EUROOPAN PARLAMENTTI

1999 *2004*

Echelon-sieppausjärjestelmää käsittelevä väliaikainen valiokunta

VÄLIAIKAINEN

18. toukokuuta 2001

KERTOMUSLUONNOS

Yksityistä ja talouselämän viestintää sieppaavan maailmanlaajuisen järjestelmän (Echelon-sieppausjärjestelmän) olemassaolo

Echelon-sieppausjärjestelmää käsittelevä väliaikainen valiokunta

Esittelijä: Gerhard Schmid

SISÄLTÖ

Sivu

ASIAN KÄSITTELY

Euroopan parlamentti päätti 5. heinäkuuta 2000 pitämässään istunnossa Echelon-sieppausjärjestelmää käsittelevän väliaikaisen valiokunnan perustamisesta. Väliaikainen valiokunta nimitti 5. heinäkuuta 2000 pidetyssä järjestäytymiskokouksessa tehtävänsä hoitamiseksi esittelijäksi Gerhard Schmidin.

Valiokunta käsitteli kertomusluonnosta ... ja ... pitämässään kokouksessa (pitämissään kokouksissa).

Viimeksi mainitussa kokouksessa se hyväksyi päätöslauselmaesityksen äänin ... puolesta, ... vastaan ja ... tyhjä(ä) / yksimielisesti.

Äänestyksessä olivat läsnä seuraavat jäsenet: ... (puheenjohtaja/puheenjohtajana), ... (varapuheenjohtaja), ... (varapuheenjohtaja), ... (esittelijä), ..., ... (... puolesta), ... (... puolesta työjärjestyksen 153 artiklan 2 kohdan mukaisesti), ... ja ....

Kertomus jätettiin käsiteltäväksi ....

Tarkistusten jättämisen määräaika ilmoitetaan sen istuntojakson esityslistaluonnoksessa, jonka aikana kertomusta käsitellään.

PÄÄTÖSLAUSELMAESITYS

Euroopan parlamentin päätöslauselma yksityistä ja talouselämän viestintää sieppaavan maailmanlaajuisen järjestelmän (Echelon-sieppausjärjestelmän) olemassaolosta

Euroopan parlamentti, joka

– ottaa huomioon Euroopan parlamentin 5. heinäkuuta 2000 tekemän päätöksen Echelon-sieppausjärjestelmää käsittelevän väliaikaisen valiokunnan asettamisesta ja sille asetetusta tehtävästä,

– ottaa huomioon EY:n perustamissopimuksen, jonka tarkoituksena on erittäin kilpailukykyisten yhteismarkkinoiden perustaminen,

– ottaa huomioon Euroopan unionista tehdyn sopimuksen, erityisesti sen 6 artiklan 2 kohdan, johon on kirjattu EU:n velvollisuus pitää arvossa perusoikeuksia, ja sen V osaston, jossa on määräyksiä yhteisestä ulko- ja turvallisuuspolitiikasta,

– ottaa huomioon EU:n perusoikeuskirjan, jonka 7 artiklassa määrätään oikeudesta yksityis- ja perhe-elämän kunnioittamiseen ja annetaan nimenomaisia määräyksiä viestien kunnioittamisesta,

– ottaa huomioon Euroopan ihmisoikeussopimuksen, erityisesti sen 8 artiklan, joka koskee yksityiselämän suojaamista, sekä lukuisat muut kansainväliset sopimukset, joissa määrätään yksityiselämän suojaamisesta,

– ottaa huomioon Echelon-sieppausjärjestelmää käsittelevän väliaikaisen valiokunnan kertomuksen yksityistä ja talouselämän viestintää sieppaavan maailmanlaajuisen järjestelmän (Echelon-sieppausjärjestelmän) olemassaolosta (A5-..../2001),

Yksityistä ja talouselämän viestintää sieppaavan maailmanlaajuisen järjestelmän (Echelon-sieppausjärjestelmän) olemassaolo

A. ottaa huomioon, että ei voida enää epäillä, että on olemassa maailmanlaajuisesti toimiva viestintäsieppausjärjestelmä, jonka toimintaan osallistuvat Yhdysvallat, Yhdistynyt kuningaskunta, Kanada, Australia ja Uusi-Seelanti UKUSA-sopimuksen puitteissa; pitää käytettävissä olevien viitteiden perusteella todennäköisenä, että sen peitenimi on todellakin Echelon, mutta viimeksi mainitulla on vain toissijainen merkitys,

B. toteaa, että järjestelmää käytetään yksityisen ja kaupallisen viestinnän, ei sotilaallisen viestinnän sieppaamiseen mutta kertomuksessa esitetty analyysi on osoittanut, ettei järjestelmän mahti voi olla läheskään niin suuri, kuin tiedotusvälineissä toisinaan oletetaan,

Sieppausjärjestelmän rajat

C. ottaa huomioon, että järjestelmä perustuu satelliittiviestinnän maailmanlaajuiseen sieppaukseen mutta alueilla, joilla viestintää on paljon, vain hyvin pieni osa viestinnästä

kulkee satelliittien kautta eikä suurinta osaa viestinnästä näin ollen voida siepata maa-asemien avulla vaan ainoastaan kaapeleita ja radioyhteyksiä salakuuntelemalla, mikä – kuten kertomukseen sisällytetyt tutkimukset ovat osoittaneet – on mahdollista vain hyvin tiukoissa rajoissa; ottaa huomioon, että siepatun viestinnän lopullinen hyväksikäyttö asettaa myös rajoituksia ja Echelon-valtioilla on siten pääsy vain hyvin pieneen osaan kaapeli- ja radioyhteyksiin perustuvasta viestinnästä ja ne voivat käyttää hyväksi vain pientä osaa viestinnästä,

Muiden sieppausjärjestelmien olemassaolon mahdollisuus

D. ottaa huomioon, että viestinnän sieppaaminen on tiedustelupalvelujen yleisesti käyttämä vakoilukeino ja myös muut valtiot voisivat pitää yllä vastaavanlaista järjestelmää, jos niillä on siihen riittävät taloudelliset ja maantieteelliset mahdollisuudet; ottaa huomioon, että Ranska pystyisi ainoana EU:n jäsenvaltiona pitämään jopa yksinään yllä maailmanlaajuista sieppausjärjestelmää ainakin maantieteellisten edellytysten puolesta merentakaisten alueidensa ansiosta ja että on lisäksi viitteitä siitä, että myös Venäjä voisi pitää yllä senkaltaista järjestelmää,

Yhteensopivuus EU:n oikeuden kanssa

E. ottaa huomioon, että arvioitaessa Echelonin kaltaisen järjestelmän yhteensopivuutta EU:n oikeuden kanssa on erotettava kaksi asiaa: Jos järjestelmää käytetään vain tiedustelupalvelutarkoituksiin, ristiriitaa EU:n oikeuden kanssa ei ole, koska valtion turvallisuutta palvelevat toiminnot eivät kuulu EY:n perustamissopimuksen soveltamisalaan. Ne kuuluisivat Euroopan unionista tehdyn sopimuksen V osaston (YUTP) alaan, mutta se ei toistaiseksi sisällä asiaa koskevia säädöksiä, joten kosketuskohdat puuttuvat. Jos järjestelmää sen sijaan käytetään kilpailuvakoiluun, järjestelmä on ristiriidassa jäsenvaltioiden välisen lojaliteettiperiaatteen sekä yhteismarkkinoiden ja vapaan kilpailun periaatteen kanssa; katsoo siihen osallistuvan jäsenvaltion siksi rikkovan EY:n oikeutta,

Tiedustelupalvelun harjoittaman viestinnän kuuntelun yhdenmukaisuus yksityisyyttä koskevan perusoikeuden kanssa (Euroopan ihmisoikeussopimuksen 8 artikla)

F. on tietoinen siitä, että kaikenlainen viestinnän kuuntelu merkitsee voimakasta puuttumista ihmisen yksityisyyteen ja että Euroopan ihmisoikeussopimuksen yksityisyyttä suojaavassa 8 artiklassa sallitaan yksityisyyteen puuttuminen ainoastaan kansallisen turvallisuuden takaamiseksi, jos säännökset on kirjattu kansalliseen lainsäädäntöön ja ne ovat yleisesti saatavilla ja jos niissä säädetään, missä oloissa ja millä ehdoilla valtiovalta saa toteuttaa kyseisiä toimia; ottaa huomioon, että yksityisyyteen puuttumisessa on lisäksi noudatettava suhteellisuutta ja siihen liittyvät hyötynäkökohdat on näin ollen arvioitava eikä Euroopan ihmisoikeustuomioistuimen oikeuskäytännön mukaan riitä, että toimenpiteet olisivat yksinkertaisesti hyödyllisiä tai toivottavia,

G. ottaa huomioon, että tiedustelupalvelujärjestelmä, jolla siepattaisiin mitä tahansa viestintää turvaamatta suhteellisuuden periaatteen noudattamista, ei olisi Euroopan ihmisoikeussopimuksen mukainen ja että Euroopan ihmisoikeussopimusta rikottaisiin myös siinä tapauksessa, että viestinnän kuuntelua säätelevällä säädöksellä ei ole

oikeusperustaa, se ei ole yleisesti saatavilla tai se on muotoiltu niin, ettei sen kansalaisille aiheuttamia seurauksia voida ennakoida; ottaa huomioon, että säännökset, joiden mukaan amerikkalaiset tiedustelupalvelut toimivat ulkomailla, ovat suurimmaksi osaksi salaisia, joten suhteellisuusperiaatteen toteutuminen on vähintäänkin kyseenalaista ja varmaankin rikotaan Euroopan ihmisoikeustuomioistuimen vahvistamia oikeussuojan saatavuuden ja vaikutusten ennakoitavuuden periaatteita,

H. ottaa huomioon, että jäsenvaltiot eivät voi välttää Euroopan ihmisoikeussopimuksesta johtuvia velvoitteita sallimalla alueellaan toimivat muiden valtioiden tiedustelupalvelut, joita eivät koske yhtä ankarat määräykset, sillä muuten laillisuusperiaate ja sen osa-alueet oikeussuojan saatavuus ja ennakoitavuus menettävät merkityksensä ja Euroopan ihmisoikeustuomioistuimen oikeuskäytännön sisältö vesittyy,

I. ottaa huomioon, että tiedustelupalvelujen lainmukaisen toiminnan yhteensovittaminen perusoikeuksien kanssa vaatii lisäksi riittäviä valvontajärjestelmiä vastapainoksi vaaralle, joka aiheutuu hallinnon osan salaisesta toiminnasta; ottaa huomioon, että Euroopan ihmisoikeustuomioistuin on nimenomaan korostanut tiedustelupalvelujen toiminnan tehokkaan valvontajärjestelmän merkitystä ja siksi tuntuu arveluttavalta, ettei kaikissa jäsenvaltioissa ole omia tiedustelupalvelujen parlamentaarisia valvontaelimiä,

Onko Euroopan unionin kansalaisilla riittävä suoja tiedustelupalvelujen toimintaa vastaan?

J. ottaa huomioon, että Euroopan unionin kansalaisten suoja riippuu yksittäisten jäsenvaltioiden oikeudellisesta tilanteesta, joka kuitenkin vaihtelee suuresti – kaikissa jäsenvaltioissa ei jopa ole lainkaan parlamentaarisia valvontaelimiä –, joten voidaan tuskin puhua riittävästä suojasta; ottaa huomioon, että Euroopan kansalaisten perustavan edun mukaista on, että kansallisissa parlamenteissa on virallisesti organisoitu valvontavaliokunta, joka seuraa ja valvoo tiedustelupalvelujen toimintaa; katsoo, että sielläkin, missä valvontaelimiä on, niillä on suuri houkutus huolehtia enemmän kotimaantiedustelupalvelujen kuin ulkomaantiedustelupalvelujen toiminnasta, koska yleensä vain ensin mainitut koskevat omia kansalaisia,

K. on tietoinen siitä, että jos tiedustelupalvelujen YUTP:n mukainen yhteistyö toteutuu, toimielinten on luotava riittävät Euroopan kansalaisia suojaavat määräykset,

Talousvakoilu

L. on tietoinen, että ulkomaantiedustelupalvelujen tehtäväkenttään kuuluu, että ne ovat kiinnostuneita taloudellisista tiedoista, jotka koskevat esimerkiksi alakohtaista kehitystä, raaka-ainemarkkinoiden kehitystä, kauppasaartojen noudattamista, kaksikäyttötuotteiden toimitussääntöjen noudattamista jne. Näistä syistä kyseisiä yrityksiä usein valvotaan salakuunnellaan,

M. katsoo, ettei voida hyväksyä, jos tiedustelupalvelut ryhtyvät kilpailuvakoilun välineiksi, niin että ne vakoilevat ulkomaisia yrityksiä hankkiakseen kilpailuetuja kotimaisille yrityksille, mutta katsoo, ettei ole todistettu yhtään tapausta, jossa maailmanlaajuista sieppausjärjestelmää olisi käytetty tähän tarkoitukseen, vaikka monia väitteitä on esitetty,

N. ottaa huomioon, että yrityksiä koskevat luottamukselliset tiedot pidetään monesti itse yrityksissä, joten kilpailijavakoilussa tietoja saadaan ennen kaikkea työntekijöiden tai solutettujen henkilöiden avulla tai tunkeutumalla sisäisiin tietoverkkoihin; ottaa huomioon, että kilpailijavakoilussa viestinnänkuuntelujärjestelmää voidaan käyttää vain silloin, kun luottamukselliset tiedot kulkevat yrityksen ulkopuolelle kaapeleita pitkin tai radioyhteyden (satelliittien) välityksellä ja tämä on aina tilanne ainoastaan seuraavissa kolmessa tapauksessa:

– yritykset, jotka toimivat kolmella aikavyöhykkeellä, niin että osavuositulokset lähetetään Euroopasta Amerikkaan ja edelleen Aasiaan
– monikansallisten konsernien videokokoukset, joissa käytetään V-Sat- tai kaapeliyhteyttä
– neuvottelut tärkeistä sopimuksista työmaalla (esimerkiksi tehdaslaitoksia, televiestintäinfrastruktuuria rakennettaessa tai uusia liikennejärjestelmiä rakennettaessa) ja kun sieltä käsin on saatava keskusteluyhteys yritykseen,

Suojautumismahdollisuudet

O. ottaa huomioon, että yritysten turvallisuus voidaan varmistaa ainoastaan, kun koko työskentely-ympäristö turvataan ja suojataan kaikki viestintäkanavat, joilla välitetään luottamuksellisia tietoja; ottaa huomioon, että Euroopan markkinoilla on riittävästi kohtuuhintaisia salausjärjestelmiä; katsoo, että myös yksityishenkilöitä on neuvottava salaamaan ehdottomasti sähköpostit ja salaamaton sähköposti on kuin ilman kirjekuorta lähetetty kirje; ottaa huomioon, että Internetissä on melko käyttäjäystävällisiä järjestelmiä, joita saa jopa ilmaiseksi yksityiskäyttöön,

Tiedustelupalvelujen yhteistyö EU:ssa

P. ottaa huomioon, että EU on sopinut tiedustelupalvelujen tiedonkeruun koordinoinnista osana oman turvallisuus- ja puolustuspolitiikan kehittämistä mutta samalla yhteistyön jatkamisesta muiden alan kumppaneiden kanssa,

Q. ottaa huomioon, että EU:ssa toimivien tiedustelupalvelujen yhteistyö vaikuttaa toivottavalta, koska ensinnäkin yhteinen turvallisuuspolitiikka, johon ei sisällytettäisi tiedustelupalveluja, olisi järjenvastaista ja toiseksi yhteistyöllä saavutettaisiin monia ammatillisia, taloudellisia ja poliittisia etuja; katsoo, että tämä vastaisi lisäksi paremmin ajatusta tasa-arvoisesta kumppanuudesta Yhdysvaltojen kanssa ja voisi sitoa kaikki jäsenvaltiot järjestelmään, joka olisi täysin Euroopan ihmisoikeussopimuksen mukainen; ottaa huomioon, että silloin on luonnollisesti varmistettava, että Euroopan parlamentilla on riittävät oikeudet valvoa yhteistyötä,

R. ottaa huomioon, että Euroopan parlamentti on parhaillaan laatimassa omia sääntöjä oikeudesta tutustua luottamuksellisiin ja arkaluonteisiin tietoihin ja asiakirjoihin,

Kansalaisten ja yritysten suojaamista koskevien kansainvälisten sopimusten tekeminen ja muuttaminen

1. kehottaa Euroopan neuvoston pääsihteeriä toimittamaan ministerikomitealle tutkimuksen siitä, olisiko aiheellista mukauttaa Euroopan ihmisoikeussopimuksen 8 artiklassa taattua yksityiselämän suojaa nykyaikaisiin viestintämenetelmiin ja kuuntelumahdollisuuksiin lisäpöytäkirjan avulla tai samalla, kun tietosuojasta annetaan sääntöjä tietosuojasta tehtyä yleissopimusta tarkistettaessa, edellyttäen että näin ei lasketa tuomioistuimen kehittämää oikeussuojan tasoa tai vähennetä uuteen kehitykseen mukautumisen edellyttämää joustavuutta;

2. kehottaa jäsenvaltioita luomaan eurooppalaisen foorumin, jossa tarkistetaan kirje- ja viestintäsalaisuuden takaamista koskevia sääntöjä, ja sopimaan lisäksi yhteisestä tekstistä, jossa taataan yksityiselämän suoja, sellaisena kuin se on määriteltynä Euroopan unionin perusoikeuskirjan 7 artiklassa, kaikille Euroopan kansalaisille jäsenvaltioiden koko alueella ja lisäksi taataan, että tiedustelupalvelut noudattavat toiminnassaan perusoikeuksia ja kertomuksen 8 luvussa, erityisesti 8.3.4 kohdassa olevia, Euroopan ihmisoikeussopimuksesta johdettuja ehtoja;

3. pyytää Euroopan neuvoston jäsenvaltioita tekemään lisäpöytäkirjan, jossa mahdollistetaan Euroopan yhteisöjen liittyminen Euroopan ihmisoikeussopimukseen, tai harkitsemaan muita toimenpiteitä, joilla voidaan ratkaista Strasbourgin ja Luxemburgin tuomioistuinten oikeuskäytännön väliset ristiriidat;

4. kehottaa YK:n pääsihteeriä pyytämään asiasta vastaavaa toimikuntaa esittämään ehdotuksia kansalaisoikeuksia ja poliittisia oikeuksia koskevan kansainvälisen yleissopimuksen yksityiselämän suojaa koskevan 17 artiklan mukauttamiseksi teknisiin uudistuksiin;

5. kehottaa Yhdysvaltoja allekirjoittamaan kansalaisoikeuksia ja poliittisia oikeuksia koskevan kansainvälisen yleissopimuksen, jotta yleissopimuksella perustettu ihmisoikeuskomitea voi ottaa käsiteltäväksi Yhdysvaltoja vastaan nostettuja yksittäisten henkilöiden valituksia sopimuksen rikkomisesta; pyytää alalla toimivia amerikkalaisia kansalaisjärjestöjä, erityisesti ACLU:a (American Civil Liberties Union) ja EPIC:iä (Electronic Privacy Information Center) painostamaan Yhdysvaltojen hallitusta asiassa;

Kansalliset lainsäädäntötoimet kansalaisten ja yritysten suojaamiseksi

6. vetoaa kaikkiin jäsenvaltioihin, jotta nämä tarkistavat oman tiedustelupalveluja koskevan lainsäädäntönsä yhteensopivuuden perusoikeuksien kanssa;

7. kehottaa jäsenvaltiota pyrkimään sellaiseen yhteiseen suojan tasoon tiedustelupalvelujen toimintoihin nähden, joka vastaa jäsenvaltioiden suojan korkeinta tasoa, koska ulkomaantiedustelupalvelun kohteena olevat kansalaiset ovat tavallisesti muiden valtioiden ja siten myös muiden jäsenvaltioiden kansalaisia;

8. kehottaa EU:n toimielimiä, jos tiedustelupalvelujen YUTP:n mukainen yhteistyö toteutuu, luomaan riittävät Euroopan kansalaisia suojaavat määräykset; katsoo, että Euroopan parlamentti on luonnollisesti valvontaelin, jonka on osaltaan luotava tarvittavat

edellytykset tämän erittäin herkän alueen valvonnalle, jotta tarvittavien valvontaoikeuksien vaatiminen olisi realistista ja perusteltua;

Erityiset oikeustoimet talousvakoilun torjumiseksi

9. kehottaa jäsenvaltioita pohtimaan, missä määrin talousvakoilua ja lahjontaa, jonka tarkoituksena on sopimusten hankkiminen, voitaisiin torjua yhteisön ja kansainvälisen oikeuden säännöksin, ja erityisesti, voitaisiinko WTO:ssa saada aikaan säännöt, joissa otetaan huomioon tällaisen toiminnan kilpailua vääristävä vaikutus siten, että tällaiset sopimukset todetaan mitättömiksi;

10. kehottaa jäsenvaltioita sitoutumaan yhteiseen yksiselitteiseen julistukseen, jonka mukaan ne pidättyvät toisiinsa kohdistuvasta talousvakoilusta, ja osoittamaan siten, että ne toimivat EY:n perustamissopimuksen hengen ja määräysten mukaisesti;

Toimet, jotka koskevat lainsäädännön soveltamista ja sen valvontaa

11. vetoaa kansallisiin parlamentteihin, joilla ei vielä ole omaa tiedustelupalveluja valvovaa parlamentaarista valvontaelintä, jotta ne perustaisivat sellaisen;

12. pyytää tiedustelupalvelujen kansallisia valvontavaliokuntia korostamaan voimakkaasti yksityisyyden suojaa käyttäessään niille myönnettyjä valvontavaltuuksia riippumatta siitä, onko kysymys omien kansalaisten, muiden EU:n kansalaisten vai yhteisön ulkopuolisten maiden kansalaisten valvonnasta;

13. vetoaa Saksaan ja Yhdistyneeseen kuningaskuntaan, jotta ne salliessaan Yhdysvaltojen tiedustelupalvelujen edelleen kuunnella viestintää alueillaan asettavat ehdoksi sen, että kyseiset toiminnot ovat Euroopan ihmisoikeussopimuksen mukaisia, ts. että ne ovat suhteellisuusperiaatteen mukaisia, niiden oikeusperusta on tiedossa, niiden vaikutukset yksittäisiin ihmisiin ovat nähtävissä ja että niitä valvotaan tehokkaasti; koska ne vastaavat alueellaan tiedustelupalvelujen ihmisoikeuksien mukaisesta tai vain siedettävästä toiminnasta;

Toimet kansalaisten ja yritysten omaehtoisen suojelun edistämiseksi

14. kehottaa komissiota ja jäsenvaltioita kehittämään ohjelmia, jotka lisäävät kansalaisten ja yritysten tietoisuutta turvallisuusongelmista ja tarjoavat samalla käytännön apua kattavien suojajärjestelmien suunnitteluun ja toteutukseen;

15. pyytää komissiota ja jäsenvaltiota laatimaan sopivia toimia eurooppalaisen salaustekniikan ja -ohjelmien edistämiseksi, kehittämiseksi ja valmistamiseksi sekä ennen kaikkea tukemaan hankkeita, jotka tähtäävät sellaisten käyttäjäystävällisten salausohjelmien kehittämiseen, joiden lähdekoodi on julkinen;

16. kehottaa komissiota ja jäsenvaltioita edistämään ohjelmistohankkeita, joissa ohjelmistojen lähdekoodi julkistetaan, sillä vain näin voidaan taata, ettei ohjelmistoihin rakenneta takaportteja (ns. open source -ohjelmistot);

17. vetoaa unionin toimielimiin ja jäsenvaltioiden julkishallintoihin sähköpostien järjestelmällisen salauksen käyttämiseksi, niin että salauksesta voisi pitkällä aikavälillä tulla normaali käytäntö;

Muut toimet

18. vetoaa yrityksiin vakoilun torjumisesta vastaavien yksikköjen kanssa tehtävän yhteistyön lujittamiseksi, erityisesti ulkopuolisten talousvakoiluun tähtäävien hyökkäysten ilmoittamiseksi viranomaisille, jotta niiden tehokkuutta voidaan näin parantaa;

19. kehottaa komissiota antamaan ehdotuksen yritysten tietojen turvaamiseen liittyviä kysymyksiä käsittelevän eurooppalaisen neuvontaelimen perustamisesta, jonka tehtäviin kuuluu ongelmasta tiedottaminen ja käytännön apu;

20. katsoo aiheelliseksi järjestää Euroopan laajuisen konferenssin yksityiselämän suojaamisesta televalvonnalta, jotta eurooppalaisille, yhdysvaltalaisille ja muiden valtioiden kansalaisjärjestöille saadaan foorumi, jossa voidaan keskustella rajat ylittävistä ja kansainvälisistä näkökohdista sekä koordinoida toiminta-aloja ja menettelyjä;

21. kehottaa puhemiestä välittämään tämän päätöslauselman neuvostolle, komissiolle, jäsenvaltioiden ja ehdokasvaltioiden hallituksille ja parlamenteille sekä Euroopan neuvostolle.

