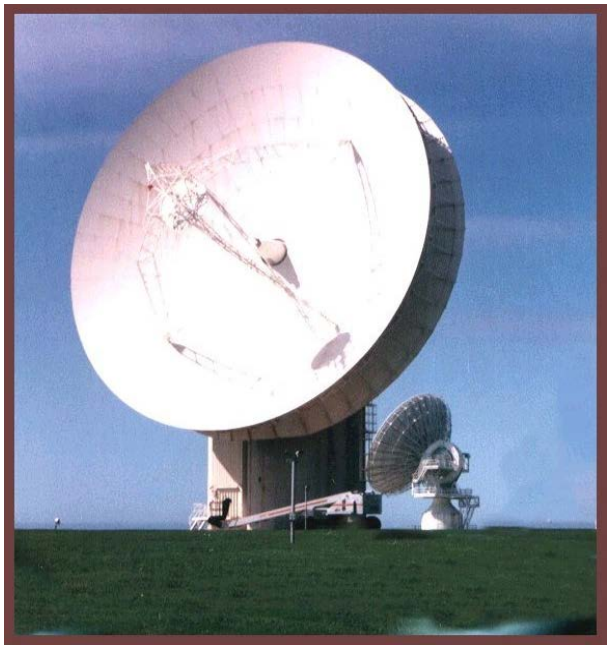
Tirsdag 16. november 1999

Interception Capabilities 2000

Aflytnings muligheder 2000



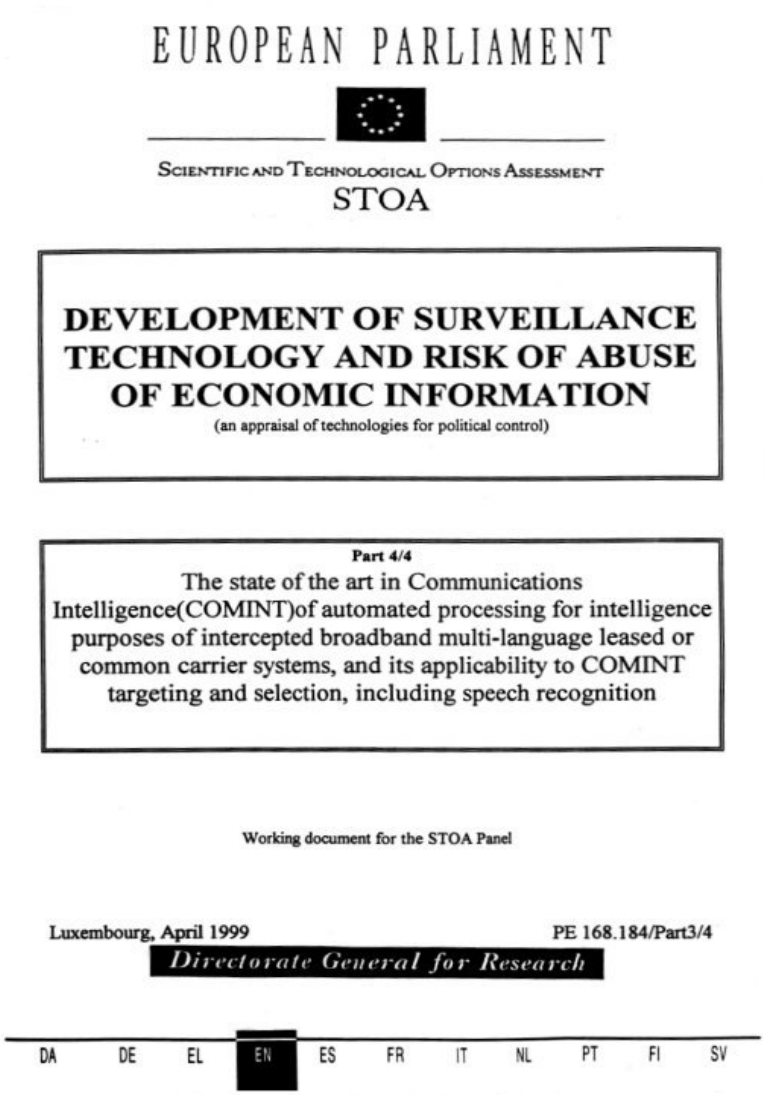
Rapport til Europa-Parlamentets Generaldirektør for Forskning
("Scientific and Technical Options Assessment" (STOA) programkontor)
om overvågningsteknologiens udvikling og risikoen for misbrug af økonomisk information.

Denne undersøgelse ser på teknikkens stade i kommunikationsefterretninger (Comint) i forbindelse med den
automatiserede behandling i efterretningsøjemed af aflyttede faste eller fælles bredbåndsforbindelser på flere sprog
og dens anvendelse på indhentning og valg af Comint, herunder også talegenkendelse.

Rapport ved : Duncan Campbell, IPTV Ltd
Edinburgh, Skotland : April, 1999

Mailto:iptv@cwcom.net

Illustration : 30 meter antenne på Composite Signals Organisation Station i Morwenstow, England,
der opsnapper kommunikation fra regionale satellitter over Atlanterhavet og det Indiske Ocean. (D Campbell)



Indhold

Kolofon

Kolofon:

Titel: **OVERVÅGNINGSTEKNOLOGIENS UDVIKLING OG RISIKOEN FOR MISBRUG AF ØKONOMISK INFORMATION**
(En vurdering af teknologier til politisk kontrol)

Del 4/4: Teknikkens stade i kommunikationsefterretninger (COMINT) i forbindelse med den automatiserede behandling i efterretningsøjemed af aflyttede faste eller fælles bredbåndsforbindelsessystemer på flere sprog og dens anvendelse på indhentning og valg af COMINT, herunder også talegenkendelse.

Udgiver: Europa-Parlamentet
Generaldirektøren for Forskning
Direktorat A
STOA-programmet

Forfatter: Duncan Campbell - IPTV Ltd - Edinburgh

Redaktør: Dick Holdsworth
Chef for STOA-enheden

Dato: April 1999

PE-nummer: PE 168.184 / Part 4/4

Oversættelse: Den danske oversættelse af rapporten, som den fremgår her, er sket på foranledning af Forskningsministeriet, som påtager sig det fulde ansvar for oversættelsens rigtighed og autencitet.

Dette dokument afspejler ikke nødvendigvis Europa-Parlamentets synspunkter

---

Yderligere information eller andre rapporter om samme emne kan fås hos Europa- Parlamentet, Luxembourg http://www.europarl.eu.int/dg4/stoa/en/ Forfatterens hjemmeside er http://www.gn.apc.org/duncan Ved oplysning af links til andre, bedes du linke til denne side

Sammendrag

1. **Kommunikationsefterretninger** (Comint), der omfatter skjult aflytning af udenlandsk kommunikation, har været praktiseret af næsten ethvert udviklet land, siden den internationale telekommunikation startede. Comint er en industriel aktivitet i stor målestok, som giver aftagerne efterretninger om diplomatiske, økonomiske og

videnskabelige udviklinger. Man kan med fordel betragte Comint-aktivitetens muligheder og begrænsninger inden for rammerne af "efterretningscyklussen" (afsnit 1).

2. Globalt bruges der ca. 15-20 mia. Euro om året på Comint og dermed beslægtede aktiviteter. Størstedelen heraf betales af de store engelsktalende lande i UKUSA-alliancen. **(1)** Denne rapport beskriver, hvordan Comint-organisationer i mere end 80 år har truffet foranstaltninger for at få adgang til en stor del af verdens internationale kommunikation. Dette omfatter ubemyndiget aflytning af kommercielle satellitter, af fjernkommunikation via rummet, af undersøiske kabler ved hjælp af ubåde samt af Internettet. Der er i øjeblikket mere end 120 satellitsystemer, der samtidig arbejder med at indsamle efterretninger (afsnit 2).

3. Det højt automatiserede UKUSA-system til behandling af Comint, der ofte kaldes ECHELON, er blevet drøftet meget i Europa efter STOA-rapporten i 1997. **(2)** Denne rapport opsummerede information fra de eneste to primære kilder, der dengang fandtes om ECHELON. **(3)** I denne rapport fremlægges original ny dokumentation om og andre beviser på ECHELON-systemet og dets inddragelse i aflytningen af kommunikationssatellitter (afsnit 3). I det tekniske tillæg findes en supplerende, detaljeret beskrivelse af Comint-behandlingsmetoderne.

4. Man har allerede længe rutinemæssigt anvendt Comint-information fra aflytning af international kommunikation til at indhente følsomme data om enkeltpersoner, regeringer, erhvervsorganisationer samt internationale organisationer. Denne rapport beskriver de organisatoriske og rapporteringsmæssige rammer, som de økonomiske følsomme oplysninger indsamles og spredes efter, og opstiller kortfattede eksempler på europæiske erhvervsorganisationer, der har været genstand for overvågning (afsnit 4).

5. Denne rapport identificerer en hidtil ukendt international organisation - "ILETS" - der uden parlamentariske drøftelser eller offentlighedens kendskab har indført omtvistede planer, der kræver, at producenter og operatører af nye kommunikationssystemer skal indbygge en overvågningskapacitet, som nationale sikkerheds- eller politiorganisationer kan bruge (afsnit 5).

6. Comint-organisationer indser nu, at der er stadig flere tekniske vanskeligheder ved at indsamle kommunikation, og at den fremtidige produktion kan være dyrere og mere begrænset, end den er i øjeblikket. Erkendelsen af sådanne vanskeligheder kan vise sig at være et nyttigt grundlag for politiske valg, der er rettet mod sikrende retsmidler vedrørende økonomiske oplysninger og effektiv kryptering (afsnit 6).

7. Blandt de **vigtigste oplysninger** om Comints tekniske stade kan nævnes:

- o Der findes omfattende systemer, som anvendes til at opnå adgang til, aflytte og behandle enhver betydende moderne kommunikationsform, med kun få undtagelser (afsnit 2, teknisk tillæg);

- o I modsætning til hvad pressen skriver, findes der endnu ikke effektive systemer, der kan genkende ord for derefter automatisk at udvælge telefonopkald af efterretningsinteresse på trods af 30 års forskning. Men der er udviklet systemer, der genkender stemmer - "stemmeaftryk", og som anvendes til at genkende bestemte personers stemmer, når de foretager internationale telefonopkald;

- o Den amerikanske regerings nylige diplomatiske initiativer, der søgte om europæisk tilslutning til "key escrow"-systemet til opsamling af krypeterede efterretninger, indgik i et langsigtet program, der har undermineret og fortsat underminerer den fortrolige kommunikation, der føres af ikke-amerikanske statsborgere, herunder også europæiske regeringer, virksomheder og borgere;

- o Der er vidtspændende beviser for, at større regeringer rutinemæssigt anvender kommunikationsefterretninger til at give virksomheder og industri en kommerciel fordel.

1. Organisationer og metoder

Hvad er kommunikationsefterretninger?

1. Kommunikationsefterretninger (Comint) defineres af NSA, det største bureau, der varetager sådanne operationer, som "tekniske og efterretningsmæssige oplysninger opsnappet fra udenlandsk kommunikation af andre end den påtænkte modtager". (4) Comint er en betydelig bestanddel af Sigint (signalefterretninger), der også omfatter opsamling af ikke-kommunikationssignaler, såsom radarstråler. (5) Selvom denne rapport omhandler

bureauer og systemer, hvis overordnede opgave kan være Sigint, tager den kun sigte mod Comint.

2. Comint har skygget udviklingen af omfattende højtydende nye civile telekommunikationssystemer og er derfor blevet en stor industriel aktivitet, der beskæftiger mange faglærte medarbejdere og anvender en exceptionel høj grad af automatisering.

3. Comint-operationerne har forskellige mål. De mest traditionelle Comint-mål er militære meddelelser og diplomatkommunikation mellem forskellige landes hovedstæder og deres repræsentationer i udlandet. Siden væksten i verdenshandelen i 1960'erne har opsamlingen af økonomiske efterretninger og information om videnskabelige og tekniske udviklinger været et stadig vigtigere aspekt for Comint. Blandt de nyere mål kan nævnes narkosmugleri, hvidvask af penge, terrorisme og organiseret kriminalitet.

4. Når der opnås adgang til internationale kommunikationskanaler med ét formål for øje, opnås der automatisk også adgang til enhver anden type kommunikation på samme kanaler, kun afhængig af hvilke opgaver, bureauerne får. Således blev Comint, der primært var opsamlet til andre formål, anvendt af den amerikanske sikkerhedstjeneste NSA og dens britiske modstykke GCHQ i årene 1967-1975 til at få oplysninger om personer fra den indenlandske politiske opposition i USA.

UKUSA-alliancen

5. USAs Sigint System (USSS) omfatter den amerikanske sikkerhedstjeneste, National Security Agency (NSA), militære støtteenheder, der under ét kaldes den centrale sikkerhedstjeneste, samt dele af efterretningstjenesten CIA og andre organisationer. Efter samarbejdet under krigen indgik Storbritannien og USA i 1947 en hemmelig aftale om fortsat at udføre verdensomspændende Comint-aktiviteter i fællesskab. Tre andre engelsktalende lande, Canada, Australien og New Zealand, sluttede sig til UKUSA-aftalen som "Sekundære parter". UKUSA-aftalen blev ikke offentligt vedkendt før i marts måned 1999, da den australske regering bekræftede, at dens Sigint-organisation, Defence Signals Directorate (DSD), "samarbejder med tilsvarende signalefterretningsorganisationer i udlandet i medfør af UKUSA-forholdet ". (6) UKUSA-aftalen fordeler anlæg, opgaver og produkter mellem de deltagende regeringer.

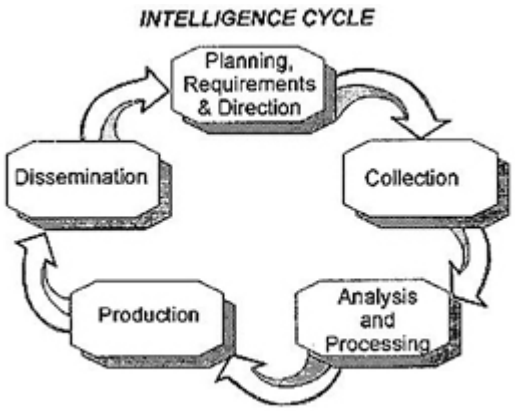
6. Selvom UKUSA-aftalens Comint-bureauers personale og budgetter er blevet mindre efter afslutningen på den kolde krig, har de igen bekræftet deres behov for adgang til hele verdens kommunikation. I en tale til NSAs stab ved sin aftræden i 1992 beskrev den daværende direktør for NSA, admiral William Studeman, hvordan "behovet for øget global adgang vokser". Han sagde, at den "globale adgangs" "forretningsgren" var et af "to forhåbentligt stærke ben, som NSA skal stå på" i det næste århundrede. (7)

Andre Comint-organisationer

7. Ud over Storbritannien og USA driver mindst 30 andre lande betydelige Comint-organisationer. Den største er den russiske FAPSI med 54.000 ansatte **.** (8) Kina opretholder et betydeligt Sigint-system, hvoraf to stationer er rettet mod Rusland og arbejder i samarbejde med USA: De fleste lande i Mellemøsten og Asien har foretaget store investeringer i Sigint, i særdeleshed Israel, Indien og Pakistan.

Sådan fungerer efterretninger

8. I tiden efter den kolde krig har Comint-opsamlingen været begrænset af genkendelige erhvervsargumenter, deriblandt kravet om at passe budgetter og evner til kundernes krav. Den flerledede proces, der anvendes til at søge, opsamle, behandle og videregive kommunikationsefterretninger er ens for alle lande og beskrives ofte som "efterretningscyklussen". Trinene i efterretningscyklussen svarer til de særlige organisatoriske og tekniske dele af Comint-produktionen. Derfor er administrationen af NSAs største jordstation i verden, der er beliggende i Menwith Hill i England og har ansvaret for at afvikle mere end 250 hemmeligstemplede projekter, opdelt i tre direktorater: OP (Operationer og planer), CP (Opsamling og behandling) samt EP (Udnyttelse og produktion) **.**



Planlægning

9. I forbindelse med planlægningen skal man først afgøre kundens behov. Kunderne omfatter de førende ministerier hos de regeringer, som betaler - navnlig dem, der beskæftiger sig med forsvar, udenrigsanliggender, sikkerhed, handel og indenlandske anliggender. Den overordnede administration af Comint omfatter identifikation af databehov samt oversættelse af behovene til potentielt opnåelige opgaver, prioritering, organisation af analyse og rapportering samt overvågningen af Comint-produktets kvalitet.

10. Når først målene er valgt, kan bestemte eksisterende eller nye opsamlingsmuligheder specificeres ud fra den type information, der skal bruges, målaktivitetens påvirkelighed over for opsamling samt den sandsynlige effektivitet af opsamlingen.

Adgang og opsamling

11. Den første væsentlige handling for Comint er at få adgang til det ønskede kommunikationsmedium, så kommunikationen kan aflyttes. Historisk set har dette været en enkel opgave i forbindelse med langbølgeradio. En række betydende moderne kommunikationssystemer er ikke "Comint-venlige" og kan fordre, at der tages usædvanlige, kostbare eller fysiske metoder i brug for at få adgang til dem. De fysiske kommunikationsmidler er normalt uafhængige af den overførte type information. For eksempel vil indenbys radiosystemer i mikrobølgeområdet, internationale satellitforbindelser og undersøiske lyslederkabler alle normalt overføre en blandet trafik af tv, telefon, fax, dataforbindelser, privat tale, video og data.

