska departementen i Afrika och Sydamerika med hemlandet.
Telekommunikationsöverföringen sker på C- och Ku-banden.

ITALSAT driver kommunikationssatelliter som täcker hela den italienska stöveln med smala täckningszoner som ligger intill varandra. Mottagningsmöjligheter finns därför bara i Italien. Telekommunikationen sker på Ku-bandet.

AMOS är en israelisk satellit för i huvudsak stationär kommunikation, som täcker Mellanöstern. Telekommunikationen sker på Ku-bandet.

De spanska satelliterna **HISPASAT** täcker Spanien och Portugal (Ku spots) och överför spanska tv-program till Nord- och Sydamerika.

[1] ARABSAT:s hemsida http://www.arabsat.com
[2] H.Dodel, Satellitenkommunikation, Hüthigverlag 1999.
[3] H.Dodel och sökningar på Internet.

4.2.4. Frekvenstilldelning

Det är International Telecommunication Union som ansvarar för fördelningen av frekvenser. För att en viss ordning skulle råda delades världen in i tre regioner för radiokommunikation:

1. Europa, Afrika, före detta Sovjetunionen, Mongoliet

2. Nord- och Sydamerika samt Grönland

3. Asien utom länderna i region 1, Australien samt södra Stilla Havet.

Denna historiskt grundade indelning har övertagits för satellitkommunikationen och har inneburit en ansamling av satelliter i vissa geostationära zoner.

De viktigaste frekvensbanden för satellitkommunikation är följande:

- L-bandet (0,4 - 1,6 GHz) för mobil satellitkommunikation, t ex via INMARSAT;

- C-bandet (3,6 - 6,6 GHz) för radiolänktrafik, t ex via INTELSAT;

- Ku-bandet (10 - 20 GHz) för radiolänktrafik, t ex INTELSAT Ku spots och EUTELSAT.

- Ka-bandet (20 - 46 GHz) för radiolänktrafik, t ex via nationella system som ITALSAT;

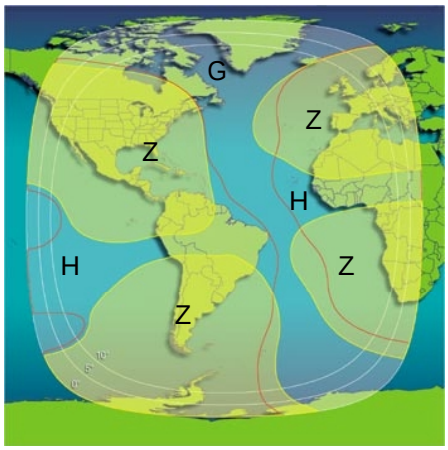
- V-bandet (46 - 56 GHz) för satellitterminaler (VSAT).

4.2.5. Satelliternas täckningsområden (footprints)

Täckningsområdet, "footprint", är den del av jordytan som nås av signalerna från satelliten. Den kan omfatta upp till 50 procent av jordytan eller genom fokusering av signalerna bara utgöra små, regionalt avgränsade fläckar, "spots".

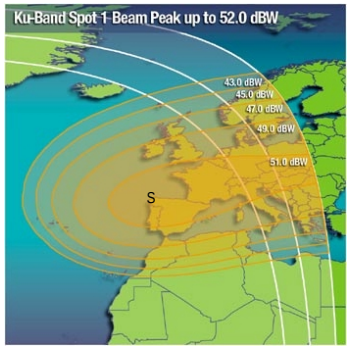
Ju högre frekvens den utsända signalen har, desto lättare är den att fokusera och desto mindre kan täckningszonen göras. Genom fokusering av den utsända signalen från satelliten på små täckningsområden kan man få en högre signalstyrka. Ju mindre täckningsområde, desto starkare signal, och desto mindre kan då mottagarantennen vara.

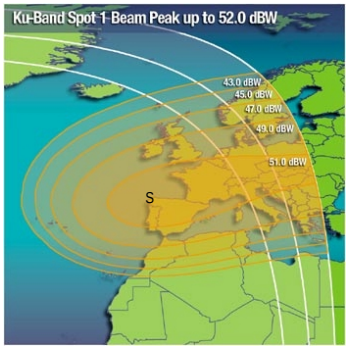
Detta illustreras närmare för INTELSAT-satelliterna:

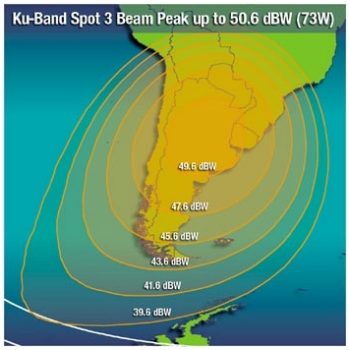


Täckningszonerna för INTELSAT-satelliterna är indelade i olika kategorier, "beams":

Global Beam (G) från respektive satellit når omkring en tredjedel av jordytan;
Hemi-Beams (H) täcker var och en ett område på omkring hälften av Global Beam; Zone Beams (Z) är spot-signaler som når specifika områden som är betydligt mindre än täckningsområdena för Hemi-Beams. Slutligen finns det så kallade Spot Beams, som alltså ger små, väl avgränsade Footprints (se nedan).







De frekvenser som tillhör C-bandet utnyttjas i G-, H- och Z-beams. För Spot Beams använder man sig av Ku-bandets frekvenser.

4.2.6. Antennstorlekar som krävs för satellitföljarstationer

Som mottagarantenner på jordytan utnyttjas parabolantenner. Parabolen reflekterar alla infallande strålar och fokuserar dem till en brännpunkt. I brännpunkten, fokus, ligger själva mottagaren. Ju större energi signalen har när den når mottagarplatsen, desto mindre kan parabolantennens diameter vara.

I det sammanhang som denna rapport gäller är den avgörande faktorn att en del av den interkontinentala kommunikationen sker på C-bandet i G-beams från INTELSAT-satelliter och andra (t ex INTERSPUTNIK), och att det kan krävas en satellitantenn med diametern ca 30 m för mottagningen (se kapitel 5). Antenner på 30 m krävdes också för de första

avlyssningsstationerna för kommunikationssatelliter, eftersom den första generationen inom INTELSAT bara hade G-beam, samtidigt som signalöverföringen inte nått samma tekniska nivå som idag. Dessa paraboler med en diameter som delvis överstiger 30 m används på sådana stationer fortfarande, även om de tekniskt sett är överdimensionerade idag.

De typiska antenner som idag krävs för INTELSAT-kommunikation på C-bandet har en diameter på 13 - 18 m. I enstaka fall (t ex för INTELSAT 511) krävs en större antenn för mottagning av G-beam. För de nyaste INTELSAT-satelliterna räcker det för mottagning av Z-beam på C-bandet med en antenn som har en diameter på upp till 5 m.
För mottagning av kommunikation på C-bandet från INTERSPUTNIK krävs antenner på mellan 2 och 25 m i diameter.

För Ku-spots från INTELSAT-satelliter, och från en del andra satelliter (EUTELSAT Ku-band; AMOS Ku-band, m fl) krävs antenner på mellan 2 och 10 m i diameter.

För satellitterminaler som arbetar på V-bandet och vilkas signal på grund av den höga frekvensen kan fokuseras ännu bättre än på Ku-bandet, räcker antenndiametrar på 0,9 - 3,7 m (t ex VSAT-kommunikation inom EUTELSAT eller INMARSAT).

5. Indicier som talar för förekomsten av minst ett globalt avlyssningssystem

5.1. Varför bara indicier?

De nationella säkerhetstjänsterna håller av naturliga skäl sitt arbete hemligt. Det finns därför inga officiella uttalanden från underrättelseorganisationerna i ECHELON-länderna som bekräftar att de gemensamt driver ett globalt avlyssningssystem. Ett bevis för att detta sker måste därför ha formen av största möjliga antal indicier, som tillsammans skapar ett övertygande indiciebevis.

Indiciekedjan för ett sådant bevis består av tre element:

- Bevis för att underrättelsetjänsterna i ECHELON-staterna avlyssnar kommunikation från privatpersoner och företag.
- Bevis för att det finns avlyssningsstationer på sådana platser som de civila kommunikationssatellitsystemen når, vilka drivs av ECHELON-staterna.
- Bevis för att det finns ett underrättelsesamarbete mellan dessa stater som går långt utöver det som varit praxis tidigare. Om detta samarbete går så långt att den ena parten kan registrera trafik och överlämna denna oanalyserad till en annan part, har mindre betydelse för beviset att det existerar ett sådant samarbete. Denna fråga får betydelse först när man vill klarlägga eventuella hierarkier inom ett sådant avlyssningssamarbete.

5.1.1. Bevis för att underrättelsetjänsterna bedriver avlyssningsverksamhet

Åtminstone i demokratiska länder bedrivs underrättelseverksamheten på grundval av lagar som fastställer verksamhetens mål och/eller befogenheter. Det är därför lätt att bevisa att det i många av dessa länder finns underrättelseverksamhet som är inriktad på avlyssning av civil kommunikation. Detta gäller också för de fem så kallade ECHELON-staterna, som alla har sådan verksamhet. Hos vart och ett av dessa länder krävs inga särskilda ytterligare bevis för att trafik till och från det egna landet avlyssnas. Från det egna territoriet kan åtminstone en del av den satellitkommunikation avlyssnas som innehåller information riktad till mottagare i utlandet. I de fem ECHELON-staterna saknas lagstiftning som begränsar denna verksamhet. Den inre logiken i metoden för strategisk kontroll av kommunikationen till och från utlandet, och dess åtminstone delvis offentliggjorda syfte, gör det omöjligt att anta något annat än att verksamheten faktiskt bedrivs på detta sätt. [1]

5.1.2. Bevis för att det finns avlyssningsstationer i de geografiskt nödvändiga områdena

Den enda begränsningen för försöket att bygga upp en heltäckande global övervakning av satellitkommunikationerna ligger i själva teknikens begränsningar. Det finns ingen plats, från vilken man kan avlyssna **all** satellittrafik (se punkt 4.2.5).

[1] Föredraganden har fått uppgift om att detta är korrekt. Källan är skyddad.

Ett globalt avlyssningssystem bygger på en av tre möjligheter:

- den som driver systemet har eget territorium i alla delar av världen som behövs;
- den som driver systemet har delvis eget territorium i alla delar av världen som krävs, och får disponera territorium i de övriga delar av världen som krävs, där stationer får drivas eller delvis disponeras;
- den som driver systemet är en allians av nationella underrättelsetjänster och driver systemet i de delar av världen som krävs.

Ingen av ECHELON-staterna skulle ensam kunna driva ett globalt system. USA har åtminstone på papperet inga kolonier. Kanada, Australien och Nya Zeeland har inte heller några egna territorier utanför det egna landets gränser. Inte heller Storbritannien skulle ensamt kunna driva ett globalt avlyssningssystem (se kapitel 6).

5.1.3. Bevis för ett intimt underrättelsesamarbete

Det är däremot inte offentligt uttalat om och hur ECHELON-staterna samarbetar med varandra i underrättelsefrågor. Normalt brukar underrättelsetjänsterna samarbeta bilateralt och på grundval av ett utbyte av analyserat material. Ett multilateralt samarbete är redan i sig något mycket ovanligt. Om därtill kommer att man regelbundet utväxlar obearbetade data har en helt ny dimension tillfogats. Ett samarbete av detta slag kan bara avslöjas med hjälp av indicier.

5.2. Hur känner man igen en avlyssningsstation för satellittrafik?

5.2.1. Kriterium 1: stationens tillgänglighet

Anläggningar med stora antenner som drivs av posten, radion eller forskningsinstitutioner är tillgängliga för besök, låt vara efter anmälan i förväg. Detta gäller inte avlyssningsanläggningar. Normalt drivs de formellt av försvaret, som också tekniskt genomför själva avlyssningen. För NSA bedriver t ex marinens Naval Security Group (NAVSECGRU) eller flygvapnets Air Intelligence Agency (AIA) sådan avlyssning. I de brittiska stationerna är det Royal Airforce som bedriver verksamheten för den brittiska underrättelsetjänstens GCHQ räkning. Detta upplägg gör det möjligt att ha en militär hård bevakning av anläggningen, samtidigt som dess syfte maskeras.

5.2.2. Kriterium 2: antenntypen

I anläggningar som uppfyller kriterium 1 kan man hitta olika slag av antenner, som skiljer sig tydligt från varandra. Formen på antennen avslöjar syftet med avlyssningsanläggningen. Man använder en uppsättning höga stavantenner, placerade i en ring med stor diameter (så kallade Wullenweber-antenner) för pejling av riktningen till signalavsändaren. Ringformigt utplacerade rombiska antenner (s k Pusher-antenner) har samma syfte. Antenner för mottagning från alla håll, eller riktantenner, som ser ut som jättelika klassiska tv-antenner, används för avlyssning av oriktade radiosignaler. **För mottagning av satellitsignaler använder man emellertid enbart parabolantenner**. Om parabolantennerna står öppet i terrängen kan man med kännedom om deras geografiska ort, deras lutningsvinkel (elevation) och deras riktning (azimut) beräkna vilken satellit som avlyssnas. Detta skulle man exempelvis kunna göra i Morwenstow i Storbritannien eller i Yakima och Sugar Grove i USA. Oftast döljs parabolantennerna emellertid under sfäriska vita skal, så kallade radomer. De skyddar antennerna men döljer samtidigt vart dessa är riktade.

Om man hittar parabolantenner eller radomer på platsen för en avlyssningsanläggning, så vet man att anläggningen avlyssnar satellittrafik. Man kan dock inte säga vilken typ av signaler som avlyssnas.

5.2.3. Kriterium 3: antennstorleken

Antenner för mottagning av satellitsignaler i en anläggning som uppfyller kriterium 1 kan ha olika syften:
- mottagning av militär trafik;
- mottagning av spionsatellitinformation (bilder, radar);
- mottagning av signaler från militära SIGINT-satelliter;
- mottagning för avlyssning av civil satellittrafik.

Man kan inte av utsidan på antennen/radomen avgöra vilket syfte de har. Det finns dock tekniskt baserade minimikrav i fråga om storlek för antenner som skall ta emot den s k Global Beam på C-bandet för civil satellitkommunikation. För den första generationen av dessa satelliter krävdes antenner med en diameter på 25 - 30 m, men idag räcker det med en diameter på 15 - 18 m. För automatisk filtrering av mottagna signaler i en dator krävs högsta möjliga signalkvalitet, varför man för underrättelseverksamhet väljer en antennstorlek i övre delen av intervallet. Eftersom antennen sitter på ett stativ är radomens diameter ännu större än antennens.

5.2.4. Slutsats

Så vitt rapportförfattaren känner till har antenner av denna storlek ingen militär användning. Om så stora antenner därför placerats på en plats som uppfyller kriterium -1 avlyssnar man där civil satellitkommunikation.

5.3. Offentligt tillgängliga uppgifter om kända avlyssningsstationer

5.3.1. Metod

För att fastställa vilka stationer som uppfyller kriterierna enligt punkt 5.2 och ingår i det globala avlyssningssystemet, och vilka uppgifter de har, har relevanta, ibland motstridiga, dokument granskats (Hager[1], Richelson[2], Campbell[3]), tidigare sekretessbelagda dokument,[4] hemsidan för Federation of American Scientists[5], hemsidan från dem som driver stationen[6] (NSA; AIA m fl) och andra Internet-publikationer. Därutöver sammanställs kommunikationssatelliternas

---

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

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

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

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

[5] Federation of American Scientists.

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

täckningszoner, de nödvändiga antennstorlekarna beräknas, och införs på världskartor tillsammans med tänkbara stationer.

5.3.2. Noggrann analys

För analysen tillämpas följande principer som sammanhänger med fysiken bakom satellitkommunikation (se även kapitel 4):

- En satellitantenn kan aldrig registrera annat än sådant som befinner innanför dess mottagningszon. För att kunna ta emot kommunikation som främst sker på C- och Ku-banden måste en antenn ligga innanför den täckningszon som gäller för C- resp Ku-bandet.
- För varje Global Bean krävs en satellitantenn, också om två satelliters Beams överlappar varandra.
- Om en satellit har fler täckningszoner än den för Global Bean, vilket är typiskt för dagens generation av satelliter, kan man inte längre med en enda satellitantenn registrera all den trafik som förmedlas av denna satellit, eftersom en enda satellitantenn inte kan befinna sig i samtliga av satellitens täckningszoner. För mottagning av Hemi-Beams och Global Beam från en satellit krävs alltså två satellitantenner på olika platser (se bilden av täckningszonerna i kapitel 4). Om ytterligare Beams tillkommer (Zone Beam, Spotbeams), krävs ytterligare satellitantenner. Olika Beams från en viss satellit kan dock överlappa och då tas emot av en enda satellitantenn, eftersom det tekniskt är möjligt att separera signaler som kommer på olika frekvensband.

Därutöver gäller de förutsättningar som omnämndes i punkt 5.2: anläggningarna är inte tillgängliga, eftersom de drivs av militären[1]; parabolantenner krävs för mottagning av satellitsignaler; och storleken på satellitantenner för mottagning av C-bandet i Global Beam är över 25 m för den första INTELSAT-generationen, och för de senare generationerna 15 - 18 m.

5.3.2.1. Parallelliteten mellan INTELSAT-utvecklingen och byggandet av stationer

Ett globalt avlyssningssystem måste växa när kommunikationen utvecklas. När satellitkommunikationen började ta fart måste alltså stationer byggas, och när nya satellitgenerationer införs uppstår nya stationer och nya antenner byggs efter de aktuella kraven. Antalet stationer och antalet antenner måste hela tiden växa för att klara av kommunikationen. Omvänt gäller att om nya stationer och nya antenner byggs där nya täckningszoner uppkommer så är detta ingen tillfällighet utan ett indicium på att det är fråga om en avlyssningsstation för kommunikation.
Eftersom INTELSAT var det första kommunikationssystemet för satelliter och täckte hela jordklotet, är det logiskt att uppkomsten och utvidgningen av stationer sker parallellt med INTELSAT.

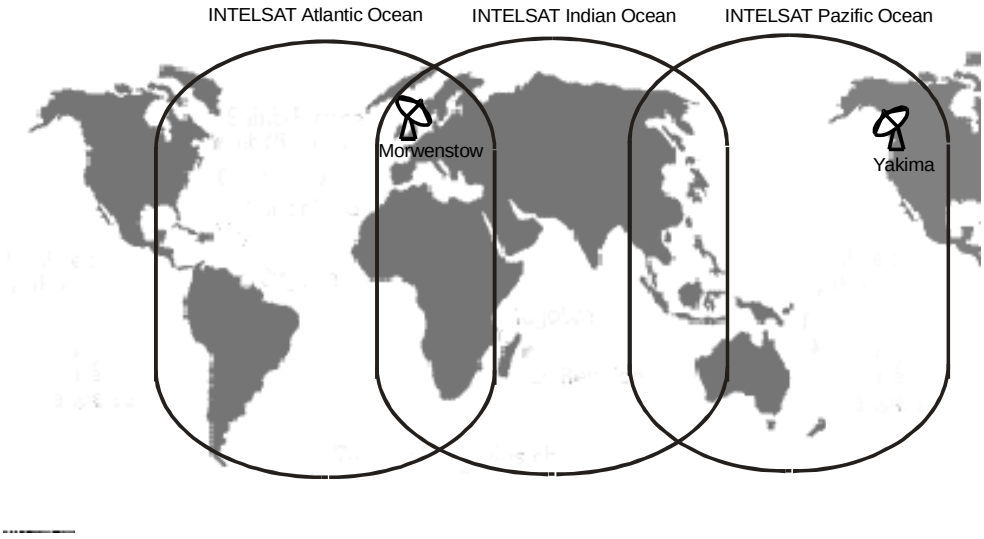
Den första generationen

Redan 1965 skickades den först INTELSAT-satelliten (Early Bird) upp i geostationär bana. Dess överföringskapacitet var fortfarande svag och täckningszonen var bara det norra halvklotet. Med INTELSAT-generationerna II och III, som togs i drift 1967 resp 1968, nådde man för första gången global täckning. Satelliternas Global Beams täckte länderna kring Atlanten, Indiska Oceanen och Stilla Havet. Det fanns ännu inte några smala täckningszoner. För att uppfånga all

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

trafik räckte det med tre satellitantenner. Eftersom två Global Beams överlappade varandra över Europa kunde man i detta område på samma station med två antenner med olika riktning avlyssna trafiken från två satelliter.

Den första globala satellitgenerationen i INTELSAT

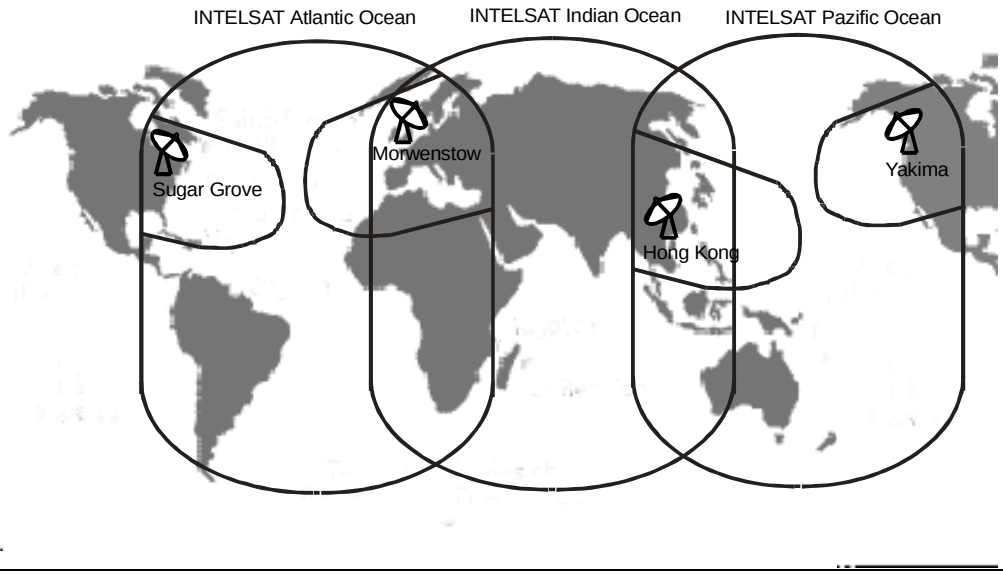


1970 grundades **Yakima** i nordvästra USA, 1972/73 **Morwenstow** i Sydengland. I Yakima fanns då en stor antenn (riktad mot Stilla Havet), Morwenstow hade två stora antenner (en riktad mot Atlanten, en mot Indiska Oceanen. Genom de båda stationernas positioner kunde all kommunikation avlyssnas. 1974 byggdes den första stora satellitantennen, i Menwith Hill.

Den andra globala generationen

Den andra generationen av INTELSAT-satelliterna (IV och IVA) utvecklades på 70-talet och skickades upp i geostationär bana (1971 och 1975). De nya satelliterna, som också gav global täckning och klarade betydligt fler telefonlinjer (4000-6000), hade utöver Global Beams och Zone Beams mot det norra halvklotet (se kapitel 4). En Zone Beam täckte östra USA, en västra USA, en västra Europa och en Ostasien. Med två stationer och tre antenner kunde man nu inte längre avlyssna all kommunikation. Med de befintliga stationerna i Yakima kunde man ta emot Zone Beam i västra USA, med den i Morwenstow Zone Beam i Europa. För att ta emot de övriga två Zone Beams blev man tvungen att bygga en station i östra USA och en i Ostasien.

Den andra globala satellitgenerationen i INTELSAT



I slutet av 70-talet byggdes **Sugar Grove** i östra USA (stationen fanns redan för avlyssning av rysk kommunikation), och togs i drift 1980. I **Hongkong** bygges också en station i slutet av 70-talet.
Därmed hade man på 80-talet med fyra stationer – Yakima, Morwenstow, Sugar Grove och Hongkong – global täckning av INTELSAT-kommunikationen.

Den senare INTELSAT-satelliterna med Zone Beams och Spot Beams utöver sina Global Beams och Hemi-Beams krävde ytterligare nya stationer på olika håll i världen. Här är det svårt att skapa ett samband mellan uppkomsten av ytterligare stationer respektive nya antenner.
Eftersom man också endast med svårighet kan få information om stationerna kan man inte exakt ange vilka satelliter och vilka Beams som avlästes av vilken station. Man kan dock fastställa inom vilka Beam-zoner kända stationer befinner sig.

5.3.2.2. Global täckning med stationer som säkert är tilldelade kommunikationssatelliter

Idag sker den globala satellitkommunikationen via INTELSAT, INMARSAT och INTERSPUTNIK. Uppdelningen på tre täckningszoner (Indiska Oceanen, Stilla Havet och Atlanten) har blivit kvar från den första satellitgenerationen.
I var och en av täckningszonerna finns stationer som uppfyller kriterierna för avlyssningsstationer.

Satelliter över Indiska Oceanen:

INTELSAT 604 (60°E), 602 (62°E), 804 (64°E), 704 (66°E) EXPRESS 6A (80°E) INMARSAT indiska zonen	Geraldton, Australien Pine Gap, Australien Morwenstow, England Menwith Hill, England

INTELSAT APR1 (83°), APR-2 (110,5°)	Geraldton, Australien Pine Gap, Australien Misawa, Japan

Satelliter över Stilla Havet:

INTELSAT 802 (174°), 702 (176°), 701 (180°) GORIZONT 41 (130°E), 42 (142°E), LM-1 (75°E) INMARSAT stillahavs-zonen	Waihopai, Nya Zeeland Geraldton, Australien Pine Gap, Australien Misawa, Japan Yakima, USA - endast Intelsat och Inmarsat

Satelliter över Atlanten:

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 atlant-zonen	Sugar Grove, USA Buckley Field, USA Sabana Seca, Puerto Rico Morwenstow, England Menwith Hill, England
INTELSAT 707 (359°)	Morwenstow, England Menwith Hill, England

Därmed är klarlagt att det är möjligt att uppnå en global avlyssning av kommunikationen

Därutöver finns ytterligare stationer, som inte uppfyller kravet på antennstorlek, men som ändå kan ingå i det globala avlyssningssystemet. Med dessa stationer kan t ex Zone Beams eller Spot Beams tas emot från satelliter vilkas Global Beams tas emot på annat håll, eller för vilkas Global Beams en mindre antenn är tillräcklig.

5.3.2.3. Närmare om stationerna

De närmare beskrivningarna av stationerna skiljer mellan sådana som enbart sysslar med att avlyssna kommunikationssatelliter (kriterier enligt punkt 5.2) och stationer vilkas uppgift inte kan fastställas med hjälp av dessa kriterier.

5.3.2.3.1. Stationer för avlyssning av kommunikationssatelliter

De kriterier som nämns i punkt 5.2 och utgör indicier för en avlyssningsstation för kommunikationssatelliter uppfylls också av följande stationer:

Yakima, USA (120°W, 46°N)
Stationen byggdes 1970 samtidigt med den första satellitgenerationen. Sedan 1995 finns här Air Intelligence Agency (AIA) med 544th Intelligence Group (Detachment 4). Här är också stationerade Naval Security Group (NAVSECGRU). På området finns sex satellitantenner, vilkas storlek inte anges i källorna. Hager beskriver antennerna som stora och anger att de är riktade mot Intelsat-satelliter över Stilla Havet (2 antenner) respektive Atlanten, liksom mot Inmarsat-satellit nr 2.
Datum för tillkomsten av Yakima-anläggningen samtidigt med den första Intelsat-generationen, liksom den allmänna beskrivningen av 544th Intelligence Group talar för att Yakima spelar en

roll för den globala avlyssningen av kommunikation. Ytterligare ett indicium för detta är Yakimas närhet till en andra satellitföljarstation, som ligger 160 km norr därom.