PERUSTELUT

1. Johdanto:

1.1. Valiokunnan nimittämisen syy

Euroopan parlamentti päätti 5. heinäkuuta 2000 asettaa Echelon-järjestelmää käsittelevän tilapäisen valiokunnan. Päätöksen syynä oli keskustelu STOA:n[1] teettämästä tutkimuksesta, joka käsitteli niin sanottua Echelon-järjestelmää[2] ja jonka laatija Duncan Campbell oli esitellyt kansalaisvapauksien ja -oikeuksien sekä oikeus- ja sisäasioiden valiokunnan kuulemisen yhteydessä. Kuulemisen aiheena oli "Euroopan unioni ja tietosuoja".

1.2. Molemmissa STOA:n tutkimuksissa esitetyt väitteet maailmanlaajuisesta sieppausjärjestelmästä, jonka peitenimi on Echelon

1.2.1. STOA:n ensimmäinen kertomus vuodelta 1997

Kertomuksessa, jonka STOA[3] oli teettänyt vuonna 1997 Omega-säätiöllä Euroopan parlamenttia varten ja jonka aiheena oli poliittiseen valvontaan käytettävien tekniikoiden arviointi, kuvattiin myös Echelonia luvussa "viestintätiedusteluun käytettävät kansalliset ja kansainväliset verkostot" Tutkimuksen laatija esitti siinä väitteen, jonka mukaan NSA (Yhdysvaltain kansallinen turvallisuuspalvelu) sieppaa Euroopassa rutiininomaisesti kaiken sähköposti-, puhelin- ja faksiviestinnän.[4] Kertomuksen myötä Echelon tuli kaikkialla Euroopassa tunnetuksi väitettynä maailmanlaajuisena, kaikenkattavana sieppausjärjestelmänä.

1.2.2. STOA:n kertomukset vuodelta 1999

Lisätietojen saamiseksi kyseisestä aihepiiristä STOA teetti vuonna 1999 viisiosaisen tutkimuksen, joka käsittelee "Tiedustelujärjestelmien sekä taloudellisen tiedon väärinkäytön riskien kehitystä". Duncan Campbellin laatimassa osassa 2/5 keskityttiin nykyisten tiedustelupalvelukapasiteettien ja erityisesti Echelonin[5] työskentelytavan tutkimiseen.

Erityistä ärtymystä aiheutti kertomuksessa esitetty väite, jonka mukaan Echelon ei enää palvele alkuperäistä tarkoitustaan, itää vastaan puolustautumista, ja sitä käytetään nykyisin talousvakoiluun. Väitteen tueksi kertomuksessa esitetään esimerkkejä väitetystä talousvakoilusta. Erityisesti Airbusin ja Thomsom CFS:n väitetään kärsineen siitä.

---

[1] STOA (Scientific and Technological Options Assessment, tieteellisten ja teknologisten vaihtoehtojen arviointi) on Euroopan parlamentin tutkimuksen pääosaston yksikkö, joka teettää tutkimuksia.

[2] The state of art in communications intelligence (COMINT) of automated processing for intelligence purposes of intercepting broadband multilanguage leased or common carrier system, and its applicability to COMINT argeting and selection, including speech recognition (October 1999). (Tiedustelutarkoitusta varten siepattujen laajakaistaisten monikielisten vuokrattujen tai yleisten teleyhteysjärjestelmien automatisoidun käsittelyn nykytila viestintätiedustelun kannalta ja sen soveltuvuus viestintätiedustelun kohdentamiseen ja valintaan puheentunnistus mukaan luettuna (lokakuu 1999).)

[3] Scientific and Technological Options Assessment, tieteellisten ja teknologisten vaihtoehtojen arviointi.

[4] Steve Wright, An appraisal of technologies for political control (1998), 20.

[5] Tiedustelutarkoitusta varten siepattujen laajakaistaisten monikielisten vuokrattujen tai yleisten teleyhteysjärjestelmien automatisoidun käsittelyn nykytila viestintätiedustelun kannalta ja sen soveltuvuus viestintätiedustelun kohdentamiseen ja valintaan puheentunnistus mukaan luettuna (lokakuu 1999), PE 168.184.

STOA:n tutkimuksen johdosta Echelonista keskusteltiin lähes kaikissa jäsenvaltioiden parlamenteissa. Ranskassa ja Belgiassa siitä laadittiin jopa mietintöjä.

1.3. Valiokunnan toimivalta

Asettaessaan määräaikaisen valiokunnan Euroopan parlamentti päätti myös sen toimivallasta. Päätöksen mukaan väliaikaisen valiokunnan toimivaltaan kuuluvat seuraavat tehtävät:

"– tutkia, onko olemassa Echelon-niminen viestintätiedustelujärjestelmä, jonka toimintaa kuvataan STOA:n teettämässä kertomuksessa valvontatekniikan sekä taloudellisen tiedon väärinkäytön riskin kehityksestä
– arvioida kyseisen järjestelmän yhteensopivuutta yhteisön lainsäädännön kanssa, erityisesti EY:n perustamissopimuksen 286 artiklan, direktiivien 95/46/EY ja 97/66/EY sekä Euroopan unionista tehdyn sopimuksen 6 artiklan 2 kohdan kanssa ottaen huomioon seuraavat kysymykset:
  – Onko unionin kansalaisten oikeudet turvattu tiedustelupalvelujen toimintaa vastaan?
  – Tarjoaako salaus riittävän suojan kansalaisten yksityisyyden takaamiseksi vai pitäisikö ryhtyä lisätoimenpiteisiin ja jos pitäisi, minkälaisiin?
  – Miten nämä vaarat voidaan saattaa paremmin EU:n toimielinten tietoisuuteen ja mihin toimenpiteisiin voidaan ryhtyä?
– todeta, onko maailmanlaajuinen tietojen sieppaus vaaraksi Euroopan teollisuudelle
– laatia tarvittaessa ehdotuksia poliittisiksi ja lainsäädäntöä koskeviksi aloitteiksi."

1.4. Miksi ei tutkintavaliokuntaa?

Euroopan parlamentti päätti asettaa väliaikaisen valiokunnan, koska tutkintavaliokunta voidaan EY:n perustamissopimuksen mukaan (193 artikla) asettaa vain tutkimaan yhteisön oikeuden rikkomuksia ja se voi näin ollen käsitellä vain yhteisön oikeuteen kuuluvia asioita. Sopimuksen V osastoon (YUTP) ja VI osastoon (poliisiyhteistyö ja oikeudellinen yhteistyö rikosasioissa) kuuluvat asiat ovat tutkintavaliokunnan toimivallan ulkopuolella. Tämän lisäksi tutkimusvaliokunnan erityiset edustajan nimeämistä ja asiakirjojen saantioikeutta koskevat valtuudet ovat toimielinten välisen päätöksen[1] mukaan voimassa vain, jollei salassapitoa taikka yleistä tai kansallista turvallisuutta koskevista seikoista kansallisen lainsäädännön mukaisesti muuta johdu. Tämä sulkisi tiedustelupalvelujen edustajien nimeämisen ilman muuta pois. Tutkintavaliokunta ei myöskään voi ulottaa työtään unionin ulkopuolisiin maihin, koska ne eivät luonnollisesti voi rikkoa EU:n lainsäädäntöä. Tutkintavaliokunnan asettaminen olisi siten merkinnyt vain sisällöllistä rajoitusta ilman lisäoikeuksia, ja siksi Euroopan parlamentin jäsenten enemmistö torjui sen.

1.5. Työmenetelmä ja työsuunnitelma

Valiokunta valitsi seuraavan toimintatavan toteuttaakseen tehtävänsä täysipainoisesti. Työohjelmassa, jota esittelijä ehdotti ja jonka valiokunta hyväksyi, oli lueteltu seuraavat olennaiset aihekokonaisuudet: 1. Echelonia koskevan tiedon varmistaminen, 2. keskustelut kansallisella parlamentti- ja hallitustasolla, 3. tiedustelupalvelut ja niiden toiminta, viestintäjärjestelmät ja niiden sieppausmahdollisuudet, 5. salaus, 6. talousvakoilu, 7. vakoilun tavoitteet ja suojatoimenpiteet sekä 8. oikeudelliset olosuhteet ja yksityisyyden suoja. Aiheet

[1] Euroopan parlamentin, neuvoston ja komission päätös, tehty 6 päivänä maaliskuuta 1995, Euroopan parlamentin tutkintaoikeuden käyttämistä koskevista yksityiskohtaisista säännöistä (95/167/EY), 3 artiklan 3–5 kohta.

käsiteltiin peräkkäin yksittäisissä istunnoissa, ja niiden järjestys määräytyi käytännön näkökohtien perusteella eikä siten kuvaa yksittäisten aihealueiden painotuksia. Yksittäisten istuntojen valmistelun yhteydessä esittelijä tarkasteli ja arvioi järjestelmällisesti käytettävissä olevaa aineistoa. Kokouksiin kutsuttiin kunkin painopistealueen vaatimusten mukaisesti kansallisten hallintoelinten (erityisesti tiedustelupalvelujen) edustajia sekä tiedustelupalvelujen valvontaeliminä toimivien parlamenttien edustajia. Lisäksi kutsuttiin oikeusasioiden sekä viestintä- ja sieppaustekniikan, yritysturvallisuuden ja salaustekniikan asiantuntijoita tieteen ja käytännön työn parista. Kokouksissa kuultiin myös toimittajia, jotka olivat tutkineet kyseistä aihetta. Kokoukset olivat yleensä avoimia, mutta toisinaan ne pidettiin suljetuin ovin, mikäli se vaikutti tiedonsaannin kannalta tarkoituksenmukaiselta. Tämän lisäksi valiokunnan puheenjohtaja ja esittelijä matkustivat yhdessä Lontooseen ja Pariisiin tapaamaan henkilöitä, jotka eri syistä eivät voineet osallistua valiokunnan kokouksiin mutta joiden osallistuminen valiokunnan työhön vaikutti kuitenkin tarkoituksenmukaiselta. Samoista syistä valiokunnan puheenjohtajisto, koordinaattorit ja esittelijä matkustivat Yhdysvaltoihin. Lisäksi esittelijä kävi lukuisia yksittäisiä keskusteluja, joista osa oli luottamuksellisia.

1.6. Echelon-järjestelmän väitetyt ominaisuudet

Echeloniksi kutsuttu sieppausjärjestelmä eroaa kaikista muista tiedustelupalvelujärjestelmistä. Se on laadultaan aivan omaa luokkaansa kahden ominaisuutensa ansiosta:
Ensinnäkin Echelonin sanotaan pystyvän käytännöllisesti katsoen täydelliseen valvontaan. Erityisesti satelliittivastaanottoasemien ja vakoilusatelliittien avulla sen väitetään pystyvän sieppaamaan kenen tahansa välittämän puhelin-, faksi-, internet- tai sähköpostiviestin, niin että sen sisällöstä päästään selville.

Toisena Echelonin ominaisuutena mainitaan, että järjestelmä toimii maailmanlaajuisesti useiden valtioiden (Yhdistyneen kuningaskunnan, Yhdysvaltojen, Kanadan, Australian ja Uuden-Seelannin) yhteistoiminnan ansiosta. Tämä merkitsee etua kansallisiin järjestelmiin verrattuna: Echelon-järjestelmään osallistuvat valtiot (Echelon-valtiot) voivat antaa sieppauslaitteistonsa toistensa käyttöön, vastata yhteisesti siitä syntyvistä kuluista ja hyödyntää saatuja tietoja yhdessä. Tämä kansainvälinen yhteistoiminta on välttämätöntä erityisesti maailmanlaajuisessa satelliittiviestinnän valvonnassa, koska vain siten voidaan varmistaa, että kansainvälisessä viestinnässä voidaan siepata keskustelun kummankin osapuolen viestit. On selvää, ettei satelliittivastaanottoasemia voida kokonsa vuoksi rakentaa jonkin valtion alueelle ilman sen suostumusta. Useiden eri puolilla maailmaa sijaitsevien valtioiden keskinäinen yhteisymmärrys ja yhteistoiminta on tässä välttämätöntä.

Echelonin kaltaisen järjestelmän yksityisyydelle tai taloudelle aiheuttamat mahdolliset uhat eivät kuitenkaan johdu vain siitä, että kyseessä on erityisen tehokas valvontajärjestelmä, vaan myös siitä, että se toimii jokseenkin lainsäädännön ulottumattomissa. Kansainvälisen viestinnän sieppausjärjestelmä ei yleensä kohdistu oman maan asukkaisiin. Sieppaustoiminnan kohteella ei ulkomaalaisena ole tällöin minkäänlaista valtion sisäistä oikeudellista suojaa. Yksilö on siten täysin järjestelmän armoilla. Parlamentaarinen valvonta on tällä alalla niin ikään riittämätöntä, koska äänestäjät olettavat, ettei asia koske heitä vaan "vain" muiden maiden ihmisiä, eivätkä ole erityisen kiinnostuneita siitä, ja poliitikot ajavat ennen kaikkea äänestäjiensä etuja. Ei olekaan ihme, että Yhdysvaltojen kongressissa pidetyissä NSA:n toimintaa koskevissa kuulemisissa käsitellään vain kysymystä siitä, koskeeko asia myös Yhdysvaltojen kansalaisia. Itse

järjestelmän olemassaolo ei sen sijaan herätä juurikaan keskustelua. On siis erityisen tärkeää käsitellä asiaa Euroopan tasolla.

2. Ulkomaantiedustelupalvelujen toiminta

2.1. Johdanto

Useimmat hallitukset pitävät maan turvallisuuden takaamiseksi poliisin lisäksi yllä myös tiedustelupalveluja. Koska niiden toiminta on useimmiten salaista, niistä käytetään myös nimitystä salainen palvelu. Näiden palvelujen tehtävänä on

– tietojen hankkiminen valtion turvallisuutta uhkaavien vaarojen torjumiseksi
– yleinen vastavakoilu
– asevoimia mahdollisesti uhkaavien vaarojen torjuminen
– tietojen hankkiminen muiden maiden asioista.

2.2. Mitä vakoilu on?

Hallituksilla on tarve kerätä ja arvioida järjestelmällisesti tietoja tietyistä muiden valtioiden asioista. Kysymys on lähinnä päätöksenteon perusteista asevoimien, ulkopolitiikan jne. alalla. Siksi valtiot pitävät yllä ulkomaantiedustelupalveluja. Tiedustelupalvelut analysoivat ensinnäkin järjestelmällisesti julkisia tiedonlähteitä. Esittelijän tietojen mukaan tämä muodostaa keskimäärin vähintään 80 prosenttia tiedustelupalvelujen toiminnasta.[1] Hallitukset ja yritykset pitävät kuitenkin erityisen merkittävät tiedot salassa, eivätkä ne siten ole yleisesti saatavilla. Jos kuitenkin haluaa päästä niihin käsiksi, ne on varastettava. Vakoilu ei ole muuta kuin organisoitua tietojen varastamista.

2.3. Vakoilun tavoitteet

Vakoilun perinteisiä kohteita ovat sotilasasioita koskevat salaisuudet ja muut valtionsalaisuudet sekä hallitusten vakautta tai horjuvuutta koskevat tiedot. Ne käsittelevät esimerkiksi uusia asejärjestelmiä, sotilaallisia strategioita tai joukkojen sijoittamista. Aivan yhtä tärkeitä ovat tiedot tulevista ulkopoliittisista tai valuuttaa koskevista ratkaisuista sekä hallituksen sisäisiä jännitteitä koskevat sisäpiirin tiedot. Myös taloudellisesti merkittävät tiedot ovat vakoilun kannalta kiinnostavia kohteita. Niihin voi kuulua toimialakohtaisten tietojen lisäksi myös uusia tekniikoita tai ulkomaisia liiketoimia koskevia yksityiskohtia.

2.4. Vakoilumenetelmät

Vakoilu merkitsee sellaisten tietojen hankkimista, joita niiden omistaja haluaa oikeastaan suojella ulkopuolisilta. Suoja on siis voitettava ja murrettava. Tämä koskee yhtä lailla poliittista vakoilua kuin talousvakoiluakin. Siksi kumpaakin vakoilun alaa koskevat samat ongelmat, ja siksi niillä käytetään myös samoja vakoilutekniikoita. Loogisesti eroa ei ole, mutta talouden alalla suojan taso on yleensä alhaisempi ja siksi talousvakoilu on monesti helpompaa. Erityisesti riskitietoisuus siepattavia viestintätekniikoita käytettäessä on taloudessa vähäisempää kuin valtion turvallisuusaloilla.

[1] "Commission on the Roles and Capabilities of the US Intelligence Community" totesi raportissaan "Preparing for the 21st Century: An Appraisal of U.S. Intelligence" että 95 % kaikesta taloudellisesta tiedusteluaineistosta on peräisin avoimista lähteistä (luku 2 "The Role of intelligence").

2.4.1. Ihmisten käyttäminen vakoilussa

Salaisten tietojen suoja on aina järjestetty samalla tavalla:
- Salainen tieto on vain harvojen ihmisten hallussa.
- Tietojen käsittelylle on vakiintuneet säännöt.
- Tietoja ei normaalisti siirretä pois suojatulta alueelta ja jos siirretään, se tapahtuu turvallisella tai salatulla tavalla. Siksi organisoidussa vakoilussa pyritään ensisijaisesti pääsemään **ihmisten** avulla ("human intelligence") käsiksi haluttuihin tietoihin suoraan ja ilman kiertoteitä. Tällöin kysymykseen tulevat
    - oman palvelun/yrityksen henkilöiden (agenttien) soluttaminen
    - kohdealueelta värvättyjen henkilöiden käyttäminen.

Värvätyt henkilöt työskentelevät vieraille palveluille/yrityksille useimmiten seuraavista syistä:
- seksuaalinen viettely
- lahjonta rahalla tai rahanarvoisilla eduilla
- kiristys
- ideologisiin syihin vetoaminen
- erityinen merkityksen tai kunnianosoituksen saavuttaminen (tyytymättömyyteen tai alemmuudentunteisiin vetoaminen).

Rajatapaus on tahaton yhteistyö, jossa viranomaisten tai yritysten työntekijät saadaan lavertelemaan näennäisen harmittomissa olosuhteissa esimerkiksi konferensseissa, alakohtaisissa kongresseissa tai hotellin baarissa käytävissä epävirallisissa keskusteluissa vetoamalla turhamaisuuteen tms.

Ihmisten käyttämisen etuna on, että haluttuihin tietoihin päästään käsiksi suoraan. Sillä on kuitenkin myös haittapuolia:
- Vastavakoilu keskittyy aina ihmisiin eli agentteihin.
- Värvättyjä henkilöitä käytettäessä ne heikkoudet, joiden avulla värväys toimi, voivat osoittautua bumerangiksi.
- Ihmiset tekevät aina virheitä ja jäävät siksi jossakin vaiheessa vakoiluntorjunnan verkkoon.

Agenttien tai värvättyjen henkilöiden käyttö pyritäänkin korvaamaan anonyymillä ja henkilöistä riippumattomalla vakoilulla aina kun se on mahdollista. Yksinkertaisinta on analysoida sotilaallisesti merkittävien laitosten tai ajoneuvojen radiosignaaleja.

2.4.2. Sähkömagneettisten signaalien analysointi

Julkisuudessa tunnetuin teknisin keinoin toteutettava vakoilun muoto on satelliittivalokuvauksen käyttö. Sen lisäksi siepataan ja arvioidaan kuitenkin kaikenlaisia sähkömagneettisia signaaleja (niin sanottu signal intelligence, SIGNINT)

2.4.2.1. Sähkömagneettiset signaalit, jotka eivät palvele viestintää

Tietyt sähkömagneettiset signaalit, esimerkiksi tutka-asemien säteet, voivat antaa sotilaallisesti arvokkaita tietoja vastustajan ilmapuolustuksen organisaatiosta (niin sanottu electronic intelligence, ELINT). Lisäksi sähkömagneettinen säteily, joka antaa tietoa joukkojen,

lentokoneiden, laivojen tai sukellusveneiden sijainnista, on tiedustelupalvelulle arvokas tietolähde. Merkittävää on myös muiden valtioiden kuvaavien vakoilusatelliittien seuraaminen ja niiden lähettämien signaalien tallentaminen ja koodinpurku.

Signaalit otetaan vastaan kiinteillä asemilla, matalalla kiertävillä satelliiteilla tai näennäisstaattisilla SIGINT-satelliiteilla. Tämä sähkömagneettisuuteen liittyvän tiedustelutoiminnan osa muodostaa määrällisesti merkittävän osuuden palvelujen sieppauskapasiteetista. Tekniikan käyttäminen ei kuitenkaan rajoitu tähän.

2.4.2.2. Siepatun viestintäaineiston analysointi

Monien valtioiden ulkomaantiedustelupalvelut kuuntelevat muiden valtioiden sotilas- ja diplomaattiviestintää. Monet näistä tiedustelupalveluista valvovat myös muiden valtioiden siviiliviestintää, jos pääsevät siihen käsiksi. Joissakin valtioissa palveluilla on oikeus valvoa myös omaan maahan tulevaa tai maasta lähtevää viestintää. Demokratioissa tiedustelupalvelujen harjoittamaa **omien** kansalaisten viestinnän valvontaa rajoittavat aina tietyt edellytykset asioihin puuttumiselle sekä kontrolli. Kansalliset säädökset suojaavat kuitenkin vain kansalaisia, jotka oleskelevat oman valtion alueella (ks. luku 8).

2.5. Eräiden tiedustelupalvelujen toiminta

Julkista keskustelua on herättänyt varsinkin Yhdysvaltojen ja Ison-Britannian tiedustelupalvelujen kuuntelutoiminta. Kritiikki on kohdistunut viestinnän (puheen, faksien ja sähköpostien) nauhoitukseen ja analysointiin. **Poliittinen** analyysi vaatii mittapuun, jota vasten tätä toimintaa voidaan arvioida. Vertailukohtana voidaan pitää EU:n ulkomaantiedustelupalvelujen kuuntelutoimintaa. Seuraavassa taulukossa 1 on esitetty yleiskuva. Siitä nähdään, ettei yksityisen viestinnän kuuntelu ole suinkaan Yhdysvaltojen tai Ison-Britannian ulkomaantiedustelupalvelun erikoisuus.