12. Opsamling følger efter aflytning, men er en særskilt aktivitet, idet mange signaltyper kan opsnappes, men ikke vil blive behandlet yderligere, måske bortset fra tekniske søgninger for at bekræfte, at kommunikationsmønsteret ikke ændrer sig. For eksempel vil en satellitaflytningsstation, som har fået til opgave at undersøge en netop opsendt kommunikationssatellit, sætte en antenne op til at opsnappe alt, hvad satellitten sender til jorden. Når først en undersøgelse har fastslået, hvilke dele af satellittens signaler der overfører fx tv eller kommunikation, der ikke har nogen interesse, vil disse signaler ikke blive behandlet yderligere i systemet.

13. Opsamling omfatter såvel indhentning af information via aflytning som overførsel af interessant information mhp. behandling og produktion. Som følge af den høje informationshastighed, der anvendes i mange moderne netværk, og kompleksiteten af signaler i dem, er det nu almindeligt, at højhastighedsoptagere eller "snapshot"-hukommelser midlertidigt rummer store mængder data, mens behandlingen finder sted. Moderne opsamlingsaktiviteter anvender sikre og hurtige kommunikationsforbindelser til at sende data via globale netværk til analytikere, som kan opholde sig på et andet kontinent. Udvælgelse af meddelelser til opsamling og behandling sker i de fleste tilfælde automatisk ved anvendelse af store on-line databanker med information om interessante mål.

Behandling

14. Under behandlingen konverteres de opsamlede informationer til en form, der egner sig til analyse eller produktion af efterretninger, enten automatisk eller under opsyn af en person. Indkommende kommunikation konverteres normalt til standardformater, der identificerer dens tekniske karakteristika sammen med information om meddelelsen (eller signalet) (fx telefonnumrene på deltagerne i en telefonsamtale).

15. Hvert opsnappet signal og hver opsnappet kanal vil på et tidligt tidspunkt, hvis det ikke ligger i udvælgelsen af meddelelsen eller samtalen, blive beskrevet med almindelige "kendingsbogstaver". Kendingsbogstaverne identificerer først de lande, hvis kommunikation er blevet opsnappet - normalt bruges der to bogstaver. Et tredje bogstav betegner den generelle kommunikationskategori: C for aflytninger af kommercielle linier, D for diplomatiske meddelelser, P for politikanaler osv. Et fjerde bogstav betegner kommunikationssystemets type (fx S for multikanal). Derefter betegner tal særlige forbindelser eller netværk. Således opsnappede og behandlede NSA i 1980'erne trafik med betegnelsen "FRD" (fransk diplomati) fra Chicksands i England, medens det britiske Comint-bureau GCHQ decifrerede "ITD" (italienske diplomatiske) budskaber på sit hovedkvarter i Cheltenham. (9)

16. Behandlingen kan også omfatte oversættelse eller "sammendrag" (udskiftning af en ordret tekst med kommunikationens mening eller hovedpunkter). Oversættelse og sammendrag kan i en vis udstrækning automatiseres.

Produktion og udbredelse

17. Comint-produktion omfatter analyse, evaluering, oversættelse og tolkning af rå data til færdige efterretninger. Det sidste trin i efterretningscyklussen er udbredelse, dvs. videregivelse af rapporter til efterretningskunderne. Sådanne rapporter kan bestå af rå (med dekrypterede og/eller oversatte) meddelelser, sammendrag, kommentarer eller omfattende analyser. Kvaliteten og relevansen af de udbredte rapporter fører på sin side til en ny specifikation af prioriteringen af efterretningsopsamling, hvorved efterretningscyklussen afsluttes.

18. Arten af udbredelse er særdeles vigtig for spørgsmål om, hvordan Comint udnyttes til at få økonomiske fordele. Comint-aktiviteter er hemmeligstemplede overalt, fordi man hævder, at viden om vellykket aflytning sandsynligvis kan få målene til at ændre deres kommunikationsmetoder for at forhindre aflytning fremover. I UKUSA-systemet er udbredelsen af Comint-rapporter begrænset til enkeltpersoner med en høj "SCI-"sikkerhedsgodkendelse. (10) Eftersom som kun sikkerhedsgodkendt personale må se Comint-rapporter, er de desuden de eneste, som kan fastsætte krav og dermed styre tildelingen af opgaver. Personale i erhvervsvirksomheder har normalt hverken sikkerhedsgodkendelse eller rutinemæssig adgang til Comint og kan derfor kun få gavn af erhvervsmæssig relevant Comint-information i det omfang, at ledende, sikkerhedsgodkendte regeringsembedsmænd tillader det. De måder, dette sker på, er beskrevet i afsnit 5.

19. Udbredelsen er desuden begrænset i UKUSA-organisationen af nationale og internationale regler, der generelt foreskriver, at hvert lands Sigint-bureauer normalt ikke må opsamle eller (hvis den uforvarende opsamles) registrere eller udbrede information om borgere i eller virksomheder registreret i noget andet UKUSA-land. Borgere og virksomheder kaldes under ét for "juridiske personer". Den modsatte procedure følges, hvis den pågældende person har været mål for dennes nationale Comint-organisation.

20. Hager (11) har fx beskrevet, hvordan embedsmænd i New Zealand blev bedt om at fjerne navnene på identificerbare UKUSA-borgere eller -virksomheder fra deres rapporter og i stedet indsætte ord som "en canadisk borger" eller "en amerikansk virksomhed". Britisk Comint-personale har beskrevet at have fulgt lignede procedurer for amerikanske borgere efter indførelsen i 1978 af lovgivning, der begrænser NSAs indenlandske efterretningsaktiviteter. (12) Den australske regering siger, at "DSD og dets modstykker benytter interne procedurer til at forvisse sig om, at deres nationale interesser og politik respekteres af de andre... reglerne [om Sigint og australiere] forbyder udbredelse af information om australiere, der er fremskaffet ved et tilfælde under en rutinemæssig opsamling af udenlandsk kommunikation, eller rapportering eller registrering af navnene på australiere, som nævnes i udenlandsk kommunikation". (13) Følgeslutningen er også sand; UKUSA-lande har ingen begrænsninger på indsamling af efterretninger, der enten vedrører borgere eller virksomheder i noget andet land, herunder lande i EU (med undtagelse af Storbritannien).

2. Aflytning af international kommunikation

Kommunikation via internationale faste operatører

21. Det er dokumenteret, at udenlandsk kommunikation til og fra eller gennem Storbritannien og USA er blevet aflyttet i mere end 80 år. (14) De fleste internationale kommunikationslinier blev dengang som nu drevet af internationale teleselskaber, normalt enkeltstående nationale teleselskaber eller private virksomheder. I begge

tilfælde udlejes kapacitet på kommunikationssystemet til enkeltstående nationale eller internationale teleselskaber. Derfor anvender Comint-organisationer udtrykket ILC (International Leased Carrier - international fast operatør) til at beskrive denne form for opsamling.

Højfrekvent radio

22. Med undtagelse af direkte linier over land mellem geografisk tilgrænsende lande var højfrekvente (HF) radiosystemer den mest almindelige form for international telekommunikation før 1960, og de blev anvendt til internationale faste operatører, diplomatiske og militære formål. Et vigtigt kendetegn ved HF radiosignaler er, at de reflekteres fra ionosfæren og fra jordens overflade samt giver rækkevidder på tusindvis af kilometer. Dette muliggør såvel modtagelse som aflytning.

Mikrobølge

23. Mikrobølge blev introduceret i 1950'erne for at tilvejebringe effektiv indenbys kommunikation til telefoni, telegrafi og senere også tv. Mikrobølge-radiokommunikation anvender transmittere med ringe effekt og parabolantenner, der anbringes på højt placerede tårne, fx på bakketoppe eller høje bygninger. Antennerne måler normalt 1-3 m i diameter. På grund af jordens krumning skal der normalt være relæstationer for hver 30-50 km.

Undersøiske kabler

24. Undersøiske telefonkabler tilvejebragte de første større, pålidelige højtydende kommunikationssystemer. De tidlige systemer var begrænset til nogle få hundrede samtidige telefonkanaler. De mest moderne lysledersystemer kan overføre op til 5 Gbps (Gigabit pr. sekund) digital information. Dette svarer nogenlunde til ca. 60.000 samtidige telefonkanaler.

Kommunikationssatellitter

25. Mikrobølgesignaler reflekteres ikke fra ionosfæren og går direkte ud i rummet. Denne egenskab har man udnyttet til at tilvejebringe såvel global kommunikation som omvendt aflytte denne kommunikation i rummet og på jorden. Den største konstellation af kommunikationssatellitter (COMSAT) drives af International Telecommunications Satellite Organisation (Intelsat), en international traktatorganisation. Kommunikationssatellitter anbringes i såkaldte "geostationære" baner, således at de for iagttageren på jorden synes at holde samme position på himlen, så de kan tilvejebringe permanent kommunikation fra punkt til punkt eller til transmissioner.

26. De første geostationære Intelsat-satellitter blev sat i omløb i 1967. Satellitteknologien udviklede sig hurtigt. Den fjerde generation Intelsat-satellitter, der blev introduceret i 1971, havde kapacitet til 4.000 samtidige telefonkanaler og kunne håndtere alle former for kommunikation samtidig - telefon, telex, telegrafi, tv, data og fax. I 1999 drev Intelsat 19 satellitter af 5. til 8. generation. Den nyeste generation kan håndtere, hvad der svarer til 90.000 samtidige opkald.

Kommunikationsteknik

27. Før 1970 anvendte de fleste kommunikationssystemer (uanset transmissionsmåde) analog eller kontinuert bølgeteknik. Siden 1990 har næsten al kommunikation været digital og giver stadig højere kapacitet. Systemerne med den højeste kapacitet, der generelt anvendes til Internet, STM-1 eller OC-3, arbejder ved en datahastighed på 155 Mbs. (Million bits pr. sekund; en hastighed på 155 Mbps svarer til at sende 3 millioner ord hvert sekund, nogenlunde teksten i 1.000 bøger i minuttet.) Man anvender fx forbindelser med denne kapacitet som backboneforbindelser i Internettet mellem Europa og USA. Det tekniske tillæg indeholder yderligere oplysninger om kommunikationsteknik.

Opsamling af kommunikation via internationale faste operatører

Adgang

28. Comint-opsamling kan ikke finde sted, medmindre opsamlingsbureauet får adgang til de kommunikationskanaler, de ønsker at undersøge. Information om de metoder, der anvendes til at få adgang er ligesom data om brydning af koder de mest beskyttede informationer i en hvilken som helst Comint-organisation. Adgang fås både med og uden netværksoperatørernes deltagelse eller samarbejde.

Operation SHAMROCK

29. Fra og med 1945 modtog NSA og dets forgængere i USA systematisk kabeltrafik fra de større kabelselskabers kontorer. Denne aktivitet gik under kodenavnet SHAMROCK (trekløver). Disse aktiviteter forblev ukendte i 30 år, indtil undersøgelser blev tilskyndet af Watergate-sagen. Den 8. august 1975 indrømmede direktøren for NSA, generalløjtnant Lew Allen, over for Pike-komitéen, der var nedsat af Repræsentanternes Hus, at:

> *"NSA systematisk aflytter international kommunikation, såvel tale som kabel".*

30. Han indrømmede også, at "meddelelser til og fra amerikanske borgere er blevet opfanget i forbindelse med indsamling af udenlandske efterretninger". Lovgiverne i USA mente, at sådanne operationer kan have været forfatningsstridige. I 1976 undersøgte et hold fra det amerikanske justitsministerium mulige strafbare forhold, begået af NSA. En del af deres rapport blev offentliggjort i 1980. Den beskrev, hvordan efterretninger om amerikanske statsborgere:

> *"blev opsnappet tilfældigt i forbindelse med NSAs aflytning af international auditiv- og ikke-auditiv (fx telex) kommunikation og modtagelsen af GCHQ-opfanget telextrafik og trafik på internationale faste operatører (SHAMROCK) " (fremhævning i original). (15)*

High frequency radio interception antenna (AN/FLR9)

DODJOCC sign at NSA station, Chicksands

Aflytning af højfrekvent radio

31. Højfrekvente radiosignaler er forholdsvis nemme at aflytte, idet de kun kræver et egnet areal i ideelt set "uforstyrrede" radioomgivelser. Fra 1945 indtil begyndelsen af 1980'erne drev såvel NSA som GCHQ HF radioaflytningssystemer, der havde til opgave at opsamle europæisk kommunikation på internationale faste operatører i Skotland. (16)

32. Den mest avancerede type HF-overvågningssystem, der blev benyttet i denne periode til Comint-formål, var en stor rund antennestruktur, også kendt som AN/FLR-9. AN/FLR-9 antenner er mere end 400 meter i diameter. De kan samtidig aflytte og bestemme pejlingen af signaler fra lige så mange retninger og på lige så mange frekvenser, som man måtte ønske sig. I 1964 blev der installeret AN/FLR-9 modtagesystemer i San Vito dei Normanni, Italien, i Chicksands, England og i Karamursel, Tyrkiet.

33. I august 1966 overførte NSA opsamlingsaktiviteterne på de internationale faste operatører fra sin skotske station i Kirknewton til Menwith Hill i England. 10 år senere blev denne aktivitet flyttet igen, denne gang til

Chicksands. Selvom Chicksands-stationens primære funktion var at aflytte kommunikation mellem det sovjetiske og warzawapagtlandenes flyvevåben, fik den også til opgave at opsamle kommunikation via internationale faste operatører og "NDC" (ikke-amerikansk diplomatkommunikation). En af de fremtrædende af disse opgaver var opsamling af FRD-trafik (dvs. fransk diplomatkommunikation). Selvom det meste personale i Chicksands indgik i det amerikanske flyvevåben, blev diplomataflytningen og aflytningen af de internationale faste operatører varetaget af civile NSA-medarbejdere i en enhed ved navn DODJOCC. (17)

34. I 1970'erne blev britiske Comint-enheder i Cypern bedt om at opsamle HF-kommunikation fra allierede NATO-lande, deriblandt også Grækenland og Tyrkiet. Aflytningen fandt sted i en britisk hærenhed i Ayios Nikolaos i det østlige Cypern. (18) I USA i 1975 afslørede en amerikansk kongreskomités undersøgelser, at NSA opsamlede diplomatmeddelelser, der blev sendt til og fra Washington fra en militær Comint-station i Vint Hill Farms, Virginia. Blandt denne stations mål var også Storbritannien. (19)

Rumaflytning af indenbys netværk

35. Udenbys mikrobølge-linier kan fordre dusinvis af mellemstationer til at modtage og videresende kommunikation. Hver efterfølgende modtagestation opsnapper kun en lille del af det oprindeligt afsendte signal - resten passerer over horisonten og ud i rummet, hvor satellitter kan opfange det. Disse principper blev udnyttet i 1960'erne til Comint-opsamling i rummet. Arten af "mikrobølgespildet" betyder, at den bedste position for disse satellitter ikke er over det valgte mål, men i en afstand af op til 80 graders længde.

36. Den første amerikanske Comint-satellit, CANYON, blev opsendt i august 1968 og efterfulgtes snart af nr. 2. Satellitterne blev styret fra en jordstation i Bad Aibling i Tyskland. For at sikre permanent dækning af de valgte mål blev der anbragt CANYON-satellitter tæt på de geostationære kredsløb. Men disse kredsløb var ikke præcise, og satellitterne skiftede dermed position og fik flere data om jordmål. (20) Der blev opsendt 7 CANYON-satellitter mellem 1968 og 1977.

37. CANYONs mål var Sovjetunionen. Større sovjetiske kommunikationsforbindelser strakte sig over tusindvis af kilometer, mange af dem på tværs af Sibirien, hvor permafrosten begrænsede den pålidelige anvendelse af underjordiske kabler. De geografiske forhold var således til fordel for NSA, idet de gjorde de interne sovjetiske kommunikationsforbindelser meget let tilgængelige. Satellitterne gav mere, end man havde forventet, og derfor blev projektet udvidet.

38. CANYONs succes førte til udformning og opsendelse af en ny klasse Comint-satellitter, CHALET. Som jordstation for CHALET-serien valgte man Menwith Hill i England. Under NSA-projekt P-285 blev amerikanske firmaer hyret til at installere og bistå med driften af satellitkontrolsystem og satellit-til-jord-forbindelsen (RUNWAY) samt behandlingssystemet på jorden (SILKWORTH). De første to CHALET-satellitter blev opsendt i juni 1978 og oktober 1979. Efter at navnet på den første satellit blev nævnt i den amerikanske presse, blev de døbt om til VORTEX. I 1982 fik NSA godkendelse til udvidede "nye missionsbehov" og fik tildelt midler og faciliteter til at drive 4 VORTEX-satellitter samtidig. Et nyt operationscenter på 5.000 m^2 (STEEPLEBUSH) blev bygget til at huse behandlingsudstyret. Da navnet VORTEX blev offentliggjort i 1987, blev satellitterne døbt om til MERCURY. (21)

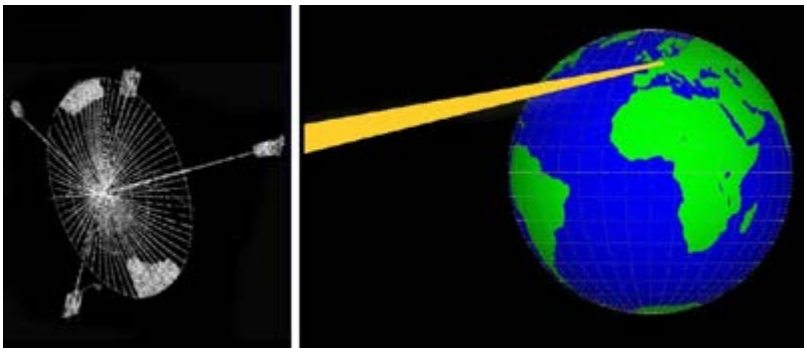
39. Den udvidede mission, som Menwith Hill fik efter 1985, omfattede MERCURY-opsamling fra Mellemøsten. Stationen fik en pris for dens støtte til de amerikanske flådeoperationer i den Persiske Golf fra 1987 til 1988. I 1991 fik den yderligere en pris for dens støtte til krigsoperationerne mod Irak, Desert Storm (Ørkenstorm) og Desert Shield (Ørkenskjold). (22) Menwith Hill er nu den førende amerikanske station for Comint-opsamling mod USAs store allierede, Israel. Dets personale omfatter lingvister, der er uddannet i hebræisk, arabisk og farsi samt europæiske sprog. Menwith Hill er for nylig blevet udvidet til også at omfatte jordforbindelser til et nyt netværk af Sigint-satellitter, der blev opsendt i 1994 og 1995 (RUTLEY). Navnet på den nye klasse af satellitter kendes endnu ikke.