Sugar Grove, USA (80°W, 39°N)
Sugar Grove grundades samtidigt med driftsättning av den andra generationens Intelsat-satelliter, i slutet av 70-talet. Här finns stationerade NAVSECGRU och AIA med 544th Intelligence Group (Detachment 3). Stationen har enligt uppgift från olika källor 10 satellitantenner, av vilka tre är större än 18 m (18,2 m, 32,3 m och 46 m), vilket entydigt säger att de är avsedda för att avlyssna kommunikationssatelliter. En uppgift för Detachment 3 av 544th Intelligence Group vid denna station är att erbjuda ”Intelligence Support” och samla in information från kommunikationssatelliter som kommer från marinens fältstationer.[1]Dessutom ligger Sugar Grove i närheten (100 km) av satellitföljarstationen i Etam.

Sabana Seca, Puerto Rico (66°W, 18°N)
1952 stationerades NAVSECGRU i Sabana Seca. Sedan 1995 finns där också AIA med 544th IG (Detachment 2). Stationen har minst en satellitantenn med diametern 32 m och 4 andra mindre antenner.
Stationens uppgift är enligt officiella källor ”performing satellite communication processing”, ”cryptologic and communications services”, samt stöd till verksamhet inom US Navy och DoD (t ex insamling av COMSAT-data, enligt beskrivning för 544th IG). I framtiden skall Sabana Seca vara den första fältstationen för analys och bearbetning av satellitkommunikation.

Morwenstow, England (4°W, 51°N)
Morwenstow grundades liksom Yakima samtidigt med den första INTELSAT-generationen i början av 70-talet. Morwenstow drivs av den brittiska underrättelsetjänsten (GCHQ). Där finns omkring 30 satellitantenner, av vilka två har en diameter på 30 m. Inga uppgifter finns om de övriga antennernas storlek.
Inga officiella uppgifter finns om stationen. Storleken på och antalet antenner liksom läget bara 110 km från telekomstationen i Goonhilly lämnar inget utrymme för tvivel på att detta är en avlyssningsstation för kommunikationssatelliter.

Menwith Hill, England (2°W, 53°N)
Menwith Hill grundades 1956 och 1974 stod här redan 8 satellitantenner. Numera är antalet antenner 30, av vilka några har en diameter på över 20 m. I Menwith Hill arbetar britter och amerikaner gemensamt. Från amerikansk sida finns där NAVSECGRU, AIA (451st IOS) samt INSCOM, som också leder stationen. Marken som Menwith Hill ligger på tillhör det brittiska försvarsdepartementet och hyrs ut till den amerikanska regeringen. Enligt officiella uppgifter är syftet med Menwith Hill ”to provide rapid radio relay and to conduct communications research”. Enligt uppgifter från Richelson och Federation of American Scientists är Menwith Hill både markstation för spionsatelliter och markstation för ryska kommunikationssatelliter.

Geraldton, Australien (114°O, 28°S)
Denna station grundades i början av 90-talet. Stationen leds av den australiska säkerhetstjänsten (DSD). Britter som varit stationerade i Hongkong (se ovan) tillhör nu denna station. Sex

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

satellitantenner, av vilka minst en har en diameter på ca 20 m (uppskattad storlek), är enligt uppgift från Hager riktade mot satelliter över Indiska Oceanen och Stilla Havet.
Enligt uppgifter av en edsvuren sakkunnig inför det australiska parlamentet avlyssnas kommunikationssatelliter i Geraldton.[1]

Pine Gap, Australien (133°O, 23°S)
Stationen i Pine Gap grundades 1966. Den leds av den australiska säkerhetstjänsten (DSD), och omkring hälften av de ca 900 personerna vid stationen är amerikaner, från CIA och NAVSECGRU.[2]
Pine Gap har 18 satellitantenner, av vilka en har diameter på ca 30 m och en på ca 20 m. Enligt officiella uppgifter och data från andra källor upprättades stationen som markstation för SIGINT-satelliter. Härifrån styrs flera spionsatelliter och deras signaler tas emot, bearbetas och analyseras. De stora satellitantennerna talar dock för att avlyssning pågår av kommunikationssatelliter, eftersom det inte behövs några stora antenner för signalerna från SIGINT-satelliterna. Fram till 1980 var australierna utestängda från signalanalysavdelningen, men har nu full tillgång till allt utom amerikanernas nationella krypteringsrum.

Misawa, Japan (141°O, 40°N)
Stationen i Misawa finns sedan 1948. Där arbetar japaner och amerikaner. Från amerikansk sida finns där NAVSECGRU, INSCOM samt några AIA-grupper (544th IG, 301st IS). På området finns omkring 14 satellitantenner, av vilka några har en diameter på ca 20 m (uppskattad storlek). Misawa är officiellt ett Cryptology Operations Center. Enligt uppgift av Richelson avlyssnas i Misawa de ryska Molnija-satelliterna och andra ryska kommunikationssatelliter.

Waihopai, Nya Zeeland (173°O, 41°S)
Waihopai grundades 1989. Sedan dess finns här en stor antenn med 18 m diameter, en andra, mindre antenn sattes upp senare. Enligt Hager är den stora antennen riktad mot Intelsat 701 ovanför Stilla Havet.

Buckley Field, USA, Denver Colorado (104°W, 40°N)
Denna station grundades 1972. Här finns 544th IG (Detachment 45). På området står ca 5 satellitantenner, av vilka 4 har en diameter på ca 20 m. Den officiella uppgiften för stationen är att registrera data om kärnexplosioner med hjälp av SIGINT-satelliter, som sedan analyseras. Storleken på satellitantennerna tyder att de även används för avlyssning av civil kommunikation.

Hong Kong (22°N, 114°O)
Denna station grundades i slutet av 70-talet när den andra INTELSAT-generationen sköts upp. Den försågs med stora satellitantenner. Inga närmare uppgifter finns om antennernas mått. 1994 började en nedmontering av stationen i Hongkong. Antennerna fraktades till Australien. Det är inte helt klart vilka stationer som tagit över det arbete som bedrevs i Hongkong: Geraldton, Pine Gap eller kanske Misawa i Japan.
Eventuellt har uppgifterna fördelats på flera stationer.

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

5.3.2.3.2. Övriga stationer

Vid följande stationer kan funktionen inte säkert beläggas utgående från de nämnda kriterierna:

Leitrim, Kanada (75°W, 45°N)
Leitrim ingår i utbytesprogrammet mellan kanadensiska och amerikanska militära enheter. Därför har US Navy enligt uppgift ca 30 personer stationerade i Leitrim. 1985 installerades den första av 4 satellitantenner, av vilka de båda större bara är ca 12 m i diameter (uppskattad storlek).
Stationens uppgift är officiellt ”cryptologic rating” och avlyssning av diplomatisk trafik.

Bad Aibling, Tyskland (12°O, 47°N)
Stationen i närheten av Bad Aibling bemannas av ca 750 amerikaner och övertogs 1952 av den amerikanska armén (från 1972 till 1994 drevs den av DoD). I Bad Aibling finns NAVSECGRU, INSCOM (66th IG, 718th IG), samt olika AIA-grupper (402nd IG, 26th IOG). Där finns 14 satellitantenner, av vilka ingen är större än 18 m. Officiellt har Bad Aibling följande uppgifter: ”Rapid Radio Relay and Secure Commo, Support to DoD and Unified Commands, Medium and Longhand Commo HF & Satellite, Communication Physics Research, Test and Evaluate Commo Equipment”. Enligt Richelson är Bad Aibling markstation för SIGINT-satelliter och ryska kommunikationssatelliter.

Ayios Nikolaos, Cypern (32°O, 35°N)
Ayios Nikolaos på Cypern är en brittisk station. Stationens uppgift, med dess 9 satellitantenner av obekant storlek, är uppdelad på två enheter, ”Signals Regiment Radio” och ”Signals Unit (RAF)”.
Läget för Ayios Nikolaos i närheten av arabstaterna och det faktum att detta är den enda stationen inom några täckningszoner (framför allt för Spot Beams) talar för att den har en viktig roll för underrättelsearbetet.

Shoal Bay, Australien (134°O, 13°S)
Shoal Bay drivs av den australiska underrättelsetjänsten. Där skall finnas 10 satellitantenner, vilkas storlek inte är närmare känd. Av de satellitantenner som finns på fotografi har de fem största högst 8 m diameter, och den synliga sjätte antennen är ännu mindre. Enligt uppgift av Richelson är antennerna inriktade på de indonesiska PALAPA-satelliterna. Det är inte klart huruvida stationen ingår i det globala systemet för avlyssning av civil kommunikation.

Guam, Stilla Havet (144°O, 13°S)
Guam finns sedan 1898. Idag finns där en Naval Computer and Telecommunication Station, som bemannas av 544th IG av AIA samt Navy-personal.
Stationen har minst två satellitantenner, vilkas storlek inte är känd. Uppgifterna för stationen på Guam är därför oklar.

Kunia, Hawaii (158°W, 21°N)
Den här stationen drivs sedan 1993 som Regional Security Operation Center (RSOC), bemannad av NAVSECGRU och AIA. Till dess uppgifter hör bearbetning av information och kommunikation, samt kryptologiskt stöd. Uppgifterna för stationen i Kunai är oklar.

Medina Annex, USA Texas (98°W, 29°N)
Medina är liksom Kunia en Regional Security Operation Center och grundades 1993. Den bemannas av NAVSECGRU och AIA och har uppgifter i Västindien-området.

Fort Gordon (81°W, 31°N)
Fort Gordon är också en Regional Security Operation Center, bemannad av INSCOM och AIA (702nd IG, 721st IB, 202nd IB, 31st IS), med oklar uppgift.

Fort Mead, USA (76°W, 39°N)
Fort Mead är NSA:s huvudkontor.

5.3.3. Sammanfattning av resultaten

Följande slutsatser kan dras av de samlade data om stationerna, satelliterna och de ovan beskrivna förutsättningarna:
1. Det finns inom varje täckningszon avlyssningssationer för minst en av Global Beams, med minst en antenn som är större än 18 m i diameter, och som drivs av amerikaner eller britter, respektive på en plats där amerikaner eller britter bedriver underrättelseverksamhet. Detta är ett starkt indicium för förekomsten av ett globalt avlyssningssystem.
2. Utvecklingen av INTELSAT-kommunikationen och den samtidiga tillkomsten av motsvarande avlyssningsstationer styrker systemets globala uppbyggnad.
3. Av punkt 1 och 2 kan man entydigt identifiera vissa stationer som avlyssningsstationer för internationell satellitkommunikation.
4. De uppgifter som finns i de tidigare sekretessbelagda dokumenten och som ges av de ansvariga organen (AIA, NSA, US Navy osv) kan användas för att styrka slutsatserna om de där omnämnda stationerna.
5. Vissa stationer är placerade så att de samtidigt kan ta emot Beams och Spots från flera satelliter, så att de kan registrera en stor del av kommunikationen.
6. Det finns ytterligare andra stationer som inte har några stora antenner, men som ändå kan ingå i systemet, genom att de kan ta emot kommunikation från Beams och Spots. Här får man släppa kravet på antennstorlek och gå på andra indicier.
7. Vissa av de nämnda stationerna ligger bevisligen i närheten av reguljära satellitföljande stationer för kommunikationssatelliter.

5.4. UKUSA-avtalet

UKUSA-avtalet betecknas ett avtal om SIGINT som undertecknades 1948 av Storbritannien (United Kingdom, UK), USA och Australien, Kanada och Nya Zeeland.

5.4.1. UKUSA-avtalets historiska utveckling[1]

UKUSA-avtalet är en fortsättning på det intima samarbete som ägde rum mellan USA och Storbritannien redan under andra världskriget och som redan börjat ta form under första världskriget.

[1] Christopher Andrew, "The making of the Anglo-American SIGINT Alliance" i E. Hayden, H. Peake and S. Halpern, eds., In the Name of Intelligence. Essays in honor of Washington Pforzheimer (Washington NIBC Press 1995) s. 95 –109.

Initiativet till bildandet av en SIGINT-allians togs av amerikanerna i augusti 1940 vid ett möte mellan amerikaner och britter i London[1] I februari 1941 levererade amerikanska kryptoanalytiker en Cipher Machine (PURPLE) till Storbritannien. På våren 1941 började det kryptoanalytiska samarbetet.[2] Samarbetet mellan underrättelsetjänsterna förstärktes vid den gemensamma insatsen av flottorna i Nordatlanten på sommaren 1941. I juni 1941 kunde britterna knäcka den tyska flottkoden ENIGMA.
Amerikas inträde i kriget hade förstärkt SIGINT-samarbetet ytterligare. 1942 började amerikanska kryptoanalytiker arbeta vid Naval SIGINT Agency i Storbritannien.[3]
Kommunikationen mellan U-boat Tracking Rooms i London, Washington, och från maj 1943 också Ottawa, Kanada, blev så intim att de berörda enligt en uppgift från en medarbetare arbetade som en enda organisation.[4]
Tidigt 1943 undertecknades avtalet BRUSA-SIGINT, och ett utbyte av personal skedde. Innehållet i avtalet gäller bl a uppdelning av arbetet och sammanfattas i de tre första styckena: Det omfattar utbyte av diverse information i samband med upptäckande, identifiering och avlyssning av signaler, samt arbete med att avslöja koder och krypton. Amerikanerna var huvudansvariga för Japan, britterna för Tyskland och Italien.[5]
Efter kriget utgick initiativet för bevarandet av en SIGINT-allians främst från Storbritannien. Grunderna för alliansen överenskoms vid en världsturné med brittiska underrättelsetjänstemän (bl a Sir Harry Hinsley, vars böcker ligger till grund för den citerade artikeln) på våren 1945. Ett mål var att skicka SIGINT-personal från Europa till Stilla Havet för kriget mot Japan. I detta sammanhang överenskoms med Australien att ställa resurser och personal (britter) till den australiska underrättelsetjänstens förfogande. Vid återfärden till USA togs vägen via Nya Zeeland och Kanada.
I september 1945 undertecknade Truman ett strängt hemligt PM, som blev hörnstenen i ett SIGINT-samarbete under fredstid.[6] Därefter fördes förhandlingar mellan britterna och amerikanerna om ett avtal. En brittisk delegation tog också kontakt med kanadensare och australier, för att diskutera deras eventuella medverkan. I februari och mars 1946 ägde en strängt hemlig angloamerkiansk SIGINT-konferens rum, där man skulle diskutera detaljerna. Britterna hade fått fullmakt av Kanada och Australien. Produkten från konferensen var ett fortfarande hemligstämplat avtal på ca 25 sidor, som fastställde detaljerna i ett SIGINT-avtal mellan USA

[1] ibidem, 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 for a free exchange of intelligence´. (COS (40)289, CAB 79/6, PRO. Smith, The Ultra Magic Deals, pp. 38, 43-4. Sir F.H. Hinsley, et al., British Intelligence in the Second World War, vol.I, s.312-13).
[2] ibidem, s. 100: „ In the spring of 1941, Steward Menzies, the Chief of SIS, appointed an SIS liason officer to the British Joint Services Missin in Washington, Tim O´Connor, …, to advice him on cryptologic collaboration"
[3] Ibidem, s. 100 (Sir F.H. Hinsley, et al., British Intelligence in the Second World War, vol II, s.56)
[4] Ibidem, s. 101 (Sir F.H. Hinsley, et al., British Intelligence in the Second World War, vol II, s.48)
[5] Ibidem, s.101-2: Interivjuer med Sir F.H. Hinsley, "Operations of the Military Intelligence Service War Department London (MIS WD London)," 11 June 1945, Tab A, RG 457 SRH-110, NAW
[6] 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." (from Bradley F. Smith, The Ultra-Magic Deals and the Most Secret Special Relationship (Novato, Ca: Presidio 1993))

och Brittiska Samväldet. Fortsatta förhandlingar fördes under de följande två åren, så att den slutliga texten i det så kallade UKUSA-avtalet kunder undertecknas i juni 1948. [1]

5.4.2. Belägg för att avtalet finns

Det finns hittills inget officiellt erkännande av UKUSA-avtalet från de undertecknande staterna. Dock finns det flera klara belägg för att avtalet existerar.

5.4.2.1. Förkortningslistan inom US Navy

UKUSA står enligt US Navy [2] för United Kingdom-USA och betecknar ett SIGINT-avtal mellan 5 nationer.

5.4.2.2. Utsaga från DSD-chefen

Chefen för den australiska underrättelsetjänsten (DSD) bekräftade existensen av detta avtal i en intervju: Enligt hans utsaga arbetar den australiska säkerhetstjänsten tillsammans med andra utländska underrättelsetjänster enligt UKUSA-avtalet. [3]

5.4.2.3. Rapport från Canadian Parliamentary Security and Intelligence Committee

I denna rapport berättas att Kanada samarbetar om underrättelser med några av sina närmaste och äldsta allierade. Rapporten nämner dessa allierade: USA (NSA), Storbritannien (GCHQ), Australien (DSD) och Nya Zeeland (GCSB). Namnet på avtalet anges inte i rapporten.

5.4.2.4. Utsaga från förre vice chefen för NSA, dr Louis Torella

I en intervju med Christopher Andrew, professor vid Cambridge University, i november 1987 och april 1992 bekräftar före vice chefen för NSA, dr Louis Torella, som var närvarande vid undertecknandet, att avtalet existerar. [4]

5.4.2.5. Brev från förre chefen för GCHQ Joe Hooper

Den tidigare chefen för GCHG, Joe Hooper, omnämner UKUSA-avtalet i ett brev till den dåvarande NSA-chefen Marshall S. Carter.

5.4.2.6. Samtal som föredraganden fört med olika personer

Föredraganden har fört samtal om avtalet med flera personer som genom sin verksamhet måste ha kännedom om UKUSA-avtalet och dess innehåll. Vid dessa tillfällen har avtalets existens indirekt bekräftats i samtliga fall genom typen av svar.

---

[1] Christopher Andrew, "The making of the Anglo-American SIGINT Alliance" i E. Hayden, H. Peake and S. Halpern eds, In the Name of Intelligence. Essays in honor of Washington Pforzheimer (Washington NIBC Press 1995) pp. 95 –109: Interviews with Sir Harry Hinsley, March/April 1994, who did a part of the negotiations; Interviews with Dr. Louis Tordella, Deputy Director of NSA from 1958 to 1974, who was present at the signing.
[2] „Terms/Abbreviations/Acronyms" offentliggjort av US Navy and Marine Corps Intelligence Training Centre (NMITC) på http://www.cnet.navy.mil/nmitc/training/u.html
[3] Martin Brady, Direktor des DSD, Canberra 16. März 2000.
[4] Andrew, Christopher „The growth of the Australian Intelligence Community and the Anglo-American Connection", pp. 223-4.

5.5. Analys av amerikanska ej hemligstämplade dokument

5.5.1. Typ av dokument

Inom ramen för "Freedom of Information Act" av 1966 (5 U.S.C. § 552) och förordning inom Department of Defense (DoD FOIA Regulation 5400.7-R av 1997) hävdes sekretessen på vissa dokument så att de blev offentligt tillgängliga.
Dokumenten är åtkomliga via National Security Archive, som grundats 1985 och har placerats vid George Washington University i Washington DC. Författaren Jeffrey Richelson, som tidigare arbetat för National Security Archives, har via Internet offentliggjort 16 dokument som ger en inblick i hur NSA (National Security Agency) uppkommit, utvecklats, styrs och regleras.[1]
Därutöver nämns i två av dessa dokument ECHELON. Dessa dokument citeras gång på gång av olika författare som skriver om ECHELON, och anförs som bevis för existensen av det globala spionagesystemet ECHELON. Därutöver finns bland de dokument som Richelson ställer till förfogande sådana som bekräftar existensen av NRO (National Reconnaissance Office) och beskriver dess funktion som ansvarig för SIGINT-satelliter.[2]

5.5.2. Dokumentens innehåll

Dokumenten innehåller fragmentariska beskrivningar av eller hänvisningar till följande:

5.5.2.1 Direktiv och bakgrund för NSAS (dokument 1, 4, 10, 11, 16)

I National Security Council Intelligence Directive 9 (NSCID 9) av den 10 mars 1950 definieras i relation till COMINT begreppet utrikeskommunikation: **utrikeskommunikation är varje regeringskommunikation i vid bemärkelse (inte endast militär), liksom all annan kommunikation som kan innehålla information av militärt, politiskt, vetenskapligt eller ekonomiskt värde.**

Direktivet (NSCID 9 rev, 52-12-29) klargör uttryckligen att endast FBI ansvarar för den inre säkerheten.

I Department of Defense (DoD) Directive av 1991-12-23 om NSA och Central Security Service (CSS) definieras uppläggningen för NSA på följande sätt:
- NSA är en separat organiserad myndighet inom Department of Defense under ledning av Secretary of Defense.
- NSA ansvarar dels för USA:s SIGINT-uppdrag, dels tillhandahåller organet säkra kommunikationssystem för alla departement och myndigheter.
- SIGINT-verksamheten inom NSA omfattar inte produktion och distribution av färdiga underrättelser. Detta hamnar inom andra departements och myndigheters uppdrag.

Därutöver skisseras i 1991 års DoD-direktiv hur strukturen ser ut i NSA respektive CSS.

I sitt vittnesmål inför House Permanent Select Committee on Intelligence, den 12 april 2000, definierar NSA-chefen Hayden NSA:s uppgifter så här:
- utrikeskommunikation för militären och politikerna (the policymakers) insamlas på elektronisk väg;

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

- NSA ger underrättelser till "US Government Consumers" gällande internationell terrorism, narkotika och vapenhandel;
- NSA:s uppdrag är inte att insamla all elektronisk kommunikation;
- NSA får bara vidarebefordra information till mottagare som godkänts av regeringen, inte direkt till amerikanska företag.

I ett memorandum från viceamiralen i US Navy W.O. Studeman, utställt i regeringens namn den 8 april 1992 hänvisas till det allt mer globala uppdrag (access) som NSA har, utöver "support of military operations".

5.5.2.2. De amerikanska underrättelsetjänsternas befogenheter (dokument 7)

Av United States Signals Intelligence Directive 18 (USSID 18) framgår att såväl kabel- som radiotrafik avlyssnas.

5.5.2.3. Samarbete med andra underrättelsetjänster (dokument 2a, 2b)

Till de uppgifter som åligger US Communications Intelligence Board hör bl a att övervaka alla "arrangements" med utländska regeringar inom området för COMINT. Till de uppgifter som åligger chefen för NSA hör att avveckla alla förbindelser med utländska COMINT-tjänster.

5.5.2.4. Omnämnande av enheter som är aktiva vid "ECHELON sites" (dokument 9, 12)

I NAVSECGRU INSTRUCTIONs C5450.48A beskrivs uppdrag, funktion och mål för Naval Security Group Activity (NAVSECGRUACT), 544th Intelligence Group, i Sugar Grove, West Virginia. Här anges att verksamheten har en särskild uppgift: "maintain and operate an ECHELON site"; därutöver nämns bearbetning av underrättelser.

I dokumentet "History of the Air Intelligence Agency – 1 January to 31 December 1994 (RCS: HAF-HO(A&SA) 7101 Volume 1)" nämns under punkten "Activation of Echelon Units" Detachment 2 och 3 av Air Intelligence Agency (AIA):

Dokumenten ger inga upplysningar om vad som menas med en "ECHELON site", vad en "ECHELON site" utför, eller vad kodnamnet ECHELON står för. Dokumenten ger inga upplysningar om UKUSA-avtalet.

5.5.2.5. Omnämnande av stationer (dokument 6, 9, 12)

- Sugar Grove, West Virginia, i NAVSECGRU INSTRUCTIONs C5450.48A
- Misawa Air Base, Japan, i History of the Air Intelligence Agency - January to 31 December 1994 (RCS: HAF-HO(A&SA)7101 Volume 1)
- Puerto Rico (dvs Sabana Seca), ibidem
- Guam, ibidem
- Yakima, Washington, ibidem
- Fort Meade, Maryland; en COMINT-rapport från NSA från Fort George G. Meade, Maryland, den 31 augusti 1972 visar att där pågått COMINT-verksamhet.

5.5.2.6. Skydd för amerikanska medborgares privatliv (dokument 7, 7a-f, 11, 16)

I NAVSECGRU INSTRUCTIONs C5450.48A anges att medborgarnas privatliv måste skyddas mot intrång.

I olika dokument anges att och hur de amerikanska medborgarnas privatliv skall skyddas mot intrång (Baker, General Counsel, NSA, brev av den 9 september 1992; United States Signals Intelligence Direcive (USSID) 18, den 20 oktober 1980, med flera tillägg.[1])

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

Department of Defense Directive av den 23 december 1991 ger noggranna definitioner av SIGINT, COMINT, ELINT och TELINT, liksom även National Security Council Intelligence Directive No. 6 av den 17 februari 1972.

Enligt dessa dokument innebär COMINT uppfångning och bearbetning av utrikeskommunikation (via elektromagnetiska medier); avlyssning och bearbetning av okrypterad kommunikation, pressinformation, propaganda, om den inte är krypterad.

5.5.3. Sammanfattning

1. Redan för 50 år sedan intresserade man sig för information inte bara på områdena politik och säkerhet, utan även på områdena vetenskap och näringsliv.
2. Dokumenten bevisar att NSA samarbetar med andra underrättelseorgan inom COMINT.
3. De dokument som ger upplysning om hur NSA är organiserat, vilka uppdrag det har och att det är underställt Department of Defense, säger i princip inte mer än den öppna information som finns på NSA:s hemsida.
4. Kabeltrafik får avlyssnas.
5. 544th Intelligence Group och Detachment 2 och 3 inom Air Intelligence Agency är verksamma med att insamla underrättelser.
6. Begreppet ECHELON dyker upp i olika sammanhang.
7. Sugar Grove i West Virginia, Misawa Air Base i Japan, Puerto Rico (dvs Sabana Seca), Guam, Yakima i delstaten Washington omnämns som SIGINT-stationer.
8. Dokumenten klargör hur de amerikanska medborgarnas privatliv skall skyddas mot intrång.

Dokumenten ger inga bevis men starka indicier, som tillsammans med andra indicier ger underlag för slutsatser.

5.6. Uppgifter från författare och journalister

5.5.1. Boken av Nicky Hager

I den 1996 utkomna boken av Nicky Hager "Secret Powers – New Zealand's role in the international spy network" beskrivs systemet Echelon för första gången utförligt. Enligt denna går dess ursprung tillbaka till år 1947, då det Förenade Kungariket i anslutning till samarbetet

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

under kriget träffade överenskommelse med Förenta staterna att fortsätta med hittillsvarande COMINT-aktiviteter globalt. Staterna skulle samverka till upprättande av ett i möjligaste mån globalt avlyssningssystem, för vilket de skulle dela de härtill erforderliga specifika anordningarna samt de därvid uppstående nödvändiga utgifterna och gemensamt äga åtkomst till resultaten. I fortsättningen anslöt sig Kanada, Australien och Nya Zeeland till UKUSA-överenskommelsen.
Hager hänvisar i sin bok till att avlyssnandet av satellitkommunikationen endast utgör en – om än viktig – komponent till avlyssningssystemet. Därutöver finns det ytterligare ett större antal anordningar för övervakning av riktad signalöverföring och kablar som emellertid är dokumenterade i mindre grad och svårare att påvisa, då de till skillnad från markstationer knappast väcker uppmärksamhet. ”Echelon” blir därmed synonymt med ett globalt avlyssningssystem.