Maa	Ulkomainen viestintä	Valtion viestintä	Siviili-viestintä
Belgia	+	+	-
Tanska	+	+	+
Suomi	+	+	+
Ranska	+	+	+
Saksa	+	+	+
Kreikka	+	+	-
Irlanti	-	-	-
Italia	+	+	+
Luxemburg	-	-	-
Alankomaat	+	+	+
Itävalta	+	+	-
Portugali	+	+	-
Ruotsi	+	+	+
Espanja	+	+	+
Yhdistynyt kuningaskunta	+	+	+
Yhdysvallat	+	+	+

Kanada	+	+	+
Australia	+	+	+
Uusi-Seelanti	+	+	+

Taulukko 1: Tiedustelupalvelujen kuuntelutoiminta EU:ssa ja Echelon-valtioissa

Sarakkeiden merkitys:
Sarake 1: kyseinen maa
Sarake 2: ulkomaista viestintää kuunnellaan
Sarake 3: valtion viestintää (armeija, suurlähetystöt jne.) kuunnellaan
Sarake 4: siviiliviestintää kuunnellaan

3. Televiestinnän kuuntelun tekniset edellytykset

3.1. Eri viestintävälineiden kuunneltavuus

Kun ihmiset haluavat viestittää toisilleen tietyltä etäisyydeltä, tarvitaan viestintäväline. Se voi olla
– ilma (ääni)
– valo (morsetus, optinen lasikuitukaapeli)
– sähkövirta (lennätin, puhelin)
– sähkömagneettinen aalto (radio eri muodoissaan).

Jos kolmas osapuoli pääsee käsiksi viestintävälineeseen, hän voi kuunnella viestintää. Käsiksi pääseminen voi olla helppoa tai vaikeaa, se voi onnistua kaikkialta tai vain joistakin asemista. Seuraavassa käsitellään kahta ääritapausta: toisaalta paikan päällä toimivan vakoojan teknisiä mahdollisuuksia ja toisaalta maailmanlaajuisesti toimivan sieppausjärjestelmän mahdollisuuksia.

3.2. Kuuntelumahdollisuudet paikan päällä[1]

Paikan päällä voidaan kuunnella kaikkea viestintää, jos salakuuntelija on päättänyt rikkoa lakia eikä kuunneltava suojaudu.

– Huoneissa käytäviä **keskusteluja** voidaan kuunnella tilaan sijoitettujen mikrofonien (niin sanottujen luteiden) avulla tai havainnoimalla ikkunalasin värähtelyä laserlaitteella.

– **Näyttölaitteista** lähtee säteilyä, joka voidaan siepata jopa 30 metrin etäisyydeltä; näytön sisältö voidaan siten nähdä.

– **Puhelinta, faksia ja sähköpostia** voidaan kuunnella, jos salakuuntelija pääsee käsiksi rakennuksesta tuleviin kaapeleihin.

– **Matkapuhelinta** voidaan kuunnella enimmillään ..... kilometrin etäisyydeltä.

– **Yrityksen sisäistä radioverkkoa** voidaan kuunnella ULA-lähetysten kantaman sisällä.

Paikan päällä suoritettavassa vakoilussa teknisten välineiden käyttöolosuhteet ovat ihanteelliset, koska kuuntelutoimet voidaan rajata yhteen kohteeseen tai kohdehenkilöön ja käytännöllisesti katsoen kaikkia viestinnän muotoja voidaan kuunnella. Haittapuolena on vain tietty kiinnijäämisen riski "luteita" asennettaessa tai kaapeleita kuunneltaessa.

3.3. Maailmanlaajuisesti toimivan sieppausjärjestelmän mahdollisuudet

Mannertenväliseen viestintään on nykyisin käytettävissä erilaisia viestintävälineitä kaikille viestinnän lajeille (puhe, faksi ja data). Maailmanlaajuisesti toimivan sieppausjärjestelmän mahdollisuuksia rajoittaa kaksi tekijää:
– viestintävälineeseen käsiksi pääseminen on rajallista
– Kiinnostava viestintä on suodatettava valtavasta viestimäärästä.

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

3.3.1. Viestintävälineisiin käsiksi pääseminen

3.3.1.1. Kaapeliviestintä

Kaapeleita pitkin välitetään kaikkia viestinnän lajeja (puhetta, fakseja, sähköpostia ja dataa). Kaapeliviestintää voidaan kuunnella vain, kun kaapeleihin päästään käsiksi. Kuunteleminen on aina mahdollista kaapeliyhteyden päätepisteessä, jos se on kuunneltavissa olevan valtion alueella. Valtion sisällä voidaan siis kuunnella **teknisesti ajatellen** kaikkia kaapeleita, jos kuuntelu on oikeudellisesti sallittua. Ulkomaisilla tiedustelupalveluilla ei kuitenkaan useimmiten ole laillista pääsyä muiden valtioiden alueella sijaitseviin kaapeleihin. Laittomasti ne voivat päästä kaapeleihin käsiksi korkeintaan satunnaisesti, ja kiinni jäämisen riski on suuri.

Mannertenväliset kaapeliyhteydet on toteutettu lennätinaikakaudelta lähtien merenalaisten kaapelien avulla. Näihin kaapeleihin voidaan aina päästä käsiksi siellä, missä ne tulevat pois veden alta. Jos useampi valtio toimii yhdessä kuunteluliitossa, niillä on pääsy kaikkiin kaapeliyhteyksien päätepisteisiin, jotka sijaitsevat kyseisissä valtioissa. Tämä oli aikaisemmin merkittävää, koska Euroopan ja Amerikan väliset ensimmäiset lennätinkaapelit ja myös merenalaiset koaksiaaliset puhelinkaapelit nousivat merestä Newfoundlandissa (Kanadan valtion alueella) ja yhteydet kulkivat Aasiaan Australian kautta, koska tarvittiin välivahvistimia. Nykyisin optiset lasikuitukaapelit asennetaan suorinta tietä välittämättä merenalaisista vuoristoista ja välivahvistimien tarpeesta, eikä niitä viedä Australian tai Uuden-Seelannin kautta.

Sähköjohtoja voidaan havainnoida induktiivisesti myös yhteyden päätepisteiden välillä (toisin sanoen sähkömagneettisesti kaapeliin liitetyn käämin avulla) luomatta suoranaista sähköä johtavaa yhteyttä. Myös merenalaisia sähkökaapeleita voidaan suurin kustannuksin kuunnella tällä tavoin sukellusveneistä käsin. Yhdysvallat käytti tätä tekniikkaa Neuvostoliiton erään merenalaisen kaapelin kuuntelemiseen. Kaapelin kautta lähetettiin salaamattomia käskyjä venäläisille ydinsukellusveneille. Tekniikan laajamittainen käyttö on jo kustannussyistä mahdotonta.

Nykyisin käytössä olevissa vanhan sukupolven lasikuitukaapeleissa induktiivinen sieppaus on mahdollista vain välivahvistimien kohdalla. Välivahvistimet muuttavat optisen signaalin sähköiseksi signaaliksi, vahvistavat sitä ja muuttavat sen taas optiseksi signaaliksi. On tosin syytä kysyä, miten sellaisessa kaapelissa kulkevat valtavat tietomäärät kuljetettaisiin sieppauspaikalta analysointipaikalle asentamatta omaa lasikuitukaapelia. Sukellusveneessä olevan analysointitekniikan käyttäminen tulisi kustannussyistä kysymykseen vain hyvin harvinaisissa tapauksissa, esimerkiksi sodassa kuunneltaessa vihollisen strategista sotilasviestintää. Kansainvälisen televiestinnän rutiininomaisessa valvonnassa sukellusveneen käyttö ei esittelijän näkemyksen mukaan tule kysymykseen. Uuden sukupolven lasikuitukaapeleissa käytetään erbiumlaseria välivahvistimena – sähkömagneettinen kytkentä sieppausta varten ei tällöin ole enää mahdollista! Tällaisia lasikuitukaapeleita voidaan siis kuunnella vain yhteyden päätepisteistä!

Käytännössä tämä merkitsee niin sanottujen **Echelon-maiden** kuunteluliitolle, että ne voivat kuunnella merenalaisia kaapeleita kohtuullisin kustannuksin vain niiden päätepisteissä, jotka sijaitsevat kyseisten maiden alueella. Ne voivat siis kuunnella lähinnä vain sellaista kaapeliviestintää, joka tulee niiden alueelle tai lähtee sieltä! Tämä merkitsee, että **Euroopassa** ne

pääsevät käsiksi maahan tulevaan ja maasta lähtevään kaapeliviestintään vain **Yhdistyneen kuningaskunnan alueella!** Kotimainen viestintä on nimittäin toistaiseksi pidetty lähinnä maan sisäisessä kaapeliverkossa. Televiestinnän yksityistämisen myötä saattaa syntyä poikkeuksia – mutta ne ovat osittaisia eivätkä ne ole ennustettavissa!

Tämä koskee ainakin puhelinta ja faksia. Internetissä kaapelin kautta tapahtuvassa viestinnässä vallitsevat eri olosuhteet. Yhteenvetona voidaan kuitenkin todeta seuraavat rajoitteet:

- Internetissä viestintä kulkee datapaketteina, jolloin samalle lähettäjälle osoitetut paketit voivat kulkea verkossa erilaisia teitä.
- Internet-ajan alussa sähköpostin välittämiseen käytettiin julkisen tiedeverkoston käyttämätöntä kapasiteettia. Viestin tietä oli siten täysin mahdoton ennustaa, yksittäiset paketit kulkivat kaoottisia teitä, joita ei voinut tietää etukäteen. Tärkein kansainvälinen yhteys oli tuohon aikaan Euroopan ja Amerikan välinen "tiederunko".
- Kun Internet kaupallistui ja Internet-palveluntarjoajat vakiinnuttivat asemansa, seurasi myös verkon kaupallistuminen. Palveluntarjoajat pitivät yllä tai vuokrasivat omia verkkoja. Ne pyrkivät siten yhä voimakkaammin pitämään viestinnän oman verkkonsa sisällä välttääkseen muille verkonkäyttäjille maksettavat käyttömaksut. Datapaketin tie verkossa ei siksi riipu nykyisin vain verkon kuormituksesta, vaan siihen liittyy myös kustannusnäkökohtia.
- Sähköpostiviesti, joka lähetetään yhden palveluntarjoajan asiakkaalta toisen palveluntarjoajan asiakkaalle, pysyy yleensä yrityksen verkossa, vaikkei se olisikaan nopein tie. Datapaketin kuljetuksen ratkaisevat verkon solmukohtiin asetetut tietokoneet (reitittimet), jotka järjestävät siirron toiseen verkkoon tietyissä yhteyskohdissa (välityslaitteissa).
- Tiederungon aikoina maailmanlaajuisen Internet-viestinnän välityslaitteet sijaitsivat Yhdysvalloissa. Siksi sikäläiset tiedustelupalvelut pääsivät tuolloin käsiksi merkittävään osaan eurooppalaisesta Internet-viestinnästä. Nykyisin Euroopan sisäinen Internet-viestintä kulkee vain hyvin pieneltä osin Yhdysvaltojen kautta.
- Pieni osa Euroopan sisäisestä viestinnästä reititetään Lontoossa sijaitsevan välityslaitteen kautta, ja Ison-Britannian tiedustelupalvelulla GCHQ:lla on pääsy siihen. Pääosa viestinnästä pysyy mantereella. Esimerkiksi yli 95 prosenttia Saksan Internet-viestinnästä kulkee Frankfurtissa sijaitsevan välityslaitteen kautta.

Käytännössä tämä merkitsee, että Echelon-valtiot voivat päästä käsiksi vain **erittäin pieneen osaan** kaapelipohjaisesta Internet-viestinnästä.

3.3.1.2. Radioaaltopohjainen viestintä[1]

Radioaaltopohjaisen viestinnän siepattavuus riippuu käytettävien sähkömagneettisten aaltojen kantavuudesta. Jos lähetettävät radioaallot kulkevat maanpinnan suuntaisesti (niin sanottu **maa-aalto**), sen ulottuvuus on pienehkö ja riippuu maaston rakenteesta, rakennuksista ja kasvustosta. Jos radioaallot kulkevat kohti avaruutta (niin sanottu **avaruusaalto**), ne kantavat huomattavan pitkien matkojen päähän, kun aallot heijastuvat ionosfääristä. Moninkertainen heijastuminen lisää kantamaa huomattavasti.

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

Kantavuus riippuu aallonpituudesta:

- Pitkät ja erittäin pitkät aallot (3 kHz–300 kHz) leviävät vain maa-aaltona, koska avaruusaalto ei heijastu. Niillä on lyhyt ulottuvuus.
- Keskipitkät aallot (300 kHz–3 MHz) leviävät maa-aaltona ja öisin myös avaruusaaltona. Niillä on keskipitkä ulottuvuus.
- Lyhyet aallot (3 MHz–30 MHz) leviävät pääasiassa avaruusaaltona ja mahdollistavat moninkertaisen heijastumisen ansiosta **maailmanlaajuisen** vastaanoton.
- Ula-aallot (30 MHz–300 MHz) leviävät vain maa-aaltona, koska avaruusaalto ei heijastu. Ne leviävät suhteellisen suoraviivaisesti valon tavoin. Niiden kantama riippuu siten maan pyöreyden vuoksi lähettäjän ja vastaanottajan antennien korkeudesta. Niiden kantama on tehosta riippuen enimmillään noin 100 km (matkapuhelimilla noin 30 km).
- Desimetri- ja senttimetriaallot (30 MHz–30 GHz) leviävät ula-aaltojakin selvemmin valon tavoin. Ne on helppo keskittää, joten ne mahdollistavat suunnatut lähetykset pienellä teholla (maanpäälliset linkkiyhteydet). Ne voidaan ottaa vastaan vain antennilla, joka sijaitsee hyvin lähellä linkkiyhteyden suuntaisesti tai itse yhteydellä tai sen jatkolla.

Pitkiä ja keskipitkiä aaltoja käytetään vain radiolähettimissä, radiosignaalia lähettävissä hätälaitteissa jne. Sotilas- ja siviilikäyttöisessä radioviestinnässä käytetään lyhyitä aaltoja sekä ennen kaikkea ula-, desimetri- ja senttimetriaaltoja.

Edellä esitetystä ilmenee, että maailmanlaajuisesti toimiva viestintäsieppausjärjestelmä pääsee käsiksi vain lyhytaaltolähetyksiin. Kaikkia muita aaltoja käytettäessä sieppausaseman on oltava 100 kilometrin päässä tai lähempänä (esim. laivalla tai suurlähetystössä).

Käytännössä tämä merkitsee, että Echelon-valtiot pääsevät käsiksi vain hyvin pieneen osaan radioviestinnästä.

3.3.1.3. Geostationaarisen tietoliikennesatelliitin kautta välitettävä viestintä[1]

Kuten sanottu, desimetri- ja senttimetriaallot on helppo keskittää linkkiyhteyksiksi. Kun luodaan linkkiyhteys korkealla stationaarisessa tilassa olevaan viestintäsatelliittiin, joka ottaa mikroaaltosignaalin vastaan, muuntaa sen ja lähettää takaisin maan pinnalle, viestejä voidaan tällä tavoin välittää pitkien matkojen päähän ilman kaapelia. Tällaisen yhteyden kantamaa rajoittaa oikeastaan vain se, ettei satelliitti voi ottaa vastaan eikä lähettää signaalia maapallon toiselle puolelle. Siksi maailmanlaajuisen peiton aikaansaamiseksi käytetään useita satelliitteja (ks. tarkemmin luku 4). Jos Echelon-valtiot pitävät sieppausasemia yllä tarpeen vaatimilla maapallon alueilla, ne voivat periaatteessa siepata kaiken puhelin-, faksi- ja dataliikenteen, joka kulkee mainittujen satelliittien kautta.

3.3.1.4. Sieppausmahdollisuudet lentokoneista ja laivoista käsin

On jo pitkään tiedetty, että AWACS-mallisia lentokoneita käytetään muiden ilma-alusten kattavaan paikannukseen. Näiden lentokoneiden tutkaa käytetään havaittujen kohteiden tunnistamiseen. Tunnistamisessa käytetään järjestelmää, joka kykenee paikantamaan ja

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

luokittelemaan sähköistä säteilyä ja sovittamaan sen yhteen tutkayhteyksien kanssa. Lentokoneella ei ole erillistä SIGINT-kykyä.[1] Sen sijaan hitaasti lentävä Yhdysvaltojen laivaston vakoilulentokone EP-3 pystyy sieppaamaan mikro-, ula- ja lyhytaaltoja. Signaalit analysoidaan suoraan itse lentokoneessa, joka palvelee puhtaasti sotilaallisia tarkoituksia.[2]

Tämän lisäksi laivoja ja maan läheisyydessä olevia sukellusveneitä käytetään sotilasradioviestinnän sieppaamiseen.[3]

3.3.1.5. Sieppausmahdollisuudet vakoilusatelliiteista käsin

Jos radioaaltoja ei keskitetä siihen vaadittavilla antenneilla, ne säteilevät kaikkiin suuntiin, siis myös avaruuteen. Matalalla kiertävät viestintätiedustelusatelliitit voivat kuunnella tiedustelun kohteena olevia lähettimiä vain muutamia minuutteja kerrallaan. Tiheästi asutuilla, voimakkaasti teollistuneilla alueilla kuuntelu vaikeutuu lähettimien tiheyden vuoksi niin paljon, että yksittäisten signaalien erottaminen suodattamalla on lähes mahdotonta.[4] Nämä satelliitit eivät sovellu siviiliradioliikenteen jatkuvaan valvontaan.

Tämän lisäksi Yhdysvalloilla on korkealle (42 000 km) sijoitettuja niin sanottuja kvasistationaarisia SIGINT-satelliitteja.[5] Erona stationaarisiin viestintäsatelliitteihin on, että näiden satelliittien inklinaatio on 3–10 astetta, apogeum 39 000–42 000 km ja perigeum 30 000–33 000 km. Satelliitit eivät siten ole liikkumattomina maahan nähden, vaan ne liikkuvat monimutkaista elliptistä rataa pitkin. Siksi ne kattavat päivän kuluessa suuremman alueen ja mahdollistavat radiolähteiden jäljittämisen. Tämä ja muut julkisesti saatavilla olevat satelliittien ominaisuudet viittaavat puhtaasti sotilaalliseen käyttöön.

Vastaanotetut signaalit välitetään vastaanottoasemalle voimakkaasti yhteen pisteeseen keskitettynä 24 GHz:n taajuudella.

3.3.2. Siepatun viestinnän automaattisen analysoinnin mahdollisuudet: suodattimien käyttö

Ulkomaista viestintää kuunneltaessa ei valvota kohdistetusti tiettyä puhelinliittymää. Pikemminkin kaikki valvottavan satelliitin tai kaapelin kautta kulkeva viestintä tai osa siitä nauhoitetaan ja suodatetaan tietokoneilla käyttämällä avainkäsitteitä. Kaiken siepatun viestinnän analysointi on näet täysin mahdotonta.

Tiettyjen liittymien kautta kulkevan viestinnän suodattaminen on yksinkertaista. Avainkäsitteillä voidaan eritellä myös fakseja ja sähköpostiviestejä. Jopa tietty ääni voidaan tunnistaa, jos se on opetettu järjestelmälle.[6] Sen sijaan sanoja, jotka puhutaan millä tahansa äänellä, ei esittelijän saamien tietojen mukaan pystytä toistaiseksi tunnistamaan. Suodattamisen mahdollisuuksia rajoittavat lisäksi muut tekijät: tietokoneiden rajallinen kapasiteetti, kieliongelma ja ennen kaikkea suodatettuja viestejä lukevien ja analysoivien henkilöiden rajallinen määrä.

[1] Saksan puolustusministeriön kansliapäällikön Walter Kolbowin 14.2.2001 päivätty kirje.
[2] Süddeutsche Zeitung n:o 80, 5.4.2001, s. 6.
[3] Jeffrey T. Richelson, The U.S. Intelligence Community, Ballinger, New York 1989, s. 188, s. 190.
[4] Saksan puolustusministeriön kansliapäällikön Walter Kolbowin 14.2.2001 päivätty kirje.
[5] Majuri Andronov, Zarubezhnoye voyennoye obozreniye, n:o 12, 1993, s. 37–43.
[6] Yksityinen ilmoitus esittelijälle, lähde suojattu.

Suodatinjärjestelmien mahdollisuuksia arvioitaessa on myös otettava huomioon, että tällaisen "pölynimuriperiaatteella" toimivan sieppausjärjestelmän täydet tekniset mahdollisuudet jakautuvat eri aihealueille. Osa avainsanoista liittyy sotilaalliseen turvallisuuteen, osa huumekauppaan ja muihin kansainvälisen rikollisuuden muotoihin, osa on peräisin kaksikäyttötuotteilla käytävän kaupan käsitemaailmasta ja osa liittyy kauppasaartojen noudattamiseen. Osa avainkäsitteistä liittyy myös talouteen. Tämä merkitsee, että järjestelmän kapasiteetti jakautuu useille alueille. Avainsanojen rajaaminen pelkästään talouden kannalta kiinnostavalle alalle ei vastaisi poliittisen johdon tiedustelupalveluille asettamia vaatimuksia, eikä näin ole menetelty kylmän sodan päättymisen jälkeenkään.[1]

3.3.3. Esimerkki: Saksan tiedustelupalvelu

Saksan tiedustelupalvelun (Bundesnachrichtendienst, BND) osasto 2 hankkii tietoja kuuntelemalla ulkomaista viestintää. Tämä oli aiheena Saksan perustuslakituomioistuimen suorittamassa tarkastuksessa. Prosessissa julkisuuteen tulleista yksityiskohdista[2] sekä liittokanslerinvirastossa toimivan tiedustelupalvelujen koordinaattorin Ernst Uhrlaun 21.11.2000 Echelon-valiokunnassa esittämistä asioista saa käsityksen tiedustelupalvelun mahdollisuuksista satelliittiavusteisen viestinnän kuuntelussa.

Muiden tiedustelupalvelujen mahdollisuudet saattavat olla joidenkin yksityiskohtien osalta suuremmat, jos niillä on oikeus kuunnella kaapelipohjaista viestintää tai jos niillä on enemmän analysointihenkilökuntaa. Kaapeliviestinnän mukaan ottaminen lisää erityisesti tilastollista osumatodennäköisyyttä mutta ei välttämättä analysoitavien viestien määrää. Oikeastaan BND:n esimerkki osoittaa esittelijälle, mitä mahdollisuuksia ja strategioita ulkomaantiedustelupalveluilla on ulkomaisen viestinnän seuraamisessa, vaikkeivät tiedustelupalvelut niitä paljastakaan.

Saksan tiedustelupalvelu yrittää saada ulkomaita koskevia tietoja ulkomailta **strategisella** televiestinnän valvonnalla. Se merkitsee satelliittiliikenteen tutkimista hakukäsitteiden avulla (joille vaaditaan Saksassa ensin niin sanotun G10-komission[3] hyväksyntä). Määrä jakaantuu seuraavasti (vuoden 2000 tilanne): Saksasta ja Saksaan kulkee päivittäin 10 miljoonaa kansainvälistä viestintäyhteyttä, joista noin 800 000 satelliitin kautta. Hakukone suodattaa näistä vajaat 10 prosenttia (75 000 yhteyttä). Tämä rajoitus ei esittelijän näkemyksen mukaan johdu laista (teoriassa olisi saatu suodattaa 100 prosenttia ainakin ennen perustuslakituomioistuimessa käytyä prosessia) vaan teknisistä esteistä, esimerkiksi rajallisesta analysointikapasiteetista.