Sigint-satellitter

40. CIA udviklede en anden Sigint-satellitklasse med supplerende anvendelsesmuligheder i perioden fra 1967 til 1985. Disse satellitter, som i starten gik under navnet RHYOLITE og senere AQUACADE, blev styret fra en jordstation i Pine Gap i det centrale Australien. Ved hjælp af en stor parabolantenne, som foldede sig ud i rummet,

opfangede RHYOLITE signaler ved en lavere frekvens i VHF- og UHF-båndet. Større og nyere satellitter af denne type har fået navnet MAGNUM og dernæst ORION. Deres mål omfatter telemetri, VHF-radio, mobiltelefoner, personsøgersignaler samt mobile dataforbindelser.

41. En tredje satellitklasse, først kaldet JUMPSEAT og senest TRUMPET, arbejder i høje elliptiske nær-polare kredsløb, så de i lange perioder kan "svære" over høje nordlige breddegrader. De sætter USA i stand til at opsamle signaler fra transmittere på høje nordlige breddegrader, som MERCURY eller ORION dækker dårligt, samt også opfange signaler, der sendes til russiske kommunikationssatellitter i samme kredsløb.



Comint satellites in geostationary orbits, such as VORTEX, intercept terrestial microwave spillage

Inter-city microwave radio relay tower pills" signals into space

42. Selvom der stadig ikke findes præcise detaljer om amerikanske rumbaserede Sigint-satellitter, opsendt efter 1990, tyder iagttagelser af de relevante jordstationer på, at opsamlingssystemerne snarere er blevet udvidet end formindsket. Hovedstationerne befinder sig i Buckley Field, Denver, Colorado, Pine Gap, Australien, Menwith Hill, England og Bad Aibling, Tyskland. Satellitterne og deres behandlingsfaciliteter er overordentlig kostbare (i størrelsesordenen USD 1 milliard hver). I 1998 annoncerede det amerikanske National Reconnaissance Office (NRO) planer om at kombinere de tre forskellige Sigint-satellitklasser til en integreret overordnet Sigint-arkitektur for at "forbedre Sigint-ydelsen og undgå omkostninger ved at konsolidere systemer med anvendelse ... af ny satellit- og databehandlingsteknologi". (23)

43. Det følger at, USA inden for de begrænsninger, der gives af budgetindskrænkninger og opgaveprioritering, hvis de vil, kan anvende rumopsamlingssystemer til at aflytte mobile kommunikationssignaler og indenbys mikrobølgetrafik overalt på kloden. De geografiske og behandlingsmæssige vanskeligheder ved samtidig opsamling af meddelelser fra alle dele af verden tyder kraftigt på, at opgaverne for disse satellitter vil være rettet mod mål af højeste national og militær prioritet. Det er derfor sandsynligt, at selvom europæisk kommunikation på indenbys mikrobølgeruter kan opsamles, vil den normalt blive ignoret. Men det er meget sandsynligt, at kommunikation til eller fra Europa, der passerer mikrobølgekommunikationsnetværk i landene i Mellemøsten, vil blive opsamlet og behandlet.

44. Intet andet land (ej heller det tidligere Sovjetunionen) har opsendt satellitter svarende til CANYON, RHYOLITE eller deres efterfølgere. Både Storbritannien (projekt ZIRCON) og Frankrig (projekt ZENON) har forsøgt at gøre det, men aldrig gennemført det. Efter 1988 købte den britiske regering kapacitet på den amerikanske VORTEX-konstellation (nu MERCURY) til brug for ensidige nationale formål. (24) En ledende britisk forbindelsesofficer og medarbejder hos GCHQ arbejder på Menwith Hill NSA-stationen og hjælper med at

tildele opgaver for og drive satellitterne.

Opsamling fra kommunikationssatellitternes internationale faste operatører

45. En systematisk opsamling af kommunikation på kommunikationssatellitterne internationale faste operatører begyndte i 1971. Der blev bygget to jordstationer til dette formål. Den første i Morwenstow, Cornwall, England havde to antenner på 30 meter. Den ene antenne aflyttede kommunikation fra Intelsat over Atlanten, den anden Intelsat over det Indiske Ocean. Den anden station til aflytning af Intelsat lå i Yakima, Washington i det nordvestlige USA. NSAs "Yakima Research Station" aflyttede kommunikation, der passerede Intelsat-satellitten over Stillehavet.

46. Mulighederne for aflytning af internationale faste operatører på kommunikationssatellitter drevet af vestlige lande lå på dette niveau indtil slutningen af 1970'erne, da netværket blev udbygget med endnu en station i Sugar Grove, West Virginia, USA. I 1980 var dets tre satellitantenner blevet overdraget til den amerikanske flådes sikkerhedsgruppe og blev brugt til aflytning af kommunikationssatellitter. Der skete en kraftig udvidelse af systemet til aflytning af internationale faste operatørers satellitter fra 1985 til 1995 i forbindelse med udbygningen af ECHELON-behandlingssystemet (afsnit 3). Der blev bygget nye stationer i USA (Sabana Seca, Puerto Rico), Canada (Leitrim, Ontario), Australien (Kojarena, Vestaustralien) og New Zealand (Waihopai, Sydøen). Kapaciteten i Yakima, Morwenstow og Sugar Grove blev udbygget og udbygges fortsat.

Baseret på en enkel optælling af antallet af antenner, der p.t. er installeret på hver kommunikationssatellit-aflytningsstation eller satellit-SIGINT-station, **viser det sig, at UKUSA-landene til sammen i øjeblikket driver mindst 120 satellitbaserede opsamlingssystemer. Det omtrentlige antal antenner i hver kategori er:**

- Rettet mod vestlige kommercielle kommunikationssatellitter (internationale faste operatører)	**40**
- Kontrol af rumbaserede signalefterretningssatellitter	**30**
- P.t. eller tidligere rettet mod sovjetiske kommunikationssatellitter	**50**

Systemer i den tredje kategori kan siden den kolde krigs afslutning være flyttet til opgaver vedrørende internationale faste operatører. (25)

47. Andre lande opsamler i stigende omfang Comint fra satellitter. Ruslands FAPSI driver store jordopsamlingsstationer i Lourdes, Cuba og i Cam Ranh Bay, Vietnam. (26) Tysklands BND og Frankrigs DGSE hævdes at samarbejde om driften af en kommunikationssatellit-opsamlingsstation i Kourou, Guyana, rettet mod "amerikansk og sydamerikansk satellitkommunikation". DGSE siges også at have kommunikationssatellit-opsamlingsstationer i Domme (Dordogne, Frankrig), i Ny Caledonien og i De Forenede Arabiske Emirater. (27) Den schweiziske efterretningstjeneste har for nyligt offentliggjort en plan for to kommunikationssatellit-aflytningsstationer. (28)

Satellite ground terminal at Etam, West Virginia connecting Europe and the US via Intelsat IV

GCHQ constructed an identical "shadow" station in 1972 to intercept Intelsat messages for UKUSA

Aflytning af undersøiske kabler

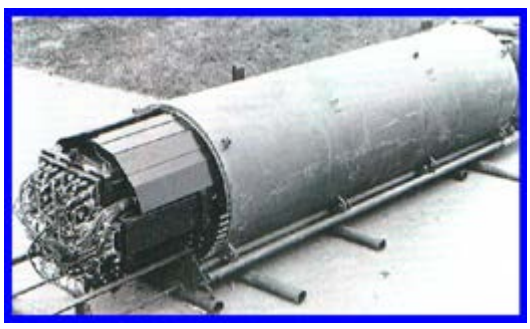
48. Undersøiske kabler spiller nu en dominerende rolle inden for international telekommunikation, eftersom optiske medier i modsætning til den begrænsede båndvidde, som rumsystemer har adgang til, byder på tilsyneladende ubegrænset kapacitet. Undtagen der hvor kabler slutter i lande, hvor teleoperatørerne giver Comint-adgang (fx Storbritannien og USA), synes undersøiske kabler at være egentligt sikre pga. havmiljøets karakter.

49. I oktober 1971 blev det påvist, at denne sikkerhed ikke eksisterede. En amerikansk ubåd, Halibut, besøgte Okhotsk-havet ud for det østlige USSR og optog kommunikation overført via et militært kabel til halvøen Khamchatka. Halibut var udstyret med et dybdedykkerkammer, der var fuldt synligt på ubådens hæk. Kammeret blev af den amerikanske flåde beskrevet som et "dybdedykkerredningsfartøj". Sandheden var, at "redningsfartøjet" var svejset solidt fast til ubåden. Når først ubåden var neddykket, forlod dybhavsdykkere ubåden og viklede aflytningsspoler omkring kablet. Efter at have bevist princippet vendte USS Halibut tilbage i 1972 og lagde en højtydende optagekapsel ved siden af kablet. Teknikken krævede ingen fysisk beskadigelse og var sandsynligvis ikke nem at opdage. (29)

50. Aflytningen af Okhotsk-kablet fortsatte i 10 år, og i denne periode aflagde tre forskellige specielt udstyrede ubåde rutinebesøg, hvor de opsamlede gamle kapsler og lagde nye, nogle gange flere på én gang. Der kom nye mål til i 1979. I sommeren 1979 sejlede en nyligt ombygget ubåd ved navn USS Parche fra San Francisco under Nordpolen til Barentshavet og lagde en ny kabelaflytning i nærheden af Murmansk. Besætningen fik hædrende omtale fra præsidenten for dens indsats. Aflytningen af Okhotsk-kablet sluttede i 1982, efter at dets placering var blevet bragt i fare af en tidligere ansat hos NSA, som solgte information om aflytningen, der havde kodenavnet IVY BELLS, til Sovjetunionen. En af IVY BELLS-kapslerne er nu udstillet på det tidligere KGBs museum i Moskva. Kabelaflytningen i Barentshavet fortsatte indtil 1992.

51. I 1985 blev kabelaflytningen udvidet til Middelhavet, hvor man aflyttede kabler mellem Europa og Vestafrika. (30) Efter den kolde krigs ophør blev USS Parche udstyret med en udbygget sektion, hvor der var plads til større kabelaflytningsudstyr og kapsler. Kabelaflytning kunne lægges ved hjælp af fjernstyring og droner. USS Parche er den dag i dag i drift, men man kender stadig ikke de præcise mål for ubådens missioner. Clinton-administrationen sætter tydeligvis stor pris på dens indsats. Hvert år fra 1994 til 1997 er ubådens besætning blevet højt rost. (31) Sandsynlige mål kan omfatte Mellemøsten, Middelhavet, det østlige Asien og Sydamerika. USA er den eneste flådenation, som vides at have anvendt dybhavsteknologi til dette formål.

52. Der er også anvendt induktive minioptagere til aflytning af underjordiske kabler. (32) Men lyslederkabler lækker ikke radiofrekvenssignaler og kan ikke aflyttes ved hjælp af induktive sløjfer. NSA og andre Comint-bureauer har brugt betydelige beløb på at forske i aflytning af lysledere, angiveligt med begrænset succes. Men fjernlyslederkabler er ikke usårlige. Den vigtigste adgangsmetode er at pille ved de optoelektroniske "forstærkere", der forstærker signalniveauet over lange afstande. Deraf følger, at et undersøisk kabelsystem, der benytter undersøiske optoelektroniske forstærkere, ikke kan anses for sikker mod aflytning og kommunikationsefterretningsaktivitet.



USS halibut with disguised chamber for diving

Cable tapping pod laid by US submarine off Khamchatka

Aflytning af Internettet

53. Det er blevet hævdet, at den dramatiske vækst i Internettets størrelse og betydning og beslægtede former for digital kommunikation udgør en udfordring for Comint-bureauerne. Dette lader ikke til at være sandt. Op igennem 1980'erne drev NSA og dets britisk/amerikanske partnere et større internationalt kommunikationsnet end det daværende Internet, men baseret på samme teknologi. (33) Ifølge NSAs britiske partner "er alle GCHQ-systemer indbyrdes forbundet i det største lokalnet i Europa og forbundet med andre steder verden over via et af verdens største fjernnet ... den primære netværksprotokol er Internet Protocol (IP). (34) Dette globale net, der blev udviklet som projekt EMBROIDERY, omfatter PATHWAY, NSAs primære computerkommunikationsnetværk. Det giver hurtig og sikker global kommunikation for ECHELON og andre systemer.

54. Siden begyndelsen af 1990'erne er der blevet udviklet hurtige og avancerede Comint-systemer til at opsamle, filtrere og analysere de former for hurtig digital kommunikation, der anvendes på Internettet. Eftersom en stor del af verdens Internet-kapacitet ligger i USA eller er forbundet til USA, vil megen kommunikation i "cyberspace" passere gennem mellempunkter i USA. Kommunikation fra Europa til og fra Asia, Oceanien, Afrika eller Sydamerika går normalt via USA.

55. De ruter, som Internet-"pakker" følger, afhænger af dataenes oprindelse og bestemmelsessted, systemerne som de går ind på og ud fra Internettet samt en vrimmel af andre faktorer, deriblandt klokkeslæt. Dermed vil routere i den vestlige del af USA være mest ledige, når trafikken i Mellemeuropa topper. Det er dermed muligt (og fornuftigt), at meddelelser, der bevæger sig en kort afstand på et travlt europæisk netværk i stedet bevæger sig fx via Internetcentraler i Californien. Deraf følger det, at en stor del af den internationale kommunikation på Internettet på grund af systemets natur passerer gennem USA og dermed er let tilgængelig for NSA.

56. Standard Internet-meddelelser består af pakker, kaldet "datagrammer". Datagrammer indeholder tal, der repræsenterer såvel deres oprindelse som deres bestemmelsessted, kaldet "IP-adresser". Adresserne er unikke for hver computer, der er koblet til Internettet. De er af naturen enkle at identificere med hensyn til oprindelses- og bestemmelsesland og -sted. Håndtering, sortering og routing af millioner af sådanne pakker hvert sekund er grundlæggende for driften af større Internetcentre. Den samme proces gør det lettere at trække trafik ud til Comint-formål.

57. Adgang til Internet-trafikken kan fås enten fra internationale kommunikationsforbindelser til USA, eller når den når de større Internet-centraler. Der er fordele ved begge metoder. Adgang til kommunikationssystemer vil sandsynligvis forblive hemmelig - hvorimod adgang til Internet-centraler kan være nemmere at opdage, men giver enklere adgang til flere data tillige med enklere sorteringsmetoder. Selvom det drejer sig om enorme mængder data, er NSA normalt juridisk begrænset til kun at se på kommunikation, der starter eller slutter i et fremmed land. Medmindre der gives særlig bemyndigelse, skal alle øvrige data normalt smides væk af maskinen, før de kan undersøges eller optages.

58. Megen anden Internet-trafik (hvad enten den stammer fra områder uden for USA eller ej) er af ubetydelig efterretningsmæssig interesse eller kan behandles på andre måder. Fx har meddelelser til "Usenet" diskussionsgrupper en størrelsesorden på 15 Gigabytes (GB) data dagligt, hvad der nogenlunde svarer til 10.000 bøger. Alle disse data sendes til alle, som ønsker (eller vil have) dem. Ligesom andre Internet-brugere har efterretningsvæsener åben adgang til disse data og til at arkivere og analysere dem. I Storbritannien har Defence Evaluation and Research Agency en database på 1 Terabyte med de seneste 90 dages Usenet-meddelelser. (35) En tilsvarende service, kaldet "Deja News", er tilgængelig for brugere af WWW (World Wide Web). Meddelelser til Usenet er nemme at sondre. Det er meningsløst at indsamle dem i hemmelighed.