5.5.2. Uppgifter av Duncan Campbell

Duncan Campbell redogjorde utförligt i STOA-studien 2/5 från 1999, vilken befattar sig ingående med den tekniska sidan, att detta, i likhet med varje medium som används till kommunikationsöverföring, kan avlyssnas. I en av sina senaste artiklar klarlägger han dock att även Echelon har sina begränsningar, den ursprungliga uppfattningen att en fullständig övervakning skulle vara möjlig har visat sig vara felaktig. ”Varken Echelon eller det elektroniska spionsystemet som det ingår i förmår detta. Den utrustning som skulle förfoga över kapaciteten att bearbeta och känna igen innehållet i varje röstmeddelande eller varje telefonsamtal finns överhuvudtaget inte.” [1]

5.5.3. Uppgifter av Jeff Richelson

Författaren Jeffrey Richelson, tidigare medlem i National Security Archives, har via Internet gjort 16 tidigare klassificerade dokument tillgängliga, vilka ger en inblick i tillkomst, utveckling, management och mandat för NSA (National Security Agency)[2].
Därutöver är han författare till åtskilliga böcker och artiklar om underrättelsetjänstverksamhet i USA. I sin 1985 utkomna bok „The Ties That Bind“[3] beskriver han utförligt tillkomsten av UKUSA-överenskommelsen och verksamheten hos de i denna överenskommelse delaktiga underrättelsetjänsterna USA’s, Storbritanniens, Kanadas, Australiens och Nya Zeelands.
I sin mycket omfattande bok „The U.S. Intelligence Community“[4] från 1999 ger han en överblick över USA’s underrättelsetjänstverksamhet, den beskriver underrättelsetjänsternas organisationsstruktur, deras metoder för samling och analys av information. I bokens kapitel 8 går han detaljerat in på underrättelsetjänsternas SIGINT-kapaciteter och beskriver några markstationer. I kapitel 13 beskriver han USA’s förbindelser med andra underrättelsetjänster, bl.a. UKUSA-överenskommelsen. Namnet ECHELON nämner han på ett ställe som kodord för ett datorbaserat utbytessystem.

[1] Duncan Campbell, Inside Echelon. Om bakgrund, teknik och funktion för det globala avlyssnings- och filtreringssystem som är känt under namnet ECHELON, 1
[2] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html
[3] Jeffrey T. Richelson, Desmond Ball 1985: The Ties That Bind, Boston UNWIN HYMAN, Sydney Wellington London
[4] Jeffrey T. Richelson 1999 (4th ed.): „The U.S. Intelligence Community“, Westview Press

I sin år 2000 utkomna artikel „Desperately seeking Signals“[1] beskriver han kortfattat UKUSA-överenskommelsen, nämner satellitavlyssningsanläggningar för kommunikationssatelliter och beskriver möjligheter och gränser för avlyssning av civil kommunikation.

5.5.4. Uppgifter av James Bamford

lämnas senare

5.5.5. Uppgifter av Bo Elkjaer och Kenan Seeberg,

De båda danska journalisterna Bo Elkjaer och Kenan Seeberg uppgav den 22 januari 2001 inför utskottet, att Echelon redan på 80-talet var långt framskridet och att Danmark sedan 1984 samarbetar med USA.

5.7 Uttalanden av tidigare underrättelsetjänstmedarbetare

5.7.1 Margaret Newsham (tidigare NSA-medarbetare)

Margaret Newsham[2] var från 1974 till 1984 anställd hos Ford och Lockheed och arbetade under denna tid enligt egen utsago för NSA. Hon hade utbildats för arbetet i NSA Headquarter i Fort George Meade i Maryland, USA, och tillsattes från 1977-1978 i Menwith Hill, den amerikanska markstationen på brittisk mark. Där har hon konstaterat att ett samtal av senator Strohm Thurmond avlyssnats. Redan 1978 kunde Echelon fånga upp en bestämd persons telekommunikation som transporterades via satellit.
Vad beträffar hennes egen roll hos NSA, skall hon ha varit ansvarig för framställning av system och program, konfigurering av dessa och för att göra dem beredda för körning på stora datorer. Mjukvaruprogrammen kallades SILKWORTH och SIRE, Echelon däremot var namnet för nätverket.

5.7.2 Wayne Madsen (tidigare NSA-medarbetare)

Wayne Madsen[3], tidigare NSA-medarbetare, bekräftar likaledes Echelons existens. Enligt hans åsikt har insamlingen av data om näringslivet högsta prioritet och används till gagn för företag i USA. Han uttalar särskilt farhågor att Echelon skulle kunna spionera på NGO såsom Amnesty International eller Greenpeace. Därtill för han fram att NSA måste tillstå, att de hade mer än 1000 sidor information beträffande prinsessan Diana, som genom sin kampanj mot landminor förhöll sig konträr till USA-politiken.

5.7.3 Mike Frost (tidigare medarbetare vid kanadensiska underrättelsetjänsten)

Mike Frost hade varit verksam vid den kanadenska underrättelsetjänsten CSE[4] i över 20 år. Avlyssningsstationen i Ottawa torde vara endast en del av ett världsomfattande nätverk av spionagestationer.[5] I en intervju med CBS förklarade han att „överallt i världen, varje dag,

---

[1] Jeffrey T. Richelson 2000: „Desperately seeking Signals“ The Bulletin of the Atomic Scientists, March/April 2000, Vol. 56, No. 2, pp. 47-51
[2] För det följande jämför Bo Elkjaer, Kenan Seeberg, Echelon was my baby – Interview with Margaret Newsham, Ekstra Bladet, 1999-01-17
[3] TV-intervju på NBC "60 Minutes" 2000-02-27; http://cryptome.org/echelon-60min.htm
[4] Communication Security Establishment, underställd det kanadensiska försvarsdepartementet, bedriver SIGINT[4]
[5] TV-intervju på NBC "60 Minutes" 2000-02-27; http://cryptome.org/echelon-60min.htm

telefonsamtal, e-post och fax övervakas av Echelon, regerigens hemliga övervakningsnätverk“.[1] Detta skulle även gälla civil kommunation. Som exempel anför han i en internvju med en australisk sändare, att namnet och telefonnumret på en kvinna, som i ett harmlöst telefonsamtal med en vän hade använt ett tvetydigt begrepp, hade noterats i en databank för möjliga terrorister av CSE. Datorn hade vid genomsökning av kommunikation funnit nyckelordet och lämnat vidare kommunikationen. Den för analysen ansvarige var inte säker och hade därför upptagit hennes personliga data.[2]
Underrättelsetjänsterna för Echelon-staterna skulle även hjälpa varandra inbördes på sådant sätt, att den ena spionerar för den andra, så att man åtminstone inte kan förebrå den hemliga underrättelsetjänsten för någonting. Så lär GCHQ ha bett den kanadensiska CSE att för sin räkning spionera på två engelska ministrar, då premiärminister Thatcher ville veta om dessa befann sig på hennes sida.[3]

5.7.4 Fred Stock (tidigare medarbetare vid kanadensiska underrättelsetjänsten)

Fred Stock har enligt egna uppgifter uteslutits ur den kanadensiska underrättelsetjänsten CSE år 1993, då han hade uttalat sig mot att den nya tyngdpunkten hos tjänsten riktades mot näringslivsinformation och civila mål. Den uppfångade kommunikationen skall ha omfattat information om affärer med andra länder och även förhandlingar om NAFTA, kinesiskt spannmålsuppköp och fransk vapenförsäljning.[4] Enligt Stock skulle tjänsten även rutinmässigt ha fått upplysningar om miljöprotestaktioner från Greenpeacefartyg till havs.

5.8 Regeringsinformation

5.8.1 Uttalanden från amerikansk sida

Den före detta CIA-direktören James Woolsey förklarade i en presskonferens, som han gav på anmodan av US-State-Department, att USA bedriver spionage i Kontinentaleuropa. „Economic Intelligence“ skall dock till 95 procent ha utvunnits genom utvärdering av offentligt tillgängliga informationskällor, endast 5 procent skulle vara stulna hemligheter. Utspionering av andra länders näringslivsdata äger rum i sådana fall där det handlar om att rätta sig efter sanktioner och om dual-use gods, liksom för att bekämpa bestickning vid ordertilldelning. Dessa upplysningar lämnas emellertid inte vidare till amerikanska företag. Woolsey betonar att till och med när man genom utspionering av näringslivsdata stöter på ekonomiskt användbar information, vore det mycket tidsödande för en analysator att analysera den stora mängden tillgängliga data i detta hänseende och att det vore ett missbruk att använda tiden till spionage på vänskapligt sinnade handelspartner. Dessutom påpekar han att även om man gjorde så, vore det på grund av den internationella sammanflätningen svårt att avgöra vilket företag som gäller som US-företag och som man sålunda skulle lämna informationen till.

---

[1] Rötzer, Die NSA geht wegen Echelon an die Öffentlichkeit; http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special
[2] TV-intervju på NBC "60 Minutes" 2000-02-27; http://cryptome.org/echelon-60min.htm
[3] Intervju på australiska Channel 9 1999-03-23; http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm
[4] Bronskill, Canada a key snooper in huge spy network, Ottawa citizen, 24.10.2000, http://www.ottawacitizen.com/national/990522/2630510.html

I en senare artikel för Wall Street Journal Europa [1] upprepade Woolsey att USA spionerar på Europa men att detta bara sker för att upptäcka mutor. Han förklarar däri även bestämt att USA använder datorer för att genomsöka data efter nyckelord.

5.8.2 Uttalanden från engelsk sida

Av diverse förfrågningar i House of Commons [2] framgår att Stationen RAF Menwith Hill tillhör det engelska försvarsministeriet men ställs till US-försvarsministeriets, i synnerhets NSA [3], som tillsätter den stationsansvarige, [4] förfogande som kommunikationsinrättning. [5] I mitten av 2000 fanns i RAF Menwith Hill 415 personer från US-militären, 5 från den brittiska militären, 989 USA-civilister och 392 brittiska civilister sysselsatta, varvid närvarande GCHQ medarbetare inte är medräknade. [6] Närvaron av USA-trupper regleras genom det Nordatlantiska fördraget och speciella hemliga [7] förvaltningsavtal, som betecknas som passande för de existerande förbindelserna mellan regeringarna i det Förenade Kungariket och USA för ett gemensamt försvar. [8] Stationen är en integrerad beståndsdel av USA försvarsministeriets världsomfattande nätverk, som stödjer brittiska, USA och NATO intressen. [9]
I årsberättelsen 1999/2000 betonas uttryckligen värdet av det nära samarbete som UK/USA-överenskommelsen medför och som återspeglas i kvaliteten hos resultaten i underrättelsetjänsthänseende. Speciellt påpekas att när under tre dagar NSA-anläggningen inte fungerade betjänade GCHQ omedelbart förutom UK-klientelet även US-klientelet. [10]

5.8.3 Uttalande från australiensisk sida [11]

Martin Brady, direktör vid den australiensiska underrättelsetjänsten DSD [12], bekräftade i ett brev till programmet "Sunday" hos den australiensiska sändaren "Channel 9", att det föreligger ett DSD-samarbete med andra underrättelsetjänster i UKUSA-avseende. I samma brev betonas att samtliga underrättelsetjänsttillhörande inrättningar tillhörande Australien drivs allena av australiensiska tjänstemän eller gemensamt med amerikanska tjänsteutövare. I de fall som inrättningar används gemensamt, har den australiensiska regeringen full kännedom om alla aktiviteter och är den australiensiska personalen delaktig på alla nivåer. [13]

5.8.4 Uttalanden från nederländsk sida

Den 19 januari 2001 presenterar den nederländska försvarsministern för det nederländska parlamentet en redogörelse över teknisk och rättslig aspekt på global avlyssning av moderna

---

[1] James Woolsey, Why America Spies on its Allies, The Wall Street Journal, 22.3.2000, 31.
[2] Commons Written Answers, House of Commons Hansard Debares.
[3] 12.7.1995.
[4] 25.10.1994.
[5] 3.12.1997.
[6] 12.5.2000.
[7] 12.7.1995.
[8] 8.3.1999, 6.7.1999.
[9] 3.12.1997.
[10] Intelligence and Security Committee, Annual Report 1999-2000, punkt 14, framlagd av premiärministern inför parlamentet i november 2000.
[11] http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp;
http://sunday.ninemsn.com/01_cover_stories/article_335.asp
[12] Defence Signals Directorate, australiensisk underrättelsetjänst, bedriver SIGINT.
[13] Brev från Martin Brady, chef för DSD, av 1999-03-16 till Ross Coulthart, Sunday Program; Jämför även:
http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp;
http://sunday.ninemsn.com/01_cover_stories/article_335.asp

telekommunikationssystem. [1] Den nederländska regeringen företräder däri åsikten att, ehuru den inte har någon egen kunskap därom, det på grund av den till förfogande stående informationen från annat håll torde vara mycket sannolikt att Echelon-nätverket existerar, men att det även kunde finnas andra system med likadana möjligheter. Den nederländska regeringen skall ha kommit till den slutsatsen att globalt uppfångande av kommunikationssystem inte är begränsat till de stater som deltar i Echelon-systemet utan även genomförs av regeringsmyndigheter i andra länder.

5.8.5 Uttalanden från italiensk sida

Luigi Ramponi, tidigare direktör vid den italienska underrättelsetjänsten SISMI, låter under sin intervju för „il mondo“ inga tvivel råda om att „Echelon“ existerar. [2] Ramponi förklarar uttryckligen att han in sin funktion som chef för SISMI kände till Echelons existens. Sedan 1992 skall han ha varit informerad om en omfattande aktivitet när det gäller avlyssning av källor av låg, mellan och hög frekvens. När han började hos SISMI år 1991, fick man sysselsätta sig allra mest med Förenade Kungariket och Förenta staterna.

5.9 Parlamentsrapporter

5.9.1 Rapporter från det belgiska kontrollutskottet Comité Permanent R

Det belgiska kontrollutskottet Comité Permanent R yttrade sig redan i två rapporter beträffande temat Echelon.
I rapporten "Rapport d'activités 1999" ägnade sig det tredje kapitlet åt frågan på vilket sätt de belgiska underrättelsetjänsterna reagerar på möjligheten till ett Echelon-system för kommunikationsövervakning. Den gott och väl 15 sidor omfattande rapporten kommer till den slutsatsen att de båda belgiska underrättelsetjänsterna Sûreté de l'Etat och Service général du Renseignement (SGR) erhåller information om Echelon endast genom offentliga dokument.
Den andra rapporten ("Rapport complémentaire d'activités 1999) befattar sig betydligt mer utförligt med Echelon-systemet. Den tar ställning till STOA-studien och ägnar en del av kommentarerna åt beskrivning av de tekniska och lagliga yttre förutsättningarna för avlyssning av telekommunikation. Dess slutsatser lyder som så att Echelon faktiskt existerar och även är i stånd att avlyssna all via Satellit överförd information (ca 1 procent av de totala internationella telefonsamtalen), såvitt sökning av nyckelord sker, och att dess kapacitet beträffande tolkning är betydligt större än vad som uppgivits från amerikansk sida. Beträffande uttalandena, att det inte utförs något industrispionage i Menwith Hill, kvarstår tvivel. Det betonas uttryckligen att det är omöjligt att med säkerhet fastställa vad Echelon gör eller inte gör.

5.9.2 Rapport från utskottet för nationellt försvar hos det franska Assemblée Nationale

I Frankrike framlades av utskottet för nationellt försvar för Assemblée Nationale en rapport över temat avlyssningssystem.[3]

---

[1] Brev till de Tweede Kamer gällande "Het grootschalig afluisteren van moderne telecommunicatiesystemen"
[2] Francesco Sorti, Dossier. exclusivo. caso Echelon. parla Luigi Ramponi. Anche I politici sapevano, il mondo, 17.4.1998
[3] Rapport d'information déposé en application de l'article 145 du règlement par la commission de la défense nationale et des forces armées, sur les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurit´nationale, N° 2623 Assemblöe nationale , enregisté à la Présidence de l'Assemblée nationale le 11 octobre 2000.

Efter att utförligt ha avhandlat de olika aspekterna kommer föredraganden till slutsatsen att Echelon existerar och att det handlar om det enda kända multinationella övervakningssystemet. Systemets kapacitet är reell, den har dock nått sin gräns, inte bara då de nedlagda ansträngningarna inte mer är proportionella till kommunikationsexplosionen utan även därför att bestämda mål har lärt sig att skydda sig.
Echelon-systemet har kommit ifrån sina ursprungliga mål, vilka var knutna till det kalla krigets sammanhang, så det är inte omöjligt att den samlade informationen sätts in för politiska och ekonomiska ändamål mot andra NATO-stater.
Echelon kunde mycket väl utgöra en fara för grundläggande friheter, det skapar i detta avseende talrika problem vilka kräver passande svar. Det vore fel att föreställa sig att medlemsländerna i Echelon ger upp sina aktiviteter. Desto mer tycks flertalet indicier peka på att ett nytt system med nya partner skapats för att övervinna Echelons begränsningar med hjälp av nya medel

6 Kan det finnas ytterligare globala avlyssningssystem?

6.1. Förutsättningar för ett sådant system

6.1.1. Teknisk-geografiska förutsättningar

För avlyssning av internationellt och via satelliter av första generationen förmedlad kommunikation utgör mottagningsstationer inom Atlantenområdet, inom Indiska Oceanen området och inom Stillahavsområdet en förutsättning. Hos den nyare satellitgenerationen, som möjliggör utstrålning i lägre områden, måste ytterligare villkor med avseende på avlyssningsstationers geografiska läge uppfyllas, när den totala över satellit förmedlade kommunikationen skall registreras.
Ett ytterligare globalt arbetande avlyssningssystem är tvunget att upprätta sina stationer utanför Echelon-staternas territorium.

6.1.2. Politisk-ekonomiska förutsättningar

Inrättningen av ett sådant globalt arbetande avlyssningssystem måste emellertid även vara ändamålsenlig ekonomiskt och politiskt för den/de som driver systemet. Nyttjaren eller nyttjarna av ett sådant system måste ha globala ekonomiska, militära eller andra säkerhetsintressen eller åtminstone tro att de tillhör de så kallade världsmakterna. Därmed begränsas kretsen i huvudsak till Kina och G8-staterna utan USA och Förenade Kungariket.

6.2. Frankrike

Frankrike förfogar inom alla de tre ovannämnda områdena över egna territorier, departement och områdesinstitutioner.
Inom Atlantområdet ligger öster om Kanada Saint Pierre et Miquelon (65° W / 47° N), nordöst om Sydamerika Guadeloupe (61° W / 16° N) och Martinique (60° W / 14° N) samt på Sydamerikas nordostkust Franska Guyana (52° W / 5° N).
Inom Indiska Oceanen-området befinner sig öster om södra Afrika Mayotte (45° O / 12° S) och La Réunion (55° O / 20° S) samt längst i söder Terres Australes et Antarctiques Francaises. Inom Stillahavsområdet ligger Nya Caledonien (165° O / 20° S), Wallis et Futana (176° W / 12° S) samt Franska Polynesien (150° W / 16° S).

Över möjliga stationer för den franska underrättelsetjänsten DGSE (Direction générale de la sécurité extérieur) inom dessa transoceana områden finns bara liten kännedom. Enligt uppgifter

från franska journalister[1] existerar stationer i Kourou i Franska Guyana samt i Mayotte. Över storleken på stationerna, antal satellitantenner och dessas storlek finns inga detaljerade uppgifter. Ytterligare stationer skall finnas lokaliserade i Frankrike i Domme i närheten av Bordeaux samt i Alluetts-le-Roi i närheten av Paris. Antalet satellitparaboler uppskattar Jauvert till totalt 30. Författaren Schmidt-Enboom[2] hävdar att en station även drivs i Nya Caledonien.

Teoretiskt skulle Frankrike likaledes kunna driva ett globalt arbetande avlyssningssystem. För ett seriöst påstående föreligger emellertid ingen tillräcklig offentligt åtkomlig information.

6.3 Ryssland

Den för kommunikationssäkerhet och SIGINT ansvariga ryska underrättelsetjänsten FAPSI bedriver enligt uppgift tillsammans med den ryska militära underrättelsetjänsten GRU markstationer i Lettland, Vietnam och Kuba.
Inom Atlantområdet ligger enligt uppgifter från Federation of American Scientists stationen i Lourdes på Kuba (82°W, 23°N) vilken drivs tillsammans med den kubanska underrättelsetjänsten. Inom Indiska Oceanen-området ligger stationer i Ryssland, över vilka ingen närmare information föreligger, samt en station i Skrunda i Lettland. Inom stillahavsområdet lär en station finnas i Cam Rank Bay i Nordvietnam. Detaljer om stationerna vad antal antenner och deras storlek beträffar är inte kända.
Tillsammans med i Ryssland självt befintliga stationer är teoretiskt en global täckning möjlig. Även här räcker den tillgängliga informationen inte till för ett seriöst påstående.

6.4 De övriga G-8 staterna och Kina

Varken de övriga G8-staterna eller Kina har eget territorium eller nära allierade i de därtill nödvändiga delarna av världen, för att driva ett globalt avlyssningssystem.

[1] Jean Guisnel, Léspionage nést plus un secret, The Tocqueville Connection, 10.7.1998
Vincent Jauvert, Espionnage comment la France, Le Nouvel Observateur, 5.4.2001, Nr. 1900, S. 14 ff.
[2] E.Schmidt-Eenboom, in: Streng Geheim, Museumsstiftung Post und Telekommunikation, Heidelberg 1999, S.180

7. Förenligheten av ett kommunikationsavlyssningssystem av typen "ECHELON" med unionsrätt

7.1 Kommentarer till frågeställningen

Utskottets mandat innehåller bland annat det uttryckliga uppdraget att pröva[1] förenligheten av ett kommunikationsavlyssningssystem av typen „ECHELON“ med förbundsrätt. Det bör särskilt bedömas om ett sådant system är förenligt med de båda datasäkerhetsriktlinjerna 95/46 EG och 97/66 EG, med Art 286 EGV, och Art 8 Abs 2 EUV.
Det tycks nödvändigt att företa granskningen från två olika synvinklar. Den första aspekten framgår av det i kapitel 5 visade indiciebeviset, av vilket framgår att det med „ECHELON“ betecknade systemet togs fram som kommunikationsuppfångningssystem, som genom insamlande och utvärdering av kommunikationsdata skall leverera information över händelser utomlands till de amerikanska, kanadensiska, australiensiska, nyzeeländska och brittiska underrättelsetjänsterna. Det rör sig följaktligen om ett klassiskt spionageinstrument för utlandsunderrättelsetjänster[2]. I ett första steg skall sålunda förenligheten av ett dylikt underrättelsetjänstsystem granskas mot unionsrätten.
Dessutom riktades i den av Campbell framlagda STOA-rapporten förebråelsen att detta system missbrukas till konkurrensspionage och att näringslivet i europeiska länder till följd därav måste utstå besvärande förluster. Därtill finns uppgifter från den tidigare CIA-direktören R. James Woolsey att USA visserligen spionerar på europeiska företag, detta emellertid bara för att åstadkomma marknadsrättvisa, då uppdragen skulle ha erhållits endast på grundval av bestickning.[3] Stämmer det att systemen används till konkurrensspionage, så uppstår frågan om förenlighet med förbundsrätt på nytt. Denna andra aspekt skall därför undersökas separat i ett ytterligare steg.

7.2 Förenligheten av ett underrättelsetjänstsystem med unionsrätt

7.2.1. Förenlighet med EG-rätt

Aktiviteter och åtgärder i statssäkerhetens tjänst respektive straffåtgärder faller principiellt inte inom EG-fördragets regelområde. Då den Europeiska Gemenskapen på grund av principen för ett begränsat särskilt bemyndigande endast kan vara verksam där motsvarande kompetens står till dess förfogande, har den följdriktigt i dataskyddsriktlinjerna, som är baserade på EG-fördraget, i synnerhet Art 95 (ex-Artikel 100a) däri, undantagit dessa områden från användningsområdet. Riktlinje 59/46/EG till skydd av fysiska personer vid bearbetning av personrelaterade data och för fri dataförbindelse[4], och riktlinje 97/66/EG över bearbetning av personrelaterade data och skydd av privatsfären inom telekommunikationsområdet[5] gäller, ingalunda för bearbetningar[6]/aktiviteter[7] beträffande den offentliga säkerheten, landsförsvar, statens säkerhet (inklusive dess ekonomiska välfärd, när bearbetningen/aktiviteten berör statens säkerhet) och statens aktiviteter inom det straffrättsliga området“. Hela formuleringen togs med i det då hos

[1] Jfr kapitel 1, 1.3 ovan
[2] Jfr kapitel 2
[3] *Jfr kapitel 5, 5,6 och 5.8*
[4] ABl 1995 L 281/31
[5] ABl 1998 L 24/1
[6] Art 3 pkt 2 dir. 95/46
[7] Art 1 pkt 3 dir. 97/66

parlamentet föreliggande riktlinjeförslaget över bearbetning av personrelaterade data och skyddet av privatsfären inom elektronisk kommunikation[1]. Deltagande av en medlemsstat i ett avlyssningssystem i statssäkerhetens tjänst kan följaktligen inte stå i strid med dataskyddsriktlinjer.
Lika lite kan en överträdelse av Art 286 EGV föreligga, vilken utvidgar användningsområdet för dataskyddsriktlinjerna till databearbetning av förbundets organ och inrättningar. Det samma gäller för förordning 45/2001 till skydd för fysiska personer vid bearbetning av personrelaterade data av förbundets organ och inrättningar och till fri datakommunikation.[2] Även denna förordning är bara användbar i den mån som organen ingriper.[3] För att undvika missförstånd bör här emellertid uttryckligen betonas att ett deltagande av förbundets organ och inrättningar i ett avlyssningssystem inte någonsin från något håll gjorts gällande och att det därför inte föreligger några som helst belägg för föredraganden.

7.2.2. Förenlighet med övrig EU-rätt

För områdena Titel V (Gemensam utrikes- och säkerhetspolitik) och VI (Polisiärt och juridiskt samarbete i brottmål) finns det inga dataskyddsbestämmelser som är jämförbara med EG-riktlinjerna. Från det europeiska parlamentets sida har man redan ett flertal gånger påpekat att här föreligger ett stort behov av att agera.[4]
Skyddet av allmänna fri- och rättigheter och grundläggande friheter för personer garanteras endast genom Art 6 och 7, särskilt genom Art 6 avsnitt 2 EUV, där unionen förpliktigar sig till att respektera allmänna fri- och rättigheter, så som de garanterats i EMRK och som framgår av de författningar som gemensamt överlämnats av medlemsstaterna. Som supplement till förpliktelsen till allmänna fri- och rättigheter och särskilt till EMRK för medlemsstaterna (jmf. därtill även med Kapitel 8 nedan) uppstår därmed en förpliktelse till allmänna fri- och rättigheter för unionen i dess verksamhet vid lagstiftning och förvaltning. Då det emellertid hittills inte finns någon reglering av det tillåtna i övervakning av telekommunikation för säkerhets- och underrättelsetjänständamål[5], går det tills vidare inte att ställa frågan om överträdelse av Art 6 Avsnitt 2 EUV.