Myös käsiteltävien hakukäsitteiden määrää rajoittavat tekniset seikat ja hyväksymismenettely. Perustuslakituomioistuimen tuomion perusteluissa mainitaan puhtaasti muodollisten hakukäsitteiden lisäksi (Saksassa asuvien ulkomaalaisten ja siellä toimivien ulkomaisten yritysten liittymät) noin 2 000 hakukäsitettä asetekniikan leviämisen alalta, 1 000 käsitettä asekaupan alalta, 500 käsitettä terrorismin alalta ja 400 käsitettä huumekaupan alalta. Terrorismin ja huumekaupan osalta menettely tosin ei ole osoittautunut kovin menestyksekkääksi.

[1] Yksityinen ilmoitus esittelijälle, lähde suojattu.
[2] Saksan perustuslakituomioistuin BverfG, 1 BvR 2226/94, 14.7.1999, kohta 1.
[3] Saksan 13.8.1968 annettu kirje-, posti- ja televiestintäsalaisuutta rajoittava laki (perustuslain 10 artiklaan liittyvä laki).

Hakukone testaa, esiintyykö telekseissä ja fakseissa hyväksyttyjä hakukäsitteitä. Kieliyhdistelmien automaattinen sanantunnistus ei tällä hetkellä ole mahdollista. Jos hakukäsitteitä ei löydy, viestit joutuvat automaattisesti paperikoriin. Niitä ei saa analysoida, koska analysoinnille ei ole oikeudellista perustaa. Päivittäin tulee noin viisi televiestinnän osapuolten viestiä, jotka kuuluvat Saksan perustuslakisuojan piiriin. Saksan tiedustelupalvelun strategisessa selvitystyössä pyritään löytämään mosaiikkipalasia, jotka auttavat jatkoselvityksessä. Sen tavoitteena ei ole ulkomaisen viestinnän täydellinen valvonta. Esittelijän tietojen mukaan tämä koskee myös muiden ulkomaantiedustelupalvelujen SIGINT-toimintaa.

4. Satelliittiavusteisen viestinnän tekniikka

4.1. Tietoliikennesatelliittien merkitys

Tietoliikennesatelliitit ovat nykyisin olennainen osa maailman televiestintäverkkoa sekä radio-, tv- ja multimediapalveluja. Siitä huolimatta satelliittiliikenteen osuus kansainvälisestä viestinnästä on viime vuosina supistunut huomattavasti Keski-Euroopassa. Joillakin alueilla se on jopa alle 10 prosenttia[1] Tämä johtuu optisten lasikuitukaapelien eduista. Ne voivat ottaa vastaan valtavasti enemmän liikennettä, ja yhteyksien laatu on parempi.

Myös puheviestintä välitetään nykyisin digitaalisesti. Satelliittien kautta välitettyjen digitaalisten yhteyksien kapasiteetti rajoittuu ISDN-standardilla (64 kb/s) **1890** puhekanavaan satelliittitransponderia kohti. Yhtä ainoaa lasikuitua pitkin voidaan puolestaan nykyisin välittää jo **241 920** samaa standardia vastaavaa kanavaa. Suhde on **1:128**!

Lisäksi satelliittiyhteyden laatu on heikompi kuin lasikuituisen merikaapeliyhteyden. Laatupuutteet, jotka johtuvat signaalien usean sadan millisekunnin kulkuajoista, eivät juuri herätä huomiota tavallisessa puheen välityksessä – joskin ne pystyy kuulemaan. Data- ja faksiyhteyksissä, jotka toteutetaan monimutkaisen "kättelymenetelmän" avulla, kaapelin edut yhteysvarmuudessa ovat selvät. Tosin vain 15 prosenttia maailman väestöstä on yhteydessä maailmanlaajuiseen kaapeliverkkoon.[2]

Joissakin sovelluksissa satelliittijärjestelmillä on siis kaikesta huolimatta tulevaisuudessakin etuja kaapeliin nähden. Muutamia esimerkkejä siviilikäytön puolelta:

- kansallinen, alueellinen ja kansainvälinen puhelin- ja dataliikenne alueilla, jolla viestintätiheys on pieni, toisin sanoen siellä, missä kaapeliyhteyttä ei kannata toteuttaa alhaisen käyttöasteen vuoksi

- väliaikaiset viestintäyhteydet katastrofiavussa, tilaisuuksien järjestämisessä, suurilla rakennustyömailla jne.

- YK-tehtävät alueilla, joiden viestintäinfrastruktuuri on alikehittynyttä

- joustava/liikkuva taloutta koskeva viestintä, jossa käytetään erittäin pieniä maa-asemia (V-SAT, ks. jäljempänä).

Satelliittien käyttäminen viestinnässä tällaisissa kohteissa johtuu seuraavista ominaisuuksista: Yhden ainoan geostationaarisen satelliitin peittoalue pystyy kattamaan lähes 50 prosenttia maapallon pinnasta, eikä vaikeakaan maasto ole este. Tällä alueella lähetys kattaa käyttäjät lähes sataprosenttisesti, olivatpa he maalla, merellä tai ilmassa. Satelliitit ovat käyttövalmiina muutamassa kuukaudessa riippumatta paikallisesta infrastruktuurista, ne ovat luotettavampia kuin kaapeli ja ne on helpompi korvata.

[1] Ks. Saksan G10-lain muutoksen perustelut.
[2] Deutsche Telekomin kotisivu: www.detesat.com/deutsch/.

Kielteisinä voidaan pitää satelliittiavusteisen viestinnän seuraavia ominaisuuksia: suhteellisen pitkät signaalien kulkuajat, hitaampi eteneminen, lyhyempi käyttöikä kaapeliin verrattuna (12-15 vuotta), suurempi haavoittuvuus ja helpompi kuunneltavuus.

4.2. Satelliittiyhteyden toimintaperiaate

Kuten edellä todettiin (ks. luku 3), mikroaallot on helppo keskittää tarkoitukseen sopivilla antenneilla. Sen vuoksi kaapeli voidaan korvata radiolinkkiyhteydellä. Jos lähetys- ja vastaanottoantenni eivät ole samalla tasolla vaan pallon pinnalla, kuten maapallon tapauksessa, vastaanottoantenni "katoaa" kaarevuuden vuoksi horisontin taakse etäisyyden kasvaessa tiettyyn pisteeseen. Antenneilla ei ole enää näköyhteyttä. Tämä tilanne vallitsisi esimerkiksi Euroopan ja Yhdysvaltojen välisessä radiolinkkiyhteydessä. Antennien pitäisi olla 1,8 kilometrin korkuisissa mastoissa, jotta yhteys voitaisiin muodostaa. Jo tästä syystä tällainen mannertenvälinen radiolinkkiyhteys ei ole mahdollinen, vaikkei edes otettaisi huomioon signaalin vaimentumista matkalla ilman ja vesihöyryn vaikutuksesta. Jos radiolinkkiyhteydelle sen sijaan onnistutaan luomaan eräänlainen peili "kiinteään asemaan" korkealle avaruuteen, signaali voidaan lähettää pitkien matkojen päähän maan kaarevuudesta huolimatta samaan tapaan kuin liikennepeilillä voidaan nähdä kulman taakse. Edellä kuvattu periaate toteutetaan käyttämällä niin sanottuja geostationaarisia satelliitteja.

4.2.1. Geostationaariset satelliitit

Kun satelliitti pannaan kiertämään maapallo 24 tunnissa päiväntasaajan suuntaisesti pyöreää rataa pitkin, se seuraa täsmälleen maapallon pyörimisliikettä. Maan pinnalta katsottuna se on 36 000 km korkeudessa paikoillaan – se on **geostationaarisessa** asemassa. Useimmat tietoliikenne- ja tv-satelliitit kuuluvat tähän satelliittityyppiin.

4.2.2. Signaalin kulku satelliittiviestintäyhteydessä

Signaalien välitys satelliittien kautta voidaan kuvata seuraavasti:

Maa-asema lähettää kaapelia pitkin tulevan signaalin paraboliantennilla ylöspäin suunnatulla radiolinkillä (**"uplink"**) satelliitille. Satelliitti ottaa signaalin vastaan, vahvistaa sen ja lähettää sen alaspäin suunnatulla radiolinkillä (**"downlink"**) takaisen toiselle maa-asemalle. Sieltä signaali jatkaa matkaansa takaisin kaapeliverkkoon.

Matkaviestinnässä signaali välitetään suoraan matkaviestintäyksiköstä satelliittiin, josta se voidaan syöttää taas maa-aseman kautta kaapeliverkkoon tai suoraan toiseen matkaviestintäyksikköön.

4.2.3. Tärkeimmät satelliittiviestintäjärjestelmät

Yleisesti käytettävissä olevista (ei välttämättä valtion) kaapeliverkoista tuleva viestintä välitetään tarvittaessa erikokoisten satelliittijärjestelmien kautta kiinteiltä linkkiasemilta ja takaisin niille ja syötetään sitten taas kaapeliverkkoihin. Satelliittijärjestelmät jaetaan

– maailmanlaajuisiin (esim. INTELSAT)

– alueellisiin (mantereenlaajuisiin) (esim. EUTELSAT)

– kansallisiin (esim. ITALSAT)

satelliittijärjestelmiin.

Useimmat näistä satelliiteista ovat geostationaarisessa asemassa. Koko maailmassa 120 yksityistä yritystä pitää yllä noin 1 000 satelliittia[1].

Tämän lisäksi pohjoisimpia alueita varten on erittäin epäkeskisiä ratoja kiertäviä satelliitteja (Venäjän Molnyia-radat). Nämä satelliitit ovat puolet kiertoajastaan pohjoisten alueiden käyttäjien näköpiirissä. Kahdella satelliitilla saavutetaan alueellinen kattavuus, jota ei voida saavuttaa päiväntasaajan yläpuolelta geostationaarisesta asemasta käsin.

Tämän lisäksi on maailmanlaajuisesti toimiva – alun perin merellä käytettäväksi tarkoitettu – INMARSAT-**matkaviestintäjärjestelmä**, jonka avulla voidaan luoda satelliittipohjaisia yhteyksiä kaikkialla maailmassa. Sekin toimii geostationaaristen satelliittien avulla.

Maailmanlaajuisesti toimiva IRIDIUM-niminen satelliittimatkapuhelinjärjestelmä, joka toimi useiden matalilla radoilla eriaikaisesti kiertävien satelliittien avulla, lopetti hiljattain toimintansa taloudellisista syistä, koska sen käyttöaste ei ollut riittävä.

Lisäksi niin sanotuille VSAT-yhteyksille (VSAT = very small aperture terminal) on nopeasti kehittyvät markkinat. Kysymyksessä ovat erittäin pienet maa-asemat, joiden antennien halkaisija on 0,9–3,7 m. Yritykset käyttävät niitä omiin tarpeisiinsa (esimerkiksi videokonferensseihin) ja matkapuhelinoperaattorit väliaikaisiin yhteystarpeisiin (esimerkiksi kokoukset). Vuonna 1996 käytössä oli maailmanlaajuisesti 200 000 erittäin pientä maa-asemaa. Volkswagen AG pitää yllä 3 000:a, Renault 4 000:a, General Motors 100 000:a ja Euroopan suurin öljy-yhtiö 12 000:a VSAT-yksikköä. Viestintä kulkee avoimesti, ellei asiakas itse huolehdi salauksesta.[2]

4.2.3.1. Maailmanlaajuisesti toimivat satelliittijärjestelmät

Näillä satelliittijärjestelmillä on katettu koko maapallo sijoittamalla useita satelliitteja Atlantin, Intian ja Tyynen valtameren alueelle.

INTELSAT[3]

INTELSAT (International Telecomunications Satellite Organisation) perustettiin vuonna 1964 viranomaiseksi, jonka organisaatiorakenne muistutti YK:ta ja jonka toiminnan tarkoituksena oli kansainvälisen viestinnän harjoittaminen. Jäseninä oli valtion omistamia postilaitoksia. Nykyisin INTELSATin jäseninä on 144 hallitusta. INTELSAT yksityistetään vuonna 2001.

Nykyisin INTELSATilla on 19 geostationaarista satelliittia, jotka yhdistävät yli 200 maata ja joiden palveluja vuokrataan INTELSATin jäsenille. Jäsenet pitävät yllä omia maa-asemiaan. INTELSAT Business Servicen (IBS) kautta myös muut kuin jäsenet (esimerkiksi puhelinyhtiöt,

[1] G. Thaller, Satelliten im Erdorbit, Franzisverlag, München 1999.
[2] H. Dodel, yksityinen ilmoitus.
[3] INTELSAT:n kotisivu: http://www.intelsat.com.

suuryritykset, kansainväliset konsernit) ovat vuodesta 1984 lähtien voineet käyttää satelliitteja. INTELSAT tarjoaa maailmanlaajuisesti erilaisia palveluja, muun muassa viestintää ja televisiopalveluja. Televiestinnän välitys tapahtuu C- ja Ku-kaistalla.

INTELSAT-satelliitit ovat tärkeimpiä kansainvälisiä tietoliikennesatelliitteja. Niiden kautta kulkee suurin osa kansainvälisestä satelliittiavusteisesta viestinnästä. Satelliitit kattavat Atlantin, Intian ja Tyynen valtameren alueen (ks. luvun 5.3 taulukko).

Atlantin yllä on kymmenen satelliittia välillä 304°E–359°E, Intian alueen kattaa kuusi satelliittia välillä 62°E–110,5°E ja Tyynenmeren alueen kolme satelliittia välillä 174°E–180°E. Atlantin alueen suuri liikennetiheys katetaan alueen yllä olevilla monilla yksittäisillä satelliiteilla.

INTERSPUTNIK[1]

Vuonna 1971 yhdeksän maata perusti kansainvälisen satelliittiviestintäjärjestön INTERSPUTNIKin entisen Neuvostoliiton agentuuriksi. Sen tehtävä oli samantapainen kuin INTELSATinkin. Nykyisin INTERSPUTNIK on hallitustenvälinen järjestö, jonka jäsenenä voi olla jokaisen valtion hallitus. Sillä on nykyisin 24 jäsenvaltiota (muun muassa Saksa) ja noin 40 käyttäjää (muun muassa Ranska ja Iso-Britannia), joita edustavat niiden postilaitokset tai teleyhtiöt. Järjestön kotipaikka on Moskova.

Televiestintä välitetään C- ja Ku-kaistalla (ks. jäljempänä).

Nämäkin satelliitit (Venäjän federaation Gorizont, Express ja Express A sekä Lockhead-Martin -yhteisyrityksen LMI-1) kattavat koko maapallon: Atlantin alueella on yksi satelliitti ja toinen on suunnitteilla, Intian alueella on kolme satelliittia ja Tyynen valtameren alueella kaksi (ks. luvun 5.3 taulukko).

INMARSAT

INMARSAT (Interim International Maritime Satellite) on tarjonnut vuodesta 1979 satelliittijärjestelmällään maailmanlaajuista **matkaviestintää** maalla, merellä ja ilmassa oleville käyttäjille. Lisäksi se on tarjonnut hätäradiojärjestelmän. INMARSAT syntyi Kansainvälisen merenkulkujärjestön aloitteesta valtioiden väliseksi järjestöksi. Nyttemmin INMARSAT on yksityistetty, ja sen kotipaikka on Lontoo.

INMARSAT-järjestelmä koostuu yhdeksästä satelliitista, jotka ovat geostationaarisessa asemassa. Satelliiteista neljä – INMARSAT III -sukupolvi – kattaa koko maapallon äärimmäisiä napa-alueita lukuun ottamatta. Jokainen niistä kattaa noin kolmanneksen maan pinnasta. Satelliittien asema neljän valtameren alueella (Itä- ja Länsi-Atlantti, Tyyni valtameri, Intian valtameri) merkitsee, että ne kattavat koko maapallon. Lisäksi jokaisella INMARSATilla on "spot-beam"-alueet, mikä mahdollistaa energian keskittämisen alueille, joilla on suuri viestintätiheys.

Televiestintä välitetään L- ja Ku-kaistalla (ks. jäljempänä 4.2.4).

[1] INTERSPUTNIKin kotisivu: http://www.intersputnik.com.

4.2.3.2. Alueelliset satelliittijärjestelmät

Alueelliset satelliittijärjestelmät kattavat yksittäisiä alueita tai mantereita. Niiden välittämää viestintää voidaan näin ollen ottaa vastaan vain kyseisillä alueilla.

EUTELSAT[1]

EUTELSATin perustivat 17 eurooppalaista postilaitosta vuonna 1977. Tavoitteena oli kattaa Euroopan erityistarpeet satelliittiviestinnän osalta ja tukea eurooppalaista avaruusteollisuutta. Eutelsatin kotipaikka on Pariisi, ja sen jäseninä on noin 40 valtiota. EUTELSAT on tarkoitus yksityistää vuonna 2001.

EUTELSAT pitää yllä 18 geostationaarista satelliittia, jotka kattavat Euroopan, Afrikan ja suuren osan Aasiasta ja mahdollistavat yhteyden Amerikkaan. Satelliittien sijainti on välillä 12,5°W–48°E. EUTELSAT tarjoaa lähinnä tv- (850 digitaalista ja analogista kanavaa) ja radiopalveluja (520 kanavaa), mutta se palvelee myös viestintää – ennen kaikkea Euroopan sisällä (Venäjä mukaan luettuna), esimerkiksi videokonferensseja, suurten yritysten yksityisiä verkkoja (muun muassa General Motors ja Fiat), uutistoimistoja (Reuters, AFP), finanssitietojen tarjoajia sekä liikkuvan tiedonvälityksen tarpeita.

Televiestintä välitetään Ku-kaistalla.

ARABSAT[2]

ARABSAT on EUTELSATin vastine arabialueella. Se on perustettu vuonna 1976, ja sen jäseninä on 21 arabimaata. ARABSAT-satelliitteja hyödynnetään sekä tv-lähetyksiin että viestintään.

Televiestintä välitetään pääasiassa C-kaistalla.

PALAPA[3]

Indonesialainen PALAPA-järjestelmä on ollut käytössä vuodesta 1995 lähtien, ja se on Eutelsatin eteläaasialainen vastine. Se kattaa Malesian, Kiinan, Japanin, Intian, Pakistanin ja muita alueen maita.

Televiestintä välitetään C- ja Ku-kaistalla.

4.2.3.2. Kansalliset satelliittijärjestelmät[4]

Monet valtiot käyttävät kansallisten tarpeiden kattamiseen omia satelliittijärjestelmiä, joilla on pienehkö peittoalue.

[1] EUTELSATin kotisivu: http://www.com.
[2] ARABSATin kotisivu: http://www.arabsat.
[3] H.Dodel, Satellitenkommunikation, Hüthigverlag 1999.
[4] H. Dodel ja Internet-tutkimukset.

Ranskan televiestintäsatelliitti **TELECOM** palvelee muun muassa Ranskan afrikkalaisten ja eteläamerikkalaisten alueiden yhteyksiä emämaahan. Televiestintä välitetään C- ja Ku-kaistalla.

ITALSAT pitää yllä televiestintäsatelliitteja, jotka kattavat pienillä peräkkäisillä peittoalueillaan koko Italian saappaan. Vastaanotto on siten mahdollista vain Italiassa. Televiestintä välitetään Ku-kaistalla.

AMOS on israelilainen lähinnä kiinteään viestintään tarkoitettu satelliitti, jonka peittoalue kattaa Lähi-idän. Televiestintä välitetään Ku-kaistalla.

Espanjan **HISPASAT**-satelliitit kattavat Espanjan ja Portugalin (Ku-Spots) ja välittävät espanjalaista tv-ohjelmaa Pohjois- ja Etelä-Amerikkaan.

4.24. Taajuuksien jakaminen

Taajuuksien jakamisesta vastaa Kansainvälinen teleliitto. Tietyn järjestyksen aikaansaamiseksi maailma jaettiin radioviestintätarkoituksissa kolmeen alueeseen:

1. Eurooppa, Afrikka, entinen Neuvostoliitto, Mongolia

2. Pohjois- ja Etelä-Amerikka sekä Grönlanti

3. Aasia (lukuun ottamatta alueen 1 maita), Australia ja eteläinen Tyynimeri

Tämä historiallisen kehityksen tuloksena syntynyt jako omaksuttiin myös satelliittiviestinnän tarkoituksiin, ja se johtaa satelliittien keskittymiseen tietyille geostationaarisille vyöhykkeille.

Satelliittiviestinnän tärkeimmät taajuusalueet ovat

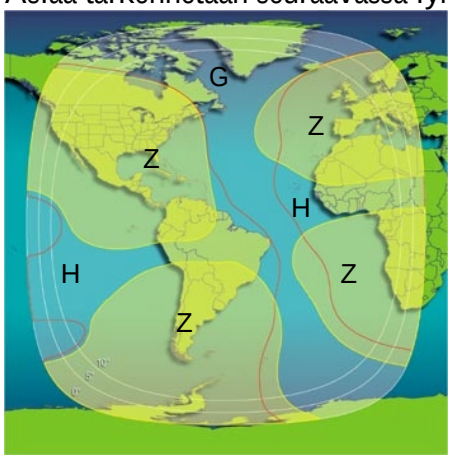
– L-kaista (0,4–1,6 GHz) matkaviestintää palvelevaa satelliittiviestintää varten esim. Inmarsatin kautta
– C-kaista (3,6–6,6 GHz) maa-asemia varten esim. Intelsatin kautta
– Ku-kaista (10–20 GHz) maa-asemia varten esim. INTELSAT-Ku-Spot ja EUTELSAT
– Ka-kaista (20–46 GHz) maa-asemia varten esim. kansallisille satelliiteille, kuten Italsatille
– V-kaista (46–56 GHz) erittäin pieniä maa-asemia varten (V-SAT).

4.2.5. Satelliittien peittoalueet (footprints)

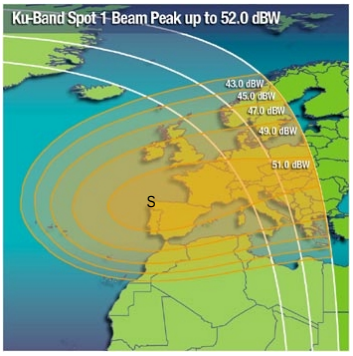
Peittoalueeksi ("footprint") nimitetään sitä aluetta, joka on satelliitin antennin lähetysalueella. Se voi kattaa enimmillään 50 prosenttia maapallon pinnasta tai se voidaan rajata pieniin alueellisiin kohteisiin keskittämällä signaali.

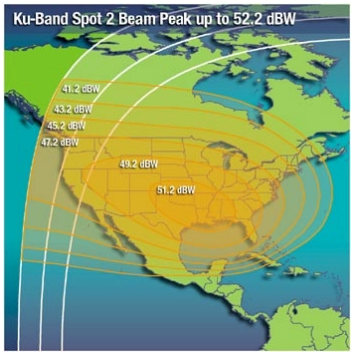
Mitä suurempi on lähetetyn signaalin taajuus, sitä tehokkaammin se voidaan keskittää ja sitä pienempi on näin ollen signaalin peittoalue. Keskittämällä satelliitin signaali pienemmälle peittoalueelle sen energiaa voidaan kasvattaa. Mitä pienempi peittoalue, sitä voimakkaampi signaali voi olla ja vastaavasti sitä pienemmät vastaanottoantennit tarvitaan.