59. Tilsvarende overvejelser gælder WWW, hvoraf størstedelen er fuldt tilgængeligt. Websteder undersøges løbende af "søgemaskiner", som udformer kataloger over indholdet. "Alta Vista" og "Hotbot" er førende offentlige steder af denne art. NSA anvender på samme måde computerrobotter ("bots") til at opsamle interessante data. Fx giver et websted i New York, kendt som JYA.COM (http://www.jya.com/crypto.htm) , omfattende offentlig information om Sigint, Comint og kryptering. Dette sted opdateres jævnligt. Optegnelser over adgang til stedet viser, at det hver morgen besøges af en "bot" fra NSAs National Computer Security Centre, der søger efter nye filer og kopierer det, den finder. (36)

60. Det følger, at udenlandsk Internet-trafik af kommunikationsefterretningsmæssig interesse - bestående af e-mail, filoverførsler, "virtuelle private netværk" der drives via Internettet og visse andre meddelelser - i bedste fald udgør nogle få procent af trafikken på de fleste amerikanske Internet-centraler eller backboneforbindelser. Ifølge en tidligere medarbejder havde NSA i 1995 installeret "sniffersoftware" til at opsamle denne trafik i 9 større Internet-centralpunkter (IXP). (37) De første to steder af denne art, der blev identificeret, FIX East og FIX West, blev drevet af bureauer under den amerikanske regering. De er tæt forbundet til nærliggende kommercielle lokaliteter, MAE East og MAE West (se tabellen). Tre andre nævnte steder var Network Access Points, der oprindeligt blev udviklet af den amerikanske National Science Foundation for at give det amerikanske Internet dets oprindelige "backbone".

Placering	**Operatør**	**Betegnelse**	
FIX East	College Park, Maryland	Den amerikanske regering	Federal Information Exchange
FIX West	Mountain View, Californien	Den amerikanske regering	Federal Information Exchange
MAE East	Washington, DC	MCI	Metropolitan Area Ethernet
New York NAP	Pennsauken, New Jersey	Sprintlink	Network Access Point
SWAB	Washington, DC	PSInet / Bell Atlantic	SMDS Washington Area Bypass
Chicago NAP	Chicago, Illinois	Ameritech / Bellcorp	Network Access Point
San Francisco NAP	San Francisco, Californien	Pacific Bell	Network Access Point
MAE West	San Jose, Californien	MCI	Metropolitan Area Ethernet
CIX	Santa Clara Californien	CIX	Commercial Internet Exchange

Tabel 1 NSA Internet Comint-adgang på IXP-steder (1995) (38)

61. I samme artikel hævdedes det, at et førende amerikansk Internet- og teleselskab havde indgået en kontrakt med NSA om udvikling af software til at opsamle interessante data på Internettet, samt at der var indgået aftaler med de førende producenter Microsoft, Lotus og Netscape om ændring af deres produkter til brug i udlandet. Den sidste påstand har vist sig at være korrekt (se det tekniske bilag). Indarbejdelse heraf ville ikke være interessant, medmindre NSA også havde sørget for generel adgang til trafikken på Internettet. Selvom NSA hverken vil bekræfte eller afvise sådanne påstande, blev der under en retssag i 1997 i Storbritannien om påstået "computer hacking" fremlagt beviser på NSAs overvågning af Internettet. Vidner fra det amerikanske flyvevåbens del af NSA vedgik brugen af "packet sniffers" og specialprogrammer til at spore forsøg på adgang til USAs militære computere. Sagen faldt, da vidnerne nægtede at fremlægge beviser om de systemer, de havde anvendt. (39)

Hemmelig opsamling af højkapacitetssignaler

62. Hvis det ikke er muligt at få adgang til interessante signaler på anden måde, har Comint-bureauer bygget særligt aflytningsudstyr til installation på ambassader eller andre diplomatlokaler, eller som kan bæres til steder af særlig interesse. Omfattende beskrivelser af denne type operationer er blevet offentliggjort af Mike Frost, en tidligere embedsmand i CSE, det canadiske Sigint-bureau. (40) Selvom ambassadelokaler i bymidten ofte er ideelt placerede til at aflytte mange forskellige typer kommunikation fra officielle biltelefoner til højkapacitets mikrobølgeforbindelser, kan det være vanskeligt at behandle og videregive disse informationer. Sådanne opsamlingsoperationer er også meget følsomme af diplomatiske årsager. Udstyr til hemmelig opsamling er derfor specialiseret, selektiv og i miniatørrelse.

63. NSA/CIA har en fælles "særlig opsamlingsservice", der fremstiller udstyr til og træner personale i hemmelige opsamlingsaktiviteter. Et væsentligt udstyr er et edb-behandlingssystem på størrelse med en kuffert, ORATORY. ORATORY er rent faktisk en miniversion af de ordbogscomputere, der beskrives i næste afsnit, og som kan udvælge ikke-verbal kommunikation af interesse fra mange forskellige former for input, efter forudprogrammerede udvælgelseskriterier. En førende leverandør til NSA ("The IDEAS Operation") tilbyder nu digitale modtagere i mikro-miniatørrelse, der samtidig kan behandle Sigint-data fra 8 uafhængige kanaler. Denne radiomodtager er på størrelse med et kreditkort. Den passer i en almindelig laptop-computer. IDEAS hævder, logisk nok, at deres små kort "udfører funktioner, der for ikke længe siden ville have krævet en hel udstyrsrack".

Nye satellitnetværk

64. Nye netværksoperatører har opbygget mobiltelefonsystemer, der byder på ubrudt global dækning ved hjælp af satellitter i lave eller mellemhøje kredsløb om jorden. Disse systemer kaldes nogle gange personlige satellitkommunikationssystemer. Eftersom hver satellit kun dækker et lille område og bevæger sig hurtigt, skal der bruges et stort antal satellitter for at sikre kontinuerlig global dækning. Satellitterne kan transmittere signaler direkte mellem hinanden eller til jordstationer. Det første system af denne art, som blev færdiggjort, Iridum, anvender 66 satellitter og blev taget i brug i 1998. Iridium synes at have skabt særlige vanskeligheder for kommunikationsefterretningsbureauerne, eftersom signalerne ned fra Iridium og tilsvarende netværk kun kan modtages i et lille område, som kan være hvor som helst på jordens overflade.

3. ECHELON og Comint-produktion

65. ECHELON-systemet blev kendt efter offentliggørelsen af STOA-rapporten. Siden da har nye beviser vist, at ECHELON har eksisteret siden 1970'erne og blev kraftigt udvidet mellem 1975 og 1995. Ligesom aflytningen af internationale faste operatører har ECHELON udviklet sig fra tidligere metoder. Dette afsnit indeholder nye oplysninger og dokumentation om ECHELON og satellitaflytning.

"Overvågningslisten"

66. Efter den offentlige afsløring af SHAMROCK-aflytningsprogrammet beskrev direktøren for NSA, generalløjtnant Lew Allen, hvordan NSA benyttede "overvågningslister" som hjælp til at holde øje med udenlandsk aktivitet af tilsyneladende efterretningsmæssig interesse". (41) "Vi har leveret detaljer ... om alle meddelelser i den udenlandske kommunikation, vi aflytter, der er relevant for navngivne enkeltpersoner eller organisationer. Disse kompileringer af navne går normalt under betegnelsen "Overvågningslister" (Watch List), sagde han. (42) Indtil 1970'erne behandledes overvågningslisten manuelt. Analytikere undersøgte kommunikation opsnappet fra internationale faste operatører, rapporterede og sammendrog eller analyserede den, der synes at vedrøre navne eller emner på overvågningslisten.

Nye oplysninger om ECHELON-stationer og -systemer

67. Det viser sig nu, at systemet, der er identificeret som ECHELON, har eksisteret i mere end 20 år. Behovet for et sådant system blev forudset i slutningen af 1960'erne, da NSA og GCHQ planlagde satellitaflytningsstationer for internationale faste operatører i Mowenstow og Yakima. Det forventedes, at mængden af meddelelser, der blev opsnappet fra de nye satellitter, ville være for stor til individuel undersøgelse. Ifølge en tidligere medarbejder hos NSA automatiserede de første ECHELON-computere Comint-behandlingen på disse stationer. (43)

68. NSA og CIA opdagede så, at Sigint-opsamling fra rummet var mere effektivt end forventet og gav

akkumulationer af optagelser, der overgik det tilgængelige udbud af lingvister og analytikere. Dokumenter viser, at da SILKWORTH behandlingssystemerne blev installeret i Menwith Hill til de nye satellitter, blev de understøttet af ECHELON 2 og andre databanker (se illustrationen).

69. I midten af 1980'erne blev kommunikation, der blev opsnappet på disse store stationer, nøje undersøgt med mange forskellige specifikationer til ikke-verbal trafik. Omfattende yderligere automatisering planlagdes i midten af 1980'erne i form af NSA Projekt P-415. Gennemførelse af dette projekt fuldendte automatiseringen af de tidligere overvågningsliste-aktiviteter. Fra og med 1987 rejste medarbejderne fra internationale Comint-bureauer til USA for at deltage i kurser om de nye edb-systemer.

70. Projekt P-415/ECHELON gjorde kraftig brug af NSAs og GCHQs globale Internet-lignende kommunikationsnet for at give efterretningskunder mulighed for at fjernbetjene computere på hver opsamlingsstation og modtage resultaterne automatisk. Systemets vigtigste komponent er lokale "ordbogscomputere" (Dictionary computere), der lagrer en omfattende database om angivne mål, herunder også navne, emner af interesse, adresser, telefonnumre og andre udvælgelseskriterier. Indgående meddelelser sammenlignes med disse kriterier, og i tilfælde af et sammenfald, sendes de rå efterretninger automatisk. Ordbogscomputere har tusindvis af forskellige opsamlingskrav at efterleve, også kaldet "numre" (4-cifrede koder).

71. Opgavetildeling og modtagelse af efterretninger fra ordbogscomputerne omfatter processer, der er velkendte for alle, som er vant til Internettet. Ordbogscomputernes sortering og udvælgelse kan sammenlignes med at bruge søgemaskiner, der udvælger websider med nøgleord eller udtryk og med angivelse af forbindelser. Ordbogscomputernes videresendelsesfunktion kan sammenlignes med e-mail. Systemet vil, når det bliver bedt derom, udarbejde lister over kommunikation, der falder sammen med hvert kriterium mhp. gennemgang, analyse, sammendrag eller videresendelse. En vigtig faktor ved det nye system er, at før ECHELON vidste forskellige lande og forskellige stationer, hvad der blev aflyttet, og hvem det blev sendt til. Nu bliver alle meddelelser, der udvælges af ordbogscomputere på fjerne steder, med undtagelse af en lille del, videresendt til NSA eller andre kunder uden at blive læst lokalt.

Internet-sted	
	
List of intelligence databanks operating at ECHELON Menwith Hill in 1979 included the second generation of ECHELON	Satellite interception site at Sugar Grove, West Virginia, showing six antennae targeted on European and Atlantic Ocean regional communications satellites

Westminster, London - Ordbogscomputer

72. I 1991 fortalte et britisk tv-program om ordbogscomputerens drift i GCHQs kontor i Westminster, London. Systemet "aflytter hemmeligt hver enkelt telex, der kommer til, fra eller igennem London; tusindvis af diplomat-, forretnings- og personlige meddelelser hver dag. Et program, der går under betegnelsen `Dictionary' (Ordbogen), fodres med disse meddelelser. Programmet finder nøgleordene fra den store masse af signalefterretninger og opsporer hundredvis af enkeltpersoner og selskaber". (44) Programmet påpegede, at selvom ordbogscomputerne blev styret og opgaverne stillet af GCHQ, blev de betjent af sikkerhedsgodkendt personale, som var ansat hos British Telecom (BT), Storbritanniens førende teleoperatør. (45) Tilstedeværelsen af ordbogscomputere er også bekræftet i Kojarena, Australien og i GCHQ Cheltenham, England. (46)

Sugar Grove, Virginia - Aflytning af kommunikationssatellitter på ECHELON-station

73. Dokumenter fra den amerikanske regering bekræfter, at satellitmodtagestationen i Sugar Grove, West Virginia er en ECHELON-station, der opsamler efterretninger fra kommunikationssatellitter. Stationen ligger ca. 400 km sydvest for Washington i et fjernt beliggende område af Shenandoah Mountains. Den drives af den amerikanske Naval Security Group og det amerikanske Air Force Intelligence Agency..

74. Et opgraderet system ved navn TIMBERLINE II blev installeret i Sugar Grove i sommeren 1990. Samtidig blev der ifølge officielle amerikanske dokumenter oprettet en "ECHELON træningsafdeling". (47) Da træningen var afsluttet, fik stationen i 1991 til opgave at "vedligeholde og drive en ECHELON-station". (48)

75. Det amerikanske flyvevåben har offentligt identificeret efterretningsvirksomheden i Sugar Grove: dets "mission er at rette sig mod satellitkommunikationsudstyr [til støtte for] forbrugere af kommunikationssatellitinformation ... Dette opnås ved at tilvejebringe trænet stampersonel bestående af opsamlingssystemoperatører, analytikere og ledere". (49) I 1990 viste satellitfotos, at der var 4 satellitantenner i Sugar Grove. I november måned 1998 afslørede en inspektion af området, at der nu var en gruppe på 9.

Sabana Seca, Puerto Rico og Leitrim, Canada - Aflytningsstationer for kommunikationssatellitter

76. Yderligere information, der er offentliggjort af det amerikanske flyvevåben, identificerer den amerikanske Naval Security Groups station i Sabana Seca, Puerto Rico som en kommunikationssatellit-aflytningsstation. Dens mission er "at blive den førende feltstation til behandling og analyse af satellitkommunikation". (50)

77. Det canadiske forsvar har offentliggjort nærmere oplysninger om stabsfunktioner på det canadiske Sigint-bureau CSEs feltstation i Leitrim. Stationen, som er beliggende i nærheden af Ottawa, Ontario, har 4 satellitterminaler, der er bygget siden 1984. Stabsrullen omfatter 7 kommunikationssatellitanalytikere, supervisorer og instruktører. (51)

78. I et offentligt tilgængeligt cv beskriver en tidligere kommunikationssatellitanalytiker, der arbejdede i Leitrim, sit job som et, hvor han fik ekspertise i "drift og analyse af talrige kommunikationssatellit-computersystemer og tilhørende undersystemer ... [hvor han anvendte] computerstøttede analysesystemer ... [og] et bredt udvalg af avanceret elektronisk udstyr til at opsnappe og undersøge udenlandsk kommunikation og elektroniske transmissioner. (52) Økonomirapporter fra CSE tyder også på, at bureauet i 1995/96 planlagde betalinger på USD 7 mio. til ECHELON og på USD 6 mio. til Cray (computere). Der var ikke yderligere detaljer om ECHELON. (53)

Waihopai, New Zealand - Intelsat-aflytning på ECHELON-station

79. New Zealands Sigint-bureau GCSB driver to satellitaflytningsterminaler i Waihopai, rettet mod Intelsat-satellitter der dækker Stillehavet. Omfattende oplysninger er allerede offentliggjort om stationens ordbogscomputere og dens rolle i ECHELON-netværket. (54) Efter offentliggørelse af bogen lykkedes det en New Zealandsk tv-station at optage billeder inde fra stationens operationscenter. Billederne blev optaget i hemmelighed ved at filme om natten gennem vinduer, hvor gardinerne delvist var trukket for. Tv-journalisten kunne optage nærbilleder af tekniske manualer, der fandtes i kontrolcentret. Det var Intelsat tekniske manualer, der bekræftede, at stationen var rettet mod disse satellitter. Overraskende nok var stationen næsten tom og fungerede fuldautomatisk. Der var én vagt indendøre, men han vidste ikke, at han blev filmet. (55)

Behandlingsteknik vedrørende internationale faste operatører

80. Det tekniske tillæg beskriver de hovedsystemer, der anvendes til at uddrage og behandle kommunikationsefterretninger. De detaljerede forklaringer af behandlingsmetoder er ikke altafgørende for at forstå det centrale i denne rapport, men er taget med, så læsere, som ved noget om telekommunikation, fuldt ud kan vurdere det tekniske stade.

81. Faxmeddelelser og computerdata (fra modemer) prioriteres i behandlingen, fordi de er nemme at forstå og analysere. Hovedmetoden til filtrering og analysering af ikke-verbal trafik, ordbogscomputerne, anvender traditionelle metoder til søgning af information, herunder også nøgleord. Hurtige specialchips gør det muligt at behandle store datamængder på denne måde. Den nyeste teknik er "topic spotting". Behandlingen af telefonopkald er fortrinsvis begrænset til identifikation af kaldrelateret information og trafikanalyse. Effektive systemer til observation af talte ord findes ikke og anvendes ikke trods rapporter om det modsatte. Men man har mindst siden 1995 anvendt identifikationssystemer af "stemmeaftrykstypen". Brugen af kraftig kryptering er langsomt ved at påvirke Comint-bureauernes muligheder. Denne vanskelighed for Comint-bureauer er opvejet af hemmelige og åbne aktiviteter, der har undergravet effektiviteten af krypteringssystemer, der er leveret fra og/eller brugt i Europa.

82. Konklusionerne, som drages i bilaget, er, at aktuelt tilgængeligt Comint-udstyr har muligheden, når det bliver bedt derom, at opsnappe, behandle og analysere hvert eneste moderne kommunikationssystem med høj kapacitet, som man får adgang til, herunder også de øverste niveauer af Internettet. Der er kun få huller i dækningen. En række systemers omfang, kapacitet og hastighed er vanskeligt at forstå fuldt ud. Der er bygget specialsystemer til at behandle papirmeddelelser, mobiltelefoner og nye satellitter.