---

[1] KOM (2000) 385 slutg, ABl C 365 E/223
[2] Förordning (EG) Nr 45/2001, ABl 2001 L 8/1
[3] Art 3, pkt 1, jfr även bakgrund 15 "Om denna bearbetning görs av gemenskapens organ och inrättningar under utövandet av verksamhet utanför det område som denna förordning gäller, särskilt verksamhet enligt EU-fördragets delar V och V, skyddas individens rättigheter och friheter med beaktande av artikel 6 i EU-fördraget."
[4] Jfr t ex punkt 25 i beslutet om aktionsplan från Rådet och Kommissionen för bästa möjliga tillämpning av bestämmelserna i Asterdam-fördraget gällande uppbyggnad av ett område för frihet, säkerhet och rättsskydd (13844/98 - C4-0692/98 - 98/0923(CNS)), AB1 C 219 1999-07-30, 61 ff
[5] Inom området för telekommunikationsövervakning finns det för närvarande inom EU endast två rättsakter, av vilka ingen behandlar frågan om tillåtlighet:
- Rådets beslut 1995-01-17 om lagenlig övervakning av kommunikation (ABl Nr C 329 v 4.11.1996), där bilagan behandlar tekniska krav på utövande av lagenlig övervakning i moderna telekommunikationssystem; samt
- rättsakten från Rådet 2000-05-29 om tillkomsten av avtalet – enligt artikel 34 i EU-fördraget – gällande rättshjälp i rättegång mellan medlemsstaterna i EU (ABl 2000 C 197/1, Art 17 f), där det fastställs vilka förutsättningar som gäller för att rättshjälp vid rättegång i samband med telekommunikationsövervakning skall kunna ges. De avlyssnades rättigheter inskränks inte av detta, eftersom den medlemsstat där den avlyssnade finns alltid kan förvägra rättshjälp om denna inte är tillåtlig enligt nationell lagstiftning.

7.3. Frågan om förenlighet i händelse av missbruk av systemet för företagsspionage

Skulle en medlemsstat understödja ett avlyssningssystem, som bland annat även bedriver konkurrensspionage, genom att denna medlemsstat låter utrusta den egna underrättelsetjänsten därför, respektive ställer eget territorium till en främmande underrättelsetjänsts förfogande för detta ändamål, skulle helt säkert en överträdelse av EG-rätten föreligga. Medlemsstaterna är nämligen enligt Art 10 EGV förpliktigade till omfattande lojalitet, speciellt till underlåtande av alla åtgärder som skulle äventyra förverkligandet av fördragets mål. Till och med om uppfångandet av telekommunikation inte sker till förmån för det inhemska näringslivet (vilket för övrigt skulle motsvara effekten av ett statsbidrag, och därmed skulle bryta mot Art 87 EGV), utan till förmån för tredje stat, skulle en sådan verksamhet stå i fundamental strid med det koncept för en gemensam marknad som ligger till grund för EG-fördraget, då den skulle innebära en snedvridning av konkurrensen.
Ett sådant förhållande skulle enligt föredraganden desutom innebära en överträdelse av dataskyddsriktlinjen för telekommunikationsområdet[1], då frågan om tillämpligheten av riktlinjerna måste lösas sett från funktionell synvinkel och inte organisatorisk sådan. Detta framgår inte bara av ordalydelsen i regleringen av användningsområdet utan även av lagens innebörd. Om underrättelsetjänster använder sin kapacitet till företagsspionage, så sker deras verksamhet inte i säkerhetens eller straffåtgärders tjänst, utan används för obehörigt ändamål och faller följaktligen fullständigt under användningsområdets riktlinje. Denna förpliktigar emellertid medlemsstaterna i sin Art 5 att säkra förtroendet för kommunikation och förbjuda i synnerhet „medlyssning, avlyssning och lagring, liksom andra typer av uppfångande eller övervakning av kommunikation från andra personers än användarens sida". Undantag får enligt Art 14 endast göras där dessa är nödvändiga för statens säkerhet, landets försvar och straffåtgärder. Då företagsspionage inte legitimerar till undantag, skulle i detta fall en kränkning av förbundsrätten föreligga.

7.4. Resultat

Sammanfattningsvis kan man säga, att i nuvarande rättsläge ett underrättelsetjänstsystem av typen Echelon därför inte kan stå i strid med unionsrätten, då det inte uppvisar de beröringspunkter med unionsrätt som vore erforderliga för en oförenlighet. Detta gäller visserligen bara så länge systemet verkligen används uteslutande i statssäkerhetens tjänst. Blir det däremot använt för obehöriga ändamål och sätts in som konkurrensspionage mot utländska företag så uppstår en motsägelse mot EG-rätten. Om en medlemsstat skulle delta däri, skulle den bryta mot förbundsrätten.

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

8. Förenligheten av underrättelsetjänstanknuten kommunikationsövervakning med fri- och rättigheter på det privata området

8.1. Kommunikationsövervakning som ingripande i fri- och rättigheter på det privata området

Varje avlyssning av kommunikation, ja redan registrering av data från underrättelsetjänstens sida för detta ändamål[1] utgör ett djupgående intrång i den enskilde individens privatliv. Endast i en 'polisstat' är ett oinskränkt förhör från statlig sida tillåtet. I EU's medlemsstater som vuxna demokratier däremot är nödvändigheten att visa respekt för privatlivet från statliga organs, och därmed också underrättelsetjänsternas sida, oomstridd och kommer i regel till uttyck i medlemsstaternas författning. Privatsfären åtnjuter därmed ett speciellt skydd, ingripandemöjligheter tillåts endast efter rättslig prövning och under beaktande av proportionalitetsprincipen.
Även i Echelon-staterna är man medveten om problematiken. De planerade skyddsbestämmelserna riktar sig här visserligen mot respekt för privatsfären för de egna innevånarna, så att den europeiska medborgaren i regel inte kan dra någon nytta därur. Så blir i de USA-föreskrifter, som reglerar villkoren för elektronisk övervakning, inte intresse för ett effektivt allmänt grundrättsskydd ställt emot statsintressena för en fungerande underrättelsetjänst, utan det erforderliga skyddet av privatsfären för "US-personer".[2]

8.2. Skyddet av det privata området genom internationella överenskommelser

Respekt för privatsfären som grundläggande rättighet har beaktats i talrika folkrättsliga överenskommelser.[3] I globalt hänseende bör nämnas i synnerhet „Den internationella överenskommelsen beträffande medborgerliga och politiska rättigheter"[4] vilken slöts 1966 inom ramen för UNO, och som i sin Art 17 garanterar skyddet av den privata sfären. Samtliga Echelon-stater har underkastat sig besluten från det konventionella utskottet för mänskliga rättigheter upprättat enligt Art 41. Utskottet är ansvarigt för frågan om folkrättsliga kränkningar

[1] Tysklands författningsdomstol (BVerfG), 1 BvR 2226/94 1999-07-14, Rz 187 "En inskränkning [....] utgör själva avlyssnandet, i den mån kommunikationen görs tillgänglig för underrättelsetjänsten och utgör grund för en efterföljande jämförelse med sökbegreppen."
[2] Jämför också rapporten till den amerikanska kongressen i slutet av februari 2000 "Legal Standards for the Intelligence Community in Conducting Electronic Surveillance", http://www.fas.org/irp/nsa/standards.html, som hänvisar till Foreign Intelligence Surveillance Act (FISA), avtryckt i Titel 50 Kapitel 36 U.S.C. § 1801 ff och Exec. Order No. 12333, 3 C.F.R. 200 (1982), avtryckt i Titel 50, Kapitel 15 U.S.C. § 401 ff http://www4.law.cornell.edu/uscode/50/index.html.
[3] Art 12 Universal Declaration of Human Rights; Art 17 UN Covenant on Civil and Political Rights; Art 7 EU:s charter, Art 8 EMRK; rekommendation från OECD:s råd om riktlinjer för informationssystems säkerhet, antagna 1993-11-26/27 C(92) 188/Final; Art 7 Europarådets konvention om skydd för personer i samband med databearbetning av persondata; jfr STOA-studien Development of surveillance tehnology and risk of abuse of economic information; Vol 4/5: The legality of the interception of electronic communications: A concise survey of the principal legal issues and instruments under international, European and national law (Chris Elliot), october 1999, 2
[4] International Covenant on Civil and Political Rights, antagen av FN:s generalförsamling 1966-12-16

av överenskommelsen i den mån det gäller klagomål från andra stater. Det tilläggsprotokoll[1], som utsträcker kompetensen hos utskottet för mänskliga rättigheter till individuella klagomål blev emellertid inte undertecknat av USA, så för privatpersoner ges inte möjlighet, i händelse av kränkring av pakten från USA's sida, att vända sig till utskottet för mänskliga rättigheter.
På EU-nivå försökte man att förverkliga ett särskilt europeiskt skydd för allmänna fri- och rättigheter genom framtagning av en "Författning över allmänna fri- och rättigheter för EU". Artikel 7 i författningen, som har titeln „Respekt för privat- och familjeliv" normerar till och med uttryckligen rätten till respekt för kommunikation.[2] Därutöver normeras i Artikel 8 allmänna fri- och rättigheter till "skydd av personrelaterade data". Detta skulle ha skyddat den enskilde individen i de fall där hans data (automatiserade eller icke-automatiserade) bearbetas, något som i regel alltid gäller vid avlyssning vid övriga uppfånganden.
Författningen har hittills inte tagits med i fördraget. Bindande avtal-effekt ger den därför endast för de tre organ som underkastat sig henne i den "högtidliga deklarationen" vid sidan om det europeiska rådet i Nice. Råd, kommission och europeiska parlamentet. Dessa är enligt föredragandens kännedom inte inblandade i några som helst underrättelsetjänstanknutna aktiviteter. Även om författningen når sin fulla giltighetskraft efter upptagande i fördraget , måste hänsyn tas till hennes begränsade användningsområde. Enligt Art 51 gäller Författningen "för organ och inrättningar i unionen och för medlemsstaterna uteslutande vid genomförande av unionens rättigheter". Författningen skulle därför i bästa fall ha verkan på instrumentet för förbud mot konkurrensvidriga statliga understöd (Se Kap. 7.7.3).
Det enda verksamma instrumentet på internationell nivå för omfattande skydd av privatsfären beskrivs i den europeiska konventionen för mänskliga rättigheter.

8.3. Reglering av den europeiska konventionen för mänskliga rättigheter (EMRK)

8.3.1. Betydelsen av EMRK i EU

Skyddet av fri- och rättigheter, som tillstås av EMRK, har såtillvida särskild betydelse, då konventionen har ratificerats av EU's samtliga medlemsstater och som därför utgör en enhetlig europeisk skyddsnivå. Avtalsstaterna har folkrättsligt förpliktigat sig att garantera de i EMRK stadfästa rättigheterna och har underkastat sig den europeiska domstolens för mänskliga rättigheter (EGMR) rättsskipning. De vid varje tillfälle nationella reglerna kan därför omprövas av EGMR beträffande sin överensstämmelse med EMRK och avtalsstaterna i händelse av kränkning av de mänskliga rättigheterna dömas och förpliktigas att erlägga förlikningsersättning. Därutöver fick EMRK betydelse genom att den upprepade gånger anlitades av EuGH inom ramen för laglig granskning gemensamt med medlemsstaternas allmänna rättsprinciper för att komma fram till ett beslut. Med fördraget från Amsterdam fastslogs därutöver skriftligen i Art 6 avsnitt 2 EUV EU's förpliktelse att respektera fri- och rättigheter så som dessa garanteras i EMRK.

8.3.2. Det rumsliga och personella skyddsomfånget hos EMRK

De i EMRK garanterade rättigheterna representerar allmänna mänskliga rättigheter och är följaktligen inte bundna till en statstillhörighet. De måste garanteras alla personer som är

[1] Opitional Protocol to the International Covenant on Civil and Political Rights, antagen av FN:s generalförsamling 1966-12-16
[2] "Varje människa har rätt till respekt för sitt privat- och familjeliv, sin bostad och sin kommunikation."

underkastade avtalsstaternas rättsskipning. De innebär att de mänskliga rättigheterna i varje fall måste uppfyllas inom det totala territoriet och att lokala undantag skulle innebära en avtalskränkning. Därutöver gäller de emellertid även utanför avtalsstaternas territorium såvida där utövas statsmakt. De av EMRK garanterade rättigheterna gentemot en avtalsstat tillkommer även personer utanför territoriet om en avtalsstat utanför sitt territorium ingriper i dennes privatsfär[1].
Det sistnämnda är därför särskilt viktigt här eftersom problematiken med fri- och rättigheter inom området telekommunikationsövervakning uppvisar den särskilda egenheten att den för övervakningen ansvariga staten, den övervakade och det faktiska avlyssningsskeendet kan falla isär rumsligt. Detta gäller i synnerhet för internationell kommunikation, under vissa omständigheter även för nationell kommunikation, när informationstransporten för över ledningar i utlandet. För förfarandet från utlandsunderrättelsetjänsternas sida är detta till och med det typiska fallet. Det kan inte heller uteslutas att information från övervakning, som en underrättelsetjänst fått fram, lämnas vidare till andra stater.

8.3.3. Det tillåtna i telekommunikationsövervakning enligt Art 8 EMRK

Enligt Art 8 avsnitt 1 MRK har „var och en […] ett anspråk på respekt för sitt privat- och familjeliv, sin bostad och sin korrespondens". Skyddet för telefoni eller telekommunikation är visserligen inte uttryckligen omnämnt men enligt EGMR's rättsskipning omfattas även de genom begreppen "privatliv" och "korrespondens" av skyddsomfånget i Art 8 MRK.[2] Skyddsomfånget för fri- och rättigheter sträcker sig därvid inte bara till kommunikationsinnehållet utan även till anteckning av yttre samtalsdata. Det betyder att även om underrättelsetjänsten bara antecknar data som tid och varaktighet för förbindelserna samt de slagna numren, utgör detta ett intrång i privatsfären.[3]
Fri- och rättigheter enligt Art 8 avsnitt 2 garanteras inte obegränsat. Intrång i fri- och rättigheter när det gäller respekt för privatsfären kan vara tillåtna om ett rättsunderlag inom den interna lagen föreligger.[4] Lagen måste vara allmänt tillgänglig och dess konsekvenser möjliga att förutse.[5]
Medlemsstaterna är därvid inte fria i utformningen av dessa intrång. Art 8 EMRK tillåter dem endast för förverkligande av de i avsnitt 2 listade ändamålen, det är i synnerhet den nationella säkerheten, allmän lag och ordning, förhindrande av brottsliga handlingar, men även landets ekonomiska välfärd[6], som emellertid inte rättfärdigar företagsspionage, då endast i ett

[1] Jämför EGMR Loizidou/Turkiet, 1995-03-23, punkt 62 med referenser "...the concept of 'jurisdiction' under this provision is not restricted to the national territory of the High Contracting Parties.[...] responsibility can be involved because of acts of their authorities, whether performed within or outside national boundaries, which produce effects outside their own territory" med hänvisning till EGMR, Drozd und Janousek, 1992-06-26, punkt 91. Jfr särskilt Jacobs, The European Convention on Human Rights (1996), 21 ff
[2] Jfr EGMR, Klass ua, 1978-09-06, punkt 41.
[3] Jfr EGMR, Malone, 1984-08-2, punkt 83 ff; samt Davy, B/Davy/U, Aspekte staatlicher Informationssammlung und Art 8 MRK, JBl 1985, 656.
[4] Enligt beslut i EGMR (särskilt Sunday Times, 26.4.1979, punkt 46 ff, Silver ua, 25.3.1983, punkt 85 ff) omfattar begreppet "law" i Art 8 punkt 2 inte bara lagstiftning i formell mening, utan också rättsföreskrifter på lägre nivå, i vissa fall även oskriven lag. En förutsättning är dock alltid att rättssubjektet kan varsebli de omständigheter vid vilka en sådan inskränkning kan ske. Jfr Wessley, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht? ÖJZ 1999, 491 ff, 495
[5] Silver ua, 25.3.1983, Z 87 f
[6] Rättsgrunden för "samhällsekonomins väl" utnyttjades av EGMR i ett fall där det handlade om vidareförmedling av medicinska data som hade betydelse för tilldelning av allmänna medel, M.S / Sverige, 1997-08-27, punkt 38, och i ett fall som gällde utvisning från Holland av en person som levde på socialhjälp sedan grunden för uppehållstillståndet upphört att gälla. Ciliz/Nederländerna, 2000-07-11, punkt 65.

demokratiskt samhälle nödvändiga" ingripanden faller därunder. För varje ingripande måste det mildaste medlet för att uppnå målet väljas, därutöver måste tillräckliga garantier mot missbruk finnas.

8.3.4. Betydelsen av Art 8 EMRK för underrättelsetjänsternas verksamhet

Dessa allmänna principer innebär för utformningen av en verksamhet hos underrättelsetjänsterna som överensstämmer med fri- och rättigheter följande: Om det för tillförsäkrande av nationell säkerhet synes nödvändigt att berättiga underrättelsetjänster till att fånga upp telekommunikationsinnehåll eller åtminstone kommunikationsdata, så måste detta dokumenteras i den interna lagen och regleringen göras tillgänglig för allmänheten. Konsekvenserna av denna måste kunna förutses av den enskilde, de särskilda sekretesskraven bör kanske emellertid beaktas. Så har domstolen i ett beslut om Art 8 konformitet med hemliga kontroller av anställda inom områden som rör den nationella säkerheten fastslagit, att anspråket på förutsebarhet i detta speciella fall inte kan vara detsamma som på andra områden.[1] Den har emellertid även här krävt att lagen i varje fall måste lämna upplysningar om under vilka omständigheter och villkor statsmakten får företa ett hemligt och därmed potentiellt farligt ingrepp i privatsfären.[2]
För en utformning av underrättelsetjänstverksamheten som står i överensstämmelse med de mänskliga rättigheterna skall därvid tas i beaktande att den nationella säkerheten visserligen utgör ett rättfärdigande skäl för denna, men att detta enligt Art 8 avsnitt 2 EMRK är underkastat proportionalitetsprincipen: även den nationella säkerheten kan rättfärdiga ingripande endast där de är nödvändiga i ett demokratiskt samhälle. EGMR har entydigt förklarat, att statens intresse att skydda sin nationella säkerhet måste vägas mot allvaret i ingripandet i den enskildes intressen när det gäller respekt för dennes privata sfär.[3] Ingripanden är visserligen inte begränsade till det absolut nödvändiga måttet, men att bara vara nyttigt eller önskvärt förslår inte[4]. Uppfattningen att en avlyssning av varje telekommunikation vore det bästa skyddet mot organiserad brottslighet skulle, även om denna vore förutsedd av den interna lagen, bryta mot artikel 8 EMRK.
Dessutom måste på grund av den speciella karaktären av underrättelsetjänstverksamheten, vilken kräver sekretess och därigenom en speciell intresseavvägning, desto starkare kontrollmöjligheter förutses. Domstolen har uttryckligen påpekat att ett hemligt övervakningssystem för säkrande av nationell säkerhet bär med sig risken att det under förevändning att försvara demokratin underminerar denna eller rent av förstör och att det därför fordras adekvata och effektiva garantier mot sådant missbruk.[5] Den lagligt legitimerade underrättelsetjänstverksamheten överensstämmer följaktligen med allmänna fri- och rättigheter endast när avtalsstaten för EMRK skapat tillräckliga kontrollsystem och andra garantier mot missbruk. Domstolen framhöll därvid i samband med verksamheten hos Sveriges underrättelsetjänst, att den fäster särskild vikt vid närvaron av parlamentsledamöter i det polisiära kontrollorganet samt övervakningen från justitieministerns, den parlamentariska ombudsmannens och det parlamentariska lagutskottets sida. Ur den här synvinkeln tycks det betänkligt att Frankrike, Grekland, Irland, Luxemburg och Spanien inte har några egna parlamentariska kontrollutskott för underrättelsetjänst[6] och inte känner till något kontrollsystem jämförbart med den parlamentariska ombudsmannen hos de

[1] EGMR, Leander, 1987-03-26, punkt 51
[2] EGMR, Malone, 1984-08-02, punkt 67
[3] EGMR, Leander, 1987-03-26, pkt 59, Sunday Times, 1979-04-26, punkt 46 ff
[4] EGMR, Silver m fl, 1983-10-24, punkt 97
[5] EGMR, Leander, 1987-03-26, punkt 60.
[6] Föredraganden känner till att varken Luxemburg eller Irland har någon underrättelsetjänst och att de inte bedriver någon SIGINT. Kravet på en särskild kontrollinstans gäller här bara underrättelseverksamhet inom landet.

nordiska staterna.[1] Föredraganden välkomnar därför strävandena hos försvarsutskottet i det franska Assemblée Nationale, att bilda ett kontrollutskott[2], särskilt som Frankrike tekniskt och geografiskt förfogar över beaktansvärda kapaciteter i underrättelsetjänsthänseende.

8.4. Förpliktelse till vaksamhet gentemot främmande underrättelsetjänstverksamhet

8.4.1. Otillbörlighet till kringgående av Art 8 EMRK genom inkoppling av främmande underrättelsetjänster

Som ovan utförligt klarlagts, måste avtalsstaterna uppfylla ett antal krav för att verksamheten hos deras underrättelsetjänster skall vara förenlig med Art 8 MRK. Det är uppenbart att underrättelsetjänsterna inte kan frigöra sig från dessa förpliktelser av det skälet att de går tillbaka till verksamheten hos andra underrättelsetjänster, vilka är underkastade mindre stränga föreskrifter. I annat fall vore legalitetsprincipen med sina båda komponenter om tillgänglighet och förutsebarhet berövad sin verkan och EGMR's rättsskipning försvagad till sitt innehåll. Detta innebär för det första att utbyte av data mellan underrättelsetjänster endast är begränsat tillåten. En underrättelsetjänst får begära uppgifter från en annan endast om dessa kunnat tas fram under förutsättningar som den egna nationella rätten förutser. Den av lagen planerade aktionsradien får inte utvidgas genom överenskommelser med andra tjänster. På samma sätt får den endast genomföra verksamheter för en främmande underrättelsetjänst enligt deras anvisningar när den har övertygat sig om deras överensstämmelse med den egna nationella rätten. Även om informationen är avsedd för en annan stat, ändrar detta inget i allvaret med avseende på fri- och rättigheter vid ett för den rättsligt utsatte oförutsebart intrång.
För det andra får avtalsstater i EMRK inte låta främmande underrättelsetjänster bli verksamma på deras territorium, om det finns anledning förmoda att deras verksamhet inte motsvarar förutsättningarna i EMRK.[3]

8.4.2. Konsekvenser för den tolererade verksamheten av utomeuropeiska underrättelsetjänster inom medlemsstaternas i EMRK territorium

8.4.2.1. Den tillämpliga rättsskipningen hos den europeiska domstolen för mänskliga rättigheter

Med ratificering av EMRK har avtalsstaterna förpliktat sig att underkasta utövningen av sin suveränitet en kontroll av fri- och rättigheter. De kan inte avstå från denna förpliktelse genom att avsäga sig sin suveränitet. Dessa stater förblir ansvariga för sitt statsterritorium och därmed förpliktigade mot dem som underkastat sig den europeiska lagen, även när utövandet av territorialmakt genom underrättelsetjänstverksamhet företas av en annan stat. Från EGMR bejakas under tiden i ordinarie rättsskipning en skyldighet för avtalsstaterna att vidta positiva åtgärder till skydd för den privata sfären, för att ingen kränkning av Art 8 EMRK från privata (!) sker, alltså till och med på horisontell plan, där den enskilde inte står mot statsmakten utan mot

[1] Beträffande kontroll av underrättelsetjänsterna i medlemsstaterna, se kapitel 9.
[2] Jfr lagförslaget "Proposition de loi tendant à la création de délégations parlementaires pour le renseignement", och motsvarande rapport från ledamoten Arthur Paecht, N° 1951 Assemblée nationale, 11e sittningen, registrerat 1999-11-23
[3] Jfr Yernault, "Echelon" et l'Europe. La protection de la vie privée face à l'espionnage des communications, Journal des tribunaux, Droit Européen 2000, 187 ff.

en annan person.[1] Om en stat tillåter en främmande underrättelsetjänst att arbeta på sitt territorium så är skyddsbehovet väsentligt större, då en annan överhet utövar sitt herravälde. Det synes här bara logiskt att utgå från att staten måste bevaka att den underrättelsetjänstrelaterade verksamheten överensstämmer med de mänskliga rättigheterna inom dess territorium.

8.4.2.2. Konsekvenser för stationer

I Tyskland kommer i Bad Aibling eget territorium att ställas till Förenta staternas förfogande för att nyttjas uteslutande för satellitmottagning. I Menwith Hill i Storbritannien kommer ett gemensamt utnyttjande av terräng att tillåtas för samma ändamål. Om i dessa stationer ickemilitär kommunikation av privata eller av företag, som stammar från en av EMRK's avtalsstater, skulle avlyssnas av en amerikansk underrättelsetjänst, så utlöser EMRK övervakningsskyldigheter. Det betyder i praktiken, att Tyskland och Förenade Kungariket som avtalsstater i EMRK är förpliktade att förvissa sig om att den amerikanska underrättelsetjänstens verksamhets överensstämmer med allmänna fri- och rättigheter. Detta gäller så mycket mer som representanter för NRO och pressen redan vid flera tillfällen visat sig bekymrade över NSA's agerande.

8.4.2.3. Konsekvenser för genomförd avlyssning på annans uppdrag

I Morwenstow i Storbritannien uppfångas i samarbete med NSA civil kommunikation strikt enligt NSA's anvisning och vidarebefordras till USA som råmaterial, enligt föreliggande information från GCHQ. Även vid uppdragsarbeten för tredje part gäller skyldigheten att pröva uppdraget mot överensstämmelse med allmänna fri- och rättigheter.

8.4.2.4. Speciell omsorgsplikt hos tredje stat

För avtalsstater i EMRK kan man upp till en viss grad ömsesidigt utgå från att den andra staten också rättar sig efter EMRK. Detta gäller i varje fall tills det för en EMRK-avtalsstat kan styrkas att den systematiskt och kroniskt kränker EMRK. I USA's fall rör det sig om en stat som inte är avtalsstat i EMRK och som inte heller har underkastat sig något jämförbart kontrollsystem. Dess underrättelsetjänsts verksamhet är mycket precist reglerad, såvitt den avser USA-medborgare respektive personer som rättmätigt uppehåller sig i USA. När det gäller NSA's verksamhet utomlands tillämpas dock andra bestämmelser, av vilka uppenbarligen flera är klassificerade och därmed oåtkomliga. Ytterligare oroväckande tycks därvid att den amerikanska underrättelsetjänsten visserligen är underkastad kontroll av utskotten i representanthuset och senaten; dessa parlamentariska utskott visar emellertid endast ringa intresse för NSA's verksamhet utomlands.
Det tycks därför lämpligt att vädja till Tyskland och England att ta de ur EMRK uppkommande förpliktelserna på allvar och att göra upplåtelse av ytterligare underrättelsetjänstrelaterade verksamheter från NSA's sida på sina territorier avhängiga av att dessa står i samklang med EMRK. Därvid skall tre huvudaspekter beaktas.
1. Enligt EMRK får intrång i den privata sfären endast ske på grund av rättsliga regleringar, som är allmänt tillgängliga och vilkas konsekvenser är möjliga att förutse för den enskilde. Detta krav är endast uppfyllt när USA yppar för den europeiska befolkningen på vilket sätt och under vilka omständigheter spaning bedrivs. Såvitt oförenligheter med EMRK föreligger, måste regleringarna anpassas till den europeiska skyddsnivån.