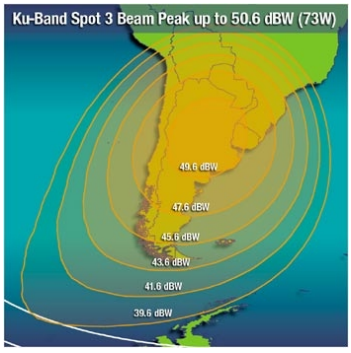
Asiaa tarkennetaan seuraavassa lyhyesti INTELSAT-satelliittien osalta:



INTELSAT-satelliittien peittoalueet on jaettu erilaisiin vyöhykkeisiin:
Kunkin satelliitin yleinen peittoalue ("global beam", G) kattaa noin kolmanneksen maapallon pinnasta,
Ns. hemi-beams-alueet (H) kattavat alueen, joka on hieman alle puolet global-beamin pinnasta. Zone-beams (Z) kattavat tietyt maapallon vyöhykkeet. Ne ovat pienempiä kuin hemi-beams-alueet. Näiden lisäksi on vielä niin sanotut spot-beams-alueet, jotka ovat pieniä, tarkkoja peittoalueita (ks. jäljempänä).







C-alueen taajuuksia on Global-, Hemi- ja Zone-Beam-alueilla. Spot-Beam-alueilla on Ku-alueen taajuuksia.

4.2.6. Maa-asemille tarvittavat antennikoot

Maanpäällisinä vastaanottoantenneina käytetään paraboliantenneja. Parabolipeili heijastaa kaikki tulevat aallot ja keskittää ne yhteen polttopisteeseen. Polttopisteessä sijaitsee varsinainen vastaanottojärjestelmä. Mitä suurempi signaalin energia on vastaanottopaikalla, sitä pienempi voi olla paraboliantennin halkaisija.

Tämän mietinnön yhteydessä suoritetun tutkimuksen tarkoituksen kannalta on ratkaisevaa, että osa mannertenvälisestä viestinnästä kulkee C-alueella Intelsat-satelliittien ja muiden satelliittien (esim. Intersputnikin) global-beam-alueilla. Tällöin vastaanottoon tarvitaan joissakin tapauksissa halkaisijaltaan noin 30-metrisiä satelliittilautasia (ks. luku 5). 30-metrisiä antenneja tarvittiin myös viestintäsatelliittien ensimmäisiin sieppausasemiin, koska ensimmäisen Intelsat-sukupolven aikana käytettiin vain global-beameja ja signaalin välitys oli vielä paljon kehittymättömämpää kuin nykyisin. Näitä lautasia, joista osa on halkaisijaltaan yli 30-metrisiä, käytetään edelleen omilla asemillaan, vaikkeivät ne olekaan teknisesti enää aivan välttämättömiä.

Tyypilliset antennit, joita tarvitaan nykyisin Intelsat-viestinnässä C-alueella, ovat halkaisijaltaan 13–18 m. Yksittäistapauksissa (esimerkiksi INTELSAT 511:ssä) tarvitaan suurempaa antennia global-beamia varten. Uusimmilla Intelsat-satelliiteilla C-kaistan zone-beam-alueillekin riittävät halkaisijaltaan enintään viisimetriset antennit.

Intersputnikin C-kaistaviestinnän vastaanottoon tarvitaan antenneja, joiden halkaisija on 2-25 metriä.

Intelsat-satelliittien mutta myös muiden satelliittien Ku-spotteihin (EUTELSAT-KU-kaista, Amosin Ku-kaista jne.) tarvitaan antenneja, joiden halkaisija on 2–10 metriä.

Pienimpiin maa-asemiin, jotka toimivat V-kaistalla ja joiden signaali voidaan suuren taajuuden ansiosta keskittää vielä voimakkaammin kuin Ku-kaistalla, riittää halkaisijaltaan 0,9–3,7 metrin antenni (esim. EUTELSATin tai INMARSATin).

5. Epäsuorat todisteet vähintään yhden maailmanlaajuisen sieppausjärjestelmän olemassaolosta

Miksi epäsuora todistusaineisto?

Tiedustelupalvelut eivät luonnollisesti paljasta työnsä yksityiskohtia. Siksi Echelon-valtioiden ulkomaantiedustelupalvelut eivät antaneet ainakaan virallista ilmoitusta siitä, että ne pitävät yhdessä yllä maailmanlaajuista sieppausjärjestelmää. Todiste on siksi löydettävä keräämällä mahdollisimman paljon aihetodisteita, joista muodostuu vakuuttava todistusaineisto.

Tällainen todisteaineisto koostuu seuraavista kolmesta aihetodiste-elementistä:

– Todiste siitä, että Echelon-valtioiden ulkomaantiedustelupalvelut sieppaavat yksityistä ja kaupallista viestintää.

– Todiste siitä, että niillä maapallon alueilla, jotka ovat välttämättömiä ei-sotilaallisen viestintäsatelliittijärjestelmän toiminnan kannalta, on Echelon-valtioiden ylläpitämiä sieppausasemia.

– Todiste siitä, että näiden valtioiden välillä on tiedustelupalveluja koskeva huomattavasti tavanomaista pitemmälle menevä liitto. Liiton olemassaolon kannalta on epäolennaista, meneekö se niin pitkälle, että kumppaneilta otetaan vastaan sieppaustoimeksiantoja ja siepattu raakamateriaali toimitetaan näille suoraan ilman omaa analysointia. Tällä kysymyksellä on merkitystä vain silloin, kun kysymys on sieppausliiton sisäisestä hierarkiasta.

5.1.1. Todiste ulkomaantiedustelupalvelujen sieppaustoiminnasta

Ainakin demokratioissa tiedustelupalvelut toimivat lakien pohjalta ja laeissa määritetään tiedustelupalvelujen tavoitteet ja/tai niiden valtuudet. On siten helppo todistaa, että useissa näistä valtioista on ulkomaantiedustelupalveluja, jotka sieppaavat siviiliviestintää. Tämä koskee myös viittä niin sanottua Echelon-valtiota, jotka kaikki pitävät yllä kyseisiä palveluja. Kunkin yksittäisen maan osalta ei tarvita lisätodisteita siitä, että ne sieppaavat maasta lähtevää ja maahan tulevaa viestintää. Oman maan alueelta on mahdollista siepata myös osa satelliittiviestinnästä, joka on tarkoitettu ulkomailla oleville vastaanottajille. Missään viidestä Echelon-valtiosta ei ole minkäänlaisia lainsäädännöllisiä rajoitteita, joiden perusteella tiedustelupalvelut eivät saisi tehdä sitä. Ulkomaisen televiestintäliikenteen strategisen valvonnan sisäinen logiikka ja sen ainakin osaksi julkinen tavoite antavat erittäin hyvän syyn olettaa, että tiedustelupalvelut todella toimivat niin.[1]

5.1.2. Todiste asemista maantieteellisesti välttämättömillä alueilla

Ainoa tekijä, joka rajoittaa yritystä rakentaa maailmanlaajuinen satelliittipohjaisen viestinnän valvontajärjestelmä, johtuu juuri kyseisen viestinnän tekniikasta. Mistään kohdasta ei voida siepata **kaikkea** satelliittiviestintää (ks. luku 4.2.5).

[1] Esittelijällä on tietoja, joiden mukaan asia on juuri näin. Lähde suojattu.

Maailmanlaajuisesti toimiva sieppausjärjestelmä voitaisiin rakentaa kolmen edellytyksen täyttyessä:

– Järjestelmän ylläpitäjävaltiolla on omia alueita kaikissa välttämättömissä maapallon osissa.

– Ylläpitäjällä on kaikissa välttämättömissä maapallon osissa osin omia alueita ja osin vierailuoikeus sekä oikeus pitää yllä ja käyttää asemia muissa tarvittavissa maapallon osissa.

– Ylläpitäjä on tiedustelupalveluun keskittyvä valtioiden liitto, joka pitää yllä järjestelmää välttämättömissä maapallon osissa.

Mikään Echelon-valtioista ei pystyisi pitämään yksin yllä maailmanlaajuista järjestelmää. Yhdysvalloilla ei ainakaan virallisesti ole siirtomaita. Kanadalla, Australialla ja Uudella-Seelannilla ei liioin ole omaa valtion aluetta maan varsinaisen alueen ulkopuolella. Yhdistynyt kuningaskuntakaan ei voisi yksin pitää yllä maailmanlaajuista järjestelmää (ks. luku 6).

5.1.3. Todiste tiiviistä tiedustelupalveluja koskevasta liitosta

Sen sijaan ei ole selvitetty, työskentelevätkö Echelon-valtiot tiedustelupalvelun alalla yhdessä ja millä tavoin. Yleensä tiedustelupalvelujen yhteistoiminta on kahdenvälistä ja perustuu analysoidun aineiston vaihtoon. Monenkeskinen liitto on jo hyvin epätavallinen. Jos lisäksi vaihdetaan säännöllisesti käsittelemätöntä aineistoa, kysymys on aivan uudenlaisesta toiminnasta. Tämänkaltaisen liiton olemassaolo voidaan osoittaa vain aihetodisteiden avulla.

5.2. Miten satelliittiviestinnän sieppausasema tunnistetaan?

5.2.1. Kriteeri 1: laitokseen pääsy

Postin, radioiden ja tutkimuslaitosten suurilla antenneilla varustetut asemat ovat vierailijoille avoimia ainakin, jos nämä ilmoittautuvat etukäteen. Sen sijaan sieppausasemat eivät ole avoimia. Ne ovat yleensä muodollisesti armeijan ylläpitämiä, ja armeija myös suorittaa sieppaamisen teknisesti. Esimerkiksi Naval Security Group (NAVSECGRU) ja Yhdysvaltojen ilmavoimien Air Intelligence Agency (AIA) vastaavat asemien käytöstä NSA:n puolesta. Britannialaisia asemia käyttää Royal Airforce Britannian tiedustelupalvelun GCHQ:n puolesta. Tämä järjestely takaa laitoksen tiukan valvonnan ja auttaa samalla toiminnan peittämisessä.

5.2.2. Kriteeri 2: antennien ominaisuudet

Kriteerin 1 täyttävissä laitoksissa on erilaisia antenneja, jotka eroavat toisistaan luonteeltaan. Niiden muoto kertoo laitteiden käyttötarkoituksesta. Esimerkiksi korkeiden sauva-antennien ympyränmuotoisia ryhmiä (niin sanottuja wullenweber-antenneja) käytetään radiosignaalien suunnan määrittämiseen. Tätä tarkoitusta palvelevat myös ympyrämäisesti ryhmitetyt vinoneliön muotoiset antennit (niin sanotut pusher-antennit). Kaikista suunnista tulevien signaalien vastaanottoon tarkoitettuja antenneja (suuntausantennit), jotka näyttävät valtavilta perinteisiltä tv-antenneilta, käytetään suuntaamattomien radiosignaalien sieppaukseen. **Satelliittisignaalien**

vastaanottoon käytetään sen sijaan pelkästään paraboliantenneja. Jos paraboliantennit sijaitsevat avoimesti maastossa, niiden sijaintipaikan, korkeuskulman ja suuntakulman avulla voidaan laskea, minkä satelliitin lähetyksiä ne ottavat vastaan. Tämä olisi mahdollista esimerkiksi Ison-Britannian Morwenstowissa sekä Yhdysvaltojen Yakimassa ja Sugar Grovessa. Useimmiten paraboliantennit ovat kuitenkin pallonmuotoisten valkoisten suojusten (niin sanottujen radomien) peitossa. Ne suojaavat antenneja mutta peittävät myös niiden suuntauksen.

Jos sieppausaseman alueella on paraboliantenneja tai radomeja, asemalla otetaan varmasti vastaan satelliittien signaaleja. Tämän perusteella ei tosin vielä tiedetä, minkälaisista signaaleista on kysymys.

5.2.3. Kriteeri 3: antennin koko

Kriteerin 1 täyttävien laitosten satelliittivastaanottoantenneja voidaan käyttää erilaisiin tarkoituksiin:
– sotilaallisen viestinnän vastaanottoasemat
– vakoilusatelliittien vastaanottoasemat (kuvat, tutka)
– sotilaallisten SIGINT-satelliittien vastaanottoasemat
– ei-sotilaallisten viestintäsatelliittien vastaanottoasemat.

Antenneista tai suojuksista (radomeista) ei näe ulkoapäin, mihin tarkoitukseen niitä käytetään. Tosin antenneilla, joilla otetaan vastaan satelliittipohjaisen kansainvälisen ei-sotilaallisen viestinnän yleistä peittoaluetta ("global beam") C-kaistalla, on tietyt tekniset vähimmäiskoot. Näiden satelliittien ensimmäistä sukupolvea käytettäessä tarvittiin halkaisijaltaan noin 25–30 metrin antenneja, nykyisin riittää 15–18 metrin halkaisija. Siepattujen signaalien automaattinen tietokonesuodatus vaatii mahdollisimman hyvää laatua, joten tiedustelupalvelun tarkoituksiin valitaan suurehko antennikoko. Koska antennit on asennettu telineille, suojusten halkaisija on vielä suurempi kuin antennien.

5.2.4. Johtopäätös

Esittelijän tietojen mukaan tämänkokoisille antenneille ei ole mitään sotilaallista käyttöä. Jos niitä siis havaitaan kriteerin 1 täyttävillä asemilla, siellä siepataan ei-sotilaallista satelliittiviestintää.

5.3. Julkisesti saatavilla olevat tiedot tunnetuista kuunteluasemista

5.3.1. Menetelmä

Sen selvittämiseksi, mitkä asemat täyttävät kappaleessa 5.2 mainitut kriteerit ja ovat osa maailmanlaajuista kuuntelujärjestelmää ja mitä tehtäviä niillä on, arvioitiin asiaa koskevaa,

osaksi keskenään ristiriitaista, kirjallisuutta (Hager[1], Richelson[2], Campbell[3]), asiakirjoja, joita ei enää ole luokiteltu salaisiksi[4], Federation of American Scientists -yhdistyksen kotisivua[5] sekä toiminnan harjoittajien[6] (NSA, AIA ym.) kotisivuja ja muita Internetin julkaisuja. Lisäksi koottiin viestintäsatelliittien peittoalueet, laskettiin antennien tarvittava koko ja sijoitettiin ne mahdollisten asemien kanssa maailman kartalle.

5.3.2. Tarkka analyysi

Arviointia koskevat seuraavat satelliittiviestinnän fysiikkaan liittyvät periaatteet (katso myös kappale 4):

– Satelliittiantenni voi ottaa vastaan vain sen, mikä on antennin senhetkisellä peittoalueella. Pääasiassa C- tai Ku-alueella tapahtuvan viestinnän vastaanottamiseksi antennin on sijaittava niiden peittoalueiden sisällä, jotka sisältävät C- tai Ku-alueen.
– Jokaista yleistä peittoaluetta varten tarvitaan yksi satelliittiantenni, myös siinä tapauksessa että kahden satelliitin peittoalueet ovat päällekkäin.
– Jos satelliitilla on useampia peittoalueita kuin yleinen peittoalue, yhdellä ainoalla satelliittiantennilla ei voida poimia kaikkea satelliitin välittämää viestintää, koska yksi ja sama satelliittiantenni ei voi olla satelliitin kaikilla peittoalueilla. Yhden satelliitin hemi beams-alueen tai yleisen peittoalueen poimimiseksi tarvitaan siis kaksi satelliittiantennia eri alueilla (katso peittoalueiden esittely kappaleessa 4). Jos alueita on vielä useampia (zone beams- ja spot beams-alueet), tarvitaan useampia satelliittiantenneja. Satelliitin toisensa peittävät alueet voidaan kuitenkin poimia yhdellä satelliittiantennilla, koska teknisesti on mahdollista erottaa eri taajuusalueita vastaanottamisen yhteydessä.

Lisäksi kappaleessa 5.2 mainitut edellytykset ovat voimassa: laitoksiin pääsy on kielletty, koska ne ovat armeijan ylläpitämiä[7], satelliittien signaalien vastaanottamiseksi tarvitaan lautasantennia ja C-alueen poimimiseksi yleisellä peittoalueella satelliittiantennin koon on oltava yli 25 metriä, jos kyseessä on Intelsat-satelliittiantennin ensimmäinen sukupolvi, tai 15 - 18 metriä, jos kyseessä ovat seuraavat sukupolvet.

---

[1] Hager, Nicky: Exposing the global surveillance system http//www.ncooic.com/echelon I.htm; Hager, Nicky: Secret power. New Zealand's role in the international spy network, New Zealend 1996.
[2] Richelson, Jeffrey, Desperately seeking Signals, 4 2000, The Bulletin of the Atomic Scientists, http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html
Richelson,T.Jeffrey, The U.S. Intelligence Community, Westview Press 1999.
[3] Campbell, Duncan, Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5, 10 1999, STOA, http://www.europarl.eu.int/dg4/stoa/en/publi/pdf/98-14-01-2en.pdf
Campbell, Duncan: Inside Echelon, 25.7.2000http://www.heise.de/tp/deutsch/special/ech/6928/1.html
Campbell, Duncan: esitetty 22. tammikuuta 2001Euroopan parlamentin Echelon-sieppausjärjestelmää käsittelevässä väliaikaisessa valiokunnassa, Federation of American Scinetists,http://www.fas.org/irp/nsa/nsafacil.html.
[4] Richelson, Jeffrey: Newly released documents on the restrictions NSA places on reporting the identities of US-persons: Declassified: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html.
[5] Federation of American Scintists.
[6] Military.com; *.mil-Homepages.
[7] Käytetyt lyhenteet: NAVSECGRU: Naval Security Group, INSCOM: United States Army Intelligence And Security Command, AIA: Air Intelligence Agency, IG: Intelligence Group, IS: Intelligence Sqadron, IW: Intelligence Wing, IOG: Information Operation Group, MIG: Military Intelligence Group.

5.3.2.1. Intelsatin kehitys ja asemien rakentaminen samanaikaisesti

Maailmalaajuisen kuuntelujärjestelmän on kasvettava yhdessä viestinnän kehityksen kanssa. Satelliittiviestinnän on siten käynnistyttävä samaan aikaan asemien perustamisen kanssa, ja uusien satelliittisukupolvien käyttöönoton tulee tapahtua samaan aikaan uusien asemien perustamisen ja uusien kulloisetkin vaatimukset täyttävien satelliittiantennien rakentamisen kanssa. Asemien ja satelliittiantennien lukumäärän on noustava silloin, kun se on välttämätöntä viestinnän vastaanottamiseksi.

Samoin jos jossakin peittoalueet lisääntyvät ja perustetaan uusia asemia ja rakennetaan uusia satelliittiantenneja, kyseessä ei ole sattuma, vaan sitä voidaan pitää merkkinä kuunteluaseman olemassaolosta.

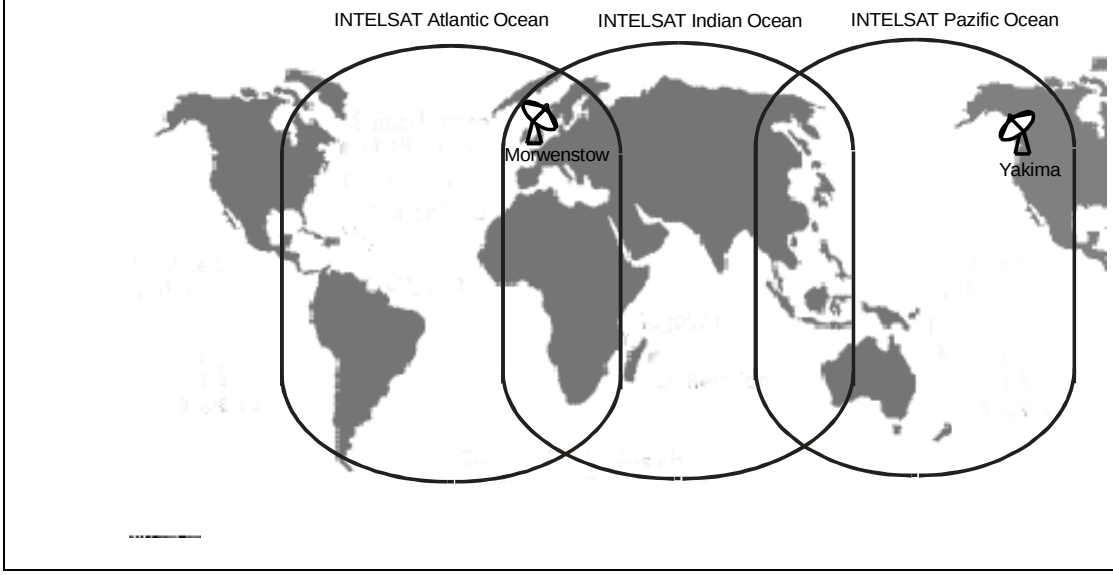
Koska Intelsat-satelliitit kattoivat ensimmäisinä viestintäsatelliitteina koko maapallon, on loogista, että asemat lisääntyvät ja kasvavat samaan aikaan Intelsat-sukupolvien kanssa.

Ensimmäinen sukupolvi

Ensimmäinen Intelsat-satelliitti (Early Bird) laukaistiin geostationääriselle radalle jo vuonna 1965. Sen siirtokapasiteetti oli vielä pieni ja peittoalue oli vain pohjoinen pallonpuolisko.

Toisen ja kolmannen Intelsat-sukupolven avulla, jotka otettiin käyttöön vuosina 1967 ja 1968, katettiin ensimmäistä kertaa koko maapallo. Satelliittien yleiset peittoalueet kattoivat Atlantin, Tyynen valtameren ja Intian valtameren alueet. Pienempiä peittoalueita ei vielä ollut. Kaiken viestinnän poimimiseksi tarvittiin vielä kolme satelliittiantennia. Koska Euroopan alueen peitti kaksi yleistä peittoaluetta, voitiin tällä alueella poimia yhdellä asemalla kahden eri tavalla suunnatun satelliittiantennin avulla kahden satelliitin maailmanlaajuinen peittoalue.

Intelsatin ensimmäinen maailmanlaajuisesti toimiva sukupolvi



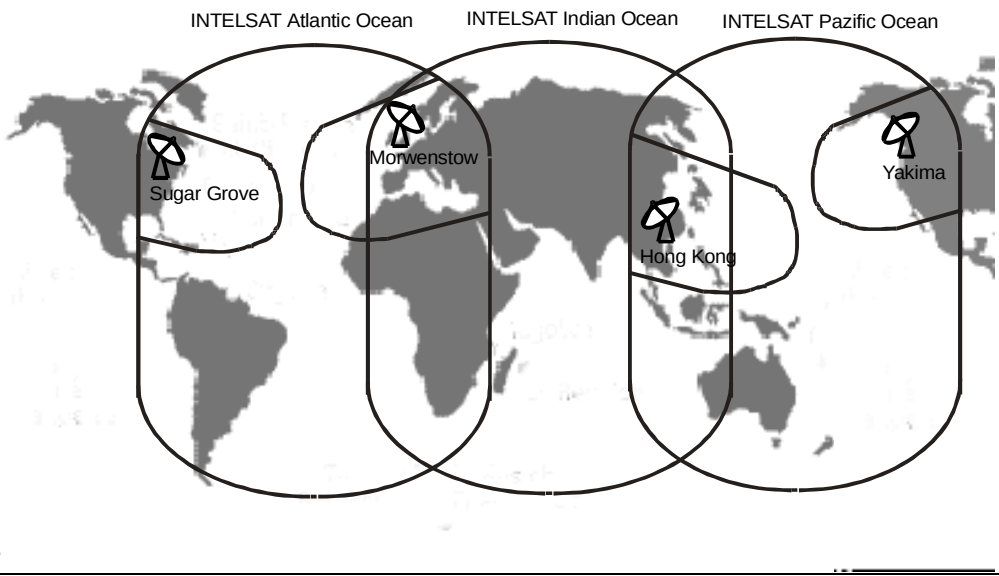
Vuonna 1970 perustettiin **Yakima**-asema Yhdysvaltojen koillisosaan ja vuosina 1972/1973 **Morwenstow** Etelä-Englantiin. Yakimassa oli jo tuolloin suuri antenni (suunnattu Tyynelle

valtamerelle), ja Morwenstow'ssa kaksi suurta antennia (toinen suunnattu Atlantille ja toinen Intian valtamerelle). Näiden asemien sijainnin ansiosta kaiken viestinnän poiminen oli mahdollista. Vuonna 1974 rakennettiin Menwith Hilliin ensimmäinen suuri satelliittiantenni.