4. Comint og retshåndhævelsen (law enforcement)

83. I 1990 og 1991 var den amerikanske regering foruroliget over, at AT&Ts markedsføring af et sikkert telefonsystem kunne indskrænke Comint-aktiviteterne. AT&T blev overtalt til at trække sit produkt tilbage. I stedet tilbød den amerikanske regering NSA "Clipper-chips" til indbygning i sikre telefoner. Disse chips ville blive fremstillet af NSA, som også ville registrere indbyggede nøgler og give denne information videre til andre officielle organer med henblik på opbevaring og om nødvendigt også hentning. Dette forslag viste sig at være særdeles upopulært og blev frafaldet. I stedet forslog den amerikanske regering, at ikke-statslige bureauer skulle opbevare kopier af hver brugers nøgler, et system ved navn "key escrow" (systemer, der er baseret på escrow encryption-standarden, og som transmitterer oplysninger om den anvendte sessionsnøgle i et særligt Law enforcement Access Field (o.a.)) og senere "key recovery" (systemer, der muliggør adgang til krypterede data uden brugerens deltagelse (o.a.)). Set i bakspejlet var det egentlige formål med disse forslag at give NSA et enkelt (eller meget få) adgangspunkter til nøgler, så de fortsat kunne få adgang til privat og kommerciel kommunikation.

Fejlagtig fremstilling af politiets aflytningsbehov

84. Mellem 1993 og 1998 førte USA vedvarende diplomatiske aktiviteter i et forsøg på at overtale landene i EU og OECD til at vedtage deres "key recovery system". I denne periode insisterede den amerikanske regering på, at formålet med initiativet var at hjælpe politimyndighederne. Dokumenter, som er fremskaffet til denne undersøgelse, antyder, at disse behov forsætligt blev fejlagtigt fremstillet i forhold til den egentlige hensigt bag den amerikanske politik. Dokumenter, der er fremskaffet i henhold til den amerikanske lov om aktindsigt, antyder, at beslutningerne udelukkende blev anført af embedsmænd fra NSA, nogle gange helt uden deltagelse af embedsmænd fra politi eller retsvæsen. Da David Aaron, den særligt udnævnte amerikanske ambassadør for kryptering, eksempelvis besøgte Storbritannien den 25 november 1996, blev han ledsaget og orienteret af NSAs højeststående repræsentant i Storbritannien, Dr. James J. Hearn, tidligere vicedirektør for NSA. David Aaron mødte eller rådførte sig ikke med FBI-embedsmænd, der var tilknyttet hans ambassade. Hans møde med embedsmænd fra det britiske ministerråd omfattede NSAs repræsentant og medarbejdere fra Storbritanniens GCHQ, men på mødet deltog ikke politifolk eller embedsmænd fra justitsministeriet i de to lande.

85. Siden 1993 har politiembedsmænd fra mange lande i EU og de fleste UKUSA-lande, uden at europæiske parlamentariske organer og deres vælgere ved det, mødtes hvert år i et separat forum for at drøfte deres behov for aflytning af kommunikation. Disse embedsmænd mødtes i en hidtil ukendts organisations regi, nemlig ILETS (International Law Enforcement Telecommunications Seminar). ILETS blev iværksat og grundlagt af FBI. I tabel 2 er opført ILETS-møder afholdt mellem 1993 og 1997.

86. På møderne i 1993 og 1994 redegjorde ILETS-deltagere for politiets behov for kommunikationsaflytning. Disse er nævnt i et dokument fra ILETS i 1994 med betegnelsen "IUR 1.0". Dette dokument var baseret på en tidligere rapport fra FBI om politiets behov for overvågning af elektronisk kommunikation (Law Enforcement Requirements for the Surveillance of Electronic Communications), der første gang blev udsendt i juli 1992 og revideredes i juni 1994. IUR-behovet var i sit indhold kun lidt anderledes end FBIs behov, men udbygget, så det

indeholdt 10 behov i stedet for 9. IUR nævnte ikke noget politibehov for "key escrow" eller "key recovery". Kryptering blev kun nævnt i forbindelse med sikkerhedsforanstaltninger for netværk.

87. Mellem 1993 og 1997 deltog politirepræsentanter fra ILETS ikke i den NSA-ledede beslutningsproces vedrørende "key recovery", og ILETS fremsatte heller ikke noget sådant forslag, heller ikke så sent som i 1997. Trods dette præsenterede den amerikanske regering gentagne gange sit politik som værende motiveret af politiorganernes formulerede behov. På mødet i 1997 i Dublin ændrede ILETS ikke IUR. Det var først i 1998, at en revideret IUR blev udarbejdet med behov vedrørende kryptering. Heraf følger det, at den amerikanske regering vildledte landene i EU og OECD om den egentlige hensigt med regeringens politik.

88. Men denne amerikanske vildledning stod klar for den højtstående kommissionsembedsmand, som har ansvaret for informationssikkerheden. I september 1996 gjorde David Herson, leder af EUs Senior Officers' Group on Information Security, rede for sin vurdering af det amerikanske "key recovery"-projekt:

> *"'Law Enforcement' er et beskyttelsesskjold for alle de øvrige regeringsaktiviteter ... Vi taler om udenlandske efterretninger - det er, hvad dette drejer sig om. Der er ikke tvivl om, [at] 'law enforcement' er et røgslør".* (56)

89. Det bør bemærkes, at politiets behov for kommunikationsaflytning teknisk, juridisk og organisationsmæssigt set adskiller sig grundlæggende fra kommunikationsefterretninger. Politiorganer ønsker normalt at aflytte en bestemt linie eller en bestemt gruppe linier og skal normalt berettige deres anmodning over for en retslig eller administrativ myndighed, før de går videre. I modsætning hertil arbejder Comint-bureauer med en bred "trawling" af international kommunikation og arbejder under blankokendelser. Sådanne operationer kræver ikke eller formoder ikke engang, at de parter, der aflyttes, er kriminelle. En sådan skelnen er altafgørende for borgernes frihed, men den risikerer at blive udhulet, hvis grænserne mellem politi- og kommunikationsefterretningsaflytning udviskes fremover.

År	**Sted**	**Deltagere fra andre end EU-lande**	**EU-deltagere**
1993	Quantico, Virginia, USA	Australien, Canada, Hong Kong, Norge, USA	Danmark, Frankrig, Holland, Spanien, Storbritannien, Sverige, Tyskland
1994	Bonn, Tyskland	Australien, Canada, Hong Kong, Norge, USA	Belgien, Danmark, Finland, Frankrig, Grækenland, Holland, Irland, Luxembourg, Portugal, Spanien, Storbritannien, Sverige, Tyskland, Østrig
1995	Canberra, Australien	Australien, Canada, Hong Kong, New Zealand, Norge, USA	Belgien, Frankrig, Grækenland, Holland, Irland, Italien, Spanien, Storbritannien, Sverige, Tyskland
1997	Dublin, Irland	Australien, Canada, Hong Kong, New Zealand, Norge, USA	Belgien, Danmark, Finland, Frankrig, Holland, Irland, Italien, Luxembourg, Portugal, Spanien, Storbritannien, Sverige, Tyskland, Østrig

Tabel 2 ILETS-møder 1993-1997

Politikommunikationsaflytning - politisk udvikling i Europa

90. Efter det andet ILETS-møde i Bonn i 1994 blev IUR 1.0 forelagt Ministerrådet og vedtaget uden at ændre et eneste ord den 17. januar 1995. (57) I 1995 skrev flere medlemmer af ILETS-gruppen uden for EU til rådet om at godkende den (ikke offentliggjorte) rådsbeslutning. Beslutningen blev ikke offentliggjort i EU-Tidende før efter næsten 2 år, den 4. november 1996.

91. Efter det tredje ILETS-møde i Canberra i 1995 blev den australske regering bedt om at forelægge IUR for International Telecommunications Union (ITU). Idet den australske regering bemærkede, at "politimyndigheder og nationale sikkerhedsorganer i et betydeligt antal ITU-medlemslande har aftalt et generisk sæt af krav vedrørende

lovlig aflytning", bad den ITU meddele sine standardorganer, at IUR-behovene skulle indarbejdes i fremtidige telekommunikationssystemer, idet "omkostningerne ved at [tilvejebringe] lovlige aflytningsmuligheder og dermed forbundne afbrydelser kan mindskes ved at tilvejebringe denne mulighed i konstruktionsfasen". (58)

92. Det ses, at ILETS mødtes igen i 1998 og reviderede og udvidede sine betingelser til også at omfatte Internet og personlige satellitkommunikationssystemer som fx Iridium. Det nye IUR anførte også "yderligere sikkerhedsbehov for netværksoperatører og serviceudbydere", omfattende nye krav om personlige oplysninger om abonnenter samt bestemmelser vedrørende håndtering af kryptering.

93. Den 3. september 1998 blev det reviderede IUR præsenteret for Police Co-operation Working Group som ENFOPOL 98. Det østrigske formandsskab foreslog, at man ligesom i 1994 vedtog det nye IUR ordret som en rådsbeslutning om aflytning "vedrørende den nye teknologi". (59) Gruppen var ikke enig. Efter gentagne nye udkast blev et nyt dokument udarbejdet af det tyske formandsskab til endelig overvejelse hos rådets indenrigs- og justitsministre. (60)

5. Comint og økonomiske efterretninger

94. Under debatten i Europa-Parlamentet i 1998 om "transatlantiske forbindelser/ECHELON-systemet" bemærkede kommissær Bangeman på Kommissionens vegne: "Hvis dette system eksisterede, ville det være et helt urimeligt angreb på de enkeltes frihedsrettigheder, på konkurrencen og på staternes sikkerhed". (61) ECHELONs eksistens blev beskrevet i afsnit 3. I dette afsnit beskrives de organisations- og rapporteringsmæssige rammer, hvorefter økonomisk følsom information, indsamlet af ECHELON og tilknyttede systemer, spredes, med sammendrag af eksempler hvor europæiske organisationer har været genstand for overvågning.

Tildeling af økonomiske efterretningsopgaver

95. Amerikanske embedsmænd indrømmer, at NSA opsamler økonomisk information, hvad enten det sker tilsigtet eller ej. Den tidligere militærefterretningsattaché oberst Dan Smith arbejdede på den amerikanske ambassade i London indtil 1993. Han modtog regelmæssigt Comint-produkter fra Menwith Hill. I 1998 fortalte han BBC, at der på Menwith Hill:

> *"Med hensyn til opfangning af kommunikation, vil der, fordi de optager på bredbåndsnettet, uundgåeligt blive aflyttet samtaler eller kommunikation, der intet har med militæret at gøre, og der vil heri sandsynligvis være nogle oplysninger om kommercielle forhold"*
>
> *"Alt vil være muligt, teknisk set. Teknisk set, kan de opfange alle disse oplysninger, sortere dem og finde ud af, hvad der evt. spørges om . . . Men der findes ingen politik om specifikt at gøre dette som svar på et bestemt firmas interesser* (62)

96. Denne udtalelse er generelt ikke forkert. Men den forbigår grundlæggende sondringer mellem tildeling af opgaver og udbredelse samt mellem kommercielle og økonomiske efterretninger. Der er ingen beviser på, at firmaer i noget UKUSA-land kan tildele Comint-opsamlingsopgaver, der passer deres eget formål. Det behøver de ikke. Hvert UKUSA-land giver de nationale organisationer, som vurderer efterretningerne, og de pågældende relevante ministerier bemyndigelse til at tildele opgaver og modtage økonomiske efterretninger fra Comint. Sådan information kan opsamles til et væld af formål, såsom vurdering af fremtidige priser på essentielle handelsvarer, bestemmelse af et andet lands position i handelsforhandlinger, overvågning af international våbenhandel, sporing af følsom teknologi eller evaluering af mållandets politiske stabilitet og/eller økonomiske styrke. Hvert af disse mål og mange andre kan frembringe efterretninger, som har direkte kommerciel relevans. Beslutningen om, hvorvidt de skal udbredes eller udnyttes træffes ikke af Comint-bureauer, men af nationale statslige organer.

Udbredelse af økonomiske efterretninger

97. Ifølge den tidligere direktør anbefalede det amerikanske Foreign Intelligence Advisory Board i 1970, at "økonomiske efterretninger herefter betragtes som en funktion af den nationale sikkerhed og prioriteres på linie med diplomat-, militære og teknologiske efterretninger". (63) Den 5. maj 1977 blev det på et møde mellem NSA, CIA og det amerikanske Handelsministerium besluttet at godkende oprettelsen af et hemmeligt nyt kontor Office of Intelligence Liaison. Dets opgave var at håndtere "udenlandske efterretninger" af interesse for

Handelsministeriet. Dets stående ordrer viser, at det var bemyndiget til at modtage og håndtere SCI-efterretninger - Comint og Sigint fra NSA. Oprettelsen af dette kontor skabte dermed en formel mekanisme, hvormed NSA-data kunne anvendes til at støtte kommercielle og økonomiske interesser. Efter at dette system blev fremhævet i et britisk tv-program i 1993, blev dets navn ændret til Office of Executive Support. (64) Samme år, dvs. 1993, udvidede præsident Clinton den amerikanske efterretningsstøtte til kommercielle organisationer med oprettelsen af et nyt nationalt økonomisk råd (National Economic Council) som en parallel til det nationale sikkerhedsråd (National Security Council).

98. Der er skrevet meget om arten af denne efterretningsstøtte. Tidligere efterretningsembedsmænd og andre eksperter siger, at tips baseret på spionage ... regelmæssigt strømmer fra Handelsministeriet til amerikanske firmaer for at hjælpe dem med at skabe kontrakter i udlandet. (65) Office of Executive Support giver sikkerhedsembedsmænd hemmeligstemplede ugentlige orienteringer. Én amerikansk avis modtog rapporter fra Handelsministeriet, der viste efterretningsstøtte til amerikanske firmaer:

> *Et af disse dokumenter er mødereferatet fra et møde, der afholdtes i august 1994 i Handelsministeriet [med den hensigt] at identificere større licitationer i Indonesien for at hjælpe amerikanske firmaer med at få kontrakten. En medarbejder fra CIA ... talte på mødet - 5 af de 16 personer på den rutinemæssige distributionsliste for mødereferatet kom fra CIA.*

99. I Storbritannien skal GCHQ ifølge loven (og når, den britiske regering beder derom) aflytte udenlandsk kommunikation "af hensyn til Storbritanniens økonomiske velbefindende ...i forhold til handlinger eller hensigter vedrørende personer uden for de britiske øer". Kommercielle aflytningsopgaver tildeles og analyseres af GCHQs K-division. Kommercielle og økonomiske mål kan specificeres af regeringens Overseas Economic Intelligence Committee, Economic Staff of the Joint Intelligence Committee (JIC), Finansministeriet eller Storbritanniens nationalbank, Bank of England. (66) Ifølge en tidligere ledende JIC-embedsmand omfatter Comint-optagelserne rutinemæssigt "firmaplaner, telexer, faxer og transskriberede telefonopkald. Mange opkald var mellem Europa og den sydlige halvkugle". (67)

100. I Australien giver DSD kommercielt relevant Comint videre til Office of National Assessments, som afgør om og i så fald hvortil denne information skal udbredes. Personalet kan give information videre til australske firmaer, hvis det menes, at et andet land har eller søger at få en uretfærdig handelsfordel. Denne aktivitet har bl.a. været rettet mod Thomson-CSF samt handelsforhandlinger med japanske købere af kul og jernmalm. Tilsvarende systemer kører i de andre UKUSA-lande, Canada og New Zealand.

Brugen af økonomiske efterretninger som Comint-produkt

Panavia European Fighter Aircraft-konsortiet og Saudi-Arabien

101. I 1993 beskrev den tidligere embedsmand i det nationale sikkerhedsråd, Howard Teicher, i et program om Menwith Hill, hvordan det europæiske Panavia-firma valgtes som mål vedrørende salg til Mellemøsten. "Jeg husker, at ordene 'Tornado' eller 'Panavia' - information om det pågældende fly - ville have været førende mål, som vi ville have ønsket information om". (68)

Thomson CSF og Brasilien

102. I 1994 aflyttede NSA telefonsamtaler mellem Thomson-CSF og Brasilien vedrørende SIVAM, et overvågningssystem til USD 1,3 mia. til regnskoven i Amazonas. Firmaet blev beskyldt for at have bestukket medlemmer af den brasilianske regerings udvælgelsespanel. Kontrakten blev givet til det amerikanske firma Raytheon Corporation - som bagefter meddelte, at "Handelsministeriet arbejdede meget hårdt for at støtte amerikansk industri i forbindelse med dette projekt". (69) Raytheon leverer også vedligeholdelses- og teknisk service til NSAs ECHELON-satellitaflytningsstation i Sugar Grove.

Airbus Industrie og Saudi-Arabien

103. Ifølge en velinformeret presserapport fra 1995 "opsnappede NSA fra en kommerciel kommunikationssatellit alle faxer og telefonopkald mellem det europæiske konsortium Airbus, det saudiarabiske nationale luftfartsselskab og den saudiarabiske regering. Bureauet opdagede, at agenter fra Airbus tilbød en saudiarabisk embedsmand

bestikkelse og gav denne oplysning videre til amerikanske embedsmænd, som arbejde for tilbuddet fra Boeing Co og McDonnell Douglas Corp., som sidste år vandt konkurrence til et beløb af USD 6 mia." (70)

Internationale handelsforhandlinger

104. Mange andre beretninger er blevet offentliggjort af velansete journalister og en række førstehåndsvidner, der påberåber sig hyppige tilfælde, hvor den amerikanske regering har anvendt Comint til nationale kommercielle formål. Dette omfatter indhentning af data om japanske bilers emissionsstandarder; (71) handelsforhandlinger i 1995 om import af japanske luksusbiler; (72) fransk deltagelse i GATT handelsforhandlingerne i 1993 og Asian-Pacific Economic Conference (APEC), 1997.