[1] EGMR, Abdulaziz, Cabales och Balkandali, 1985-05-28, punkt 67; X o Y/Nederländerna, 1985-03-26, punkt 23; Gaskin vs Förenade kungariket 1989-07-07, punkt 38; Powell och Rayner, 1990-02-21, punkt 418.4.2.4

2. Ingripanden får enligt EMRK inte vara överdrivna. Dessutom måste det mildaste medlet väljas. För den europeiske medborgaren kan ett ingripande som företas från europeisk sida betraktas som mindre omvälvande än ett från amerikansk sida, då endast i det första fallet rättsförfarande vid nationella instanser står öppen.[1] Ingripanden måste därför så långt som möjligt göras från tysk respektive engelsk sida, följdriktigt i varje fall de i det straffrättsliga förfarandets tjänst. Från amerikansk sida har man upprepade gånger försökt att rättfärdiga avlyssningen av telekommunikation med förebråelse om korruption och bestickning från europeisk sida.[2] USA har uppmärksammats på att alla EU-stater förfogar över fungerande straffrättssystem. Om misstanksmoment föreligger, så har USA överlåtit det straffrättsliga förfarandet till gästländerna. Om inga misstanksmoment föreligger, så strider en överdrivet inlagd övervakning följaktligen mot mänskliga rättigheter och är därför inte tillåten. Överensstämmelse med EMRK medges därför endast när USA begränsar övervakningsåtgärder, som tjänar deras nationella säkerhet, men bortser från sådana som har straffrättsligt förfarande som syfte.
3. Som ovan redan beskrivits, har EGMR i sin rättsskipning för överensstämmelse med allmänna fri- och rättigheter krävt, att det finns tillräckliga kontrollsystem och garantier mot missbruk. Detta innebär att amerikansk telekommunikationsövervakning från europeisk mark endast överensstämmer med mänskliga rättigheter om USA för sådana fall, där USA därifrån uppfångar kommunikation för ändamål som avser deras nationella säkerhet, skapar motsvarande effektiva kontroller, respektive om USA i sin verksamhet på europeisk mark underkastar sig värdlandets (alltså Tysklands respektive Storbritanniens) kontrollinrättningar.
Endast om överensstämmelse med i dessa tre punkter nedskrivna krav föreligger, kan konformiteten med avseende på USA's förfarande vid uppfångande av telekommunikation säkerställas med EMRK och den av EMRK enhetligt garanterade skyddsnivån i Europa upprätthållas.

[1] Därigenom uppnås också konformitet med Art 13 EMRK, som tillerkänner målsägaren rätt till besvär mot de nationella instanserna
[2] Woolsey (tidigare chef för CIA), Why America Spies on its Allies, The Wall Street Journal Europe, 2000-03-22, 31

9. Är EU-medborgare tillräckligt skyddade mot underrättelsetjänsternas verksamhet?

9.1. Skydd mot underrättelsetjänstverksamhet: en uppgift för de nationella parlamenten

Då underrättelsetjänsternas verksamhet visserligen framdeles kan utgöra en aspekt för GASP, föreligger i nuvarande läge dock inga bestämmelser beträffande detta på EU-nivå,[1] och därför är utformningen av skyddet mot underrättelsetjänsternas verksamhet endast avhängigt av de nationella rättsreglementen.
De nationella parlamenten utövar härvid en dubbel funktion: Som lagstiftare beslutar de om underrättelsetjänsternas bestånd och behörigheter samt över utformningen av kontrollen av underrättelsetjänstverksamhet. Som redogjorts för i förra kapitlet, måste parlamenten vid regleringen av frågan beträffande det tillåtna i telekommunikationsövervakning hålla sig till de i Art 8 EMRK fastställda gränserna, dvs. regleringarna måste vara nödvändiga och proportionerliga och deras konsekvenser möjliga att förutse för den enskilde. Dessutom måste adekvata och effektiva kontrollmekanismer skapas i enlighet med övervakningsmyndigheternas befogenheter.
Därutöver har de nationella parlamenten i de flesta stater en aktiv roll som kontrollmyndighet, då kontrollen av den verkställande makten (och därmed också underrättelsetjänsterna) jämsides med lagstiftningen är den andra „klassiska“ funktionen hos ett parlament. Utformningen hos EU's medlemsstater sker emellertid på mycket olika sätt, ofta existerar parlamentariska och ickeparlamentariska organ sida vid sida.

9.2. Nationella myndigheters befogenhet att företa övervakningsåtgärder

Övervakningsåtgärder från statlig sida får i regel företas för åtalsärenden, för att bereda lag och ordning och för statssäkerhet[2] (gentemot utlandet).
När det gäller straffrättsliga ändamål får i alla medlemsstater telesekretessen brytas, i den mån som tillräcklig misstanke finns att en brottslig handling (emellanåt mycket kvalificerad sådan, alltså med en högre ovärdighetsgrad) begåtts av en konkret person. På grund av den allvarliga arten i ingripandet, krävs för detta i regel en domstols godkännande,[3] det finns precisa föreskrifter beträffande tillåten varaktighet av övervakningen, dess kontroll och raderingen av data.
För garanterande av inre säkerhet och ordning utvidgas den statliga informationsanskaffningen utanför individuella undersökningar i fallet med konkreta misstankar om brottslig handling. För en tidig identifiering av extremistiska eller omstörtande rörelser, av terrorism och organiserad kriminalitet tillåter den nationella lagstiftaren ytterligare informationsutvinning beträffande bestämda personer eller grupperingar. Insamlingen av relevanta data samt analysen därav sker därvid genom speciella inrikes underrättelsetjänster.

[1] Jfr kapitel 7
[2] Detta syfte erkänns också i Art 8, punkt 2 EMRK som grund för intrång i den privata sfären. Jfr 8.3.2 ovan.
[3] I brittisk rätt däremot har beslutet företräde framför godkännande från Secretary of State (Regulation of Investigatory Powers Act 2000, Section 5 (1) och (3) (b)

Som slutsats kan sägas att de åtgärder som sker i statssäkerhetens tjänst utgör en viktig del av övervakningsåtgärderna. Bearbetning, utvärdering och tolkning av relevant information om främmande land åligger i regel en egen utlandsunderrättelsetjänst.[1] Övervakningens mål är i regel inga konkreta enstaka personer, snarare omfattas bestämda områden respektive frekvenser. Beroende på de medel och rättsliga befogenheter som står till utlandsunderrättelsetjänstens förfogande, finns det ett brett spektrum som sträcker sig från ren militär radiospaning inom kortvågsområdet till övervakning av alla slags telekommunikationsförbindelser med utlandet. I många medlemsstater är övervakningen av telekommunikation för rena underrättelsetjänstrelaterade ändamål överhuvudtaget förbjuden,[2] i andra medlemsstater är den – delvis med förbehåll för godkännande av en oavhängig kommission[3] – tillåten på order av en minister,[4], för många kommunikationsvägar till och med utan någon som helst begränsning.[5] De förhållandevis omfattande befogenheterna för många utlandsunderrättelsetjänster beror på att de avser övervakning av utlandskommunikation och därför endast drabbar en ringa del av dem som lyder under den egna lagen; bekymret för detta är sålunda väsentligt mindre.

9.3. Kontrollen av underrättelsetjänsterna

En effektiv och omfattande kontroll är därför mycket viktig, då för det första underrättelsetjänster arbetar i hemlighet, deras arbete är långsiktigt inriktad, de berörda personerna under lång tid inte får reda på något eller (beroende på rättsläget) överhuvudtaget inte får vetskap om den genomförda övervakningen och för det andra att övervakningsåtgärder ofta gäller större, oklart definierade grupper av personer så att staten mycket snabbt kan få fram en stor mängd personliga data.
Det ställer sig naturligt för alla kontrollutskott – helt oberoende av deras utformning – att problemet ofta knappast kan fastställas på grund av den speciella karaktären av underrättelsetjänster, om de facto all information ställs till förfogande eller en del undanhålles. Desto noggrannare måste reglementeringen ske. I princip bör man kunna utgå från att en hög kontrollverksamhet och därmed en omfattande garanti för ingripandenas laglighet har givits, när förordnande om telekommunikationsövervakning är förbehållen den högsta förvaltningsnivån, när den fordras för genomförande av ett tidigare domstolsgodkännande och ett oavhängigt organ också övervakar verkställigheten av åtgärderna. Därutöver är det önskvärt för demokratipolitiska och rättsstatliga överväganden, att underrättelsetjänsternas arbete i sin helhet, i överensstämmelse med principen för maktfördelning, är underkastat kontroll från ett parlamentariskt organ.
Detta har i stor utsträckning förverkligats i Tyskland. Där förordnas åtgärder för telekommunikationsövervakning av den ansvarige förbundsministern. Förutom när det är fara å färde skall en egen, oavhängig, direktivfri kommission (”G10-kommission”[6]), som beslutar om nödvändigheten och det lagliga i åtgärden, underrättas före genomförandet. I de fall där den

[1] Betr underrättelsetjänsternas verksamhet se kapitel 2.
[2] Detta gäller i Österrike och Belgien
[3] Detta gäller i Tyskland, Gesetz zur Beschränkung des Brief-, Post-, und Fernmeldegeheimnisses (Gesetz zu Artikel 10 Grundgesetz). Enligt §9 skall kommissionen (om inte dröjsmål innebär fara) underrättas före verkställighet.
[4] Detta gäller i Storbritannien (Regulation of Investigatory Powers Act, Section 1) och i Frankrike i fråga om kabelburen kommunikation (Art 3 une 4 Loi 91-646 du 10 Juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications)
[5] Detta gäller kabelburen kommunikation i Frankrike (Art 20 Loi 91-646 du 10 Juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications)
[6] Jfr särskilt: Die Parlamentarische Kontrolle der Nachrichtendienste in Deutschland, Stand 9.9.2000, utgivet av Deutschen Bundestag, Sekretariat des PKGr

tyska utlandsunderrättelsetjänsten BND kan berättigas till övervakning av den inte ledningsbundna telekommunikationsverksamheten med hjälp av filtrering genom sökbegrepp, beslutar kommissionen även över tillåtelse av sökbegreppen. G-10-kommissionen åligger dessutom kontrollen över det i lag föreskrivna meddelandet till berörda liksom över utplåning av de data som utvunnits av BND.
Dessutom finns det ett parlamentariskt kontrollutskott (PKGr)[1], som är sammansatt av 9 ledamöter av det nationella parlamentet och som övervakar alla de tre tyska underrättelsetjänsternas verksamhet. PKGr har rätt till dokumentinsyn, till utfrågning av medarbetare i underrättelsetjänsten samt till besök hos underrättelsetjänsterna och till underrättelse, varvid det sistnämnda endast kan nekas när det av tvingande skäl hos underrättelsetillgången eller av skäl som gäller skydd av personlighetsrätt för tredje man är nödvändigt, eller när kärnområdet för det exekutiva egenansvaret drabbats. PKGr's överläggningar är hemliga, medlemmarna är förpliktade – även efter sin avgång – att iaktta sekretess. I mitten och i slutet av valperioden avlägger PKGr rapport över kontrollverksamheten för den tyska förbundsdagen.
En sådan omfattande, praktiskt taget komplett kontroll av underrättelsetjänsterna utgör i varje fall ett undantag hos medlemsstaterna.
I Frankrike[2] till exempel behöver bara övervakningsåtgärder som kräver inkoppling på ledningar, premiärministerns tillstånd. Endast de är underkastade övervakning genom den särskilt inrättade kommissionen (Commission nationale de contrôle des interceptions de sécurité), som en parlamentsledamot och en senator ingår i. Godkännande av en av en minister eller dennes delegerad begärd avlyssningsåtgärd delges kommissionens ordförande, som vid tvivel beträffande dess laglighet låter kommissionen befatta sig därmed. Denna lämnar sedan rekommendationer och i händelse av förmodan om en straffrättsligt relevant lagöverträdelse underrättar åklagarmyndigheten. Avlyssningsåtgärder för försvar av nationella intressen, vilka omfattar avlyssning av radiotrafik, alltså även kommunikation via satellit, är inte underkastade någon som helst inskränkning och därmed inte heller en kommissions kontroll.
De franska underrättelsetjänsternas arbete är inte heller i övrigt underkastade kontroll av ett eget parlamentariskt kontrollutskott, dock är arbeten i gång i detta avseende. Av försvarsutskottet hos Assemblée Nationale antogs redan ett förslag beträffande detta[3], en diskussion därom har emellertid för närvarande ännu inte ägt rum i plenum.
I Förenade Kungariket fordrar varje kommunikationsövervakning på brittisk mark godkännande på ministernivå (Secretary of State). Formuleringen av lagen låter dock oklarhet föreligga om inte det målinriktade, breda uppfångandet av kommunikation, som granskas på nyckelord, även skulle falla under det av „Regulation of Investigatory Powers Act 2000" (RIP) använda begreppet „interception", när utvärderingen inte sker på brittisk mark, utan „råmaterialet" utan utvärdering förmedlas utomlands. Kontrollen av att bestämmelserna i RIP 2000 iakttas sker (ex-post) genom kommitterade, av premiärministern utnämnda tjänstgörande eller före detta högre domare. Den för avlyssningsåtgärder ansvarige kommitterade (Interception Commissioner) övervakar tilldelningen av avlyssningstillstånd och stödjer undersökningen av klagomål över avlyssningsåtgärder. Den kommitterade för Intelligence Service övervakar godkännandena för

[1] Gesetz über die Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG) av den 17 juni 1999 BGBl I 1334 idgF.
[2] Loi 91-646 du 10 Juillet 1991, loi relative au secret des correspondances émises par la voie des t´lécommunications
[3] Jfr lagförslaget "Proposition de loi tendant à la création de délégations parlementaires pour le renseignement", och motsvarande rapport från ledamoten Arthur Paecht, N° 1951 Assmeblée nationale, 11e sittningen, registrerat 1999-11-23

aktiviteter hos underrättelse- och säkerhetstjänsten och stödjer undersökningar av klagomål över dessa tjänster. Investigatory Powers Tribunal, för vilken en högre domare är ordförande, undersöker alla överklaganden av avlyssningsåtgärder och tjänsternas verksamheter.
Den parlamentariska kontrollen sker genom Intelligence and Security Committee (ISC),[1] vilken övervakar verksamheten hos alla tre civila underrättelsetjänster (MI5, MI6 und GCHQ). Den åligger i synnerhet granskning av utgifter och förvaltning samt kontroll av säkerhetstjänstens, underrättelsetjänstens och GCHQ's agerande. Utskottet består av 9 medlemmar från underhuset och överhuset bland vilka det inte får finnas någon minister. Till skillnad från kontrollutskotten hos andra stater, som i regel är valda eller utnämnda av parlamentet respektive parlamentets talman, utses de av premiärministern efter konsultation av oppositionsledaren.
Redan med hjälp av dessa exempel visar det sig att skyddsnivån är mycket varierande. Vad den parlamentariska kontrollen anbelangar, så skulle föredraganden vilja peka på att existensen av egna kontrollutskott för övervaktning av underrättelsetjänster är mycket viktig. De har nämligen gentemot huvudutskotten den fördelen, att de åtnjuter stort förtroende hos underrättelsetjänsterna, då deras medlemmar är underkastade sekretess och att sammanträdena äger rum med uteslutande av allmänheten. Dessutom är de för fullgörande av sin speciella uppgift utrustade med speciella befogenheter, något som är absolut nödvändigt för övervakning av verksamheter inom hemligstämplat område.
Glädjande nog har flertalet av medlemsstaterna i EU tillsatt egna parlamentariska kontrollutskott för kontroll av underrättelsetjänsterna. I Belgien[2], Danmark[3], Tyskland[4], Italien[5], Nederländerna[6] och Portugal[7] finns det ett parlamentariskt kontrollutskott, som är ansvarigt såväl för kontrollen av den militära underrättelsetjänsten som för kontrollen av den civila. I Förenade Kungariket[8] övervakar det särskilda kontrollutskottet endast de (visserligen väsentligt mer betydande) civila underrättelsetjänsterna, den militära övervakas av det normala försvarsutskottet. I Österrike[9] bevakas de båda grenarna av underrättelsetjänsten av två olika kontrollutskott, vilka dock är lika organiserade och utrustade med samma befogenheter. I de nordiska staterna Finland[10] och Sverige[11] bevakar ombudsmän de parlamentariska kontrolluppgifterna; de är autonoma och väljs

[1] Intelligence services act 1994, Section 10
[2] Comité permanent de contrôle des services de renseignements et de sécurité, Comité permanent R, Loi du 18 juillet 1991 /IV, organique du contrôle des services de police et de renseignements.
[3] Udvalget vedrørende efterretningstjenesterne, Lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester, lov 378 af 6/7/88.
[4] Das parlamentarische Kontrollgremium (PKGr), Gesetz über die Kontrolle nachrichtendienstlicher Tätigkeit des Bundes (PKGrG)vom 17. Juni 1999 BGBl I 1334 idgF.
[5] Comitato parlamentare, L. 24 ottobre 1977, n. 801, art. 11, Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato.
[6] Tweede-Kamercommissie voor de Inlichtingen- en Veiligheidsdiensten, 17. Reglement van orde van de Tweede Kamer der Staten-General, Art. 22.
[7] Conselho de Fiscalização dos Serviços de Informações (CFSI), Gesetz 30/84 vom 5. September 1984, geändert durch das Gesetz 4/95 vom 21. Februar 1995, das Gesetz 15/96 vom 30. April 1996 und das Gesetz 75-A/97 vom 22. Juli 1997.
[8] Intelligence and Security Committee (ISC), intelligence services act 1994, Section 10.
[9] Ständigen Unterausschuss des Landesverteidigungsausschusses zur Überprüfung von nachrichtendienstlichen Maßnahmen zur Sicherung der militärischen Landesverteidigung und dem Ständigen Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit, Art 52a B-VG, §§ 32b ff Geschäftsordnungsgesetz 1975.
[10] Ombudsman, laglig grund för polisens kontroll (SUPO): Poliisilaki 493/1995 §33 och Laki pakkokeinolain 5 a luvun muuttamisesta 366/1999 §15, för militärens kontroll: Poliisilaki 493/1995 §33 och Laki poliisin tehtävien suorittamisesta puolustusvoimissa 1251/1995 §5.
[11] Rikspolisstyrelsens ledning, Förordning (1989:773) med instruktion för Rikspolisstyrelsen.

av parlamentet. I Frankrike, Grekland, Irland, Luxemburg och Spanien finns det inga egna parlamentariska utskott, kontrolluppgifterna verkställs här endast av huvudutskotten inom ramen för den allmänna parlamentariska verksamheten.

9.4. Bedömning av situationen för den europeiske medborgaren

Situationen i Europa tycks föga tillfredsställande för den europeiske medborgaren. Underrättelsetjänsternas befogenheter inom området telekommunikationsövervakning är i sin räckvidd mycket olika, samma gäller för kontrollutskotten. Inte alla medlemsstater, som bedriver en underrättelsetjänst, förfogar dessutom över oavhängiga parlamentariska kontrollutskott som är utrustade med motsvarande kontrollbefogenheter. Man är långt borta från en enhetlig skyddsnivå.
Från europeisk synvinkel är detta desto mer beklagansvärt som detta tillstånd inte så mycket gäller de egna medborgarna i dessa stater, vilka genom ett motsvarande valbeteende kan påverka skyddsnivån. De ogynnsamma följderna drabbar framför allt medborgarna i andra stater, då verksamhetsområdet för utlandsunderrättelsetjänster naturenligt är riktad mot främmande land. Den enskilde är relativt försvarslöst utlämnad till utländska system, skyddsbehovet är ännu större här. Man får heller inte glömma att på grund av den speciella karaktären hos underrättelsetjänster, kan EU-medborgare vara drabbade av verksamheten hos flerfaldiga underrättelsetjänster samtidigt. En enhetlig skyddsnivå som gör rättvisa åt de demokratiska fri- och rättigheterna, vore önskvärd här. Det borde i detta sammanhang även funderas på i vilken utsträckning dataskyddsbestämmelser på EU-nivå synes realiserbara på detta område.
Därutöver uppstår en helt ny fråga om skydd för den europeiska medborgaren om inom ramen för en gemensam säkerhetspolitik man börjar med ett samarbete mellan medlemsstaternas underrättelsetjänster. Här ställs då krav på de europeiska institutionerna att utfärda tillräckliga skyddsbestämmelser. Det kommer att vara det europeiska parlamentets uppgift som förfäktare av rättsstatliga principer att yrka på att det därefter från parlamentets sida som demokratiskt legitimerat organ sker en motsvarande kontroll. Det europeiska parlamentet är emellertid här även kallat att skapa förutsättningarna för att den konfidentiella behandlingen av så känsliga data liksom av andra hemliga dokument av ett särskilt utformat utskott, vars medlemmar är förpliktade till tystnad, kan garanteras. Endast när dessa förutsättningar föreligger, blir det realistiskt och med hänsyn till ett – för en gemensam säkerhetspolitik, som bör tas på allvar, absolut nödvändigt – fungerande samarbete mellan underrättelsetjänsterna ansvara för att dessa kontrollrättigheter begärs in.

10 Skydd mot företagsspionage

10.1. Företagen som mål för spionage

När det gäller frågan om sekretessbelagd information kan man dela upp företagens information i tre typer. Den första typen är information som avsiktligt **sprids i så stor utsträckning som möjligt**. Till denna informationstyp hör information om företagets produkter (exempelvis produktegenskaper, priser osv) och information som fungerar som reklam och påverkar företagets image.
Sedan finns det information som **vare sig hemlighålls eller sprids aktivt**, eftersom den inte påverkar företagets konkurrensposition. Exempel på sådan information är datum för

företagsutflykter, menyn i företagsmatsalen eller vilket märke företaget använder när det gäller faxar.
Slutligen finns det information som är **sekretessbelagd i avsikt att hemlighållas**. Denna information hemlighålls också för konkurrerande företag men också, när ett företag inte följer gällande lagstiftning, för staten (skatt, embargoregler osv). Det finns flera olika typer av skydd till och med sträng sekretess, som råder vid exempelvis forskningsresultat innan patentanmälan är gjord, eller vid tillverkning av krigsmaterial.[1].
Spionage har i det aktuella diskuterade fallet att göra med anskaffning av information som hemlighålls av ett företag. Om angriparen är ett konkurrerande företag talar man om **konkurrensspionage** (eller industrispionage). Om det handlar om att en statlig underrättelsetjänst gör intrång talar man om **företagsspionage.**

10.1.1. Detaljerad information om syftet med spionage

Strategisk information, som är av betydelse för företagsspionage, kan delas in i branscher eller företagsområden.

10.1.1.1. Branscher

Det är självklart att information från följande branscher är mycket intressant: Bioteknik, genteknologi, medicinteknik, miljöteknik, högpresterande datorer, programvara, optoelektronik, bild- sensor- och signalteknik, datalagring, teknisk keramik, högproduktiva legeringar, nanoteknik. Listan är inte fullständig och ändras också ständigt på grund av den tekniska utvecklingen. Inom dessa områden handlar spionage framför allt om att stjäla forskningsresultat eller speciella produktionstekniker.

10.1.1.2 Företagsområden

Angreppsmålet för spionage ligger helt logiskt inom företagsområdena forskning och utveckling, inköp, personal, produktion, distribution, försäljning, marknadsföring, produktlinjer och ekonomi. Ofta underskattas värdet och betydelsen av sådan information (se nedan 10.1.4)

10.1.2 Konkurrensspionage

Ett företags strategiska marknadsposition beror på hur forskning och utveckling, produktionssätt, produktlinjer, finansiering, marknadsföring, försäljning, distribution, inköp och arbetskraft är organiserat[2] . Information om dessa områden är mycket intressant för alla konkurrenter på marknaden, eftersom den ger upplysning om planer och svagheter och därmed ger möjlighet till strategiska motåtgärder.
En del av denna information är offentligt tillgänglig. Det finns högt specialiserade konsultföretag som på helt lagligt sätt utför konkurrensanalyser, däribland så renommerade företag som Roland&Berger i Tyskland. "Competitive Intelligence" är numera ett standardverktyg för företagsledningarna i USA [3]. Professionellt hanterat skapar man då en tydlig bild av situationen utifrån ett stort antal enskilda informationsdelar.

[1] Information för företag som får säkerhetsskydd, BMWI 1997
[2] M.F.Porter, Competitive Strategy
[3] Hummelt, Roman, Wirtschaftsspionage auf dem Datenhighway, Hanserverlag, München 1997.

Skillnaden mellan legala åtgärder och straffbart konkurrensspionage beror på vilka medel man väljer för att skaffa fram information. Det är först när de använda medlen är illegala under gällande lagstiftning som det är fråga om brottsliga handlingar – det är inte i sig straffbart att samla ihop material till och genomföra analyser. Sådan information som är speciellt intressant för konkurrenter skyddas naturligtvis mot åtkomst och kan bara skaffas fram genom att bryta mot lagen. De tekniker som används för detta skiljer sig inte från de allmänna metoder för spionage som beskrivs i kapitel 2.
Det finns inga exakta uppgifter över hur utbrett konkurrensspionage är. Mörkertalet är mycket högt, precis som vid klassiskt spionage. Båda parter (gärningsman och offer) är ointresserade av publicitet. För de drabbade företagen betyder detta alltid en imageförlust och angriparna har naturligtvis inte heller något intresse av att deras aktiviteter offentliggörs. Det är anledningen till att bara ett fåtal fall avgörs i domstol.
Trots detta förekommer ofta reportage om konkurrensspionage i pressen. Journalisten har då dessutom intervjuat säkerhetschefer i stora tyska företag [1] och chefer i amerikanska och europeiska företag. Sammanfattningsvis kan man slå fast att konkurrensspionage upptäcks gång på gång men att det inte spelar någon avgörande roll för det dagliga arbetet i företagen.

10.2 Skador förorsakade av företagsspionage

På grund av de höga mörkertalen går det inte att få någon exakt statistik över hur utbrett konkurrensspionage/företagsspionage egentligen är. Dessutom är det så att en del av de nämnda talen är höga eftersom det finns intresse av att de ska vara höga: Säkerhetsföretag och säkerhetstjänster har ett lättförståeligt intresse av att placera de skador som sker i den övre delen av en realistiskt möjlig skala. Dessa tal är trots detta ganska talande.
Redan 1988 uppskattade det tyska Max Planck-institutet att de skador som uppkommit genom företagsspionage motsvarade minst 8 miljarder DM[2]. Ordförande för föreningen för säkerhetsrådgivningsföretag i Tyskland åberopar experter när de nämner ett belopp på 15 miljarder DM per år. Ordföranden i de europeiska polisfackförbunden, Hermann Lutz, uppskattar att skadorna kostar 20 miljarder DM varje år. FBI[3] menar att skadorna för konkurrens- och företagsspionage kostat de amerikanska företagen 1,7 miljarder amerikanska dollar under åren 1992 och 1993. Den förre ordföranden för underrättelsetjänstens kontrollutskott för House of Representatives i USA talar om 100 miljarder dollar i förluster, som uppkommit genom förlorade uppdrag och exktrakostnader för forskning och utveckling. Mellan 1990 och 1996 har detta inneburit en förlust av 6 miljoner arbetstillfällen.[4]
Det är egentligen inte nödvändigt att känna till exakt hur stora skadorna är. Statens skyldighet kvarstår att med hjälp av polis och säkerhetstjänst vidta åtgärder mot konkurrens- och företagsspionage oberoende av hur stora de nationalekonomiska skadorna är. Den samlade statistiken över skador är inte heller användbar som utgångspunkt för företagens beslut hur informationen ska skyddas och för att vidta åtgärder för att skydda sig mot spionage. Varje enskilt företag måste själv beräkna maximalt möjlig skada som informationsstöld kan medföra, sannolikheten att intrång sker och sedan jämföra detta med kostnaderna för säkerhet. Det egentliga problemet består inte i att det saknas exakt statistik över de totala skadorna. Det är

[1] Information och namn är skyddade.
[2] IMPULSE,3/97,s 13 ff.
[3] Redogörelse i amerikanska Kongressen, L.J.Freech, chef för FBI, 9 maj 1996.
[4] Robert Lyle, Radio Liberty/Radio free Europe, 10 februari 1999.

snarare så att det – förutom i storföretagen – knappast görs sådana beräkningar av kostnader/intäkter och att säkerheten därför försummas.