Toinen maailmanlaajuinen sukupolvi

Intelsat-satelliittien toinen sukupolvi (IV ja IVA) kehitettiin ja laukaistiin geostationääriselle radalle 70-luvulla (1971 ja 1975). Uusilla satelliiteilla, jotka kattoivat myös koko maapallon ja joilla oli useita (4 000 - 6 000) puhelukanavaa, oli global beam-alueen lisäksi pohjoisella pallonpuoliskolla myös zone beams -alueita (katso kappale 4). Yksi zone beams -alue peitti Yhdysvaltojen itäosat, yksi länsiosat, yksi Länsi-Euroopan ja yksi Itä-Aasian. Kahdella asemalla ja niillä sijaitsevilla kolmella antennilla ei siis enää voitu poimia kaikkea viestintää. Olemassa olevista asemista Yakiman asemalla voitiin poimia Yhdysvaltojen länsiosan zone beams -alue ja Morwenstow'n asemalla Euroopan zone beams -alue. Kahden muun zone beams -alueen poimimiseksi oli tarpeen perustaa asema Yhdysvaltojen itäosaan ja toinen Itä-Aasiaan.

Intelsatin toinen maailmanlaajuinen sukupolvi



70-luvun lopulla perustettiin **Sugar Grove** -asema Yhdysvaltojen itäosaan (asema oli jo olemassa Neuvostoliiton viestinnän kuuntelua varten), ja sen toiminta käynnistyi vuonna 1980. Samoin 70-luvulla perustettiin asema **Hongkongiin**.

Näin ollen 80-luvulla voitiin neljän aseman avulla – Yakima, Morwenstow, Sugar Grove ja Hongkong – kuunnella maailmanlaajuisesti Intelsat-satelliitin viestintää.

Myöhempien Intelsat-sukupolvien vuoksi, joilla oli global beams -alueen ja hemi beams -alueen lisäksi zone beams- ja spot beams -alueita, oli välttämätöntä perustaa uusia asemia eri puolille maailmaa. Tässä yhteydessä uusien asemien perustamisen ja uusien satelliittiantennien rakentamisen välistä yhteyttä on vaikea havaita.

Koska lisäksi asemia koskeva tieto on vaikeasti saatavilla, ei ole mahdollista selvittää tarkasti, mitkä asemat poimivat kunkin satelliitin peittoalueet. Voidaan kuitenkin havaita, minkä peittoalueiden alueella tunnetut asemat sijaitsevat.

5.3.2.2. Maailmanlaajuinen peitto viestintäsatelliitteja kuuntelevien asemien avulla

Nykyisin maailmanlaajuinen satelliittiviestintä hoidetaan Intelsat-, Inmarsat- ja Intersputnik-satelliittien avulla. Jako kolmeen peittoalueeseen (Intian valtameren, Tyynen valtameren ja Atlantin alueet) on säilytetty. Jokaisella peittoalueella on asemia, jotka täyttävät kuunteluasemille tyypilliset kriteerit:

Intian valtameren yläpuolella olevat satelliitit:

INTELSAT 604 (60°E), 602 (62°E), 804 (64°E), 704 (66°E) EXPRESS 6A (80°E) INMARSAT Intian valtameren alue	Geraldton, Australia Pine Gap, Australia Morwenstow, Englanti Menwith Hill, Englanti
INTELSAT APR1 (83°), APR-2 (110,5°)	Geraldton, Australia Pine Gap, Australia Misawa, Japani

Tyynen valtameren yläpuolella olevat satelliitit:

INTELSAT 802 (174°), 702 (176°), 701 (180°) GORIZONT 41 (130°E), 42 (142°E), LM-1 (75°E) INMARSAT Tyynen valtameren alue	Waihopai, Uusi-Seelanti Geraldton, Australia Pine Gap, Australia Misawa, Japani Yakima, USA - vain Intelsat ja Inmarsat

Atlantin yläpuolella olevat satelliitit:

INTELSAT 805 (304,5°), 706 (307°), 709 (310°) 601 (325,5°), 801 (328°), 511(330,5°), 605 (332,5°), 603 (335,5°), 705 (342°) EXPRESS 2 (14°W), 3A (11°W) INMARSAT atlantischer Bereich	Sugar Grove, USA Buckley Field, USA Sabana Seca, Puerto Rico Morwenstow, Englanti Menwith Hill, Englanti
INTELSAT 707 (359°)	Morwenstow, Englanti Menwith Hill, Englanti

Näin voidaan osoittaa, että viestinnän kuuntelu on mahdollista maailmanlaajuisesti.

Lisäksi on muita asemia, jotka eivät täytä antennin koon kriteeriä, mutta voivat kuitenkin olla osa maailmanlaajuista kuuntelujärjestelmää. Näillä asemilla voidaan esimerkiksi poimia sellaisten satelliittien zone beams- tai spot beams -alueita, joiden global beams -aluetta kuuntelevat muut asemat tai joiden global beams -alueita varten ei tarvita suurta antennia.

5.3.2.3.Asemien yksityiskohtainen esittely

Asemien yksityiskohtaisessa kuvauksessa erotetaan toisistaan asemat, jotka selvästi kuuntelevat viestintäsatelliitteja (kappaleessa 5.2. esitetyt kriteerit) ja asemat, joiden tehtäviä edellä mainitut kriteerit eivät kata.

5.3.2.3.1. Viestintäsatelliittien kuunteluun tarkoitetut asemat

Seuraavat asemat täyttävät kappaleessa 5.2 esitetyt kriteerit, joita voidaan pitää merkkeinä viestintäsatelliittien kuunteluun tarkoitetuista asemista:

Yakima, Yhdysvallat (120°W, 46°N)
Asema perustettiin vuonna 1970 samaan aikaan ensimmäisen satelliittisukupolven kanssa. Vuodesta 1995 siellä on toiminut Air Intelligence Agency (AIA) sekä 544. tiedusteluryhmä (554. Intelligence Group (IG), Detachment 4). Siellä toimii myös merivoimien turvallisuusryhmä (NAVSECGRU). Alueelle on asennettu kuusi satelliittiantennia, joiden koosta lähdemateriaalissa ei ole tietoa. Hager kuvaa satelliittiantennit suuriksi ja olettaa, että ne on suunnattu Tyynen valtameren yläpuolella oleviin Intelsat-satelliitteihin (2 antennia) ja Atlantin yläpuolella oleviin satelliitteihin sekä Inmarsat-satelliitteihin (2 antennia).

Yakiman perustaminen samaan aikaan ensimmäisen Intelsat-sukupolven kanssa sekä 544. tiedusteluryhmän tehtävien yleinen kuvaus antavat ymmärtää, että asemalla on rooli kansainvälisen viestinnän kuuntelussa. Toinen merkki siitä on Yakiman sijainti lähellä satelliittien vastaanottoasemaa, joka sijaitsee vain sata mailia Yakimasta pohjoiseen.

Sugar Grove, Yhdysvallat (80°W, 39°N)
Sugar Grove perustettiin samaan aikaan Intelsat-satelliittien toisen sukupolven käyttöönoton kanssa 70-luvun lopulla. Sinne on sijoitettu NAVSECGRU sekä AIA ja 544. tiedusteluryhmä, IG (Detachment 3). Asemalla on eri lähteiden mukaan 10 satelliittiantennia, joista kolme on kooltaan yli 18 metriä (18,2 m, 32,3 m ja 46 m), ja niiden tehtävä on siten selvästi viestintäsatelliittien kuuntelu. 544. IG:n Detachment 3:n yhtenä tehtävänä on tarjota tiedustelutukea viestintäsatelliittien tietojen keräämiseksi merivoimien kenttäasemien avulla[1].

Lisäksi Sugar Grove sijaitsee lähellä (60 mailia) Etamin satelliittien vastaanottoasemaa.

Sabana Seca, Puerto Rico (66°W, 18°N)
NAVSECGRU sijoitettiin Sabana Secaan vuonna 1952. Vuodesta 1995 lähtien siellä ovat toimineet myös AIA ja 554 IG (Detachment 2). Asemalla on ainakin yksi antenni, jonka halkaisija on 2 metriä, sekä neljä pienempää antennia.

Aseman tehtävä on virallisten tietojen mukaan satelliittiviestinnän käsittely (performing satellite communication processing), salausta ja viestintää koskevat palvelut sekä merivoimien ja puolustusministeriön tehtävien tukeminen (mm. Comsatin tietojen keruu) (tiedot 544. IG:n kuvauksesta). Tulevaisuudessa Sabana Secan on tarkoitus olla ensimmäinen kenttäasema, jota käytetään satelliittiviestinnän analysointiin ja käsittelyyn.

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

Morwenstow, Englanti (4°W, 51°N)
Morwenstow perustettiin samoin kuin Yakima samaan aikaan Intelsat-satelliittien ensimmäisen sukupolven kanssa 70-luvun alussa. Morwenstow'n toimintaa harjoittaa Ison-Britannian viestintäpalvelu (GCHQ). Asemalla on noin 30 satelliittiantennia, joista kahden halkaisija on 30 metriä ja muiden koosta ei ole tietoa.

Aseman tehtävistä ei ole virallisia tietoja. Satelliittiantennien koko ja lukumäärä sekä aseman sijainti vain 110 kilometrin päässä Goonhillyssä sijaitsevasta valtion puhelinlaitoksen asemasta eivät jätä sijaa epäilyksille sen tehtävästä viestintäsatelliittien kuunteluasemana.

Menwith Hill, Englanti (2°W, 53°N)
Menwith Hill perustettiin vuonna 1956. Vuonna 1974 käytössä oli jo kahdeksan antennia. Nykyisin asemalla on noin 30 satelliittiantennia, joista joidenkin halkaisija on yli 20 metriä. Menwith Hillissä britit ja amerikkalaiset toimivat yhteistyössä. Yhdysvaltojen yksiköistä siellä on NAVSECGRU, AIA (451. IOS) sekä INSCOM, joka vastaa aseman johdosta. Maa, jolla Menwith Hill sijaitsee, kuuluu Ison-Britannian puolustusministeriölle ja on vuokrattu Yhdysvaltojen hallitukselle. Virallisen tiedon mukaan aseman tehtävänä on tarjota nopeita radioyhteyksiä ja ohjata viestinnän tutkimusta. Richelssonin ja Federation of American Scientists -yhdistyksen mukaan Menwith Hill on sekä vakoilusatelliittien että venäläisten viestintäsatelliittien maa-asema.

Geraldton, Australia (114°O, 28°S)
Asema on ollut olemassa 90-luvun alusta lähtien. Aseman toimintaa johtaa Australian salainen palvelu (DSD). Aikaisemmin Hongkongiin sijoitetut britit kuuluvat nyt aseman miehitykseen. Hagerin mukaan kuusi satelliittia, joista ainakin yhden halkaisija on noin 20 metriä (arvio), on suunnattu Intian valtameren ja Tyynen valtameren yläpuolella oleviin satelliitteihin.

Australian parlamentissa valan vannoneen asiantuntijan mukaan Geraldtonissa kuunnellaan viestintäsatelliitteja.[1]

Pine Gap, Australia (133°O, 23°S)
Pine Gapin asema perustettiin vuonna 1966. Sitä johtaa Australian salainen palvelu (DSD). Noin puolet sinne sijoitetuista 900 henkilöstä on amerikkalaisia CIA:n ja NAVSECGRU:n edustajia.[2]

Pine Gapissa on 18 satelliittiantennia, joista yhden halkaisija on noin 30 metriä ja yhden noin 20 metriä. Virallisten tietojen sekä eri lähteiden tietojen mukaan asema on ollut alusta lähtien Signit-satelliittien maa-asema. Sieltä käsin valvotaan ja ohjataan useita vakoilusatelliitteja ja otetaan vastaan, työstetään ja analysoidaan signaaleja. Suuret satelliittiantennit puhuvat myös viestintäsatelliittien kuuntelun puolesta, koska Signit-satelliitteja varten ei tarvita suuria satelliittiantenneja. Vuoteen 1980 asti Australia oli suljettu pois signaalien käsittelystä vastaavasta osastosta, mutta nykyään australialaisilla on vapaa pääsy kaikkialle muualle paitsi Yhdysvaltojen salakirjoitukselle varattuihin tiloihin.

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

Misawa, Japani (141°O, 40°N)
Misawan asema on ollut olemassa vuodesta 1948 asti. Sinne on sijoitettu japanilaisia ja amerikkalaisia. Amerikkalaisista siellä toimivat NAVSECGRU, INSCOM ja joitakin AIA:n joukkoja (544. IG, 301. IS). Alueella on noin 14 satelliittiantennia, joista joidenkin halkaisija on noin 20 metriä (arvio). Misawa toimii virallisesti salaustoimintojen keskuksena. Richelsonin tietojen mukaan Misawan avulla kuunnellaan venäläisiä Molnyia-satelliitteja sekä muita venäläisiä viestintäsatelliitteja.

Waihopai, Uusi-Seelanti (173°O, 41°S)
Waihopai on ollut olemassa vuodesta 1989 asti. Sen jälkeen sinne on pystytetty yksi suuri antenni, jonka halkaisija on 18 metriä, ja myöhemmin sen lisäksi on rakennettu kaksi pienempää. Hagerin mukaan suuri antenni on suunnattu Tyynen valtameren yläpuolella olevaan Intelsat 701:een.

Buckley Field, Yhdysvallat, Denver Colorado (104°W, 40°N)
Asema perustettiin vuonna 1972. Sinne on sijoitettu 544. IG (Det. 45). Alueella on noin viisi satelliittiantennia, joista neljän halkaisija on noin 20 metriä. Virallisesti aseman tehtävä on kerätä, arvioida ja analysoida Signit-satelliittien hankkimia tietoja radioaktiivisista tapahtumista. Satelliittiantennien koko viittaa kuitenkin siviiliviestinnän vastaanottamiseen.

Hongkong (22°N, 114°O)
Asema perustettiin 70-luvun lopulla samaan aikaan toisen Intelsat-sukupolven kanssa, ja siellä oli suuria satelliittiantenneja. Niiden koosta ei ole tarkkoja tietoja. Vuonna 1994 asemaa alettiin purkaa, ja antennit vietiin Australiaan. Ei ole selvää, onko Geraldton, Pine Gap vai Japanin Misawa ottanut hoitaakseen Hongkongin aseman tehtävät. Mahdollisesti tehtävät on jaettu eri asemien kesken.

5.3.2.3.2. Muut asemat

Edellä mainittujen kriteerien avulla ei kyetty osoittamaan yksiselitteisesti seuraavien asemien toimintaa:

Leitrim, Kanada (75°W, 45°N)
Leitrim on osa Kanadan ja Yhdysvaltojen sotilasyksiköiden vaihto-ohjelmaa. Leitrimissa on merivoimilta saatujen tiedon mukaan noin 30 työntekijää. Ensimmäinen neljästä satelliittiantennista asennettiin vuonna 1985. Kahden suuremman antennin halkaisija on ainoastaan n. 12 metriä (arvio). Aseman tehtäviin kuuluu virallisten tietojen mukaan "cryptologic rating" ja diplomaattisen viestinnän seuranta.

Bad Aibling, Saksa (12°O, 47°N)
Asema sijaitsee Bad Aiblingin lähellä, ja siellä työskentelee n. 750 amerikkalaista. Yhdysvaltain armeija otti aseman hallintaansa vuonna 1952 (se kuului puolustusministeriölle vuosina 1972–1994), Bad Aiblingiin on sijoitettu NAVSECGRU, INSCOM (66. IG, 718. IG) sekä AIA:n eri ryhmiä (402. IG, 26. IOG). Asemalla on 14 satelliittiantennia, joista yhdenkään halkaisija ei ole yli 18-metrinen. Virallisten tietojen mukaan Bad aiblingin tehtäviin kuuluu "Rapid Radio Relay and Secure Commo, Support to DoD and unified Commands, Medium and Longhand Commo HF&Satellite, Communication Physics Research, Test and Evaluate Commo Equipment".

Richelsonin mukaan Bad Aibling toimii SIGINT-satelliittien ja Venäjän viestintäsatelliittien maa-asemana.

Ayios Nikolaos, Kypros (32°O, 35°N)
Kyproksella sijaitseva Ayios Nikolaos on brittien asema. Asemalla on 9 satelliittiantennia, joiden koko ei ole tiedossa, ja sen tehtävät jakaantuvat kahteen yksikköön "Signals Regiment Radio" ja "Signals Unit (RAF)".

Ayios Nikolaos sijaitsee arabimaiden läheisyydessä ja se on ainoa alueen tietyillä (erityisesti (kohdekeilojen) peittoaloilla toimiva asema, joten sillä on varmasti tärkeä rooli tietojen hankinnassa.

Shoal Bay, Australia (134°O, 13°S)
Shoal Bay on ainoastaan Australian tiedustelupalvelun ylläpitämä asema. Asemalla on tietojen mukaan 10 satelliittiantennia, joiden koosta ei ole annettu tarkempia tietoja. Valokuvissa näkyvistä satelliittiantenneista 5 suurinta on halkaisijaltaan enintään 8-metrisiä ja kuudes näkyvä antenni on vielä pienempi. Richelsonin tietojen mukaan antennit on suunnattu Indonesian PALAPA-satelliittiin. On epäselvää, onko asema osa siviiliviestinnän salakuunteluun tarkoitettua maailmanlaajuista järjestelmää.

Guam, Tyyni Valtameri (144°O, 13°S)
Guam on ollut olemassa vuodesta 1898. Nykyisin siellä on merivoimien tietokone- ja televiestintäkeskus, jonne on sijoitettu AIA:n 544. IG sekä merivoimien sotilaita. Asemalla on ainakin kaksi satelliittiantennia, joiden koko ei ole tiedossa. Tästä syystä Guamin toiminta on jäänyt epäselväksi.

Kunia, Havaiji (158°W, 21°N)
Asema on toiminut vuodesta 1993 NAVSECGRU:n ja AIA:n ylläpitämänä alueellisen turvallisuuden operaatiokeskuksena Sen tehtäviin kuuluu tietojen ja viestinnän käyttöön asettaminen sekä salakirjoitusalan tuki. Kunian toiminta on jäänyt epäselväksi.

Medina Annex, Yhdysvallat Texas (98°W, 29°N)
Medina on Kunian tavoin alueellisen turvallisuuden operaatiokeskus, joka on perustettu vuonna 1993. Se on NAVSECGRU:n ja AIA-yksikköjen ylläpitämä ja se hoitaa tehtäviä Karibialla.

Fort Gordon (81°W, 31°N)
Fort Gordon on myös alueellisen turvallisuuden operaatiokeskus, jota ylläpitävät INSCOM ja AIA (702. IG, 721 IB, 202 IB, 31 IS). Sen tehtävistä ei ole saatu selkoa.

Fort Mead, Yhdysvallat (76°W, 39°N)
Fort Mead on NSA:n päämaja.

5.3.3. Yhteenveto tuloksista

Asemia ja satelliitteja koskevista tiedoista ja edellä kuvatuista ehdoista voidaan tehdä seuraavat johtopäätökset:

1. Kullakin peittoalueella on ainakin muutamia maapallon peittäviä keiloja hyödyntäviä kuunteluasemia, joissa kussakin on vähintään yksi halkaisijaltaan yli 18 metriä suuri antenni ja joita amerikkalaiset tai britit ylläpitävät eli joista käsin he harjoittavat tiedustelutoimintaa. Tämä on vahva todiste maailmanlaajuisen kuuntelujärjestelmän olemassaolosta.

2. INTELSAT-viestinnän kehittyminen ja samanaikainen tarvittavien kuunteluasemien rakentaminen on osoitus maailmanlaajuisesta järjestelmän varustamisesta.

3. Kohtien 1 ja 2 perusteella on mahdollista tunnistaa jotkut asemat selvästi asemiksi, joilla kuunnellaan kansainvälistä tietoliikenneviestintää.

4. Luottamukselliseksi luokittelemattomien asiakirjojen ja niiden ylläpitäjien (AIA, NSA, merivoimat jne.) tietoja on pidettävä todisteina asiakirjoissa mainituista asemista.

5. Jotkut asemat sijaitsevat samanaikaisesti useiden eri satelliittien beam- tai spot-alueilla, mikä mahdollistaa sen, että suuri osa viestinnästä voidaan siepata.

6. Lisäksi on olemassa joitakin muita asemia, joilla ei ole suuria antenneja, mutta jotka voivat tästä huolimatta olla osa järjestelmää, sillä ne voivat siepata viestejä beam- tai spot-alueilta. Tällöin ei voida tuijottaa antennin kokoon, vaan on arvioitava myös muita seikkoja.

7. Jotkut mainituista asemista sijaitsevat todistettavasti tietoliikennesatelliittien maa-asemien välittömässä läheisyydessä.

5.4. UKUSA-sopimus

UKUSA-sopimuksella tarkoitetaan vuonna 1948 allekirjoitettua Ison-Britannian (Yhdistynyt kuningaskunta, UK), Yhdysvaltojen (USA), Australian, Kanadan ja Uuden-Seelannin välistä SIGINT-sopimusta tietoliikenteen vakoilusta.

5.4.1. UKUSA-sopimuksen historiallinen tausta[1]

UKUSA-sopimus on jatkoa ensimmäisen maailmansodan aikana orastaneelle Yhdysvaltojen ja Ison-Britannian yhteistyölle, joka jo toisen maailmansodan aikana oli erittäin tiivistä.

Aloitteen SIGINT-allianssista tekivät amerikkalaiset elokuussa vuonna 1940 Lontoossa järjestetyssä amerikkalaisten ja brittien tapaamisessa[2]. Helmikuussa 1941 amerikkalaiset salakirjoituksen tutkijat toimittivat Isoon-Britanniaan koodinpurkulaitteen (PURPLE). Keväällä 1941 alkoi salakirjoituksen koodaamiseen liittyvä yhteistyö[3]. Yhteistyö tiedustelupalvelun alalla

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

[2] ibidem, p. 99: "At a metteing in London on 31 August 1940 between the British Chiefs of Staff and the American Military Observer Mission, the US Army representative, Brigadier General George V. Strong, reported that ´it had recently been arranged in principle between the British and the United States Governments that periodic exchange of information would be desirable,´ and said that ´the time had come or a free exchange of intelligence´. (COS (40)289, CAB 79/6, PRO. Smith, The Ultra Magic Deals, pp. 38, 43-4. Sir F.H. Hinsley, et al., British Intellgence in the Second Worls War, vol.I, pp. 312-13)

[3] Ibidem, p. 100: " In the spring of 1941, Steward Menzies, the Chief of SIS, appointed an SIS liason officer to the British Joint Services Missin in Washington, Tim O´Connor, …, to advice him on cryptologic collaboration".

vahvistui, kun laivastot toimivat kesällä 1941 yhdessä pohjoisella Atlantilla. Kesäkuussa 1941 britit onnistuivat murtamaan saksalaisen laivastokoodin ENIGMAn.

Amerikkalaisten mukaantulo sotaan vahvisti entisestään yhteistyötä tietoliikenteen vakoilun alalla. Vuonna 1942 amerikkalaiset "naval SIGINT agency" -toimiston salakirjoituksen koodaajat alkoivat työskennellä Isossa-Britanniassa[1]. Viestintä Lontoossa, Washingtonissa ja toukokuusta 1943 lähtien myös Ottawassa Kanadassa sijanneiden sukellusveneiden seuranta-asemien välillä oli niin vilkasta, että erään aikalaistodistajan mukaan ne toimivat lopulta kuten yksi organisaatio[2].