Med værtslandene som mål

105. Spørgsmålet, om USA anvender kommunikationsefterretningsfaciliteter såsom Menwith Hill eller Bad Aibling til at angribe værtslandenes kommunikation opstår også. De beviser, der findes, tyder på, at en sådan adfærd normalt undgås. Ifølge den tidligere embedsmand i det nationale sikkerhedsråd, Howard Teicher, ville den amerikanske regering ikke pålægge NSA at udspionere en værtsregering såsom Storbritannien:

" [Men] jeg ville aldrig sige aldrig i denne branche, for når alt kommer til alt er nationale interesser nationale interesser ... nogle gange har vi ikke samme interesser. Så man skal aldrig sige aldrig - navnlig ikke i denne branche"

6. Comint-muligheder efter år 2000

Teknologiske udviklinger

106. Siden midten af 1960'erne har kommunikationsefterretningsbureauer haft betydelige vanskeligheder ved at opretholde global adgang til kommunikationssystemer. Disse vanskeligheder vil blive større i og efter år 2000. Hovedårsagen er, at telekommunikation nu er skiftet til lysledernet med høj kapacitet. Der skal være fysisk adgang til kablerne for at aflytte dem. Medmindre et lysledernet ligger i eller passerer igennem et samarbejdsland, er en effektiv aflytning kun praktisk mulig, hvis man piller ved de optoelektroniske forstærkere (når de er installeret). Denne begrænsning vil sandsynligvis betyde, at mange udenlandske landbaserede lysledernet med høj kapacitet er uden for rækkevidde. Den fysiske størrelse af det udstyr, der skal bruges til at behandle trafikken, betyder sammen med el-, kommunikations- og optagesystemer, at hemmelige aktiviteter bliver uigennemførlige og risikable.

107. Selv hvor der er nem adgang (fx kommunikationssatellitter), vil udbredelsen af nye systemet begrænse opsamlingsaktiviteterne, delvist fordi budgetbegrænsninger vil begrænse nye anvendelser, og delvist fordi eksisterende systemer ikke kan få adgang til bestemte systemer (fx Iridium).

108. I de sidste 15 år er det store teknologiske forspring inden for computere og informationsteknologi, som Comint-organisationerne engang havde, næsten helt forsvundet. Deres vigtigste computersystemer købes direkte fra hylden og svarer til eller er endog ringere end dem, der bruges af førende industri- og akademiske organisationer. Den eneste forskel er, at de er "TEMPEST-afskærmede", så de ikke udsender radiosignaler, der kunne anvendes til at analysere Sigint-aktiviteter.

109. Kommunikationsefterretningsorganisationer anerkender, at den langvarige krig mod civil og kommerciel kryptering er tabt. Et blomstrende akademisk og industriel fællesskab har stor rutine i kryptering og kryptologi. Internettet og det globale marked har skabt en fri strøm af information, systemer og software. NSA har forfejlet sin mission om at sikre fremtidig adgang hertil ved at foregive, at key escrow-systemet og lignende systemer havde til formål at støtte politiets (og ikke Comint) behov.

110. Fremtidige tendenser i Comint vil sandsynligvis omfatte begrænsninger af investeringer i Comint-opsamling fra rummet, en øget anvendelse af mennesker som agenter til at anbringe opsamlingsudstyr eller finde koder end før i tiden samt en styrket indsats for at angribe udenlandske edb-systemer ved hjælp af Internet og andre midler (herunder især få adgang til beskyttede filer eller kommunikation, før de krypteres).

111. Forsøg på at begrænse krypteringen har ikke desto mindre forsinket en omfattende indføring af effektive

kryptografiske sikkerhedssystemer. De lavere priser på regnekraft har også sat Comint-bureauer i stand til at indsætte hurtige og avancerede behandlings- og sorteringsværktøjer.

112. Nylige kommentarer til CIA-veteraner fra stabslederen for det stående efterretningsudvalg under Repræsentanternes Hus (Permanent Select Committee on Intelligence), den tidligere CIA-embedsmand John Millis, viser, hvordan NSA ser på de samme spørgsmål:

> *"Signalefterretninger er inde i en krise. ... I løbet af de sidste 50 år... Tidligere var teknologien NSAs ven, men i de sidste 4-5 år er teknologien ikke længere Sigints ven, men dets fjende.*
>
> *Telekommunikationsmediet er ikke længere Sigint-venlig. Det var det før. Når man lavede RF-signaler, kunne alle inden for rækkevidde af dette RF-signal modtage det lige så tydeligt som den påtænkte modtager. Vi gik fra det over til mikrobølger, og folk udtænkte en fantastisk måde at udnytte dem på. Nu går vi til medier, som er meget vanskelige at få adgang til.*
>
> *Kryptering findes, og den vil vokse meget hurtigt. Det er dårlige nyheder for Sigint... Det vil kræve en enorm investering i ny teknologi at få adgang til og mulighed for at få de oplysninger ud, som vi fortsat skal have fra Sigint".*

Politiske spørgsmål for Europa-Parlamentet

1. Parlamentets beslutning i 1998 om "transatlantiske forbindelser/ECHELON-systemet" (73) krævede "sikrende retsmidler vedrørende økonomiske oplysninger og effektiv kryptering". Tilvejebringelse af disse retsmidler kan gøres lettere gennem opnåelse af en tilbundsgående forståelse af nuværende og fremtidige Comint-muligheder.

2. På det tekniske stade kan sikrende retsmidler bedst fokuseres på at forpurre fjendtlig Comint-aktivitet ved at nægte adgang, eller hvor dette er uigennemførligt eller umuligt, forhindre behandling af meddelelsens indhold og tilhørende trafikinformation ved en generel anvendelse af kryptering.

3. Som Kommissionens SOGIS-gruppe har anerkendt, (74) er landenes modstridende interesser en kompliceret sag. Større lande har foretaget betydelige investeringer i Comint-muligheder. Ét medlemsland deltager aktivt i UKUSA-alliancen, mens andre er enten "tredjeparter" i forhold til UKUSA eller har indgået bilaterale aftaler med NSA. Nogle af disse ordninger er en arv fra den Kolde Krig, andre fortsætter. Disse spørgsmål skaber interne og internationale interessekonflikter. Tekniske løsninger er ikke indlysende. Det burde være muligt at definere en fælles interesse i at indføre retsmidler for at forpurre fremtidige eksterne Comint-aktiviteter rettet mod europæiske lande, deres borgere og kommercielle aktiviteter.

4. Endnu et tilsyneladende konfliktområde vedrører landenes ønske om at tilvejebringe kommunikationsaflytning til retmæssige politiformål. De tekniske og juridiske processer ved tilvejebringelse af aflytning til politiformål er væsentligt forskellige fra dem, der anvendes i kommunikationsefterretninger. Delvis pga. manglen på parlamentært og offentligt kendskab til Comint-aktiviteter, tilsløres denne skelnen ofte, navnlig af lande, der investerer kraftigt i Comint. Enhver manglende skelnen mellem retmæssig politiaflytningsbehov og aflytning til hemmelige efterretningsformål rejser alvorlige spørgsmål om de enkeltes frihedsrettigheder. En klar grænse mellem politiarbejde og "nationale sikkerhedsaflytningsaktiviteter" er tvingende nødvendig for at beskytte menneskerettighederne og de grundlæggende frihedsrettigheder.

5. I øjeblikket er Internet browsere og anden software, der bruges i næsten hver eneste pc i Europa, forsætligt deaktiveret, så "sikker" kommunikation, der sendes derfra, hvis den opsamles uden besvær, kan læses af NSA. Amerikanske producenter er tvunget til at foretage disse dispositioner i henhold til amerikanske eksportregler. Det er vigtigt at sikre ens betingelser. Man kunne overveje en modforanstaltning, hvor systemer med deaktiverede krypteringssystemer, der sælges uden for USA, skal opfylde en "åben standard", således at tredjemand og andre lande kan tilvejebringe yderligere applikationer, der giver mindst samme sikkerhedsniveau, som det kunder i USA har.

6. ILETS' arbejde har varet i 6 år uden parlamenternes deltagelse og uden samråd med de industriorganisationer, hvis vitale interesser deres arbejde påvirker. Det er beklageligt, at der før offentliggørelsen af denne rapport ikke har været offentlig information i landene om omfanget af beslutningsprocesserne i og uden for EU, der har ført til udarbejdelsen af eksisterende og nye politibehov (law enforcement "user requirements"). Den nuværende

beslutningsproces skal som en hastesag åbnes og drøftes i offentligheden, medlemslandenes parlamenter og EP, så der kan opnås en passende balance mellem sikkerhed og privatlivets fred for borgere og erhvervsvirksomheder, kommunikationsnetværkernes operatører og serviceudbydernes finansielle og tekniske interesser samt behovet for at støtte politiaktiviteter, der har til formål at begrænse alvorlig kriminalitet og terrorisme.

Technical annexe

Broadband (high capacity multi-channel) communications

1. From 1950 until the early 1980s, high capacity multi-channel analogue communications systems were usually engineered using separate communications channels carried at different frequencies The combined signal, which could include 2,000 or more speech channels, was a "multiplex". The resulting "frequency division multiplex" (FDM) signal was then carried on a much higher frequency, such as by a microwave radio signal.

2. Digital communications have almost universally taken over from analogue methods. The basic system of digital multi-channel communications is time division multiplexing (TDM). In a TDM telephony system, the individual conversational channels are first digitised. Information concerning each channel is then transmitted sequentially rather than simultaneously, with each link occupying successive time "slots".

3. Standards for digital communications evolved separately within Europe and North America. In the United States, the then dominant public network carrier (the Bell system, run by AT&T) established digital data standards. The basic building block, a T-1 link, carries the equivalent of 24 telephone channels at a rate of 1.544 Mbps. Higher capacity systems operate at greater data transmission rates Thus, the highest transmission rate, T-5, carries the equivalent of 8,000 speech channels at a data rate of 560 Mbps.

4. Europe adopted a different framework for digital communications, based on standards originally agreed by the CEPT. The basic European standard digital link, E-1, carries 30 telephone channels at a data rate of 2 Mbps. Most European telecommunications systems are based on E-1 links or (as in North America), multiples thereof. The distinction is significant because most Comint processing equipment manufactured in the United States is designed to handle intercepted communications working to the European forms of digital communications.

5. Recent digital systems utilise synchronised signals carried by very high capacity optical fibres. Synchronising signals enables single channels to be easily extracted from high capacity links. The new system is known in the US as the synchronous optical network (SONET), although three equivalent definitions and labels are in use. (75)

Communications intelligence equipment

6. Dozens of US defence contractors, many located in Silicon Valley (California) or in the Maryland "Beltway" area near Washington, manufacture sophisticated Sigint equipment for NSA. Major US corporations, such as Lockheed Martin, Space Systems/Loral, TRW, Raytheon and Bendix are also contracted by NSA to operate major Sigint collection sites. A full report on their products and services is beyond the scope of this study. The state of the art in contemporary communications intelligence may usefully be demonstrated, however, by examining some of the Comint processing products of two specialist NSA niche suppliers: Applied Signal Technology Inc (AST), of Sunnyvale, California, and The IDEAS Operation of Columbia, Maryland (part of Science Applications International Corporation (SAIC)). (76)

7. Both companies include senior ex-NSA staff as directors. When not explicitly stated, their products can be identified as intended for Sigint by virtue of being "TEMPEST screened". AST states generally that its "equipment is used for signal reconnaissance of foreign telecommunications by the United States government". One leading cryptographer has aptly and and engagingly described AST as a "one-stop ECHELON shop".

Wideband extraction and signal analysis

8. Wideband (or broadband) signals are normally intercepted from satellites or tapped cables in the form of multiplex microwave or high frequency signals. The first step in processing such signals for Comint purposes is "wideband extraction". An extensive range of Sigint equipment is manufactured for this purpose, enabling newly

intercepted systems to be surveyed and analysed. These include transponder survey equipment which identify and classify satellite downlinks, demodulators, decoders, demultiplexers, microwave radio link analysers, link survey units, carrier analysis systems, and many other forms of hardware and software.

9. A newly intercepted communications satellite or data link can be analysed using the AST Model 196 "Transponder characterisation system". Once its basic communications structure has been analysed, the Model 195 "Wideband snapshot analyser", also known as SNAPPER, can record sample data from even the highest capacity systems, sufficient to analyse communications in minute detail. By the start of 1999, operating in conjunction with the Model 990 "Flexible Data Acquisition Unit", this systems was able to record, playback and analyse at data rates up to 2.488 Gbps (SONET OC-48). This is 16 times faster than the largest backbone links in general use on the Internet; larger than the telephony capacity of any current communications satellite; and equivalent to 40,000 simultaneous telephone calls. It can be fitted with 48 Gbyte of memory (500-1000 times larger than found in an average personal computer), enabling relatively lengthy recordings of high-speed data links. The 2.5 Gbps capacity of a single SNAPPER unit exceeds the current daily maximum data rate found on a typical large Internet exchange. (77)

10. Both AST and IDEAS offer a wide range of recorders, demultiplexers, scanners and processors, mostly designed to process European type (CEPT) E-1, E-3 (etc) signals at data rates of up to 160 Mbps. Signals may be recorded to banks of high-speed tape recorders, or into high capacity "RAID" (78) hard disk networks. Intercepted optical signals can be examined with the AST Model 257E "SONET analyser".

11. Once communications links have been analysed and broken down to their constituent parts, the next stage of Comint collection involves multi-channel processors which extract and filter messages and signals from the desired channels. There are three broad categories of interest: "voice grade channels", normally carrying telephony; fax communications; and analogue data modems. A wide selection of multi-channel Comint processors are available. Almost all of them separate voice, fax and data messages into distinct "streams" for downstream processing and analysis.

12. The AST Model 120 multi-channel processor - used by NSA in different configurations known as STARQUAKE, COBRA and COPPERHEAD - can handle 1,000 simultaneous voice channels and automatically extract fax, data and voice traffic. Model 128, larger still, can process 16 European E-3 channels (a data rate of 500 Mbps) and extract 480 channels of interest. The 1999 giant of AST's range, the Model 132 "Voice Channel Demultiplexer", can scan up to 56,700 communications channels, extracting more than 3,000 voice channels of interest. AST also provides Sigint equipment to intercept low capacity VSAT (79) satellite services used by smaller businesses and domestic users. These systems can be intercepted by the AST Model 285 SCPS processor, which identifies and extracts up to 48 channels of interest, distinguished between voice, fax and data.

13. According to US government publications, an early Wideband Extraction system was installed at NSA's Vint Hill Farms field station in 1970, about the time that systematic COMSAT interception collection began. That station is now closed. US publications identify the NSA/CSS Regional Sigint Operations Centre at San Antonio, Texas, as a site currently providing a multi-channel Wideband Extraction service.

Filtering, data processing, and facsimile analysis

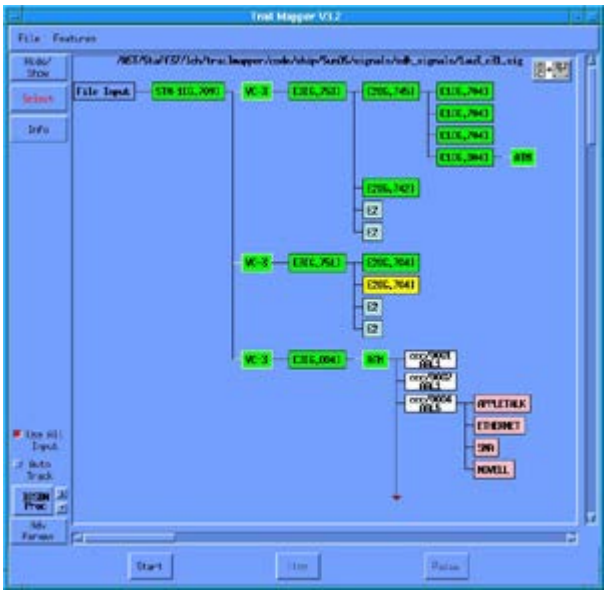
14. Once communications channels have been identified and signals of interest extracted, they are analysed further by sophisticated workstations using special purpose software. AST's ELVIRA Signals Analysis Workstation is typical of this type of Sigint equipment. This system, which can be used on a laptop computer in covert locations, surveys incoming channels and extracts standard Comint data, including technical specifications (STRUM) and information about call destinations (SRI, or signal related information). Selected communications are relayed to distant locations using NSA standard "Collected Signals Data Format" (CSDF). (80)

15. High-speed data systems can also be passed to AST's TRAILMAPPER software system, which works at a data rate of up to 2.5 Gbps. It can interpret and analyse every type of telecommunications system, including European, American and optical standards. TRAILMAPPER appears to have been designed with a view to analysing ATM (asynchronous transfer mode) communications. ATM is a modern, high-capacity digital communications system. It is better suited than standard Internet connections to carrying multimedia traffic and to providing business with private networks (VPN, LAN or WAN). TRAILMAPPER will identify and characterise such business networks.

16. In the next stage downstream, intercepted signals are processed according to whether they are voice, fax or data. AST's "Data Workstation" is designed to categorise all aspects of data communications, including systems for handling e-mail or sending files on the Internet. (81) Although the very latest modem systems (other than ISDN) are not included in its advertised specification, it is clear from published research that AST has developed the technology to intercept and process the latest data communications systems used by individuals and business to access the Internet. (82) The Data Workstation can stored and automatically process 10,000 different recorded signals.