10.3 Vem spionerar?

De största uppdragsgivarna när det gäller företagsspionage är enligt en studie som konsultföretaget Ernst Young LLP [1] utfört följande : 39 procent är konkurrenter, 19 procent är kunder , 9 procent är leverantörer och 7 procent underrättelsetjänster. Det är egna anställda, privata spionageföretag, betalda datahackare och proffs från underrättelsetjänsten som spionerar [2]

10.3.1. Anställda (insiderbrott)

All litteratur med uppgifter från experter i utskott och journalister som intervjuat säkerhetschefer och myndigheter som motarbetar spionage visar samma sak: Det är besvikna och otillfredsställda anställda som utgör den största faran vad gäller spionage. Eftersom de är anställda har de direkt tillgång till information, låter sig värvas för pengar och håller utkik efter företagshemligheter att vidarebefordra till sina uppdragsgivare.
Det finns också stora risker när personer byter arbetsgivare. Nuförtiden är det inte nödvändigt att kopiera högar av papper för att kunna föra ut viktig information från företagen. Det går att spara information på disketter utan att det märks. Disketterna kan sedan tas med till den nya arbetsgivaren.

10.3.2. Privata spioneriföretag

Antalet företag som har specialiserat sig på att få fram information växer ständigt. Till viss del är det före detta anställda från underrättelsetjänster som arbetar i dessa företag. Dessa företag arbetar ofta både med säkerhetsrådgivning och med anställda detektiver, som får i uppdrag att skaffa fram information. För det mesta används legala metoder men det finns också företag som använder sig av illegala metoder.

10.3.3. Hackare

Hackare är datorspecialister som använder sina kunskaper för att komma åt nätverken utifrån. Förut var hackare datornördar som tyckte det var roligt att överlista datorernas säkerhetssystem. Idag finns det hackare som arbetar på uppdrag av både underrättelsetjänster och ute på marknaden.

10.3.4. Underrättelsetjänster

Efter det kalla krigets slut har underrättelsetjänsternas arbete ändrats. Internationellt organiserad kriminalitet och sakförhållanden på företagen är nya arbetsfält (mer information om detta finns i kapitel 10.5)

10.4 Hur går spionaget till?

Uppgifter från säkerhetstjänsten och från säkerhetschefer i stora företag visar att när det gäller företagsspionage används alla beprövade metoder och instrument från underrättelsetjänsten (se

[1] Computerzeitung, 30 nov 1995, s 2.
[2] R.Hummelt, Spionage auf dem Datenhighway, München 1997, s 49 ff.

kapitel 2.4.). Företag har oftare en öppnare struktur än militär, underrättelsetjänst och regeringsorgan. När det gäller företagsspionage tillkommer därför följande risker:

- Det är lättare att värva anställda eftersom möjligheterna när det gäller företagssäkerhet inte går att jämföra med den kontroll som sker på säkerhetstjänsten
- mobiliteten på dagens arbetsplatser leder till att viktig information kan föras ut på en bärbar dator. Det är därför mycket vanligt vid företagsspionage att bärbara datorer stjäls eller att hårddisken kopieras vid inbrott på ett hotellrum.
- Det är lättare att bryta sig in i datornät på företag än på statliga institutioner med hög säkerhetströskel, eftersom små och medelstora företag i mycket lägre utsträckning ägnar tid åt något säkerhetstänkande och har vidtagit säkerhetsåtgärder för att förhindra intrång.
- Av samma skäl är det lättare att avlyssna på plats (se kapitel 3.2)

Utvärderingen av den insamlade informationen visar att företagsspionaget i huvudsak sker på plats eller på mobila arbetsplatser, eftersom det med få undantag (se nedan 10.6) inte går att få tag i den eftersökta informationen genom avlyssning av det internationella telekommunikationsnätet.

10.5 Stater som utför företagsspionage

10.5.1. Strategiskt företagsspionage utfört av underrättelsetjänster

Efter det kalla krigets slut har underrättelsekapacitet frigjorts, som nu används inom andra områden. USA deklarerar öppet att den del av landets underrättelsetjänst gäller näringslivet. Dit hör exempelvis övervakningen av att ekonomiska sanktioner följs, övervakning av lagar för vapenleveranser och så kallade dual use-produkter, utvecklingen på råvarumarknaderna och händelserna på de internationella finansmarknaderna. Journalisterna vet att det inte bara är den amerikanska underrättelsetjänsten som arbetar på detta sätt och därför finns det ingen massiv kritik av detta.

10.5.2. Underrättelsetjänster som agenter vid konkurrensspionage

Kritik sker i stället när den statliga underrättelsetjänsten missbrukas för detta ändamål och när företag med hjälp av staten och spionage skaffar sig internationella konkurrensfördelar. Här är det fråga om två typer[1]

10.5.2.1. Hightech-länder

Högutvecklade industriländer kan avgjort tjäna på industrispionage. Genom att få fram utvecklingsstatus i en bransch kan det medföra egna internationella ekonomiska och subventionspolitiska åtgärder som antingen gör den egna industrin mer konkurrenskraftig eller sparar in subventioner. Det kan också vara viktigt att få fram detaljerad information vid uppdrag med högt uppdragsvärde (se nedan 10.6).

10.5.2.2. Tekniskt mindre utvecklade stater

För en del av dessa stater rör det sig om att skaffa teknisk kunskap för att kunna hämta in en del av försprånget åt den egna industrin utan att behöva investera i utvecklingskostnader och licensavgifter. Det kan dessutom gälla att skaffa produktförlagor och tillverkningstekniker för att

[1] Upplysning från person på säkerhetstjänsten till journalisten, skyddad källa.

kunna konkurrera på världsmarknaden med billigare (löner !) framställda produkter. Det är bevisat att den ryska underrättelsetjänsten har fått detta arbete i uppdrag. I den ryska federationens lagparagraf 5 om utländsk underrättelseverksamhet nämns uttryckligen anskaffning av företags- och företagsteknisk information som en av underrättelsetjänstens uppgifter.
För en rad andra stater (t. ex Iran, Irak, Syrien, Libyen, Nordkorea, Indien och Pakistan) gäller det att få fram information för de nationella rustningsprogrammen inom framför allt atomområdet och för biologiska och kemiska vapen. En annan del av underrättelsetjänstens arbete i dessa länder består i att bedriva täckfirmor för oskyldiga inköp av dual use-produkter.

10.6. Fungerar ECHELON för industrispionage?

Via den strategiska kontrollen av internationell teletrafik upptäcks viktig information om konkurrensspionage enbart av slump. Faktum är att känslig företagsinformation framför allt finns inne på företagen, **vilket innebär att konkurrensspionage i första hand lyckas när man försöker få tag i information via anställda** eller inslussade personer eller när man lyckas tränga in i företagens nätverk. Det är bara när känslig information skickas via kabel eller radio (satellit) som det är möjligt att sätta in ett kommunikationsövervakningssystem för konkurrensspionage. Detta gäller systematiskt i följande tre fall:
- för företag som arbetar i tre olika tidzoner så att information skickas från Europa till Amerika och vidare till Asien.

- När det förekommer videokonferenser i multinationella koncerner som sänds via V-Sat eller kabel.
- När det sker förhandling om viktiga uppdrag på plats (exempelvis vid anläggningsarbeten, uppbyggnad av infrastruktur för telekommunikation, nybyggnad av transportsystem etc.), och man därifrån måste överlägga med huvudkontoret per telefon**.**

När företagen inte skyddar sådan kommunikationen ger avlyssning av denna kommunikation värdefull information vid konkurrensspionage.

10.7. Offentliggjorda fall

Det finns vissa fall av företags- respektive konkurrensspionage som har beskrivits i den offentliga pressen respektive i facklitteraturen. En del av dessa källor har blivit utvärderade. Resultatet sammanfattas i nedanstående tabell. Där nämns det i korthet vem som var inblandad i fallet, när fallet inträffade, vad det i detalj handlade om, vad syftet var och vilka följderna har blivit.

Fall	Vem	När	Vad	Hur	Mål	Följder	Källa
Air France	DGSE	Till 1994	Samtal resande affärsmän	I 1:aklasskabinerna på Air France uptäcktes vägglöss – flygföretaget bad offentligt om ursäkt	Inhämtande av information	Ej angivna	”Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“ av Arno Schütze, 1/
Airbus	NSA	1994	Informationer om flygaffär mellan Airbus och saudi-arabisk flyglinje	Avlyssning av fax och telefonsamtal mellan förhandlingsparterna	Vidarebefordran av information till de amerikanska konkurrenterna Boeing och Mc-Donnell-Douglas	Amerikanerna avslutar 6-miljarder-dollar-affären	”Antennen gedreht”, Wirtschaftswoche nr 46 / 9 november 2000
Airbus	NSA	1994	Avtal om 6 miljarder $ med Saudiarabien Upptäckt av bestickning av det europeiska Airbus-konsortiet	Avlyssnande av fax och telefonsamtal mellan: europeiska Airbus-konsortiet och saudiska flygbolaget/regeringen om kommunikationssatelliter	Avslöjande av bestickning	McDonnel-Douglas, den amerikanska konkurrenten till Airbus, avslutar affären	“Development of Surveillance Technology and Risk of Abuse of Economic Information”, Vol 2/5 10 1999 STOA, von Duncan Campbell
BASF	Försäljare	Ej angivet	Beskrivning av förfarandet för produktion av företaget BASF:s (kosmetikdelen) hudkrämsråvara	ej angivet	ej angivet	Inga, eftersom givit sig av	”Nicht gerade zimperlich”, Wirtschaftswoche nr 43 / 16 oktober 1992
Tyska för-bunds-ministeriet för näringslivet	CIA	1997	Informationer om high-tech-produkter i förbundsministeriet för näringslivet	Insats av agent	Inhämtande av information	Agenten blir avslöjad vid försöket och utvisad	”Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?” av Arno Schütze, 1/98
Tyska förbunds-ministeriet för näringslivet	CIA	1997	Bakgrunden till Berliner-Mykonos-prozessen, hermeskrediter hänförliga till Iran-exporten, uppgifter om tyska företag som levererar high-tech-produkter till Iran	CIA-agent avslöjad som USA-sändebud för vänskapliga samtal med ledaren för det arabiska området (tyngdpunkt Iran) bemyndigad referat i förbundsministeriet för näringslivet	Inhämtande av information	Ej angivet Tjänsteman vänder sig till tyska säkerhetsmyndigheter, som låter amerikanerna veta att CIA-operationen inte är önskvärd. CIA-Agenten blir därefter ”bortflyttad”.	”Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichten-dienste”, Landesamt für Verfassungsschutz Baden-Württemberg, Stuttgart, Stand: 1998
Dasa	Ryska ND:er	1996 – 1999	Försäljning och vidare-befordran av rustningstekniska underlag från ett försvars-tekniskt företag i München (enligt SZ / 2000-05-30: rustningskoncernen Dasa i Ottobrunn)	2 tyskar i uppdraget	Inhämtande av information c styrda missiler, vapensystem, (värn mot pansar och flyg)	SZ /2000-05-30: ”(...)Förräderiet från militär synpunkt inte speciellt allvarligt”. Detta torde också gälla för de ekonomiska skadorna, fastslog rätten.	”Anmerkungen zur Sicherheitslage der deutschen Wirtschaft”, ASW; Bonn, april 2001 ”Haftstrafe wegen spionage für Russland”, SDZ / 30 maj 2000
Embargo	BND	Omkring tt 1990	Förnyad export av embargo-skyddad teknik till Libyen (bl.a.genom Siemens)	Avlyssning av teletrafiken	Avslöjande av illegala vapen- och. Tekniköverföringar	Inga speciella konsekvenser, leveranser hindras inte	”Maulwürfe in Nadelstreifen”, Andreas Förster, s. 110

Fall	Vem	När	Vad	Hur	Mål	Följder	Källa
Enercon	Vindkrafts-experter fr. Oldenburg och kvinnlig medarbetare till Kenetech	Ej angivet	Aurich-firman Enercons vind-kraftanläggning	ej angivet	ej angivet	ej angivet	”Anmerkungen zur Sicherheitslage der deutschen Wirtschaft”, ASW; Bonn, attpril 2001
Enercon	NSA	Ej angivet	Vindsnurra för strömalstring, utvecklad av ostfriesiske ingenjören Wobben	Ej angivet	Vidarebefordran av Wobbens’ tekniska uppgifter till USA-företag	USA-företaget ansöker om patent på vindsnurra före Wobben. Denne stäms av USA:s advokatkansli (patentintrång)	”Aktenkrieger”, SZ, 29 mars 2001
Enercon	USA-firman Kenetech Windpower Corp	1994	Viktiga detaljer av en high-tech-vindanläggning (från kopplingsanläggningar till kretskort)	Fotografier	Framgångsrikt patentförfarande i USA	Enercon GmbH lägger planerna på att öppna den amerikanska marknaden på is	”Sicherheit muss künftig zur Chefsache werden”, HB / 29 attugusti 1996
Enercon	Oldenburg-ingenjören W. och USA-firman Kenetech	Mars 1994	Enercons vindgenerator typ E-40	Ingenjören W. vidarebefordrar kunskaper, kvinnlig med-arbetare till Kenetech fotograferar anläggning + elektriska. detaljer	Kenetech: söker bevis för senare (1995) stämning mot Enercon för patentintrång. Enercon: illegalt Inhämtande av information om affärshemligheter TV-journalist skall från tidigare NSA-medarbetare ha erfarit att detaljinformationer från Enercon via Echelon vidare-befordrades till Kenetech av amerikanerna.	ej angivet	”Klettern für die Konkurrenz”, SZ 13 oktober 2000
Enercon	Kenetech Windpower	Före 1996	Data för Enercons vindenergi-anläggning	Kenetech-ingenjörer fotograferar anläggning	Kenetech kopierar anläggning	Enercon får rätt; straffyrkande mot spionerna framställs; uppskattad förlust: Flera hundra miljoner D-mark	”Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?” av Arno Schütze, 1/98
Japans handelsminist erium	CIA	1996	Förhandlingar om importkvoter för USA-bilar på den japanska marknaden	”Hacking” i japanska handels-inisteriets datorsystem	USA-underhandlaren Mickey Kantor skall acceptera lägsta anbudet	Kantor accepterar lägsta anbudet	Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?” av Arno Schütze, 1/98
Japanska bilar	USA :s regering	Ej angivet	Förhandlingar om import av japanska lyxbilar Information om emissions-standarder för japanska bilar	COMINT, inte närmare beskrivet	Inhämtande av information	Inga uppgifter	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, av Duncan Campbell

Fall	Vem	När	Vad	Hur	Mål	Följder	Källa
López	NSA	Ej angivet	Videokonferens med VW och López	Avlyssning från bas i Bad Aibling	Vidarebeforran av information till General Motors och Opel	Genom avlyssningsåtgärden hade statsadvokatkåren kunnat få ”mycket exakta upplysningar” för förmedling	Kaptenen i förbundsförsvaret Erich Schmidt-Eenboom, citerad i ”Wenn Freunde spionieren” www.zdf.msnbc.de/news/54637.asp?cp1=1
López	López och tre av hans med-arbetare	1992 - 1993	Handlingar och data från områdena forskning, planering, tillverkning och inköp (under-lag för fabrik i Spanien, kostnadsdata för olika modellinjer, inköps- och besparingsstrategier)	Insamling av material	Användning av underlag från General Motors-genom VW	Efter straffrättslig utredning förlikas koncernerna. López träder 1996 tillbaka som VW-chef. VW gör sig 1997 av med ytterligare tre medarbetare till López-teamet, betalar 100 miljoner dollar till GM/Opel (kallade advokatkostnader) och förvärvar under 7 år reservdelar för sammanlagt 1 miljard dollar från GM/Opel	”Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichten-dienste”, Landesamt für Verfassungsschutz Baden-Württemberg, Stuttgart, Stand: 1998
López	NSA	1993	Videokonferens mellan José Ignacio López och VW-chefen Ferdinand Piëch	Medskrift av videokonferensen och vidarebefordran därav till General Motors (GM)	Skydd för de amerikanska GM-affärshemligheterna, som López ville vidarebefordra till VW (prislistor, hemliga planer om ny bilfabrik och ny småbil))	López ger sig av. Strafförfarandet ställs in 1998 mot betalande av penningböter. För NSA inga	”Antennen gedreht”, Wirtschaftswoche nr 46 / 9 november 2000 ”Abgehört”, Berliner Zeitung, 22. Januar 1996 ”Die Affäre López ist beendet”, Wirtschaftsspiegel, 28 juli 1998 ”Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?” av Arno Schütze, 1/98
Los Alamos	Israel	1988	Två av det israeliska atomforskningsprogrammets medarbetare knäcker central-daton i atomvapenlaboratoriet i Los Alamos	”Hacking””	Inhämtande av information om nya USA-atomvapentändare	Inga speciella konsekvenser, då hackarna flyr till Israel. En av dem blir tillfälligt fasttagen. Om förbindelse med israeliska underrättelsetjänsten sägs ingenting officiellt.	"Maulwürfe in Nadelstreifen", Andreas Förster, s. 137
Smuggling	BND	70-talet	Smuggling av datoranlägg-ningar till DDR	ej angivet	Avslöjande av tekniköverföring till Östblocket	Inga speciella konsekvenser. Leveranserna förhindras inte.	"Maulwürfe in Nadelstreifen", Andreas Förster, s. 113

Fall	Vem	När	Vad	Hur	Mål	Följder	Källa
TGV	DGSE	1993	Kostnadskalkyl från Siemens Uppdrag för leverans av höghastighetståg till Sydkorea	Ej angivet	Prisunderbjudande	ICE-tillverkaren förlorar uppdraget, som går till Alcatel-Alsthom	”Wirtschaftsspionage: Varas macht eigentlich die Konkurrenz?” av Arno Schütze, 1/98
TGV	Okänd	1993	Kostnadskalkyl från AEG och Siemens. avseende statligt uppdrag i Sydkorea om leverans av höghastighetståg	Siemens anklagar för av-lyssning av företagets telefon- och faxförbindelser vid företagets filial i Seoul	Förhandlingsfördel för den brittisk-franska konkurrrenten GEC Alsthom	Uppdragsgivarna bestämmer sig för GEC Alsthom fastän det tyska anbudet först var bättre	Abgehört“, Berliner Zeitung, 22. Januari 1996
Thomson-Alcatel mot Raytheon	CIA/ NSA	1994	Bortskänkning till franska Thomson-Alcatel (1,4 mjdr $) av ett brasilianskt miljard-uppdrag om satellit-övervakning av Amazonas	Avlyssning av kommunikationen med vinnaren (Thomson-Alcatel, FR)	Avslöjande av korruption (utbetalning av mutor))	Clinton besvärar sig hos den brasilianska regeringen under tryck från USA-regeringen om förnyande av uppdraget till USA-företaget "Raytheon"	"Maulwürfe in Nadelstreifen", Andreas Förster, s. 91
Thomson-Alcatel mot Raytheon	USA :s ministerium för närings-livet ”må ha bemödat sig”	1994	Förhandlingar om miljard-projekt för radaröverövakning av den brasilianska regnskogen	Ej angivet	Övertagande av uppdraget	Den franska koncernen Thomson CSF och Alcatel förlorar uppdraget, som går till USA-företaget Raytheon	"Antennen gedreht“, Wirtschaftswoche nr.46 / 9 denovember 2000
Thomson-Alcatel mot Raytheon	NSA Department of Commerce	Departm ent of Commer ce	Förhandlingar om miljard-projekt (1.4 mjdr $) för över-vakning av Amazonas (SIVA) Upptäckt av bestickning av den brasilisanska selektions-panelen Anmärkning av Campbell: Rayethon utrustar avlyssnings-station i Sugar Grove	Avlyssning av förhandlingen mellan Thomson-CSF och Brasilien samt vidarebefordran av utgången till Raytheon Corp.	Avslöjande av bestickning Övertagande av uppdraget	Raytheon får uppdraget	”Development of Surveillance Technology and Risk of Abuse of Economic Information”, Vol 2/5 10 1999 STOA, av Duncan Campbell http://www:rayethon:com/sivam/contract:html
Thyssen	BP	1990	Miljonuppdrag om gas- och oljebefrämjande i Nordsjön	Avlyssning av vinnarens (Thyssen) faxar	Avslöjande av korruption	BP stämmer Thyssen med krav på skadestånd	"Maulwürfe in Nadelstreifen", Andreas Förster, s. 92
VW	Okänd	”Gångna år”	Ej angivet	Bl.a. infrarödkamera, som är ingrävd i jordhög och som vidarebefordrar bilder via radio	Inhämtande av information om nyutvecklingar	V W anger vinnarförluster på tresiffrig nivå	"Sicherheit muss künftig zur Chefsache werden“, HB / 29 augusti 1996
VW	Okänd	1996	VW:s teststräcka i Ehra-Lessien	Dold kanamera	Informationer om nya modeller från VW	Ej angivet	"Auf Schritt und Tritt“ Wirtschaftswoche nr. 25, 11 jaguni 1998

10.8. Skydd mot företagsspionage

10.8.1 Rättsligt skydd

I alla industristaters rättsordningar är stöld av företagshemligheter straffbelagd. Som i alla andra fall inom straffrätten är även den nationella skyddsnivån gestaltad mer eller mindre tätt. I regel gäller emellertid att straffskalan har förblivit tydligt lägre än för spionage i samband med militär säkerhet. I många fall är dock konkurrensspionage förbjudet bara mot företag i det egna landet, inte mot företag i utlandet. Detta gäller även Förenta staterna.

De ifrågavarande lagarna förbjuder i sin kärna bara spionageverksamheter som bedrivs av industriföretag sinsemellan. Huruvida de också inskränker statliga underrättelsetjänsters verksamhet är tvivelaktigt. Normalt skulle detta inte avslöjas på grundval av de lagar som ger underrättelsetjänsterna speciella befogenheter. Speciellt inom EU Skulle detta stå i strid mot EEG-fördraget (se kapitel ...).

Oberoende av detta skulle det emellertid i praxis vara mycket svårt att förverkliga ett ianspråktagande av rättsligt skydd genom åberopande av lagar för ett företag.

10.8.2 Övriga hinder för företagsspionage

Att underrättelsetjänster med syfte att skaffa sig allmänna strategiska informationer är verksamma även inom företagsområdet är accepterat stater emellan. Massiva brott mot detta ”gentlemen’s agreement” sker dock vid konkurrensspionage till förmån för den egna industrin. Om en stat därvid bevisligen naglas fast får den massiva politiska problem. Detta gäller också, och direkt, för en världsmakt som USA, vars anspråk på globalt politiskt ledrskap därvid skulle bli dramatiskt skadat. Mellanmakter skulle kunna kosta på sig att uppvisas på detta sätt, en världsmakt inte.

Utöver de politiska problemen uppkommer också den praktiska frågan, vilket individuellt företag som skulle få resultaten av konkurrensspionage ställda till förfogande. Inom området för flygplanstillverkning kan den frågan enkelt besvaras, eftersom det globalt bara finns två stora anbudsgivare. I alla andra fall är det ytterst vanskligt att gynna ett enstaka företag, i den mån det finns flera anbudsgivare som inte är statsägda. När det gäller vidarebefordran av detaljinformation om konkurrenternas anbud till vissa företag i samband med internationella offentliga anbudsförfrågningar kunde det dock vara tänkbart att vidarebefordra spionageinformationen till alla medkonkurrenter inom det egna landet. Detta gäller speciellt i de fall där regeringen tillhandahåller en understödsstruktur som är lika tillgänglig för alla konkurrenterna inom det egna landet, såsom i USA med dess s.k. Advocacy center. Vid teknologistöld, som obligatoriskt måste utmynna i en patentansökan, skulle en likformig behandling att företag inte vara logiskt möjlig.

Detta skulle otvivelaktigt vara ett stort problem speciellt i det amerikanska politiska systemet. Amerikanska politiker är för finansieringen av valkampanjerna massivt beroende av medel från industrin i sina respektive valkretsar. Om gynnande av enstaka företag med hjälp av underrättelsetjänster skulle offentliggöras bara i ett enstaka fall, för statuerande av ett exempel,

skulle detta ge upphov till jättestarka fördömanden i det politiska systemet. Som den tidigare CIA-direktören Wolsey har formulerat det i ett samtal med representanter för utskottet har formulerat det, ”In this case the hill (i.e. the US-Congress) would go mad!” Där han har rätt har han rätt!

10.9 USA och företagsspionage

10.9.1 Den officiella inställningen till företagsspionage på den amerikanska sidan

Den förre CIA-direktören Wolsey och ordföranden för Representanthusets underrättelsetjänstutskott Porter Gross har, kort sammanfattat, vid samtal företrätt följande position:

1. USA övervakar internationell teletrafik för att få allmänna informationer om företagsutvecklingar, leveranser av dual-use-gods och beläggande med kvarstad.

2. USA övervakar teletrafik från individuell företag i samband med upphandling av uppdrag med sikte på att förhindra att marknaden snedvrids genom bestickning till nackdel för USA-företag.

Bestickning skall vara förbjuden för amerikanska företag, och auktoriserade revisorer skall va skyldiga att anmäla när de stöter på betalning av mutor. Om bestickning i samband med offentliga uppdrag fastslås genom kommunikationsövervakning, skulle det amerikanska sändebudet hos det ifrågavarande landets regering intervenera. Medkonkurrerande USA-företag skulle emellertid inte informeras direkt.

10.9.2 Den roll som spelas av Advocacy Center vid befrämjandet av USAexporten

10.9.2.1 Uppgiften för Advocacy Center

Advocacy Center, som är placerat inom USA:s handelsministerium, är hjärtpunkten för den nationella exportstrategi som bedrevs av president Clinton och fortsätts av Bush. Detta center, grundat år 1993, har sedan dess hjälpt hundratals USA-företag att få offentliga updrag utomlands. Det förenar USAregeringens relevanta resurser från expertis inom enskilda områden via ambassadernas handelsattachéer till Vita Huset.

10.9.2.2 Centrets arbetssätt

I själva centret arbetar bara en liten stabc av 12 personer (gäller 20010206). Centret betjänar företagen som central startpunkt för USA-administrationens myndigheter som har med exportbefrämjandet att göra. Det arbetar på ett sätt som inte diskriminerar företagen men stöder

enligt klara regler endast projekt i USA:s nationella intresse. Sålunda måste värdet av de levererade produkterna till minst 50 procent härröra från USA.

10.9.2.3 Öppna frågor i samband med Centret

Den amerikanska regeringen har inte tillåtit det planerade samtalet mellan medlemmar av utskottet och Centret. Därför kunde två frågor, till vilka tvivel var knutet, inte genomdiskuteras:

a. Dokument som förefaller att belägga delaktighet från CIA:s sida i arbeten inom centret föreligger för utskottet.

b. Centret anger inom ramen för den på Internet befintliga informationen att det knyter samman resurserna från 19 ”U.S. government agencies” På annat ställe nämns emellertid bara 14 agencies. Det ger upphov till en fråga, varför namnen på 5 agencies inte nämns offentligt.