Keväällä 1943 allekirjoitettiin BRUSA–SIGINT-sopimus ja sovittiin henkilöstön vaihdosta. Sopimuksen sisältö koskee ennen kaikkea työnjakoa ja se on tiivistetty sopimuksen kolmeen ensimmäiseen kappaleeseen: niihin sisältyy signaalien havaitsemista, tunnistamista ja kuuntelemista koskeva tietojenvaihto sekä koodien ja salakielen purkaminen. Amerikkalaiset olivat päävastuussa Japanista, britit Saksasta ja Italiasta[3].

Sodan jälkeen aloite säilyttää SIGINT-allianssi oli lähtöisin pääasiassa Isosta-Britanniasta. Yhteistyön edellytykset luotiin brittiläisen tiedustelupalvelun työntekijöiden (mm. Sir Harry Hinsley, jonka kirjoihin siteerattu artikkeli perustuu) maailmanympärimatkalla keväällä 1945. Matkan yhtenä tarkoituksena oli toimittaa SIGINT-henkilökuntaa Euroopasta Tyynelle valtamerelle Japanin kanssa käytävän sodan vuoksi. Tässä yhteydessä Australian kanssa sovittiin, että sen tiedustelupalvelulle annettaisiin käyttöön (brittiläisiä) resursseja ja henkilökuntaa. Paluumatka USA:han tehtiin Uuden-Seelannin ja Kanadan kautta.

Syyskuussa 1945 Truman allekirjoitti erittäin salaisen muistion, jolla luotiin perusta rauhanajan SIGINT-allianssille[4]. Siihen liittyen aloitettiin jälleen brittien ja amerikkalaisten neuvottelut sopimukseen pääsemiseksi. Brittivaltuuskunta otti lisäksi yhteyttä kanadalaisiin ja australialaisiin, jotta voitaisiin keskustella heidän mahdollisesta mukaantulostaan. Helmi- ja maaliskuussa 1946 järjestettiin erittäin salainen englantilaisten ja amerikkalaisten välinen SIGINT-konferenssi, jossa keskusteltiin yksityiskohdista. Britit saivat valtuudet kanadalaisilta ja australialaisilta. Konferenssin tuloksena syntyi noin 25 sivun pituinen yhä salaiseksi luokiteltu sopimus, jossa lyötiin lukkoon Yhdysvaltojen ja Brittiläisen kansainyhteisön välisen SIGINT-sopimuksen yksityiskohdat. Seuraavien kahden vuoden aikana neuvotteluja käytiin lisää, kunnes niin kutsutun UKUSA-sopimuksen lopullinen teksti allekirjoitettiin kesäkuussa 1948[5].

[1] Ibidem, p. 100 (Sir F.H. Hinsley, et al., British Intellgence in the Second Worls War, vol II, p.56)
[2] Ibidem, p. 101 (Sir F.H. Hinsley, et al., British Intellgence in the Second Worls War, vol. II, p 48)
[3] Ibidem, p. 101-2: Interivews mit Sir F.H. Hinsley, "Operations of the Military Intelligence Service War Department London (MIS WD London)," 11 June 1945, Tab A, RG 457 SRH-110, NAW
[4] Truman, Memorandum for the Secretaries of the State, War and the Navy, 12 Sept. 1945: "The Secretary of War and the Secretary of the Navy are hereby authorised ti direct the Chief of Staff, U.S. Army and the Commander in Chief, U.S. Fleet; and Chief of Naval Oerations to continue collaboration in the field of communication intelligence between the United States Army and Navy and the British, and to extend, modify or discontinue this collaboration, as determined to be in the best interests of the United States.“ (from Bradley F. Smith, The Ultra-Magic Deals and the Most Secret Special Relationship (Novato, Ca: Presidio 1993)).
[5] Christopher Andrew, “The making of the Anglo-American SIGINT Alliance" in E. Hayden, h. Peake and S. Halpern eds, In the Name of Inteligence. Essays in honor of Washington Pforzheimer (Washington NIBC Press 1995) pp. 95 –109: Interviews with Sir Harry Hinsley, March/April 1994, who did a part of the negotiations; Interviews with Dr. Louis Tordella, Deputy Director of NSA from 1958 to 1974, who was present at the signing.

5.4.2. Todisteet sopimuksen olemassaolosta

Tähän mennessä UKUSA-sopimuksen allekirjoittaneet valtiot eivät ole myöntäneet virallisesti sopimuksen olemassaoloa. Siitä on kuitenkin useita todisteita.

5.4.2.1. Yhdysvaltain merivoimien akronyymiluettelo

Yhdysvaltain merivoimien mukaan[1] UKUSA tulee sanoista "Yhdistynyt kuningaskunta (UK)–USA" ja viittaa viiden valtion väliseen SIGINT-sopimukseen.

5.4.2.2. Australian tiedustelupalvelun DSD:n johtajan lausunto

DSD:n johtaja vahvisti sopimuksen olemassaolon eräässä haastattelussa: hänen tietojensa mukaan Australian tiedustelupalvelu tekee valtameren takaisten muiden tiedustelupalveluiden kanssa yhteistyötä UKUSA-sopimuksen puitteissa[2].

5.4.2.3. Kanadan parlamentin turvallisuus- ja tiedusteluasioista vastaavan valiokunnan mietintö

Mietinnössä kerrotaan, että Kanada tekee joidenkin lähimpien ja pitkäaikaisimpien liittolaistensa kanssa yhteistyötä tiedustelupalvelun alalla. Mietinnössä luetellaan liittolaiset: Yhdysvallat (NSA), Iso-Britannia (GCHQ), Australia (DSD) ja Uusi-Seelanti (GCSB). Sopimuksen nimeä ei mainita mietinnössä.

5.4.2.4. NSA:n entisen johtajan Louis Torellan lausunto

Cambridgen yliopiston professorin Christopher Andrewn haastattelussa marraskuussa 1987 ja huhtikuussa 1992 NSA:n entinen varajohtaja Louis Torella, joka oli läsnä sopimusta allekirjoitettaessa, vahvisti sopimuksen olemassaolon.[3]

5.4.2.5. Ison-Britannian tiedustelupalvelun GCHQ:n entisen johtajan Joe Hooperin kirje

GCHQ:n entinen johtaja mainitsee UKUSA-sopimuksen kirjeessä NSA:n entiselle johtajalle Marshall S. Carterille.

5.4.2.6. Esittelijän keskustelukumppanit

Esittelijä on keskustellut sopimuksesta useiden sellaisten henkilöiden kanssa, jotka tuntenevat tehtäviensä vuoksi UKUSA-sopimuksen ja sen sisällön. Keskustelujen yhteydessä sopimuksen olemassaolo on käynyt kaikissa tapauksissa epäsuorasti vastauksista ilmi.

[1] US Nave and Marine Corps Intelligence Training Centre -keskuksen (NMITC) osoitteessa http://www.cnet.navy.mil/nmitc/training/u.html julkaisemat tiedot "Terms/Abbreviations/Acronyms".
[2] DSD:n johtaja Martin Brady, Canberra 16. maaliskuuta 2000.
[3] Andrew, Christopher "The growth of the Australian Intelligence Community and the Anglo-American Connection", pp. 223-4.

5.5. Amerikkalaisten luokittelemattomien asiakirjojen arviointi

5.5.1. Asiakirjojen laji

Vuoden 1966 tiedonsaannin vapautta koskevan lain ("Freedom of Information Act", 5 U.S.C. § 552) ja Yhdysvaltojen puolustusministeriön asetuksen (DoD FOIA Regulation 5400.7-R, v. 1997) myötä luokiteltuja asiakirjoja muutettiin luokittelemattomiksi, jolloin niistä tuli julkisia. Asiakirjat ovat julkisesti saatavilla vuonna 1985 perustetun kansallisen turvallisuusarkiston kautta (George Washington University, Washington D.C.). Kirjoittaja Jeffrey Richelson, kansallisen turvallisuusarkiston entinen jäsen, on asettanut Internetin kautta saataville 16 asiakirjaa, jotka antavat kuvan NSA:n (National Security Agency) synnystä, kehityksestä, johdosta ja toimivallasta.[1] Lisäksi kahdessa näistä asiakirjoista mainitaan Echelon. Eri kirjoittajat, jotka ovat käsitelleet Echelonia, siteeraavat yhä uudelleen näitä asiakirjoja maailmanlaajuisen Echelon-vakoilujärjestelmän olemassaolon todisteina. Lisäksi Richelsonin luovuttamien asiakirjojen joukossa on sellaisia, jotka vahvistavat NRO:n (National Reconnaissance Office) olemassaolon ja kuvaavat sen toimintaa SIGINT-satelliittien ylläpitäjänä ja käyttäjänä.[2]

5.5.2. Asiakirjojen sisältö

Asiakirjat sisältävät katkelmanomaisia kuvauksia tai mainintoja seuraavista aiheista:

5.5.2.1. NSA:n tehtävä ja toimintatapa (asiakirjat 1, 4, 10, 11 ja 16)

Maaliskuun 10. päivänä 1950 annetussa National Security Council Intelligence Directive 9:ssä (NSCID 9) määritellään ulkomaantiedustelun käsite COMINT-tarkoituksiin. Sen mukaan **ulkomaantiedustelu sisältää kaiken hallinnollisen viestinnän laajassa mielessä (ei ainoastaan sotilaallista viestintää) sekä kaiken muun viestinnän, joka saattaa sisältää sotilaallisesti, poliittisesti, tieteellisesti tai taloudellisesti arvokasta tietoa.**

Direktiivissä (NSCID 9 rev, 29. 12. 52) tehdään nimenomaan selväksi, että sisäisestä turvallisuudesta vastaa yksin FBI.

Puolustusministeriön (Department of Defense, DoD) 23. joulukuuta 1991 NSA:sta ja keskusturvallisuuspalvelusta (Central Security Service, CSS) antamassa direktiivissä määritellään NSA:n toimintatapa seuraavasti:

– NSA on puolustusministeriön sisällä ja puolustusministerin alaisuudessa toimiva yksikkö, jolla on oma organisaatio.
– NSA huolehtii ensinnäkin Yhdysvaltojen SIGINT-tehtävien täyttämisestä, toiseksi se antaa turvalliset viestintäjärjestelmät kaikkien osastojen ja yksiköiden käyttöön.
– NSA:n SIGINT-toiminta ei sisällä valmiiden viestien tuottamista ja jakelua. Tämä on muiden osastojen ja yksiköiden tehtävä.

Tämän lisäksi vuoden 1991 DoD-direktiivissä hahmotellaan NSA:n ja CSS:n rakenne.

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

Pysyvälle tiedustelukomitealle (House Permanent Select Committee on Intelligence) 12. huhtikuuta 2000 antamassaan lausunnossa NSA:n johtaja Hayden määritteli NSA:n tehtävät seuraavasti:

– Elektronisen valvonnan avulla kerätään ulkomaista viestintää armeijalle ja poliitikoille.
– NSA toimittaa Yhdysvaltojen hallinnon käyttöön ("U.S. Government consumers") tiedusteluaineistoa kansainvälisestä terrorismista, huumeista, asekaupasta.
– NSA:n tehtäviin ei kuulu kaiken sähköisen viestinnän kerääminen.
– NSA saa välittää tietoja vain hallituksen valtuuttamille vastaanottajille, ei kuitenkaan suoraan yhdysvaltalaisille yrityksille.

Yhdysvaltain laivaston amiraalin W.O. Studemanin hallituksen nimissä laatimassa 8. huhtikuuta 1992 päivätyssä muistiossa viitataan yhä useammin NSA:n maailmanlaajuiseen tehtävään (global access) ja sotilasoperaatioiden tukemiseen.

5.5.2.2. Tiedustelupalvelujen valtuudet (asiakirja 7)

Yhdysvaltojen signaalitiedustelupalveludirektiivistä 18 (United States Signals Intelligence Directive, USSID 18) nähdään, että sieppauksen kohteena ovat sekä kaapeli- että radiosignaalit.

5.5.2.3. Yhteistyö muiden tiedustelupalvelujen kanssa (asiakirjat 2a ja 2b)

Yhdysvaltojen viestintätiedustelulautakunnan (U.S. Communications Intelligence Board) tehtäviin kuuluu muun muassa kaikkien ulkomaisten hallitusten kanssa tehtyjen COMINT-alaa koskevien järjestelyjen ("arrangements") valvonta. NSA:n johtajan tehtäviin kuuluu yhteyksien hoito kaikkiin ulkomaisiin COMINT-palveluihin.

5.5.2.4. "Echelon-asemilla" toimivien yksiköiden nimeäminen (asiakirjat 9 ja 12)

NAVSECGRU INSTRUCTIONs C5450.48A kuvaa laivaston turvallisuusryhmän toiminnan (Naval Security Group Activity, NAVSECGRUACT, 544th Intelligence Group, Sugar Grove, West Virginia) tehtävän, toiminnan ja tavoitteen. Ohjeiden mukaan yksi erityistehtävä on "Echelon-aseman ylläpito ja käyttö". Lisäksi yhtenä tehtävänä mainitaan tiedustelupalveluaineiston käsittely.

Asiakirjassa "History of the Air Intelligence Agency – 1 January to 31 December 1994 (RCS: HAF-HO(A&SA)7101 Volume 1) mainitaan Air Intelligence Agency (AIA), Detachment 2 ja 3 kohdassa "Activation of Echelon Units":

Asiakirjat eivät anna tietoa siitä, mikä on "Echelon-asema", mitä "Echelon-asemalla" tehdään ja mitä peitenimi Echelon merkitsee. Asiakirjoista ei löydy tietoa UKUSA-sopimuksesta.

5.5.2.5. Asemien nimeäminen (asiakirjat 6, 9 ja 12)

– Sugar Grove, West Virginia: NAVSECGRU INSTRUCTIONs C5450.48A
– Misawan lentotukikohta, Japani: kirjassa "History of the Air Intelligence Agency - January to 31 December 1994 (RCS: HAF-HO(A&SA)7101 Volume 1)"
– Puerto Rico (toisin sanoen Sabana Seca): ks. edellinen

– Guam: ks. edellinen
– Yakima: Washington, ks. edellinen
– Fort Meade, Maryland: NSA:n COMINT-raportti Fort George G. Meadesta (Maryland), 31. elokuuta 1972, todistaa, että siellä harjoitetaan COMINT-toimintaa.

5.5.2.6. Yhdysvaltojen kansalaisten yksityisyyden suoja (asiakirjat 7, 7a–f, 11 ja 16)

NAVSECGRU INSTRUCTIONs C5450.48A -ohjeissa todetaan, että kansalaisten yksityisyys on turvattava.

Eri asiakirjoissa selvitetään, että Yhdysvaltojen kansalaisten yksityisyys on suojattava ja millä tavoin se on suojattava (Baker, General Counsel, NSA, 9. syyskuuta 1992 päivätty kirje, Yhdysvaltojen signaalitiedusteludirektiivi (USSID) 18, 20. lokakuuta 1980 erilaisine täydennyksineen).[1]

5.5.2.7. Määritelmät (asiakirjat 4, 5a ja 7)

Puolustusministeriön 23. joulukuuta 1991 antamassa direktiivissä annetaan tarkat määritelmät käsitteille SIGINT, COMINT, ELINT ja TELINT, samoin kuin kansallisen turvallisuusneuvoston 17. helmikuuta 1972 annetussa tiedusteludirektiivissä nro 6.

Sen mukaan COMINT tarkoittaa ulkomaisen (sähkömagneettisesti välitetyn) viestinnän keräämistä ja käsittelyä lukuun ottamatta salaamattoman kirjallisen viestinnän, lehdistön ja propagandan sieppaamista ja käsittelyä.

5.5.3. Yhteenveto

1. Jo 50 vuotta sitten kiinnostus kohdistui paitsi politiikkaa ja turvallisuutta, myös tiedettä ja taloutta koskevaan tietoon.

2. Asiakirjat todistavat, että NSA harjoittaa COMINT-yhteistyötä muiden tiedustelupalvelujen kanssa.

3. Asiakirjat, jotka kertovat NSA:n organisaatiosta ja tehtävistä ja joista ilmenee, että se on puolustusministeriön alainen, eivät anna juurikaan lisätietoa NSA:n kotisivuilla oleviin julkisesti saatavilla oleviin tietoihin nähden.

4. Kaapeliviestinnän kuuntelu on sallittua.

5. Ilmatiedustelutoimiston (Air Intelligence Agency) yksiköt 544th Intelligence group sekä Detachment 2 ja 3 osallistuvat tiedusteluaineiston keräämiseen.

6. Käsite "Echelon" esiintyy erilaisissa yhteyksissä.

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

7. Sugar Grove (Länsi-Virginia), Misawan lentotukikohta (Japani), Puerto Rico (toisin sanoen Sabana Seca), Guam ja Yakima (Washingtonin osavaltio) mainitaan SIGINT-asemina.

8. Asiakirjoissa selitetään, miten Yhdysvaltojen kansalaisten yksityisyys on suojattava.

Asiakirjoista ei löydy suoraa todistetta mutta erittäin voimakkaita viitteitä (aihetodisteita), joista voidaan tehdä johtopäätöksiä yhdessä muiden viitteitten kanssa.

5.6. Alan kirjoittajien ja toimittajien tiedot

5.6.1. Nicky Hagerin kirja

Vuonna 1996 julkaistussa Nicky Hagerin kirjassa "Secret Powers – New Zealand's role in the international spy network" Echelon-järjestelmää kuvataan ensimmäisen kerran yksityiskohtaisesti. Kirjan mukaan se juontaa juurensa vuodesta 1947, jolloin Yhdistynyt kuningaskunta solmi Yhdysvaltojen kanssa sodanaikaisen yhteistyön jatkoksi sopimuksen, jonka mukaan maat jatkaisivat yhdessä siihenastisia COMINT-toimintoja. Tarkoituksena oli mahdollisuuksien mukaan maailmanlaajuisen sieppausjärjestelmän perustaminen. Maiden oli määrä jakaa siihen vaadittavat erityislaitteistot ja niistä syntyvät kustannukset ja hyödyntää tuloksia yhdessä. Myöhemmin Kanada, Australia ja Uusi-Seelanti liittyivät UKUSA-sopimukseen.

Hagerin mukaan satelliittiviestinnän sieppaus muodostaa nykyisen järjestelmän ytimen. Jo 70-luvulla alettiin siepata Intelsat-satelliittien – ensimmäisen maailmanlaajuisen satelliittiviestintäjärjestelmän[1] – kautta lähetettyjä viestejä maa-asemien avulla. Näistä viesteistä tutkitaan tietokoneen avulla määrätyt avainsanat ja osoitteet olennaisten viestien suodattamiseksi. Myöhemmin valvonta laajennettiin muun muassa Inmarsatin[2] satelliitteihin. Inmarsat keskittyi merialueiden viestintään.

Hager viittaa kirjassaan siihen, että satelliittiviestinnän sieppaus muodostaa vain yhden – joskin tärkeän – osan sieppausjärjestelmää. Sen lisäksi on vielä lukuisia radio- ja kaapeliyhteyksien kuunteluun tarkoitettuja laitteistoja. Niistä tosin on vähemmän aineistoa ja niitä on vaikeampi todistaa, koska ne eivät juuri herätä huomiota toisin kuin maa-asemat. "Echelonista" tuli näin maailmanlaajuisen sieppausjärjestelmän synonyymi.

5.6.2. Duncan Campbellin tiedot

Duncan Campbellin vuoden 1999 STOA-tutkimuksessa 2/5 tarkasteltiin perusteellisesti teknisiä seikkoja. Siinä todettiin, että jokaista viestien välittämiseen käytettävää välinettä voidaan kuunnella, ja selitetään myös, miten tämä tapahtuu. Yhdessä tuoreimmista kirjoituksistaan hän kuitenkin tarkentaa, että Echelonillakin on rajansa. Alkuperäinen käsitys, jonka mukaan aukoton valvonta olisi mahdollista, on hänen mukaansa osoittautunut vääräksi: "Siihen ei pysty Echelon eikä se elektroninen vakoilujärjestelmä, jonka osa se on. Ei myöskään ole olemassa sellaista

[1] Vrt. http://www.intelsat.int/index.htm.
[2] Vrt. http://www.inmarsat.org/index3.html.

laitteistoa, jonka kapasiteetti riittäisi jokaisen puheviestin tai jokaisen puhelun sisällön käsittelyyn ja tunnistamiseen."[1]

5.6.3. Jeff Richelsonin tiedot

Kansallisen turvallisuuspalvelun NSA:n entinen jäsen Jeffrey Richardson on siirtänyt Internetiin 16 entiseksi luokiteltua asiakirjaa, jotka valottavat NSA:n perustamista, kehittämistä, johtamista ja valtuuksia[2].

Lisäksi hän on kirjoittanut useita kirjoja ja artikkeleita Yhdysvaltojen tiedustelupalvelutoiminnasta. Vuonna 1985 julkaistussaan kirjassa "The Ties That Bind"[3] hän kuvaa perusteellisesti UKUSA-sopimuksen syntymistä ja sopimukseen osallistuneiden Yhdysvaltojen, Iso-Britanniana, Kanadan, Australian ja Uuden-Seelannin tiedustelupalvelujen toimintaa.

Kattavassa (vuonna 1999 julkaistussa) teoksessaan "The U.S. Intelligence Community"[4] hän valottaa Yhdysvaltain tiedustelupalvelun toimintaa, kuvaa sen organisaatiorakennetta, sekä tietojen keräämis- ja analysointimenetelmiä. Kirjan 8. luvussa käsitellään yksityiskohtaisesti tiedustelupalvelun SIGINT-kapasiteettia ja kuvaillaan eräitä asemia. Kirjan 13. luvussa käsitellään Yhdysvaltojen suhteita muihin tiedustelupalveluihin, ja esim. UKUSA-yleissopimusta. Echelon-nimi mainitaan kerran tietokonepohjaisen vaihtojärjestelmän tunnussanana.

Richelson kuvaa vuonna 2000 julkaisemassaan artikkelissa "Desperately Seeking Signals"[5] lyhyesti UKUSA-yleissopimusta, mainitsee viestintäsatelliittien sieppauslaitteet ja kuvaa siviiliviestinnän kuuntelun mahdollisuuksia ja rajoituksia.

5.6.4. James Bamfordin tiedot

toimitetaan myöhemmin

5.6.5. Bo Elkjaerin ja Kenan Seebergin tiedot

Tanskalaiset toimittajat Bo Elkjaer ja Kenan Seeberg ilmoittivat 22. tammikuuta 2001 valiokunnassa, että Echelon oli erittäin edistynyt järjestelmä jo 80-luvulla ja että Tanska toimi yhteistyössä Yhdysvaltojen kanssa vuodesta 1984 lähtien.

---

[1] Duncan Campbell, Inside Echelon. Zur Geschichte, Tehnik und Funktion des unter dem Namen Echelon bekannten globalen Abhör- und Filtersystems, 1.
[2] http://ww.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/index.html
[3] Jeffrey T. Richelson, Desmond Ball 1985: The Ties That Bind, Boston UNWIN HYMAN, Sydney Wellington London.
[4] Jeffrey T. Richelson 1999 (4th ed.): The U.S. Intelligence Community, Westview Press.
[5] Jeffrey T. Richelson 2000: Desperately Seeking Signals, The Bulletin of the Atomic Scientists, March/April 2000, Vol. 56, No 2, pp. 47-51.