17. Fax messages are processed by AST's Fax Image Workstation. This is described as a "user friendly, interactive analysis tool for rapid examination images stored on disk. Although not mentioned in AST's literature, standard fax pre-processing for Dictionary computers involves automatic "optical character recognition" (OCR) software. This turns the typescript into computer readable (and processable) text. The effectiveness of these systems makes fax-derived Comint an important collection subsystem. It has one drawback. OCR computer systems that can reliably recognise handwriting do not exist. No one knows how to design such a system. It follows that, perversely, hand-written fax messages may be a secure form of communication that can evade Dictionary surveillance criteria, provided always that the associated "signal related information" (calling and receiving fax numbers) have not been recognised as being of interest and directed to a Fax Image Workstation.

18. AST also make a "Pager Identification and Message Extraction" system which automatically collects and processes data from commercial paging systems. IDEAS offer a Video Teleconferencing Processor that can simultaneously view or record two simultaneous teleconferencing sessions. Sigint systems to intercept cellular mobile phone networks such as GSM are not advertised by AST or IDEAS, but are available from other US contractors. The specifications and ready availability of such systems indicate how industrialised and pervasive Comint has became. It has moved far from the era when (albeit erroneously), it was publicly associated only with monitoring diplomatic or military messages.



NSA "Trailmapper software showing atomatic detection of private networks inside intercepted high capacity STM-1 digital communications system

Traffic analysis, keyword recognition, text retrieval, and topic analysis

19. Traffic analysis is a method of obtaining intelligence from signal related information, such as the number dialled on a telephone call, or the Calling Line Identification Data (CLID) which identifies the person making the call. Traffic analysis can be used where message content is not available, for example when encryption is used. By analysing calling patterns, networks of personal associations may be analysed and studied. This is a principal method of examining voice communications.

20. Whenever machine readable communications are available, keyword recognition is fundamental to Dictionary computers, and to the ECHELON system. The Dictionary function is straightforward. Its basic mode of operation is akin to web search engines. The differences are of substance and of scale. Dictionaries implement the tasking of

their host station against the entire mass of collected communications, and automate the distribution of selected raw product.

21. Advanced systems have been developed to perform very high speed sorting of large volumes of intercepted information. In the late 1980s, the manufacturers of the RHYOLITE Sigint satellites, TRW, designed and manufactured a Fast Data Finder (FDF) microchip for NSA. The FDF chip was declassified in 1972 and made available for commercial use by a spin-off company, Paracel. Since then Paracel has sold over 150 information filtering systems, many of them to the US government. Paracel describes its current FDF technology as the "fastest, most accurate adaptive filtering system in the world":

> *A single TextFinder application may involve trillions of bytes of textual archive and thousands of online users, or gigabytes of live data stream per day that are filtered against tens of thousands of complex interest profiles ... the TextFinder chip implements the most comprehensive character-string comparison functions of any text retrieval system in the world.*

Devices like this are ideal for use in ECHELON and the Dictionary system.

22. A lower capacity system, the PRP-9800 Pattern Recognition Processor, is manufactured by IDEAS. This is a computer card which can be fitted to a standard PC. It can analyse data streams at up to 34 Mbps (the European E-3 standard), matching every single bit to more than 1000 pre-selected patterns.

23. Powerful though Dictionary methods and keyword search engines may be, however, they and their giant associated intelligence databases may soon seem archaic. Topic analysis is a more powerful and intuitive technique, and one that NSA is developing and promoting with confidence. Topic analysis enables Comint customers to ask their computers to "find me documents about subject X". X might be "Shakespeare in love" or "Arms to Iran".

24. In a standard US test used to evaluate topic analysis systems, (83) one task the analysis program is given is to find information about "Airbus subsidies". The traditional approach involves supplying the computer with the key terms, other relevant data, and synonyms. In this example, the designations A-300 or A-320 might be synonymous with "Airbus". The disadvantage of this approach is that it may find irrelevant intelligence (for example, reports about export subsidies to goods flown on an Airbus) and miss relevant material (for example a financial analysis of a company in the consortium which does not mention the Airbus product by name). Topic analysis overcomes this and is better matched to human intelligence.

25. The main detectable thrust of NSA research on topic analysis centres on a method called N-gram analysis. Developed inside NSA's Research group - responsible for Sigint automation - N-gram analysis is a fast, general method of sorting and retrieving machine-readable text according to language and/or topic. The N-gram system is claimed to work independently of the language used or the topic studied. NSA patented the method in 1995. (84)

26. To use N-gram analysis, the operator ignores keywords and defines the enquiry by providing the system with selected written documents concerning the topic of interest. The system determines what the topic is from the seed group of documents, and then calculates the probability that other documents cover the same topic. In 1994, NSA made its N-gram system available for commercial exploitation. NSA's research group claimed that it could be used on "very large data sets (millions of documents)", could be quickly implemented on any computer system and that it could operate effectively "in text containing a great many errors (typically 10-15% of all characters)".

27. According to former NSA Director William Studeman, "information management will be the single most important problem for the (US) Intelligence Community" in the future. (85) Explaining this point in 1992, he described the type of filtering involved in systems like ECHELON:

> *One [unidentified] intelligence collection system alone can generate a million inputs per half hour; filters throw away all but 6500 inputs; only 1,000 inputs meet forwarding criteria; 10 inputs are normally selected by analysts and only one report Is produced. These are routine statistics for a number of intelligence collection and analysis systems which collect technical intelligence.*

The "Data Workstation" Comint software system analyses up to 10,000 recorded messages, identifying Internet traccif, e-mail messages and attachments.

Speech recognition systems

28. For more than 40 years, NSA, ARPA, GCHQ and the British government Joint Speech Research Unit have conducted and sponsored research into speech recognition. Many press reports (and the previous STOA report) have suggested that such research has provided systems which can automatically select telephone communications of intelligence interest based on the use of particular "key words" by a speaker. If available, such systems would enable vastly more extensive Comint information to be gathered from telephone conversations than is available from other methods of analysis. The contention that telephone word-spotting systems are readily available appears to by supported by the recent availability of a string of low-cost software products resulting from this research. These products permit PC users to dictate to their computers instead of entering data through the keyboard. (86)

29. The problem is that for Comint applications, unlike personal computer dictation products, speech recognition systems have to operate in a multi-speaker, multi-language environment where numerous previously never heard speakers may each feature physiological differences, dialect variations, and speech traits. Commercial PC systems usually require one or more hours of training in order reliably to recognise a single speaker. Even then, such systems may mistranscribe 10% or more of the words spoken.

30. In PC dictation applications, the speaker can correct mistranscriptions and continually retrain the recognition system, making a moderate error rate acceptable. For use in Comint, where the interception system has no prior knowledge of what has been said (or even the language in use), and has to operate in the poorer signal environment of a telephone speech channel, such error rates are unachievable. Worse still, even moderate error rates can make a keyword recognition system worthless by generating both false positive outputs (words wrongly identified as keywords) and false negative outputs (missing genuine keywords).

31. This study has found no evidence that voice keyword recognition systems are currently operationally deployed, nor that they are yet sufficiently accurate to be worth using for intelligence purposes.

Continuous speech recognition

32. The fundamental technique in many speech recognition applications is a statistical method called Hidden Markov Modelling (HMM). HMM systems have been developed at many centres and are claimed academically to offer "good word spotting performance ... using very little or no acoustic speech training". (87) The team which reported this result tested its system using data from the US Department of Defense "Switchboard Data", containing recordings of thousand of different US telephone conversations. On a limited test the probabilities of correctly detecting the occurrences of 22 keywords ranged from 45-68% on settings which allowed for 10 false positive results per keyword per hour. Thus if 1000 genuine keywords appeared during an hour's conversation, there would be at least 300 missed key words, plus 220 false alarms.

33. At about the same time, (February 1990), the Canadian Sigint organisation CSE awarded a Montreal-based computer research consultancy the first of a series of contracts to develop a Comint wordspotting system. (88) The goal of the project was to build a word-spotter that worked well even for noisy calls. Three years later, CRIM reported that "our experience has taught us that, regardless of the environmental conditions, wordspotting remains a difficult problem". The key problem, which is familiar to human listeners, is that a single word heard on its own can easily be misinterpreted, whereas in continuous speech the meaning may be deduced from surrounding words.

CRIM concluded in 1993 that "it is probable that the most effective way of building a reliable wordspotter is to build a large vocabulary continuous speech recognition (CSR) system".

34. Continuous speech recognition software working in real time needs a powerful fast, processor. Because of the lack of training and the complex signal environment found in intercepted telephone calls, it is likely that even faster processors and better software than used in modern PCs would yield poorer results than are now provided by well-trained commercial systems. Significantly, an underlying problem is that voice keyword recognition is, as with machine-readable messages, an imperfect means to the more useful intelligence goal - topic spotting.

35. In 1993, having failed to build a workable wordspotter, CRIM suggesting "bypassing" the problem and attempting instead to develop a voice topic spotter. CRIM reported that "preliminary experiments reported at a recent meeting of American defense contractors ... indicate that this may in fact be an excellent approach to the problem". They offered to produce an "operational topic spotting" system by 1995. They did not succeed. Four years later, they were still experimenting on how to built a voice topic spotter. (89) They received a further research contract. One method CRIM proposed was NSA's N-gram technique.

Speaker identification and other voice message selection techniques

36. In 1993, CRIM also undertook to supply CSE with an operational speaker identification module by March 1995. Nothing more was said about this project, suggesting that the target may have been met. In the same year, according to NSA documents, the IDEAS company supplied a "Voice Activity Detector and Analyser", Model TE464375-1, to NSA's offices inside GCHQ Cheltenham. The unit formed the centre of a 14-position computer driven voice monitoring system. This too may have been an early speaker identification system.

37. In 1995, widely quoted reports suggested that NSA speaker identification had been used to help capture the drug cartel leader Pablo Escobar. The reports bore strong resemblance to a novel by Tom Clancy, suggesting that the story may have owed more to Hollywood than high tech. In 1997, the Canadian CRE awarded a contract to another researcher to develop "new retrieval algorithms for speech characteristics used for speaker identification", suggesting this method was not by then a fully mature technology. According to Sigint staff familiar with the current use of Dictionary, it can be programmed to search to identify particular speakers on telephone channels. But speaker identification is still not a particularly reliablr or effective Comint technique. (90)

38. In the absence of effective wordspotting or speaker identification techniques, NSA has sought alternative means of automatically analysing telephone communications. According NSA's classification guide, other techniques examined include Speech detection - detecting the presence or absence of speech activity; Speaker discrimination - techniques to distinguish between the speech of two or more speakers; and Readability estimation - techniques to determine the quality of speech signals. System descriptions must be classified "secret" if NSA "determines that they represent major advances over techniques known in the research community". (91)

"Workfactor reduction"; the subversion of cryptographic systems

39. From the 1940s to date, NSA has undermined the effectiveness of cryptographic systems made or used in Europe. The most important target of NSA activity was a prominent Swiss manufacturing company, Crypto AG. Crypto AG established a strong position as a supplier of code and cypher systems after the second world war. Many governments would not trust products offered for sale by major powers. In contrast, Swiss companies in this sector benefited from Switzerland's neutrality and image of integrity.

40. NSA arranged to rig encryption systems sold by Crypto AG, enabling UKUSA agencies to read the coded diplomatic and military traffic of more than 130 countries. NSA's covert intervention was arranged through the company's owner and founder Boris Hagelin, and involved periodic visits to Switzerland by US "consultants" working for NSA. One was Nora L MacKabee, a career NSA employee. A US newspaper obtained copies of confidential Crypto AG documents recording Ms Mackebee's attendance at discussion meetings in 1975 to design a new Crypto AG machine". (92)

41. The purpose of NSA's interventions were to ensure that while its coding systems should appear secure to other cryptologists, it was not secure. Each time a machine was used, its users would select a long numerical key, changed periodically. Naturally users wished to selected their own keys, unknown to NSA. If Crypto AG's

machines were to appear strong to outside testers, then its coding system should work, and actually be strong. NSA's solution to this apparent condundrum was to design the machine so that it broadcast the key it was using to listeners. To prevent other listeners recognising what was happening, the key too had also to be sent in code - a different code, known only to NSA. Thus, every time NSA or GCHQ intercepted a message sent using these machines, they would first read their own coded part of the message, called the "hilfsinformationen" (help information field) and extract the key the target was using. They could then read the message itself as fast or even faster than the intended recipient (93)

42. The same technique was re-used in 1995, when NSA became concerned about cryptographic security systems being built into Internet and E-mail software by Microsoft, Netscape and Lotus. The companies agreed to adapt their software to reduce the level of security provided to users outside the United States. In the case of Lotus Notes, which includes a secure e-mail system, the built-in cryptographic system uses a 64 bit encryption key. This provides a medium level of security, which might at present only be broken by NSA in months or years.

43. Lotus built in an NSA "help information" trapdoor to its Notes system, as the Swedish government discovered to its embarrassment in 1997. By then, the system was in daily use for confidential mail by Swedish MPs, 15,000 tax agency staff and 400,000 to 500,000 citizens. Lotus Notes incorporates a "workfactor reduction field" (WRF) into all e-mails sent by non US users of the system. Like its predecessor the Crypto AG "help information field" this device reduces NSA's difficulty in reading European and other e-mail from an almost intractable problem to a few seconds work. The WRF broadcasts 24 of the 64 bits of the key used for each communication. The WRF is encoded, using a "public key" system which can only be read by NSA. Lotus, a subsidiary of IBM, admits this. The company told Svenska Dagbladet:

> *"The difference between the American Notes version and the export version lies in degrees of encryption. We deliver 64 bit keys to all customers, but 24 bits of those in the version that we deliver outside of the United States are deposited with the American government".* (94)

44. Similar arrangements are built into all export versions of the web "browsers" manufactured by Microsoft and Netscape. Each uses a standard 128 bit key. In the export version, this key is not reduced in length. Instead, 88 bits of the key are broadcast with each message; 40 bits remain secret. It follows that almost every computer in Europe has, as a built-in standard feature, an NSA workfactor reduction system to enable NSA (alone) to break the user's code and read secure messages.

45. The use of powerful and effective encryption systems will increasingly restrict the ability of Comint agencies to process collected intelligence. "Moore's law" asserts that the cost of computational power halves every 18 months. This affects both the agencies and their targets. Cheap PCs can now efficiently perform complex mathematical calculations need for effective cryptography. In the absence of new discoveries in physics or mathematics Moore's law favours codemakers, not codebreakers.

Ordliste og definitioner

ATM	Asynchronous Transfer Mode; en hurtig form for digital kommunikation, der i stadig højere grad bruges på Internettet
BND	Bundesachrichtendienst; Forbundsrepublikken Tysklands efterretningstjeneste. Dens funktioner omfatter Sigint
CCITT	Consultative Committee for International Telephony and Telegraphy; FN-agentur, der udarbejder standarder og protokoller for telekommunikation; en del af ITU; kaldes også ITU-T
CEPT	Conference Europeene des Postes et des Telecommunications
CLID	Calling Line Identification Data
Comint	Comint Communications Intelligence

COMSAT	(Civil eller kommerciel) kommunikationsatellit; til brug for militær kommunikation vendes udtrykket ofte om, dvs. SATCOM.
CRIM	CRIM Centre de Recherche Informatique de Montreal
CSDF	CSDF Collected Signals Data Format; et udtryk, der kun anvendes i Sigint
CSE	CSE Communications Security Establishment, Canadas Sigint-bureau
CSS	CSS Central Security Service; NSAs militære komponent
DARPA	DARPA Defense Advanced Research Projects Agency (under USAs forsvarsministerium)
DGSE	Directorate General de Securite Exteriere, Frankrigs efterretningstjeneste. Dens funktioner omfatter Sigint
DSD	DSD Defence Signals Directorate, Australiens Sigint-bureau
DODJOCC	DODJOCC Department of Defense Joint Operations Centre Chicksands (Forsvarsministeriets Fællesoperationscenter i Chicksands)
E1, E3 (etc)	Standard for digitale TDM-kommunikaitonssystemer, defineret af CEPT og primært anvendt i Europa og uden for Nordamerika
ENFOPOL	EU-betegnelse for dokumenter vedrørende rethåndhævelsessager/politi
FAPSI	Federalnoe Agenstvo Pravitelstvennoi Svyazi i Informatsii, Ruslands forbundsstatslige agentur for regeringskommunikation og information. Dens funktioner omfatter Sigint
FBI	FBI Federal Bureau of Investigation; USAs nationale bureau for retshåndhævelse og kontraspionage
FDF	FDF Fast Data Finder
FDM	FDM Frequency Division Multiplex; en form for multikanal-kommunikation baseret på analoge signaler
FISA	FISA Foreign Intelligence Surveillance Act (USA) (loven om overvågning af udenlandske efterretninger)
FISINT	FISINT Foreign Instrumentation Signals Intelligence, Sigints 3. gren
Gbps	Gigabit pr. sekund
GCHQ	GCHQ Government Communications Headquarters; Storbritanniens Sigint-bureau
GHz	GigaHertz
Gisting (sammendrag)	I Sigint - den analytiske opgave hvor en ordret tekst erstattes med kommunikationens mening eller hovedpunkter
HDLC	HDLC High-level Data Link Control
HF	HF High Frequency; frekvenser fra 3 MHz til 30 MHz