10.10 Säkerheten i datornät

Kommer i efterhand

10.11 Underskattning av riskerna

Kommer i efterhand

10.11.1 Storföretag

10.11.2 Små och medelstora företag

10.11.3 Europeiska institutioner

10.11.4 Forskningsinstitutioner

11 Skydd genom kryptering

11.1. Syftet med krypteringsnycklar och beskrivning av hur dessa fungerar

11.1.1 Syftet med krypteringsnycklar

Varje gång information skickas finns det risk för att den hamnar i orätta händer. Om man i vill förhindra att utomstående får kännedom om meddelandets innehåll måste man göra det oläsbart eller omöjligt att avlyssna, dvs. kryptera det. Inom militären och när det gäller diplomatiska frågor har krypteringsteknik alltid använts.[1]
Under de senaste 20 åren har kryptering blivit allt viktigare eftersom en allt större andel kommunikation sker med utlandet där nationalstaterna inte kunnat skydda brev- och telehemligheter. Dessutom har den egna statens utvidgade tekniska möjligheter att legalt avlyssna/spela in kommunikation lett till att oroade medborgare önskar högre skyddsbehov. Och slutligen har de kriminellas ökade intresset av illegal tillgång till informationen och att kunna förfalska denna lett till skyddsåtgärder (exempelvis inom banksektorn).
När den elektriska och elektroniska kommunikationen uppfanns (telegraf, telefon, radio, teleprinter, fax och Internet) blev det mycket enklare och gick enormt mycket snabbare att skicka nyheter. Nackdelen var att det inte fanns någon typ av **tekniskt** skydd mot avlyssning/inspelning och att var och en som hade motsvarande utrustning kunde få tillgång till kommunikationen när han fick tillgång till kommunikationsbäraren. Om avlyssning utförs professionellt efterlämnar det mycket små eller inga spår. Detta gjorde att kryptering fick en helt ny betydelse. Det var banksektorn som, i och med den elektroniska penninghanteringen, var först med att regelbundet skydda denna typ av kommunikation genom kryptering. Den ökande internationaliseringen av ekonomin innebär att kommunikationen åtminstone delvis skyddas av kryptering. I och med det den stora, fullständigt oskyddade kommunikationen på Internet har även privatpersoners behov vuxit att skydda kommunikation från avlyssning.
I och med denna rapport uppstår frågan om det finns billiga, legala, tillräckligt säkra och lättanvända krypteringsmetoder för kommunikation som ger ett skydd mot avlyssning.

11.1.2 Hur en krypteringsnyckel fungerar

Principen för en krypteringsnyckel är att en förståelig text omvandlas till en text som är obegriplig eller ger annan, felaktig information. De invigda vet hur man omvandlar denna text tillbaka till originaltexten. En begriplig sammansättning av bokstäver blir vid kryptering obegriplig så att ingen utomstående förstår innehållet.
Detta sker med hjälp av en viss metod (krypteringsalgoritmer), som bygger på att bokstäverna kastas om (transposition) eller ersätts (substitution). **Krypteringsmetoden** (algoritmen) är inte hemlig nuförtiden. Tvärtom: Nyligen gavs det en offentlig information om hur den nya globala standarden för kryptering ska användas i näringslivet. Detta gäller också när det gäller att använda en viss krypteringsalgoritm i maskinvara i en maskin, till exempel i en fax med inbyggd kryptering.

[1] Det finns bevis för att detta använts ända sedan antiken, spartanerna använde exempelvis skyter redan på 400-talet.

Det **hemliga** är den så kallade **nyckeln.** Detta kan enklast förklaras med ett exempel från ett närliggande område. Hur dörrlås fungerar vet de flesta och det finns patenterade och därmed beskrivna dörrlås. Det individuella skyddet för en viss dörr utgår från att det för en viss låstyp kan finnas flera olika nycklar. Det förhåller sig på samma sätt när det gäller kryptering av information: Med en **offentligt bekant metod** för kryptering (algoritm) går det att hålla hemligt **många** olika meddelanden, med hjälp av **hemliga** individuella nycklar som bara berörda personer har tillgång till.
För att förklara de ovan nämnda begreppen beskrivs nedan den så kallade "Cesarkrypteringen". Den romerske fältherren krypterade meddelanden genom att ersätta varje bokstav i meddelandet med den bokstav som stod tre bokstäver senare i alfabetet. Han ersatte alltså A med D, B med E. Ordet **ECHELON** blir då **HFKHORQ. Krypteringsalgoritmen** betyder alltså här att man **förskjuter bokstäver** inom alfabetet. Den konkreta **nyckeln** är informationen att gå **tre bokstäver åt höger i alfabetet!** Både krypteringen och avkrypteringen sker på samma sätt: genom att förskjuta bokstäverna tre bokstäver. Det handlar alltså om ett symmetriskt tillvägagångssätt. Nuförtiden skulle en sådan kryptering inte hålla ens en sekund! Om det är en bra kryptering kan metoden vara välkänd och trots det kan krypteringen betraktas som säker. Därför krävs det att det finns ett så stort antal nycklar att det inte är möjligt att testa alla nycklar (så kallad **brute force attack**) även om man använder datorer under ansenlig tid. Å andra sidan är en stor uppsättning nycklar i sig inget tecken på kryptologisk säkerhet, om krypteringsmetoden ger en krypterad text, som ger stöd för viss dechiffrering (till exempel genom att vissa bokstäver hopas på varandra). [1] Cesars kryptering är ingen säker kryptering med tanke på båda dessa aspekter. En enkel substitution kan snabbt knäckas, på grund av hur olika ofta bokstäver förekommer i ett språk. Dessutom finns det endast 27 förskjutningsmöjligheter eftersom alfabetet ju endast har 28 bokstäver. En motståndare kan genom att helt enkelt pröva sig fram snabbt hitta den nyckel som passar och dechiffrera texten. Nedan diskuteras hur ett säkert system måste se ut.

11.2 Säkerheten vad gäller krypteringssystem

11.2.1 Allmänt vad gäller begreppet säkerhet vid kryptering

Om man kräver att ett krypteringssystem ska vara "säkert" så kan man mena två olika saker med detta. Det kan dels betyda att det är helt säkert, att det alltså är omöjligt att dechiffrera innehållet utan att känna till nyckeln och att det är matematiskt möjligt att bevisa detta. Det kan också betyda att koden inte kan brytas med den teknik som finns idag och därmed ger säkerhet för en viss tidsperiod, som är betydligt längre än den "kritiska" tid som meddelandet måste hållas hemligt.

11.2.2 Absolut säkerhet: s.k. one-time pad

Ett absolut säkert förfarande erbjuder för närvarande endast "one-time pad" (engångskrypto). Detta system utvecklades mot slutet av första världskriget [2], men används också för den heta linje som finns mellan Moskva och Washington. Det fungerar så att det finns en nyckel som består av helt slumpmässigt sammanlänkade bokstäver, där sammanlänkningen inte upprepas. Sändare och mottagare krypterar utifrån dessa bokstavslänkningar och raderar nyckeln så fort

[1] Jämför också Leiberich, Vom diplomatischen Code zur Fallfürfunktion - Hundert Jahre Kryptographie in Deutschland, Spektrum der Wissenschaft, Juni 1999, s 26 ff.
[2] Infördes av major Joseph Mauborgne, ledare för den kryptografiska forskningsavdelningen i den amerikanska armén . Jfr också Singh, Geheime Botschaften (1999), 151.

den har använts. Eftersom det inte finns någon inre ordning för hur nyckeln fungerar är det omöjligt att knäcka koden. Detta kan också bevisas matematiskt. [1]
Nackdelen med detta tillvägagångssätt är att det är svårt att skapa stora mängder slumpmässiga nycklar av denna typ, [2] och att det är svårt och opraktiskt att distribuera nycklarna på ett säkert sätt. Därför används inte denna metod i allmän kommunikation inom företagen.

11.2.3 Relativ säkerhet som motsvarar den tekniska utvecklingen

11.2.3.1. Använda maskiner för att kryptera och avkryptera

Redan innan ”one-time pad” uppfanns utvecklades krypteringslösningar som innehöll ett stort antal nycklar och alstrade kodade texter som innehåll så få regelbundenheter som möjligt i texten och därmed i princip gjorde omöjligt att analysera krypteringsnyckeln. Maskiner för kryptering och avkryptering utvecklades för att tillräckligt snabbt få fram användbara metoder. Den kanske mest spektakulära maskinen var ENIGMA [3], som användes av tyskarna under andra världskriget. En armé av dechiffreringsexperter, som arbetade i Bletchley Park i England, lyckades knäcka krypteringsnyckeln för ENIGMA med hjälp av speciella maskiner, så kallade "Bomber". Både ENIGMA och "Bomben" var mekaniska apparater.

11.2.3.2. Datoranvändning vid kryptering

När datorn uppfanns var det en banbrytande innovation för krypteringsvetenskapen eftersom dess prestanda gjorde det möjligt att använda allt mer komplexa system. Även om det inte påverkade grundprinciperna för kryptering så medförde det vissa nyheter. För det första mångdubblades graden av krypteringsnycklarnas komplexitet eftersom nycklarna inte längre begränsades av vad som var möjligt rent mekaniskt och dessutom ökade hastigheten drastiskt vad gällde själva krypteringsprocessen.
Informationen bearbetas digitalt av datorerna med binära tal. Det betyder att informationen i tur och ordning uttrycks i form av två signaler, nämligen 0 och 1. 1 motsvarar en elektrisk spänning, magnetisering, inom fysiken, ("Ljus på"), 0 motsvarar när spänningen, magnetiseringen, upphör ("Ljus av"). Det är ASCII [4]-standarden som används. Där representeras varje bokstav av en sjusiffrig kombination av 0 och 1 [5]. En text förvandlas till en rad med siffror av 0 och 1 och i stället för att bokstäverna krypteras, krypteras talen.
På så sätt är det möjligt att använde både transposition (tecknen byter plats) och substitution (tecknen ersätts). Substitution kan gå till så att en nyckel tillfogas i form av en valfri rad av tal. Enligt de regler som finns i den binära matematiken blir lika tal noll när de adderas (dvs. 0 +0=0 och 1 +1=0), och olika tal blir ett (0+1=1). Den nya krypterade rad av tal som uppstår genom addition är därmed en binär följd som antingen kan bearbetas vidare digitalt eller, genom att man drar ifrån den tillagda nyckeln, åter kan göras läsbar.
Datorerna gör det möjligt att använda komplexa krypteringsalgoritmer och alstra kodade texter som i princip inte går att knäcka med krypteringsanalys. Det enda möjliga sättet att komma åt koden är att prova samtliga möjliga nycklar. Ju längre nyckeln är desto

[1] Jämför Singh, Geheime Botschaften (1999), 151 ff.
[2] Jämför Wobst, Abenteuer Kryptologie[2] (1998), 60.
[3] Enigma utvecklades av Arthur Scherbius och patentskyddades 1928 patentiert. Maskinen liknade på sätt och vis en skrivmaskin eftersom den hade ett tangentbord som den riktiga texten skrevs in på. Genom en ///stickproppsplanka och roterande valsar kodades texten enligt order och avkodades sedan med samma maskin och kodböcker.
[4] American Standard Code for Information Interchange.
[5] A = 1000001, B= 1000010, C= 1000011, D= 1000100, E = 1000101, etc.

större är chansen att denna metod misslyckas – även om högpresterande datorer används – eftersom det tar för lång tid. Det finns alltså hanterbara sätt som med nuvarande teknik kan betraktas som säkra

11.2.4. Standardisering och föreskriven begränsning av säkerheten

På grund av det ökade datoranvändandet under 1970-talet blev det alltmer brådskande att standardisera systemen för krypteringsnycklar eftersom det var enda möjligheten för företag att säkra kommunikationen med sina partner utan oproportionerligt stort arbete. Det första arbetet med detta gjordes i USA.
En komplex krypteringsnyckel kan även användas för ohederliga ändamål eller av potentiella militära fiender och kan försvåra eller omöjliggöra elektroniskt spionage. Därför var det av stort intresse från NSA att man valde en krypteringsstandard som var tillräckligt säker för företag men som NSA på grund av sin extremt avancerade tekniska utrustning skulle kunna dechiffrera. Därför begränsades krypteringsnyckelns längd till 56 bitar. Det minskar antalet möjliga nycklar till 100 000 000 000 000 000 stycken [1]. Den 23 november 1976 antogs officiellt det så kallade Lucifer-chiffret, gjort av Horst Feistel i **56-bitarsversion,** och fick namnet Data Encryption Standard (DES), vilken för ett kvartssekel representerade den officiella amerikanska krypteringsnyckelstandarden. [2] Denna standard antogs även i Europa och Japan och då framför allt inom banksektorn. DES-algoritmen har, tvärt emot vad som sagts i olika medier, hittills inte knäckts men det finns numera maskinvara som är kraftig nog att kunna gå igenom samtliga nycklar ("brute force attack"). Triple-DES, som har en 112-bitars krypteringsnyckel räknas fortfarande som säker. DES efterföljare, som kallas AES (Advanced Encryption Standard), är en europeisk standard [3], som utarbetats under namnet Rijndael i Leuven, Belgien. **Den är snabb och antas vara säker eftersom man har undvikit att begränsa längden på krypteringsnyckeln.** Det beror på en ändrad amerikansk politik vad gäller kryptering (se punkt 1.4)
Standardiseringen innebar en betydande lättnad för företagen när det gällde kryptering. Problemet med hur nycklarna skulle distribueras kvarstod dock.

11.3. Säkerhetsproblemet vid distribution/överlämnande av nycklar

11.3.1. Asymmetrisk kryptering: förfarandet med offentliga nycklar

Så länge ett system arbetar med en nyckel som används för både kryptering och dekryptering (symmetrisk kryptering) kan man bara med svårighet hantera det när man har **många** kommunikationspartner. Nyckeln måste nämligen **i förväg** vara överlämnad till varje ny kommunikationspartner på sådant sätt att ingen tredje har fått kännedom om den. Detta möter praktiska svårigheter för företag och organisationer, och för privatpersoner är det bara i undantagsfall möjligt.

En lösning av detta problem är att använda asymmetrisk kryptering: man använder inte samma nyckel för kryptering och dekryptering. Texten krypteras med en nyckel som helt enkelt kan vara känd för alla, den **offentliga nyckeln**. Metoden är som en enkelriktad gata i det att en

[1] Detta tal, visat binärt, består 56 nollor och ettor. Jfr Singh, Geheime Botschaften (1999), 03.
[2] Jfr Singh, Geheime Botschaften (1999), 302 ff.
[3] Den skapades av två belgiska kryptografer på det katolska universitetet i Leuven, Joan Daemen und Vincent Rijmen.

omvandling tillbaka till klartexten inte kan göras med den offentliga nyckeln. Därför kan var och en som vill ta emot ett krypterat meddelande delge kommunikationspartnern sin offentliga nyckel, även på en osäker väg, i och för kryptering av meddelandet. För dekryptering av den sedermera mottagna texten används en annan nyckel, den **privata nyckeln**, som hemlighålls och inte sänds. [1]. Den liknelse som är mest klargörande för förståelsen av förfarandet är med ett hänglås; vem som helst kan anbringa ett hänglås och därmed försluta en kassakista på ett säkert sätt, men den enda som kan öppna låset är den som har den rätta nyckeln. [2] Det finns ett samband mellan den offentliga nyckeln och den privata, men man kan inte beräkna den privata nyckeln ur den offentliga.

Ron Rivest, Adi Shamir och Leonard Adleman har uppfunnit en asymmetrisk kryptering i och med RSA-förfarandet, som har fått sitt namn efter dem. I en envägsfunktion (en så kallad fallucksfunktion) sätter man in resultatet av en multiplikation av två mycket stora primtal som en del av den offentliga nyckeln. Det är med denna nyckel som klartexten krypteras. Dekrypteringen är möjlig enbart för den som känner till de båda primtalens värden. Det finns emellertid inget känt matematiskt förfarande som möjliggör en omvändning av en multiplikation av två primtal på sådant sätt att man ur resultatet av multiplikationen kan härleda de ursprungliga primtalen. Än så länge är en sådan härledning inte möjlig på annat sätt än genom systematiska försök. Därför är krypteringsförfarandet på vetenskapens nuvarande ståndpunkt säkert under förutsättning att man väljer tillräckligt stora primtal. Den enda risken ligger i att någon briljant matematiker skulle kunna finna ett snabbare sätt för uppdelning i faktorer. Trots stora ansträngningar har dock hittills ingen lyckats med detta. [3] Ofta hävdas det rentav att problemet är olösligt, men något exakt bevis för detta har hittills inte framlagts. [4]

I jämförelse med symmetriska krypteringsförfaranden (t ex DES) kräver krypteringen med offentliga nycklar ofrånkomligen vida längre räknetid på persondatorer eller insättande av snabba stordatorer.

11.3.2. Kryptering med offentliga nycklar för privatpersoner

För att göra förfarandet med offentliga nycklar allmänt tillgängligt kom Phil Zimmerman på idén att det beräkningsmässigt tunga förfarandet med offentliga nycklar skulle förbindas med ett snabbare symmetriskt förfarande. Själva meddelandet skulle krypteras med ett symmetriskt förfarande, nämligen det i Zürich utvecklade IDEA-förfarandet, medan nyckeln för den symmetriska krypteringen samtidigt skulle överföras med förfarandet med offentliga nycklar. Zimmermann skapade ett användarvänligt program, benämnt Pretty Good Privacy, som med en tangenttryckning (respektive ett musklick) skapar den erforderliga nyckeln och genomför krypteringen. Programmet lades ut på Internet, så att vem som helst kunde ladda ned det. PGP köptes slutligen av det amerikanska företaget NAI men ställs fortfarande gratis till förfogande för privatpersoner. [5] Den förutvarande versionens källtext gjordes offentlig, så att man kan utgå ifrån att det inte finns några bakdörrar inbyggda. Källtexten för den nyaste versionen, PGP7, som utmärker sig genom ett uttalat användarvänligt grafiskt gränssnitt, är tyvärr inte längre offentlig.

---

[1] Idén till den asymmetriska krypteringen i formen av förfarandet med offentliga nycklar härrör från Whitfield Diffie och Martin Hellmann.
[2] Singh, Geheime Botschaften (1999), 327.
[3] Jämför Buchmann, Faktorisierung großer Zahlen, Spektrum der Wissenschft 2 1999, 6 ff.
[4] Jämför Singh, Geheime Botschaften (1999), 335 f.
[5] Information om programvaran finns på www.pgpi.com

Det finns dock ännu en annan implementering av standarden OpenPGP: GnuPG. Den erbjuder samma krypteringsmetoder som PGP, och den är även kompatibel med PGP. Därvid rör det sig emellertid om fri programvara; dess källkod är känd, och vem som helst kan använda den och lämna den vidare. Det tyska Förbundsministeriet för ekonomi (Ruth: näringsliv?) och teknologi har stött porteringen av GnuPG till Windows och utvecklingen av ett grafiskt gränssnitt, men tyvärr är programvarorna för dessa för närvarande inte helt mogna. Enligt information som är tillgänglig för rapportförfattaren arbetas det dock på detta.

Dessutom finns det ytterligare standarder som konkurrerar med OpenPGP, såsom S/MIME, som stöds av många e-postprogram. Rapportförfattaren har dock inga informationer om fria implementeringar av dessa.

11.3.3. Framtida förfaranden

Helt nya aspekter för säker överföring av nycklar kan i framtiden öppnas genom kvantkryptografin. Denna säkerställer att en avlyssning av en nyckelöverföring upptäcks. Om man sänder polariserade fotoner går det inte att undersöka dessas polarisering utan att denna förändras. Lyssnare på dataförbindelsen kan därför ofelbart upptäckas. Då kan man se till att använda en nyckel som inte har avlyssnats. Vid försök har man hittills lyckats med överföring genom 48 km glasfiberkabel och på 500 meters avstånd genom luften. [1]

11.4. Krypteringsprodukternas säkerhet

I diskussionen om olika krypteringsmetoders faktiska säkerhet har amerikanska produkter gång på gång anklagats för att vara försedda med bakdörrar. Sålunda har stora rubriker ägnats åt Excel, varom det har påstått att, i den europeiska versionen, hälften av nyckeln ligger öppen i datafilens header. Vidare har Microsoft väckt uppmärksamhet i pressen genom att en hackare har funnit en ”NSA-nyckel” gömd i programmet, något som Microsoft naturligtvis häftigt har dementerat. Då Microsoft inte har offentliggjort sin källkod är varje bedömning av detta ren spekulation. För de tidigare versionerna av PGP och GnuPG kan sådana bakdörrar i varje fall med stor säkerhet uteslutas, eftersom deras källkod har gjorts öppen.

11.5. Kryptering i konflikt med statsintressen

11.5.1. Försök att begränsa krypteringen

I några stater är användning av krypteringsprogramvara och krypteringsutrustning för närvarande förbjuden, och dispens kräver särskilt tillstånd. Detta gäller inte bara diktaturer som Kina, Iran och Irak. Även demokratiska stater har infört lagliga begränsningar för användning eller försäljning av program och maskiner för kryptering. Kommunikationen skall (?) visserligen vara skyddad mot att läsas av obehöriga privatpersoner, men staten skall även i fortsättningen behålla möjligheten till laglig avlyssning i givna fall. Myndigheternas förlust av den tekniska överlägsenheten motvägs av lagstadgade förbud. I Frankrike har det sålunda ända till nyligen rått ett allmänt förbud mot användning av kryptografi utan tillstånd i varje särskilt fall. I Tyskland fördes för några år sedan en debatt om inskränkningar i krypteringen och om

[1] Till kvantkryptografi, jämför Wobst, Abenteuer Kryptographie[2] (1998), 234 ff.

obligatorisk nyckeldeponering. I USA har det i stället tidigare rått en begränsning av nyckellängden.

11.5.2. Den säkra krypteringens betydelse för e-handeln

Emellertid torde dessa försök en gång för alla ha misslyckats. Statens intresse av tillgång till dekrypteringen och därmed till klartexten står nämligen i konflikt inte bara med skyddet av den privata sfären, utan också med handfasta ekonomiska intressen. Ty e-handel och electronic banking är beroende av säker kommunikation över Internet. Utan garanti för denna säkerhet är dessa tekniker dömda till undergång, eftersom kundens förtroende då inte längre skulle vara givet. Detta sammanhang förklarar förvandlingen av den amerikanska och franska krypteringspolitiken.

Här kan det påpekas att e-handeln behöver säkra krypteringsförfaranden på två sätt: inte bara för kryptering av meddelanden, utan också för att med full säkerhet kunna kontrollera affärspartnerns identitet. Den elektroniska underskriften kan nämligen produceras genom att man tillämpar förfarandet med offentliga nycklar baklänges: den privata nyckeln används för krypteringen och den offentliga för dekrypteringen. Denna form av kryptering bekräftar upphovet till underskriften. Vem som helst kan använda en persons offentliga nyckel för att övertyga sig om underskriftens äkthet men däremot inte efterapa själva underskriften. Även denna funktion är inarbetad i PGP på ett användarvänligt sätt.

11.5.3. Problem för affärsresande

I många stater är det förbjudet för affärsresande att använda krypteringsprogram på medförda knädatorer. Detta förhindrar varje skydd för kommunikationen med det egna företaget och gör det omöjligt att få medförda data säkra mot tillgrepp.

11.6. Praktiska frågor för krypteringen

Om man vill besvara frågan, vem man skall råda att använda kryptering och under vilka omständigheter detta skall gälla, synes det riktigt att skilja mellan privatpersoner och företag.

Vad beträffar privatpersoner måste det öppet sägas ut att kryptering av fax och telefonsamtal med hjälp av Kryptotelefon respektive Cypherfax i verkligheten inte är realiserbar, detta inte bara därför att anskaffningskostnaderna för dessa apparater är relativt höga, utan också därför att apparaternas användbarhet förutsätter att kommunikationspartnern förfogar över sådan utrustning, något som väl är mycket sällsynt.

E-post, däremot, kan och bör krypteras av alla. Det ofta framförda påståendet, att man inte har några hemligheter och därför inte behöver kryptera, måste bemötas med att man ju normalt inte heller sänder skriftliga meddelanden på brevkort. Ett okrypterat e-brev är helt enkelt ingenting annat än ett brev utan kuvert. Kryptering av e-post är säker och relativt problemfri; på Internet finns redan användarvänliga system, t ex PGP/GnuPG, som rentav gratis ställs till förfogande för privatpersoner. Men tyvärr saknas den nödvändiga utbredningen. Här skulle det vara önskvärt att det offentliga skulle föregå med gott exempel och självt införa kryptering som standard för att avmystifiera krypteringen.

Inom företag borde man strängt bevaka att överföring av känslig information begränsas till säkrade kommunikationsvägar. Detta kan förefalla självklart, och är det väl också för storföretagens del, men inom små och medelstora företag vidarebefordras ofta företagsintern information okrypterad med e-post eftersom problemmedvetandet inte är tillräckligt utbrett. Här är det att hoppas att industrisammanslutningar och handelskammare bemödar sig mera om upplysning. Visserligen är kryptering av e-brev bara en säkerhetsfråga bland många, och framför allt verkningslös när informationen redan före krypteringen görs tillgänglig för andra. Detta innebär att hela arbetsområdet måste säkras och att man följaktligen måste skaffa garanti för lokalernas säkerhet och överpröva den fysiska tillgången till kontor och datorer. Men även obehörig tillgång till information via Nätet måste förhindras med hjälp av lämpliga brandväggar. Speciellt riskabel är sammanknytningen mellan internt nät och Internet. Om man tar säkerhetsfrågan på allvar bör man vidare enbart använda sådana operativsystem vilkas källkod är öppen och utprovad, eftersom man bara då med säkerhet kan säga vad som händer med ens data. Företag har alltså ett flertal arbetsuppgifter att genomföra. På marknaden finns redan talrika firmor ger säkerhetsråd och genomför säkerhetsåtgärder till överkomligt pris, och med stigande efterfrågan stiger också utbudet hela tiden. Därutöver är det emellertid att hoppas att industrisammanslutningar och handelskammare tar sig an dessa problem och speciellt gör småföretag uppmärksamma på säkerhetsproblematiken samt understöder ett omfattande skyddskoncept i samband med både planering och förverkligande.

12. EU:s externa relationer och insamling av underrättelser

12.1 Introduktion

I och med antagandet av Maastrichtfördraget år 1991 etablerades den gemensamma utrikes- och säkerhetspolitiken (Common Foreign and Security Policy, CFSP) i sin mest elementära form som ett nytt politiskt instrument för Europeiska unionen. Amsterdamfördraget sex år senare gav ytterligare struktur åt CFSP och skapade förutsättningarna för gemensamma försvarsinitiativ inom Europeiska unionen samtidigt som befintliga allianser kunde bibehållas. På grundval av Amsterdamfördraget och med erfarenheterna från Kosovo i åtanke lanserade Europarådet i Helsingfors i december 1999 Europeiska Säkerhets- och Försvarsinitiativet. Detta initiativ syftar till skapande av en multinationell styrka, bestående av ca 50 000 à 60 000 man, till andra halvåret år 2003. Existensen av en sådan multinationell styrka kommer att göra det oundvikligt att utveckla en självständig underrättelsekapacitet. Den enkla integrationen av WEU:s befintliga underrättelsekapacitet kommer att vara otillräcklig för detta ändamål. Ett längre gående samarbete mellan medlemsstaternas underrättelseorgan långt utöver de befintliga formerna för samarbete kan inte undvikas.