HMM	HMM Hidden Markov Modelling, en udbredt teknik i talegenkendelsessystemer
ILETS	ILETS International Law Enforcement Telecommunications Seminar
Intelsat	International telekommunikationssatellit
IOSA	IOSA Interim Overhead Sigint Architecture (midlertidig overordnet Sigint-arkitektur)
Iridium	Satellite Personal Communications System med 66 satellitter i lave kredsløb om jorden, giver global kommunikation fra mobiltelefoner
ISDN	ISDN Integrated Services Data Network (digitalnet)
ISP	ISP Internet-serviceudbyder
ITU	ITU International Telecommunications Union
IUR	IUR International User Requirements (for kommunikationsaflytning); IUR 1.0 blev udarbejdet af ILETS (s.d.) i 1994
IXP	IXP Internet Exchange Point
LAN	LAN Local Area Network (lokalnet)
LES	LEA Law Enforcement Agency (amerikansk anvendelse)
Mbps	Megabit pr. sekund
MHz	MegaHertz
Microwave (mikrobølge)	Radiosignaler med bølgelængder på 10 cm eller kortere; frekvenser over 1 GHz
Modem	Modem til at sende data til og fra (fx) en computer; (en modulator-demodulator)
MIME	MIME Multipurpose Internet Message Extension; et system til at sende filer, billeder, dokumenter og programmer som "vedhæftninger" til en e-mail-meddelelse
N-gram analysis	Et system til analyse af tekstdokumenter - i denne sammenhæng et system til at matche en stor gruppe dokumenter til en mindre gruppe med et interessant emne. Metoden afhænger af at tælle den hyppighed, som karaktergrupper af længden N forekommer med i hvert dokument (deraf navnet N-gram)
NSA	NSA National Security Agency, USAs Sigint-bureau
OCR	Optical Character Recognition (optisk tegngenkendelse)
PC	Personlig computer
PCS	Personlige kommunikationssystemer - udtrykket omfatter mobiltelefonsystemer, personsøgersystemer og fremtidige fjern-radiodataforbindelser til pc'er, osv.
POP/ POP3	Post Office Program; et system der bruges til at modtage og opbevare e-mails

PTT	Posts Telegraph and Telephone (administration eller myndighed)
RAID	Redundant Array of Inexpensive Disks (diskarrays)
SCI	Sensitive Compartmented Intelligence; bruges til at begrænse adgang til Comint-information ifølge "rum"
SCPC	Single Channel Per Carrier; satellitkommunikationssystem med lav kapacitet
SMTP	Standard Mail Transport Protocol
Sigint	Signals Intelligence (signalefterretninger)
SONET	Synchronous Optical Network (synkront optisk netværk)
SMDS	Switched Multi-Megabit Data Service
SMO	Support for Military Operations (støtte til militære operationer)
SPCS	Satellite Personal Communications Systems (personlige satellitkommunikationssystemer)
SRI	Signal Related Information; et udtryk, der kun anvendes i Sigint
STOA	Science and Technology Assessments Office of the European Parliament; organet som har bestilt denne rapport
T1,T3 (etc)	Digital eller TDM kommunikationssystemer, der oprindeligt blev defineret af Bell-telefonsystemet i Nordamerika og primært anvendes der
TCP/IP	Terminal Control Protocol/Internet Protocol
TDM	Time Division Muliplex; en form for multikanal-kommunikation, der normalt baseres på digitale signaler
Traffic analysis	I Sigint, en metode til at analysere og hente efterretninger fra meddelelser på uden henvisning til deres indhold, fx ved at se på meddelelsernes oprindelse og bestemmelsessted for finde ud af forholdet mellem afsender og modtager, eller afsender- og modtagergrupper
UKUSA	Aftale mellem Storbritannien og USA
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal; satellitkommunikationssystem med lav kapacitet, der betjener private brugere og erhvervsbrugere
WAN	Wide Area Network (fjernnet)
WRF	Workfactor Reduction Field
WWW	World Wide Web
	X.25, V.21, V.34, V.90, V.100 (osv.) er telekommunikationsstandarder fastsat af CCITT

Noter

1.UKUSA henviser til aftalen fra 1947 mellem Storbritannien (UK) og USA vedrørende signalefterretninger. Landene i UKUSA-alliancen er USA ("First Party"), Storbritannien, Canada, Australien og New Zealand ("Second Parties").

2."An appraisal of the Technologies of Political Control", Steve Wright, Omega Foundation, European Parliament (STOA), 6. januar 1998.

3."They've got it taped", Duncan Campbell, New Statesman, 12. august 1988. "Secret Power : New Zealand's Role in the International Spy Network", Nicky Hager, Craig Potton Publishing, PO Box 555, Nelson, New Zealand, 1996.

4.National Security Council Intelligence Directive No 6, National Security Council of the United States, 17. februar 1972 (første gang udsendt i 1952).

5.SIGINT defineres i øjeblikket som COMINT, ELINT (elektroniske eller ikke-kommunikationsefterretninger og FISINT (udenlandske signalefterretninger fra instrumenter).

6.Erklæring fremsat af Martin Brady, direktør for DSD, 16. marts 1999. Sendtes i søndagsprogrammet, Channel 9 TV (Australien), maj 1999.

7."Farewell", meddelelse til alt personale i NSA, William Studeman, 8. april 1992. De to forretningsområder, som Studeman henviste til, var "øget global adgang" og "SMO" (støtte til militære operationer).

8. *Federalnoe Agenstvo Pravitelstvennoi Svyazi i Informatsii* , det (russiske) forbundsstatslige agentur for regeringskommunikation og -information. FAPSIs funktioner går ud over Comint og består også i at tilvejebringe regerings- og kommercielle kommunikationssystemer.

9.Privat kommunikation fra tidligere ansatte i NSA og GCHQ.

10.Sensitive Compartmented Intelligence.

11.Se note 1.

12. Privat kommunikation fra tidligere ansatte i GCHQ; den amerikanske lov er Foreign Intelligence Surveillance Act (FISA).

13. Se note 6.

14. I 1919 forsøgte kommercielle amerikanske kabelselskaber at modstå den britiske regerings krav om adgang til alle oversøiske telegrammer. 3 kabelselskaber aflagde forklaring over for det amerikanske Senat om denne praksis i december 1920. Samme år gennemførte den britiske regering lovgivning (Official Secrets Act, 1920, § 4), der gav adgang til alle eller enhver angivet kommunikationskategori. Samme beføjelse blev samlet igen i 1985, hvor der blev givet lovlig adgang i forbindelse med Comint-formål til al "ekstern kommunikation", defineret som enhver kommunikation, der sendes fra eller modtages uden for Storbritannien (Interception of Communication Act 1984, § 3(2)). Tilsvarende krav til teleoperatørerne er indeholdt i lovene i de øvrige UKUSA-lande. Se også "Operation SHAMROCK" (afsnit 3).

15."The Puzzle Palace", James Bamford, Houghton Mifflin, Boston, 1982, s. 331.

16.Personlig kommunikation fra tidligere ansatte hos NSA og GCHQ.

17."Dispatches : The Hill", sendt af Channel 4 Television (Storbritannien), 6. oktober 1993. DODJOCC stod for Department of Defense Joint Operations Centre Chicksands (Forsvarsministeriets Fællesoperationscenter i Chicksands).

18."The Justice Game", Geoffrey Robertson, Kapitel 5, Chatto and Windus, London, 1998

19.Fink-rapport til House Committee on Government Operations (Repræsentanternes Hus' Komité om regeringsoperationer), 1975, citeret i "NSA spies on the British government", New Statesman, 25. juli 1980

20."Amerikanskiye sputniki radioelektronnoy razvedki na Geosynchronnykh orbitakh" ("Amerikanske geosynkrone SIGINT-satellitter"), major A. Andronov, Zarubezhnoye Voyennoye Obozreniye, Nr. 12, 1993, ss. 37-43.

21."Space collection", i The US Intelligence Community (4. udgave), Jeffrey Richelson, Westview, Boulder, Colorado, 1999, ss. 185-191.

22.Se note 18.

23.Richelson, op cit.

24."UK Eyes Alpha", Mark Urban, Faber and Faber, London, 1996, ss. 56-65.

25.Bortset fra de nævnte stationer ligger der en stor jordstation, hvis mål tidligere omfattede sovjetiske kommunikationssatellitter, i Misawa, Japan. Mindre jordstationer er beliggende i Cheltenham, England og Shoal Bay, Australien.

26."Sword and Shield : The Soviet Intelligence and Security Apparatus", Jeffrey Richelson, Ballinger, Cambridge, Massachusetts, 1986.

27."Les Francais aussi ecountent leurs allies", Jean Guisnel, Le Point, 6. juni 1998.

28.Intelligence (Paris), 93, 15. februar 1999, s. 3.

29."Blind mans Bluff : the untold story of American submarine espionage", Sherry Sontag og Christopher Drew, Public Affairs, New York, 1998.

30.Ibid.

31.Ibid

32.Et eksemplar af IVY BELLS-aflytningsudstyret findes på det tidligere KGBs museum i Moskva. Det blev brugt på et kabel fra Moskva til en nærliggende videnskabelig og teknisk institution.

33.TCP/IP. TCP/IP står for Terminal Control Protocol/Internet Protocol. IP er Internettets grundlæggende netværkslag.

34.GCHQ websted på http://www.gchq.gov.uk/technol.html

35.Personlig kommunikation fra DERA. 1 Terabyte er et tusind Gigabyte, dvs. 1012 bytes.

36.Personlig kommunikation fra John Young.

37."Puzzle palace conducting internet surveillance", Wayne Madsen, Computer Fraud and Security Bulletin, juni 1995.

38.Ibid.

39."More Naked Gun than Top Gun", Duncan Campbell, Guardian, 26. november 1997.

40."Spyworld", Mike Frost and Michel Gratton, Doubleday Canada, Toronto, 1994.

41.The National Security Agency and Fourth Amendment Rights, Høringer ved et udvalg, der skulle undersøge regeringsoperationer vedrørende efterretningsaktiviteter, det amerikanske Senat, Washington, 1976.

42.Brev fra generalløjtnant Lew Allen, direktør for NSA til den amerikanske justitsminister Elliot Richardson, 4. oktober 1973; indeholdt i det tidligere dokument.

43.Privat kommunikation.

44.World in Action, Granada TV.

45.Dette arrangement synes at være et forsøg på at overholde lovmæssige begrænsninger i loven om kommunikationsaflytning (Interception of Communications Act 1985), der forbyder GCHQ at behandle meddelelser, bortset fra dem der er nævnt i "regeringscertifikater", der "beskriver det opsnappede materiale, som skulle undersøges". Loven bestemmer, at "den del af det opsnappede materiale, der ikke er godkendt i certifikatet, må ikke læses, ses på eller lyttes til af nogen person". Heraf fremgår det, at selvom alle meddelelser, der passerer igennem Storbritannien, opsnappes og sendes til GCHQs kontor i London, betragter organisation, at meddelelserne, når personale fra telefonselskabet British Telecom (BT) betjener ordbogscomputeren, stadig er under teleoperatørens kontrol, medmindre og indtil de vælges af ordbogen og overgår fra BT til GCHQ.

46.Privat kommunikation.

47."Naval Security Group Detachment, Sugar Grove History for 1990", den amerikanske flåde, 1. april 1991.

48.Missioner, funktioner og opgaver for Naval Security Group Activity (NAVSECGRUACT) Sugar Grove, West Virginia, NAVSECGRU INSTRUCTION C5450.48A, 3 September 1991.

49.Rapport om opgaver for Detachment 3 , 544 Air Intelligence Group, Air Intelligence Agency Almanac, det amerikanske flyvevåben, 1998-99.

50.Ibid, Detachment 2, 544 Air Intelligence Group.

51.Information indhentet af Bill Robinson, Conrad Grebel College, Waterloo, Ontario. CDF- og CFS-dokumenter blev fremskaffet i henhold

til loven om informationsfrihed (Freedom of Information Act) eller var offentliggjort på World Wide Web (WWW).

52.C.v. for Patrick D Duguay, offentliggjort på: http://home.istar.ca/~pdduguay/resume.htm

53.CSE Financial Status Report, 1. marts 1996, frigivet i henhold til loven om informationsfrihed (Freedom of Information Act). Yderligere oplysninger om "ECHELON' blev ikke givet. Det er derfor tvetydigt, om udgifterne var beregnet til ECHELON-computersystemet eller til andre funktioner (fx telekommunikation eller strømforsyning).

54."Secret Power", op cit.

55.Twenty/Twenty, TV3 (New Zealand), oktober 1999.

56.Interview med David Herson, chef for Senior Officers' Group on Information Security, EU, med medarbejdere hos Ingeniøren (Danmark), 25. september 1996. Offentliggjort på http://www.ing.dk/arkiv/herson.htm

57.Rådsbeslutning om lovlig aflytning af telekommunikation, 17. januar 1995, (96C_329/01)

58."International Harmonisation of Technical Requirements for Legal Interception of Telecommunications", Beslutning 1115, ITU Councils 10. plenarforsamling, Genève, 27. juni 1997.

59.ENFOPOL 98, Udkast til rådsbeslutning om telekommunikationsaflytning vedrørende ny teknologi, fremsat af det østrigske formandsskab. Bruxelles, 3. september 1998.

60.ENFOPOL 19, 13. marts 1999.

61.Europa-Parlamentet, 14. september 1998.

62."Uncle Sam's Eavesdroppers", Close Up North, BBC North, 3. december 1998; rapporteret i "Star Wars strikes back", Guardian, 3. december 1998

63."Dispatches : The Hill", Channel 4 Television (Storbritannien), 6. oktober 1993

64.Ibid.

65."Mixing business with spying; secret information is passed routinely to U.S.", Scott Shane, Baltimore Sun, 1. november 1996.

66."UK Eyes Alpha", op cit, p235.

67.Privat kommunikation.

68.Se note 62.

69.Raytheon Corp's pressemeddelelse: offentliggjort på: http://www.raytheon.com/sivam/contract.html

70."America's Fortress of Spies", Scott Shane og Tom Bowman, Baltimore Sun, 3. december 1995.

71."Company Spies", Robert Dreyfuss, Mother Jones, maj/juni 1994.

72.Financial Post, Canada, 28. februar 1998.

73.Europa-Parlamentet, 16. september 1998.

74.Se note 56.

75.Tilsvarende kommunikation kan gå under betegnelsen STM-signaler (Synchronous Transport Module) i Synchronous Digital Hierarchy (ITU-standard), STS (Synchronous Transport Signals) i det amerikanske SONET-system eller OC-signaler (Optical Carrier).

76.Informationen om disse Sigint-systemer er (udelukkende) hentet fra åbne kilder.

77.I april 1999 var den største datahastighed på MAE West mindre end 1,9 Gbps.

78.RAID (Redundant Arrays of Inexpensive Disks eller diskarray).

79.Very Small Aperture Terminal; SCPC er Single Channel Per Carrier.

80."Collected Signals Data Format"; defineret i det amerikanske Signals Intelligence Directive 126 og i NSAs CSDF-manual. To tilknyttede publikationer fra NSA, der indeholder yderligere orientering, er Voice Processing Systems Data Element Dictionary og Facsimile Data Element Dictionary, begge udsendt i marts 1997.

81.Edb-arbejdsstationen bearbejder TCP/IP, PP, SMTP, POP3, MIME, HDLC, X.25, V.100 samt modemprotokoller til og med V.42 (se ordliste).

82."Practical Blind Demodulators for high-order QAM signals", J R Treichler, M G Larimore og J C Harp, Proc IEEE, 86, 10, 1998, s. 1907. J R Treichler er teknisk direktør for AST. Dokumentet beskriver et system, der bruges til at opsnappe flere V.34-signaler og kan udvides til de nyere protokoller.

83.Opgaverne blev fastsat på den anden Text Retrieval Conference (TREC), der blev organiseret af ARPA og det amerikanske National Institute of Science and Technology (NIST), Gaithersburg, Maryland. Den 7. årlige TREC-konference blev afholdt i Maryland i 1999.

84."Method of retrieving documents that concern the same topic"; Amerikansk patentnummer 5418951, udstedt den 23. maj 1995; opfinder Marc Damashek; rettigheder overdraget til NSA.

85.Tale til Symposiet om "National Security and National Competitiveness : Open Source Solutions" ved viceadmiral William Studeman, vicedirektør for Central Intelligence og tidligere direktør for NSA, 1. december 1992, McLean, Virginia.

86.Fx IBM Via Voice, Dragon Naturally Speaking, Lemout og Hauspe Voice Xpress.

87."A Hidden Markov Model based keyword recognition system", R.C.Rose og D.B.Paul, Proceedings of the International Conference on Accoustics, Speech and Signal processing, april 1990.

88.Centre de Recherche Informatique de Montreal.

89."Projet detection des Themes", CRIM, 1997; offentliggjort på: http://www.crim.ca/adi/projet2.html .

90.Privat kommunikation.

91.NSA/CSS Classification Guide, NSA, ændret den 1. april 1983.

92."Rigging the game: Spy Sting", Tom Bowman, Scott Shane, Baltimore Sun, 10. december 1995.

93."Wer ist der Befugte Vierte?", Der Spiegel, 36, 1996, ss. 206-7.

94."Secret Swedish E-Mail Can Be Read by the U.S.A", Fredrik Laurin, Calle Froste, Svenska Dagbladet, 18. november 1997.

Yderligere oplysninger kan fås ved henvendelse til:
Schade-Sørensen, Helle