Vidareutvecklingen Av CFSP är emellertid inte det enda element som leder till en utvidgning av samarbetet mellan Unionens underrättelsetjänster. En fortsatt ekonomisk integration inom Europeiska unionen kommer att nödvändiggöra ett intensivare samarbete på underrättelseinsamlingens område. En enhetliggjord europeisk ekonomisk politik kräver en enhetlig uppfattning om de ekonomiska realiteterna i världen utanför Europeiska unionen. Ett enhetligt ställningstagande i handelsförhandlingarna inom WTO eller med tredje land förutsätter ett gemensamt skydd för förhandlingspositionen. Starka europeiska industrier behöver ett gemensamt skydd mot ekonomiskt spionage från områden utanför Europeiska unionen.

Slutligen måste det betonas att vidare utveckling av Unionens andra pelare och Unionens aktiviteter inom området för hem- och justitieärenden också måste leda till ett vidare samarbete mellan underrättelsetjänsterna. Speciellt kan den samfällda kampen mot terrorism, illegal handel med vapen, handel med människor samt penningtvätt inte bedrivas utan intensivt samarbete mellan underrättelsetjänsterna.

12.2. Möjligheter för samarbete inom EU

12.2.1. Befintligt samarbete

Trots att det inom underrättelsetjänsterna finns en lång tradition av att lita enbart på den information som de själva samlar in, och kanske även misstro mellan de olika underrättelsetjänsterna inom Europeiska unionen, är samarbetet mellan tjänsterna redan gradvis växande. Det förekommer täta kontakter inom ramen för NATO och WEU samt inom Europeiska unionen. Och under det att underrättelsetjänsterna inom ramen för NATO fortfarande tungt stöder sig på de långt mera avancerade bidragen från Förenta staterna har tillkomsten av WEU:s satellitcenter i Torrejon (Spanien) och en underrättelsesektion på WEU-högkvarterets nivå bidragit till en mera självständig europeisk verksamhet på detta fält.

12.2.2. Fördelar med en förenad europeisk underrättelsepolitik

Bortsett från denna utveckling, som redan pågår, måste det betonas att det faktiskt finns objektiva fördelar med en förenad europeisk underrättelsepolitik. Dessa fördelar kan beskrivas som följer.

12.2.2.1. Yrkesmässiga fördelar

Till en början kan det konstateras att det helt enkelt finns för mycket hemligt och öppet material tillgängligt för att samlas in, analyseras och utvärderas av ett enda organ eller genom bilateralt avtal inom Västeuropa. Kraven på underrättelsetjänster sträcker sig från försvarets underrättelseverksamhet genom underrättelseverksamhet som är inriktad på tredje stats interna och internationella ekonomiska politik till underrättelseverksamhet till stöd för kampen mot organiserad kriminalitet och narkotikahandel. Även om samarbete bara existerade på den mest grundläggande nivån, alltså när det gäller insamling av material från öppna källor (open-source intelligence, OSINT), skulle redan resultaten av detta samarbete vara av stor betydelse för Europeiska unionens politik.

12.2.2.2. Budgetfördelar

På senare tid har budgetarna för underrättelseinsamling skurits ned, och i vissa fall fortsätter de att reduceras. Samtidigt har kraven på information och därigenom underrättelseverksamhet vuxit. Det är inte bara så, att budgetnedskärningarna gör detta samarbete möjligt, utan dessutom gör de på lång sikt samarbetet lönsamt. Speciellt för upprättande och vidmakthållande av tekniska resurser när medlen är knappa är samfällda operationer av intresse, men också inom området för utvärdering av den insamlade informationen. Utvidgat samarbete kommer att öka effektiviteten i insamlingen av underrättelser.

12.2.2.3. Politiska fördelar

I princip används insamlade underrättelser för att ge regeringar möjlighet till bättre och mera välgrundat beslutsfattande. Ytterligare politisk och ekonomisk integration på Europeiska unionens nivå förutsätter att underrättelserna är tillgängliga på europeisk nivå och dessutom är grundade på mer än en enda källa.

12.2.3. Slutanmärkningar

Dessa objektiva fördelar är bara illustrationer av den växande betydelsen av samarbete inom Europeiska unionen. I det förgångna arbetade nationalstaterna var och en på egen hand med att garantera yttre säkerhet, inre ordning, nationellt välstånd och kulturell identitet. I dag är Europeiska unionen på många områden inbegripen i att ta upp en roll som åtminstone är ett komplement till nationalstatens roll. Det är omöjligt att underrättelsetjänsterna skall bli den sista och enda domän som inte påverkas av den europeiska integrationsprocessen.

12.3. Samarbete över Europeiska unionens nivå

Sedan andra världskriget skedde samarbetet inom underrättelsefältet inte i första hand på europanivå, utan betydligt mera på transatlantisk nivå. Det har redan i det föregående belysts att mycket täta relationer inom området för insamling av underrättelser upprättades mellan Förenade kungariket och Förenta staterna. Men också när det gäller försvarsunderrättelser inom och bortom ramen för NATO var och är Förenta staterna den absolut dominerande parten. Den viktigaste frågan är således om odlande av ett europeiskt samarbete på underrättelseinsamlingens område kommer att allvarligt störa relationerna med Förenta Staterna eller om det kanske tvärtom kan leda till en förstärkning av dessa relationer.

Hur kommer EU/US-relationerna att utvecklas under den nya Bush-administrationen? Och särskilt, hur kommer det speciella förhållandet mellan Förenta staterna och Förenade kungariket att upprätthållas inom denna ram?

Några är av den uppfattningen, att det inte behöver finnas någon motsägelse mellan å ena sidan den speciella relationen mellan Storbritannien och USA och å andra sidan den fortsatta utvecklingen av CFSP. Andra tror att speciellt insamlingen av underrättelser kan vara den fråga som kan tvinga Förenade kungariket att bestämma sig för om dess öde är europeiskt eller transatlantiskt. Storbritanniens intima förbindelser med USA (och det de andra parterna i UKUSA-överenskommelsen) kan göra det svårare för andra EU-stater att dela med sig av underrättelser sinsemellan – eftersom Storbritannien kanske är mindre intresserad av intraeuropeiskt delande och eftersom dess EU-partner kanske litar mindre på Storbritannien. På samma sätt, om USA tror att Storbritannien har utvecklat speciella länkar med sina EU-partner, och om detta är en del av ett speciellt europeiskt avtal, kan USA bli mindre villiga att fortsätta att dela med sig av sina underrättelser med De Förenade Kungarikena. Ytterligare EU-samarbete om underrättelserna kan därför komma att utgöra ett allvarligt test på Förenade kungariket europeiska ambitioner liksom på EU:s integrationskapacitet.

Under nuvarande omständigheter är det emellertid högeligen osannolikt att ens extremt snabba framsteg i samarbetet mellan de europeiska partnerna på kort sikt, men även på lång sikt, kan uppväga Förenta staternas tekniska fördel. Europeiska unionen kommer inte att kunna upprätta ett avancerat nät av SIGINT-satelliter, bildsatelliter och markstationer. Inte heller kommer Europeiska unionen att ha förmåga att på kort sikt utveckla ett sådant högeligen avancerat nät av datorer som behövs för urvalet och utvärderingen av det insamlade materialet. Europeiska Unionen kommer inte att vara beredd att göra erforderliga budgetmedel tillgängliga för att åstadkomma ett reellt alternativ till Förenta staternas underrättelseinsatser. Därför kommer det redan ur ett tekniskt och budgetmässigt perspektiv att vara i Europeiska unionens intresse att upprätthålla en nära relation med Förenta staterna när det gäller insamling av underrättelser. Men även ur en mera politisk synvinkel kommer det att vara viktigt att upprätthålla och, där så erfordras, förstärka relationerna med Förenta staterna, speciellt i fråga om den samfällda kampen mot organiserad brottslighet, terrorism, handel med narkotika och vapen samt penningtvätt. Samfällda underrättelseoperationer behövs för stöd åt en samfälld kamp. Samfällda fredsbevarande insatser sådana som i det förutvarande Jugoslavien kräver ett större europeiskt bidrag inom alla insatsfält.

Å andra sidan bör ett växande europeiskt medvetande åtföljas av ett större europeiskt ansvar. Europeiska unionen bör bli en mera likställd partner, inte bara i fråga om ekonomi, utan också i fråga om försvar och följaktligen i fråga om insamling av underrättelser. En mera självständig europeisk underrättelsekapacitet bör därför inte ses som en försvagning av de transatlantiska relationerna, utan utnyttjas som en förstärkning genom att Europeiska unionen etableras som en mera likställd och mera kapabel partner. Samtidigt måste Europeiska unionen göra en självständig insats för att skydda sin ekonomi och sin industri mot olagliga och ovälkomna hot, sådana som ekonomiskt spionage, cyberbrott och terroristattacker. Å andra sidan är transatlantisk förståelse nödvändig på området för industriellt spionage. Europeiska unionen och Förenta staterna bör komma överens om en samling regler om vad som är tillåtet och otillåtet på den punkten. För att förstärka det transatlantiska samarbetet på detta område kunde man ta ett samfällt initiativ på WTO-nivån för att utnyttja denna organisations mekanismer för skydd åt en rättvis ekonomisk utveckling över hela världen.

12.4. Slutanmärkningar

Medan det fundamentala skyddet av de europeiska medborgarnas privatliv måste upprätthållas bör en ytterligare utveckling av en för Europeiska unionen gemensam underrättelsekapacitet anses som nödvändig och ofrånkomlig. Samarbete med tredje land, och speciellt Förenta staterna, bör upprätthållas och med stor sannolikhet förstärkas. Detta betyder inte nödvändigtvis att europeiska SIGINT-aktiviteter automatiskt bör integreras i ett oberoende ECHELON-system för Europeiska unionen eller att Europeiska unionen bör bli en fullvärdig partner i det nuvarande UKUSA-avtalet. Utveckling av ett adekvat europeiskt ansvar på underrättelseinsamlingens område måste emellertid aktivt övervägas. En integrerad europeisk underrättelsekapacitet kräver samtidigt ett system för europeisk politisk kontroll av dessa organs aktiviteter. Beslut kommer att behöva fattas om medel för bedömning av underrättelser och för fattande av de politiska beslut som en analys av underrättelserapporter resulterar i. Avsaknad av ett sådant system för politisk kontroll och därmed även för politisk medvetenhet och ansvar för underrättelseinsamlingens process skulle vara skadlig för den europeiska integrationsprocessen.

13 lutsatser och rekommendationer

13.1. Inledning

I detta kapitel sammanfattas information och möjliga slutsatser. Det får inte uppfattas som slutgiltigt. Snarare vill rapportförfattaren skapa en arbetsgrundval för den politiska debatt som nu skall föras inom utskottet (eller kommittén? Ö.a.) Texten kommer därefter att behöva ändras på nytt för att element av denna diskussion skall kunna tas upp.

13.2. Slutsatser

Om existensen av ett globalt avlyssningssystem för privat- och företagskommunikation (Avlyssningssystemet ECHELON)

Det kan inte längre betvivlas att det existerar ett över hela världen arbetande avlyssningssystem som inom ramen för UKUSA-avtalet fungerar genom andelsmässig samverkan mellan USA, De Förenade Kungarikena, Kanada, Australien och Nya Zeeland. Att dess namn faktiskt är ”ECHELON” förefaller på grundval av föreliggande indicier sannolikt men är i alla händelser av underordnad betydelse. Viktigt är att systemet inte är till för avlyssning av militär kommunikation, utan privat kommunikation och företagskommunikation.

Analysen har visat att systemets mäktighet inte på långa vägar är så stor som delar av medierna har antagit.

Om avlyssningssystemets gränser

Övervakningssystemet är baserat på global avlyssning av satellitkommunikation. Inom områden med stor kommunikationstäthet förmedlas emellertid trafiken bara till en mycket ringa del via satelliter. Detta innebär att den övervägande delen av kommunikationen inte kan avlyssnas av markstationer, utan bara genom avtappning av kablar och uppsnappande av radiotrafik. Undersökningarna har emellertid visat att ECHELON-staterna bara kan komma åt en mycket begränsad del av kabel- och radiokommunikationen och dessutom, på grund av det stora personalbehovet, bara kan utvärdera en begränsad del av kommunikationen.

Om den möjliga förekomsten av andra avlyssningssystem

Eftersom avlyssning av kommunikation är en mycket vanlig spionagemetod inom underrättelsetjänsterna skulle ett sådant system också kunna drivas av andra stater i den mån dessa förfogar över motsvarande ekonomiska medel och har de geografiska förutsättningarna. Frankrike skulle – åtminstone vad beträffar de geografiska förutsättningarna, med sina territorier på andra kontinenter – som enda EU-medlemsstat rent av kunna vara i stånd att ensamt upprätta ett globalt avlyssningssystem. Det finns tecken på att även Ryssland skulle kunna driva ett sådant system.

Om förenlighet med EU-rätten

Vad beträffar förenligheten med EU-rätten av ett system av ECHELON-typ måste man skilja mellan olika fall: om systemet enbart används för underrättelseändamål står det inte i motsättning till EU-rätten, eftersom aktiviteter till tjänst för statssäkerheten inte omfattas av EGV, utan det skulle falla under titel V EUV (GASP), där det emellertid för närvarande inte finns några dithörande regleringar och där det följaktligen saknas beröringspunkter. Om systemet däremot missbrukas för konkurrensspionage står det i motsättning till

medlemsstaternas lojalitetsplikt och till begreppet gemensam marknad med fri konkurrens. Om en medlemsstat ägnar sig åt sådan verksamhet bryter den mot EU-rätten.

Om förenlighet med grundlagen om den privata sfären (Art. 8 EMRK)

Varje avlyssning av kommunikation utgör ett djupt ingrepp i den enskildes privata sfär. Art. 8 EMRK, som skyddar den privata sfären, tillåter ingrepp endast för att garantera den nationella säkerheten, såvida regleringarna finns i den inomstatliga rätten, är allmänt tillgängliga och anger under vilka omständigheter och betingelser statsmakten får tillämpas. Ingrepp måste vara proportionerliga, och därför måste en intresseavvägning göras. Att det är rent nyttigt eller önskvärt räcker inte.

Ett underrättelsetjänstsystem som skulle fånga upp kommunikation utan garanti för tillämpning av proportionerlighetsprincipen skulle inte vara förenlig med EMRK. På samma sätt skulle det vara ett brott mot EMRK när den reglering, enligt vilken kommunikationsövervakningen sker, inte har någon rättslig grundval, när den inte är allmänt tillgänglig eller när den är formulerad på ett sådant sätt att dess konsekvenser för den enskilde inte kan förutses. Eftersom de regleringar som gäller för amerikanska underrättelser utomlands till största delen är hemliga, kan garantin för proportionerlighetsprincipen åtminstone ifrågasättas. Det föreligger emellertid en försyndelse mot de av EGMR uppställda principerna om rättens tillgänglighet och om möjligheten att förutse dess verkan. Även om USA inte hör till EMRK:s fördragsstater måste dock medlemsstaterna förhålla sig konformt till EMRK. De kan inte dra sig ur sina EMRK-skyldigheter genom att inom sina territorier, där mindre stränga bestämmelser råder, låta andra staters underrättelsetjänster verka. Annars skulle legalitetsprincipen med sina båda komponenter, tillgängligheten och förutsebarheten, berövas sin verkan, och EGMR skulle bli innehållsmässigt urholkat.

Grundlagskonformiteten av rättsligt legitimerad verksamhet från underrättelsetjänsters sida kräver därtill att det finns kontrollsystem, tillräckliga för att skapa en anpassning till den risk som det hemliga agerandet inom en del av förvaltningsapparaten medför. I betraktande av det faktum, att den europeiska domstolen för mänskliga rättigheter uttryckligen betonade vikten av ett effektivt kontrollsystem för underrättelsetjänstens verksamhet förefaller det betänkligt att vissa medlemsstater inte förfogar över något eget parlamentariskt kontrollorgan för underrättelsetjänster.

Frågan, om EU-medborgare åtnjuter tillräckligt skydd mot underrättelsetjänster

Eftersom skyddet för EU-medborgare beror av rättsläget i de enskilda medlemsstaterna och är gestaltat på mycket olika sätt, där det delvis inte finns några som helst parlamentariska kontrollorgan, kan man knappast tala om ett tillräckligt skydd. De europeiska medborgarna har ett fundamentalt intresse av att deras nationella parlament har ett formellt strukturerat, speciellt kontrollutskott, som övervakar och kontrollerar underrättelsetjänsternas aktiviteter. Men även där det finns kontrollorgan kan dessa känna en stor frestelse att bry sig mera om inlandsunderrättelsetjänster än om utlandsunderrättelsetjänster, eftersom det i regel bara är i det första fallet som de egna medborgarna är berörda.

I händelse av samarbete mellan underrättelsetjänsterna inom ramen för GASP är institutionerna skyldiga att skapa tillräckliga bestämmelser till skydd för de europeiska medborgarna.

Till företagsspionage

I utlandsunderrättelsetjänsternas uppgifter ingår det att intressera sig för företagsdata såsom branschutvecklingar, utveckling av råvarumarknader, upprätthållande av ekonomisk kvarstad, upprätthållande av leveransregler för dual-use-gods etc. På dessa grunder bevakas berörda företag ofta. Situationen blir inte tolerabel om underrättelsetjänster lånar sig till konkurrensspionage i det att de spionerar på utländska företag för att skapa konkurrensfördelar för inhemska sådana. Att de globala avlyssningssystemet sattes in för sådant har visserligen flera gånger påståtts, men det finns inte något belagt fall.

I verkligheten finns känsliga företagsdata framför allt inom företagen själva, varför konkurrensspionage i första hand bedrivs på det sättet, att man försöker få informationer genom medarbetare eller inslussade personer eller genom att göra intrång i datornäten. Endast när känsliga data kommer ut via kabel eller radio (satellit) kan ett kommunikationsövervakningssystem sättas in för konkurrensspionage. Detta görs systematiskt i följande tre fall:

- vid företag som arbetar i tre tidszoner, så att mellanresultaten sänds från Europa till Amerika och vidare till Asien.

- under videokonferenser i multinationella koncerner via V-Sat eller kabel.

- när det förhandlas om viktiga uppdrag på ort och ställe (såsom för anläggningsarbeten, telekommunikationsinfrastruktur, nyetablering av transportsystem etc.), och när man därifrån måste överlägga med företagets huvudkontor.

Till möjligheterna att skydda sig själv

Företag måste säkra hela arbetsområdet såväl som alla kommunikationsvägar på vilka känsliga informationer överförs. Det finns på den europeiska marknaden krypteringssystem som är tillräckligt säkra och betingar överkomliga priser. Även privata måste starkt tillrådas att kryptera e-brev; ett okrypterat e-brev är som ett brev utan kuvert. På Internet finns relativt användarvänliga system, som till och med ställs till privatpersoners förfogande utan kostnad.

Till ett samarbete mellan underrättelsetjänsterna inom EU

EU har förklarat sig vilja samordna informationsinsamling för underrättelseändamål inom ramen för utvecklingen av en egen säkerhets- och försvarspolitik men att därvid också fortsätta samarbetet med andra partner om dessa frågor. Ett samarbete mellan underrättelsetjänsterna inom EU synes så till vida vara önskvärt som å ena sidan en gemensam säkerhetspolitik utan involvering av underrättelsetjänsterna vore förnuftsvidrig och å andra sidan talrika fördelar i yrkesmässigt, finansiellt och politiskt hänseende skulle vara förknippade med ett sådant samarbete. Vidare skulle detta bättre motsvara idén om en likaberättigad partner till USA, och det kunde knyta ihop samtliga medlemsstater i ett system som upprättas i full konformitet med EMRK. En motsvarande kontroll från Europaparlamentets sida måste naturligtvis då säkerställas. Europaparlamentet står i begrepp att ställa upp egna regler för tillgrepp av förtrolig och känslig information och motsvarande dokument.

13.3. Rekommendationer

Om slutande och ändning av internationella fördrag till skydd för medborgare och företag

1. Europarådets generalsekreterare uppmanas att – i ett tilläggsprotokoll eller tillsammans med regleringen av dataskyddet inom ramen för en revidering av dataskyddskonventionen – underställa ministerkommittén en undersökning av huruvida det vore meningsfullt att anpassa det i art. 8 EMRK garanterade skyddet för den privata sfären till de moderna kommunikationsmetoderna och avlyssningsmöjligheterna, detta under förutsättning att det varken skulle medföra någon sänkning av den av domstol utvecklade rättsskyddsnivån eller en minskning av den flexibilitet som är nödvändig för anpassning till framtida utveckling.

2. Medlemsstaterna uppmanas att skapa en europeisk plattform för en överprövning av lagreglerna för bevarande av brev- och telefonhemligheten och att därutöver ena sig om en gemensam text som för alla europeiska medborgare inom medlemsstaternas territorier som helhet säkerställer skyddet för den privata sfären, så som detta skydd är definierat i art. 7 av den europeiska författningsurkunden om de grundläggande rättigheterna, och därutöver garantera att underrättelsetjänsternas verksamhet är konform med grundlagen och följaktligen svarar mot betingelserna enligt kapitel 8 i denna rapport, och speciellt 8.3.4, vilka är härledda ur art. 8 EMRK.

3. Europarådets medlemsstater uppfordras att besluta om ett tilläggsprotokoll, som gör det möjligt för de europeiska gemenskaperna att biträda EMRK eller tänka igenom andra åtgärder som utesluter konflikter i rättskipningen mellan domstolarna i Strassburg och Luxemburg.

4. FN:s generalsekreterare anmodas att uppdraga åt det ansvariga utskottet att framlägga förslag som syftar till en anpassning av art. 17 i den internationella pakten om medborgerliga och politiska rättigheter, vilken gäller skyddet för den privata sfären, till de tekniska förändringarna.

5. USA uppfordras att underteckna tilläggsprotokollet rörande den internationella pakten om medborgerliga och politiska rättigheter, så att det blir lagligt att inför det konventionella människorättsutskottet anföra individuella besvär mot USA för överträdelse; de ifrågavarande amerikanska NGO:erna, speciellt ACLU (American Civil Liberties Union) och EPIC (Electronic Privacy Information Center), ombeds att utöva ett motsvarande tryck på den amerikanska regeringen.

Om nationella lagstiftningsåtgärder till skydd för medborgare och företag

6. Till alla medlemsstater riktas en appell om att överpröva sin egen lagstiftning om underrättelsetjänsters verksamhet med hänsyn till konformiteten med grundlagen.
7. Medlemsstaterna uppfordras att för skyddet mot underrättelsetjänstaktiviteter eftersträva en gemensam nivå som är orienterad mot det starkaste medlemsstatsskyddet, då de medborgare som berörs av en utlandsunderrättelsetjänst i regel hör till andra staters och därför även de övriga medlemsstaternas medborgare.

8. EU-institutionerna uppmanas att i fråga om samarbete mellan underrättelsetjänsterna inom ramen för GASP antaga tillräckliga skyddsbestämmelser till förmån för de europeiska medborgarna. Europaparlamentet måste å sin sida som logiskt kontrollorgan skapa de förutsättningar som övervakningen av detta höggradigt känsliga område kräver, så att det blir realistiskt, men också ansvarsfullt, att infordra de erforderliga kontrollrättigheterna.

Om speciella rättsliga åtgärder för bekämpande av företagsspionage

9. Medlemsstaterna uppfordras att föra överläggningar om i vilken mån företagsspionage och bestickning för förvärvande av uppdrag kan bekämpas genom regleringar i den europeiska och internationella rätten och speciellt om en reglering inom ramen för WTO skulle vara möjlig, en reglering som tar hänsyn till den snedvridning av konkurrensen som ett sådant handlande medför, t.ex. genom att fastslå att sådana överenskommelser är ogiltiga.

10. Medlemsstaterna uppfordras att i en gemensam, entydig förklaring förplikta sig själva att avstå från att bedriva företagsspionage mot varandra och att de därmed signalerar sin samklang med EG-fördragets anda och bestämmelser.

Om åtgärder inom rättstillämpningen och kontrollen över denna

11. Till de nationella parlament, som inte förfogar över egna parlamentariska kontrollorgan för övervakning av underrättelsetjänsterna, riktas en appell om inrättande av sådana organ.

12. De nationella kontrollkommittéerna för underrättelsetjänsterna anmodas att vid utövandet av de kontrollbefogenheter som har anförtrotts åt dem tillmäta skyddet för privatsfären stor vikt, oberoende av om det gäller övervakning av egna medborgare, medborgare i andra medlemsländer eller medborgare i tredje stat.

13. Medlemsstaternas underrättelsetjänster uppfordras att inte ta emot data från andra underrättelsetjänster annat än där dessa kunde fås fram under sådana förutsättningar som den egna nationella rätten förutser, då medlemsstaterna inte kan komma ifrån sina från EMRK härrörande förpliktelser genom att koppla in andra underrättelsetjänster.

14. Till Tyskland och USA riktas en appell om att de inom sina områden skall låta ytterligare tillstånd till kommunikationsavlyssnande, genomfört av USA, bli beroende av att denna verksamhet står i samklang med EMRK, d.v.s. att det följer principen om proportionerlighet, håller rättsgrundvalen tillgänglig, gör effekten för den enskilde förutsebar och bedriver en motsvarande effektiv kontroll, då de är ansvariga för att accepterad eller åtminstone tolererad underrättelseverksamhet inom deras territorier är konform med de mänskliga rättigheterna.

Om åtgärder för befordrande av medborgares och företags självskydd

15. Kommissionen och medlemsstaterna uppfordras att utveckla program som befrämjar medborgarnas och företagens medvetenhet om säkerhetsproblematiken och samtidigt erbjuder praktisk hjälp med planering och förverkligande av omfattande skyddskoncept.

16. Kommissionen och medlemsstaterna anmodas att vidta lämpliga åtgärder för främjande, utveckling och framställning av europeisk krypteringsteknik och

programvara samt framför allt understödja projekt som syftar till utveckling av användarvänlig krypteringsprogramvara vars källtext framläggs öppet.

17. Kommissionen och medlemsstaterna uppfordras att befrämja programvaruprojekt vilkas källtext läggs öppen, eftersom detta är det enda sättet att garantera att det inte finns några ”bakdörrar” inbyggda (s.k. open source software).

18. En vädjan riktas till de europeiska institutionerna och medlemsstaternas offentliga förvaltningar om att systematiskt sätta in kryptering av e-post för att därigenom på lång sikt göra kryptering till normalfallet.

Om andra åtgärder

19. Till företagen riktas en vädjan om att samarbeta starkare med organen för avvärjande av spionage och informera dessa framför allt om angrepp utifrån för företagsspionage för att på detta sätt höja dessa organs effektivitet.

20. Kommissionen uppfordras att framlägga ett förslag om inrättande av en europeisk rådgivningsorganisation för frågor om företagens informationssäkerhet, en organisation vars arbetsuppgifter innefattar – förutom en förstärkning av problemmedvetenheten – praktisk, sakkunnig observation och sakligt stöd.

21. Europaparlamentet uppfordras att organisera en övereuropeisk kongress för skydd åt den privata sfären mot telekommunikationsövervakning, detta för att ge NGO:er från Europa, USA och andra stater en plattform där gränsöverskridande och internationella aspekter kan diskuteras och där verksamhetsfält och tillvägagångssätt kan samordnas.