5.7. Tiedustelupalvelujen entisten työntekijöiden lausunnot

5.7.1. Margaret Newsham (NSA:n entinen työntekijä)

Margaret Newsham[1] oli työssä Fordilla ja Lockheedilla vuosina 1974–1984 ja työskenteli ilmoituksensa mukaan NSA:lle mainittuna aikana. Hän oli saanut työtä varten koulutuksen NSA:n päämajassa Fort George Meadessa (Maryland, USA), ja vuosiksi 1977–1978 hänet sijoitettiin Menwith Hilliin, Isossa-Britanniassa sijaitsevalle yhdysvaltalaiselle maa-asemalle. Siellä hän totesi, että Yhdysvaltojen senaattori Strohm Thurmondin erästä keskustelua kuunneltiin. Jo vuonna 1978 ECHELON pystyi sieppaamaan tietyn henkilön televiestintää, joka lähetettiin satelliitin kautta.

Margaret Newshamin tehtävänä NSA:ssa oli järjestelmien ja ohjelmien kehittäminen, konfigurointi ja käyttövalmiiksi saattaminen suuria tietokoneita varten. Tietokoneohjelmista käytettiin nimityksiä SILKWORTH ja SIRE. ECHELON oli sen sijaan verkoston nimi.

5.7.2. Wayne Madsen (NSA:n entinen työntekijä)

Myös NSA:n entinen työntekijä Wayne Madsen[2] vahvistaa Echelonin olemassaolon. Hänen mielestään taloutta koskevien tietojen kerääminen on ehdottomasti etusijalla ja niitä käytetään yhdysvaltalaisyritysten hyväksi. Hän on erityisen huolissaan siitä, että Echelon saattaisi vakoilla kansalaisjärjestöjä, kuten Amnesty Internationalia tai Greenpeacea. Lisäksi NSA joutui hänen mukaansa tunnustamaan, että sillä oli yli 1 000 sivua tietoa prinsessa Dianasta, joka toimi Yhdysvaltojen politiikan vastaisesti kampanjoimalla maamiinoja vastaan.

5.7.3. Mike Frost (kanadalainen entinen salaisen palvelun työntekijä)

Mike Frost oli yli 20 vuotta Kanadan salaisen palvelun CSE:n[3] palveluksessa. Hänen mukaansa Ottawan sieppausasema on vain osa maailmanlaajuista vakoiluasemien verkostoa.[4] CBS-yhtiön haastattelussa hän selitti, että "Echelon, hallituksen salainen valvontaverkosto, valvoo kaikkialla maailmassa joka päivä puheluja, sähköposteja ja fakseja".[5] Tämä koskee myös siviiliviestintää. Esimerkkinä hän mainitsi australialaisen tv-yhtiön haastattelussa tapauksen, jossa CSE oli kirjannut erään naisen nimen ja puhelinnumeron mahdollisten terroristien tietokantaan, koska tämä oli käyttänyt kaksiselitteistä käsitettä ystävänsä kanssa käymässään harmittomassa puhelinkeskustelussa. Tietokone oli viestintää analysoidessaan löytänyt avainsanan ja toistanut keskustelun. Analyysista vastaava henkilö oli epävarma ja kirjasi siksi hänen henkilötietonsa muistiin.[6]

Echelon-valtioiden tiedustelupalvelut auttavat Frostin mukaan toisiaan myös vakoilemalla toinen toistensa hyväksi, niin ettei ainakaan oman maan tiedustelupalvelua voida moittia. Esimerkiksi

[1] Vrt. Bo Elkjaer, Kenan Seeberg, Echelon was my baby – Interview with Margaret Newsham, Ekstra Bladet, 17.1.1999.
[2] Tv-haastattelu NBC:n "60 Minutes" -ohjelmassa 27.2.2000; http://cryptome.org/echelon-60min.htm.
[3] Communication Security Establishment, toimii Kanadan puolustusministeriön alaisuudessa, harjoittaa SIGINT-toimintaa.
[4] Tv-haastattelu NBC:n "60 Minutes" -ohjelmassa 27.2.2000; http://cryptome.org/echelon-60min.htm.
[5] Rötzer, Die NSA geht wegen Echelon an die Öffentlichkeit;
http://www.heise.de/bin/tp/issue/download.cgi?artikelnr=6633&rub_ordner=special.
[6] Tv-haastattelu NBC:n "60 Minutes" -ohjelmassa 27.2.2000; http://cryptome.org/echelon-60min.htm.

GCHQ pyysi kanadalaista CSE:tä vakoilemaan puolestaan kahta Ison-Britannian ministeriä, kun pääministeri Thatcher halusi tietää, olivatko nämä hänen puolellaan.[1]

5.7.4. Fred Stock (kanadalainen entinen salaisen palvelun työntekijä)

Fred Stock erotettiin omien sanojensa mukaan Kanadan salaisesta palvelusta CSE:stä vuonna 1993, koska hän oli vastustanut palvelun uutta jättiläistä, joka kohdistui taloutta koskevaan tietoon ja siviilikohteisiin. Siepattu viestintä sisälsi tietoja muiden maiden kanssa solmittavista kaupoista, muun muassa NAFTAA koskevista neuvotteluista, kiinalaisten viljaostoista ja ranskalaisten asemyynneistä. Stockin mukaan salainen palvelu sai myös säännöllisesti viestejä Greenpeacen laivojen avomerellä toteuttamista ympäristöprotesteista.[2]

5.8. Hallitusten antamat tiedot

5.8.1. Yhdysvaltojen taholta annetut lausunnot

CIA:n entinen johtaja James Woolsey kertoi lehdistötilaisuudessa,[3] jonka hän piti Yhdysvaltojen ulkoministeriön pyynnöstä, että Yhdysvallat harjoittaa vakoilua Manner-Euroopassa. Taloutta koskevasta tiedusteluaineistosta ("Economic Intelligence") hankitaan hänen mukaansa kuitenkin 95 prosenttia julkisesti saatavilla olevista tietolähteistä, ja vain viisi prosenttia on varastettuja salaisuuksia. Taloutta koskevia muiden maiden tietoja vakoillaan silloin, kun niissä on kysymys pakotteiden noudattamisesta tai kaksikäyttötuotteista. Lisäksi vakoilua käytetään lahjonnan torjuntaan tarjouskilpailujen yhteydessä. Näitä tietoja ei kuitenkaan luovuteta yhdysvaltalaisille yrityksille. Woolsey korosti, että vaikka taloutta koskevia tietoja vakoiltaessa käsiin osuisikin taloudellisesti hyödynnettävissä olevaa tietoa, analysoijalta kuluisi erittäin paljon aikaa tietojen analysointiin tältä kannalta ja hän syyllistyisi väärinkäytökseen käyttäessään aikaa kauppakumppaniensa vakoiluun. Lisäksi Woolsey muistutti, että vaikka näin tehtäisiinkin, olisi kansainvälisen verkottumisen vuoksi vaikea päättää, mitä yritystä tulisi pitää yhdysvaltalaisena yrityksenä, jolle tietoja siis annettaisiin.

Myöhemmin Woolsey toisti The Wall Street Journal Europe -lehden artikkelissa,[4] että Yhdysvallat vakoilee Eurooppaa mutta että tämä tapahtuu vain lahjonnan paljastamiseksi. Hän toteaa artikkelissa myös selkeästi, että Yhdysvallat käyttää tietokoneita avainsanojen etsimiseen aineistosta.

5.8.2. Ison-Britannian taholta annetut lausunnot

Useista Yhdistyneen kuningaskunnan parlamentin alahuoneen kyselyistä[5] ilmenee, että RAF Menwith Hillin asema kuuluu Yhdistyneen kuningaskunnan puolustusministeriölle mutta on annettu viestintälaitteistoksi Yhdysvaltojen puolustusministeriön, erityisesti NSA:n[6] käyttöön.

---

[1] Australialaisen Tv-yhtiön Channel 9:n haastattelu, 23.3.1999; http://www.geocities.com/CapitolHill/Senate/8789/sunday1.htm.
[2] Bronskill, Canada a key snooper in huge spy network, Ottawa citizen, 24.10.2000, http://www.ottawacitizen.com/national/990522/2630510.html.
[3] Transcript, 7.3.2000, http://cryptome.org/echelon-cia.htm.
[4] James Woolsey, Why America Spies on its Allies, The Wall Street Journal, 22.3.2000, 31.
[5] Commons Written Answers, House of Commons Hansard Debares.
[6] 12.7.1995.

NSA nimittää myös laitoksen johtajan[1].[2] Vuoden 2000 puolivälissä RAF Menwith Hillissä työskenteli 415 Yhdysvaltojen armeijan sotilasta, viisi Ison-Britannian armeijan sotilasta, 989 yhdysvaltalaista siviiliä ja 392 britannialaista siviiliä. Läsnä olevat GCHQ:n työntekijät eivät ole mukana luvuissa.[3] Yhdysvaltojen joukkojen läsnäoloa säätelee Pohjois-Atlantin sopimus ja erityiset salaiset[4] hallintosopimukset, joita pidetään yhteisen puolustuksen kannalta sopivina Yhdysvaltojen ja Ison-Britannian hallitusten nykyiset suhteet huomioon ottaen.[5] Asema on olennainen osa Yhdysvaltojen puolustusministeriön maailmanlaajuista verkostoa, joka tukee Ison-Britannian, Yhdysvaltojen ja Naton etuja.[6]

Vuosikertomuksessa 1999/2000 korostetaan nimenomaisesti UKUSA-sopimuksen mukaisen tiiviin yhteistyön arvoa, joka näkyy tiedustelutoiminnan tulosten laadussa. Erityisesti kertomuksessa viitataan siihen, että kun NSA:n laitteet olivat epäkunnossa kolmen päivän ajan, GCHQ palveli britannialaisten asiakkaiden ohella suoraan myös yhdysvaltalaisia asiakkaita.[7]

5.8.3. Australian taholta annetut lausunnot[8]

Australian tiedustelupalvelun DSD:n[9] johtaja Martin Brady vahvisti kirjeessään australialaisen "Channel 9" -televisiokanavan "Sunday"-ohjelmalle, että DSD harjoittaa yhteistyötä muiden UKUSA-liitossa toimivien tiedustelupalvelujen kanssa. Samassa kirjeessä korostetaan, että kaikkia australialaisia tiedustelupalvelun laitteistoja pitävät yllä australialaiset tiedustelupalvelut yksinään tai yhdessä yhdysvaltalaisten palvelujen kanssa. Kaikissa tapauksissa, joissa laitteistoja käytetään yhdessä, Australian hallitus on täysin tietoinen kaikista toiminnoista ja australialaista henkilöstöä osallistuu toimintaan kaikilla tasoilla.[10]

5.8.4. Alankomaiden taholta annetut lausunnot

Alankomaiden puolustusministeri esitti 19. tammikuuta 2001 Alankomaiden parlamentille kertomuksen nykyaikaisten televiestintäjärjestelmien maailmanlaajuisen sieppaamisen teknisistä ja oikeudellisista näkökohdista.[11] Alankomaiden hallitus edusti siinä näkemystä, että vaikkei sillä olekaan asiasta omia tietoja, on kolmansien osapuolten käytettävissä olevien tietojen perusteella erittäin todennäköistä, että Echelon-verkosto on olemassa mutta että lisäksi on muita järjestelmiä, joilla on samanlaiset mahdollisuudet. Alankomaiden hallitus oli tullut siihen tulokseen, ettei viestintäjärjestelmien maailmanlaajuinen sieppaaminen rajoitu Echelon-järjestelmään osallistuviin valtioihin vaan että sitä harjoittavat myös muiden maiden hallintoviranomaiset.

5.8.5. Italian taholta annetut lausunnot

---

[1] 25.10.1994.
[2] 3.12.1997.
[3] 12.5.2000.
[4] 12.7.1995.
[5] 8.3.1999, 6.7.1999.
[6] 3.12.1997.
[7] Intelligence and Security Committee, Annual Report 1999-2000, jonka pääministeri esitteli parlamentille marraskuussa 2000, rivi 14.
[8] http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp.
[9] Defence Signals Directorate, australialainen tiedustelupalvelu, joka harjoittaa SIGINT-toimintaa.
[10] DSD:n johtajan Martin Bradyn 16. maaliskuuta 1999 päivätty kirje Ross Coulthartille, Sunday Program; vrt. myös: http://sunday.ninemsn.com/01_cover_stories/transcript_335.asp; http://sunday.ninemsn.com/01_cover_stories/article_335.asp.
[11] Brief aan de Tweede Kamer betreffende "Het grootschalig afluisteren van moderne telecommunicatiesystemen" vom 19.01.01.

Italian tiedustelupalvelun SISMI:n entinen johtaja Luigi Ramponi ei jättänyt epäilykselle sijaa Echelonin olemassaolosta "il mondo" -lehdelle antamassaan haastattelussa[1] Ramponi selitti nimenomaan, että hän tiesi Echelonin olemassaolosta SISMIN:n johtajan ominaisuudessa. Vuodesta 1992 lähtien hän tiesi laajamittaisesta pieni-, keski- ja suuritaajuisten aaltojen sieppaustoiminnasta. Kun hän aloitti toimintansa SISMI:ssä vuonna 1991, Yhdistynyt kuningaskunta ja Yhdysvallat teettivät eniten töitä.

5.9. Parlamenttien mietinnöt

5.9.1. Belgian valvontavaliokunnan Comité Permanent R:n mietinnöt

Belgialainen valvontavaliokunta Comité Permanent R on ilmaissut kantansa Echeloniin jo kahdessa mietinnössä.

Mietinnön "Rapport d'activités 1999" 3. luvussa keskityttiin kysymykseen siitä, miten Belgian tiedustelupalvelut reagoivat viestintävalvontaa harjoittavan Echelon-järjestelmän mahdollisuuteen. Runsaan 15 sivun mittaisessa mietinnössä tullaan siihen tulokseen, että Belgian molemmat tiedustelupalvelut, Sûreté de l'Etat ja Service général du Renseignement (SGR) saivat Echelonista tietoa vain virallisten asiakirjojen kautta.

Toisessa mietinnössä "Rapport complémentaire d'activités 1999" tarkastellaan Echelon-järjestelmää huomattavasti yksityiskohtaisemmin. Siinä otetaan kantaa STOA:n tutkimuksiin, ja osassa mietintöä keskitytään televiestinnän sieppaamisen teknisten ja oikeudellisten edellytysten kuvaukseen. Johtopäätöksissä tullaan siihen tulokseen, että Echelon on todella olemassa ja pystyy myös sieppaamaan kaiken satelliittien kautta välitettävän tiedon (n. yksi prosentti kaikista kansainvälisistä puheluista) avainsanoja käytettäessä. Lisäksi sen salauksenpurkukapasiteetti on huomattavasti suurempi kuin Yhdysvallat väittää. On syytä epäillä lausumaa, jonka mukaan Menwith Hillissä ei harjoiteta teollisuusvakoilua. Mietinnössä korostetaan nimenomaan, että on mahdotonta todeta varmuudella, mitä Echelon tekee tai mitä se ei tee.

5.9.2. Ranskan kansalliskokouksen kansallisen puolustuksen valiokunnan mietintö

Ranskassa kansallisen puolustuksen valiokunta esitti kansalliskokoukselle sieppausjärjestelmiä koskevan mietinnön.[2]

Valotettuaan perusteellisesti eri näkökohtia esittelijä Arthur Paecht tuli siihen tulokseen, että Echelon on olemassa ja että se on ainoa tunnettu monikansallinen valvontajärjestelmä. Sen kapasiteetti on todellista, mutta se on saavuttanut rajansa, koska käytetty panostus ei ole suhteessa viestinnän räjähdysmäiseen kasvuun ja koska tietyt kohteet ovat myös oppineet suojautumaan.

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

Echelon-järjestelmä ei mietinnön mukaan palvele enää alkuperäisiä tavoitteitaan, jotka liittyivät kylmään sotaan, joten ei ole mahdotonta, että kerättyjä tietoja käytettäisiin poliittisiin ja taloudellisiin tarkoituksiin muita Nato-maita vastaan.

Mietinnössä todetaan, että Echelon saattaa hyvinkin merkitä vaaraa perusvapauksille ja aiheuttaa tähän liittyen useita ongelmia, jotka vaativat asianmukaisia vastauksia. Olisi väärin kuvitella, että Echelonin jäsenvaltiot luopuvat toiminnastaan. Pikemminkin monet asiat näyttävät viittaavan siihen, että on luotu uusi järjestelmä uusien kumppanien kanssa Echelonin saavuttamien rajojen murtamiseksi uusien keinojen avulla.

6. Voiko muita maailmanlaajuisia sieppausjärjestelmiä olla?

6.1. Maailmanlaajuisen sieppausjärjestelmän edellytykset

6.1.1. Tekniset ja maantieteelliset edellytykset

Kansainvälisen ja ensimmäisen sukupolven satelliittien kautta välitettävän viestinnän sieppaamisen edellytyksenä ovat vastaanottoasemat Atlantin, Intian valtameren sekä Tyynenmeren alueella. Käytettäessä uuden sukupolven satelliitteja, jotka mahdollistavat lähetyksen alhaisilla taajuusalueilla, on täytettävä muitakin sieppausasemien maantieteellistä asemaa koskevia edellytyksiä, jotta kaikki satelliittien kautta välitetty viestintä voitaisiin ottaa vastaan.

Toisen maailmanlaajuisesti toimivan sieppausjärjestelmän on sijoitettava asemansa Echelon-valtioiden alueiden ulkopuolelle.

6.1.2. Poliittiset ja taloudelliset edellytykset

Tällaisen maailmanlaajuisen järjestelmän luomisen on kuitenkin oltava myös käyttäjälle tai käyttäjille taloudellisesti ja poliittisesti mielekästä. Järjestelmästä hyötyvällä tai hyötyvillä on oltava maailmanlaajuisia taloudellisia, sotilaallisia tai muita turvallisuusintressejä tai sen tai niiden on ainakin uskottava kuuluvansa niin sanottuihin maailmanmahteihin. Näin ollen mahdollisuudet rajoittuvat lähinnä Kiinaan ja G8-maihin lukuun ottamatta Yhdysvaltoja ja Yhdistynyttä kuningaskuntaa.

6.2. Ranska

Ranskalla on omia alueita, departementteja ja ulkoalueita kaikilla mainituilla maantieteellisillä alueilla.

Atlantin alueella Kanadasta itään sijaitsee Saint Pierre et Miquelon (65° W / 47° N), Etelä-Amerikan koillispuolella Guadeloupe (61° W / 16° N) ja Martinique (60° W / 14° N) sekä Etelä-Amerikan koillisrannikolla Ranskan Guyana (52° W / 5° N).

Intian valtameren alueella sijaitsevat eteläisen Afrikan itäpuolella Mayotte (45° O / 12° S) ja La Réunion (55° O / 20° S) sekä aivan etelässä Terres Australes et Antarticques Francaises. Tyynenmeren alueella sijaitsevat Uusi-Kaledonia (165° O / 20° S), Wallis et Futana (176° W / 12° S) ja Ranskan Polynesia (150° W / 16° S).

Ranskan tiedustelupalvelun DGSE:n (Direction générale de la sécurité extérieur) mahdollisista asemista näillä merentakaisilla alueilla on vain vähän tietoja. Ranskalaisten toimittajien mukaan[1] Ranskan Guyanan Kouroussa sekä Mayottessa on asemat. Asemien koosta sekä satelliittiantennien määrästä ja koosta ei ole yksityiskohtaisia tietoja. Muita asemia sanotaan olevan Ranskan Dommessa, Bordeaux'n lähellä, sekä Alluetts-le-Roissa Pariisin lähellä. Jauvert arvioi satelliittilautasten määräksi yhteensä 30. Kirjailija Schmidt-Enboom[2] väittää, että myös Uudessa-Kaledoniassa pidetään yllä asemaa.

Teoriassa Ranskakin voisi pitää yllä maailmanlaajuisesti toimivaa sieppausjärjestelmää. Esittelijän käytettävissä ei kuitenkaan ole riittävästi julkista aineistoa, jotta voitaisiin esittää tätä koskeva vakavasti otettava väite.

6.3. Venäjä

Viestintäturvallisuudesta ja SIGINT-toiminnasta vastaavan Venäjän tiedustelupalvelun FAPSIn väitetään pitävän yllä maa-asemia Latviassa, Vietnamissa ja Kuubassa yhdessä Venäjän armeijan tiedustelupalvelun GRU:n kanssa.

Atlantin alueella sijaitsee Amerikan tiedemiesliiton tietojen mukaan Lourdesin asema Kuubassa (82°W, 23°N). Sitä pidetään yllä yhdessä Kuuban tiedustelupalvelun kanssa. Venäjällä on asemia Intian valtameren alueella, mutta niistä ei ole tarkempia tietoja. Lisäksi Latviassa sijaitsee Skrundan asema. Tyynenmeren alueella väitetään olevan asema Pohjois-Vietnamin Cam Rank Bayssä. Yksityiskohtia asemien antennien määrästä ja koosta ei tunneta.

Yhdessä itse Venäjällä sijaitsevien asemien kanssa maailmanlaajuinen peitto on teoriassa mahdollinen. Tässäkään kohden käytettävissä olevat tiedot eivät riitä vakavasti otettavaan väitteeseen.

6.4. Muut G-8-maat ja Kiina

Muilla G8-mailla ja Kiinalla ei ole omaa maa-aluetta eikä niiden kanssa tiiviissä liitossa olevia maita maailmanlaajuisen sieppausjärjestelmän ylläpitoon tarvittavissa maapallon osissa.

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

7. Echelonin tyyppisen viestintäsieppausjärjestelmän yhteensopivuus unionin oikeuden kanssa

7.1. Selvennyksiä kysymyksenasetteluun

Valiokunnan toimivaltaan kuuluu muun muassa nimenomainen tehtävä tarkistaa Echelonin tyyppisen viestintäsieppausjärjestelmän yhteensopivuus yhtiön oikeuden kanssa.[1] Erityisesti on määrä selvittää, sopiiko tällainen järjestelmä yhteen tietosuojadirektiivien 95/46 EY ja 97/66 EY, EY:n perustamissopimuksen 286 artiklan ja Euroopan unionista tehdyn sopimuksen 8 artiklan 2 kohdan kanssa.

Kysymystä on syytä tarkastella kahdesta eri näkökulmasta. Ensimmäinen näkökulma perustuu luvussa 5 esitettyyn epäsuoraan todisteeseen, josta ilmenee, että Echeloniksi kutsuttu järjestelmä suunniteltiin viestintäsieppausjärjestelmäksi, jonka on tarkoitus toimittaa Yhdysvaltojen, Kanadan, Australian, Uuden-Seelannin ja Ison-Britannian tiedustelupalveluille tietoa ulkomaiden tapahtumista keräämällä ja analysoimalla viestintätietoa. Kysymys on näin ollen perinteisestä ulkomaantiedustelupalvelujen vakoilukeinosta.[2] Ensimmäisenä askeleena pyritään siten selvittämään tämänkaltaisen tiedustelupalvelujärjestelmän yhteensopivuus unionin oikeuden kanssa.

Tämän lisäksi Campbellin laatimassa STOA-kertomuksessa esitettiin syytös, jonka mukaan järjestelmää käytetään väärin kilpailuvakoiluun ja Euroopan maiden talous on kärsinyt sen vuoksi suuria tappioita. CIA:n entisen johtajan R. James Woolseyn lausunnon mukaan Yhdysvallat kylläkin vakoilee eurooppalaisia yrityksiä mutta vain huolehtiakseen markkinoiden oikeudenmukaisuudesta, sillä toimeksiantoja annetaan ainoastaan lahjonnan perusteella.[3] Jos pitää paikkansa, että järjestelmiä käytetään kilpailuvakoiluun, kysymys yhteensopivuudesta yhteisön oikeuden kanssa on nähtävä uudessa valossa. Tätä toista näkökulmaa tutkitaan siksi erikseen toisessa vaiheessa.

7.2. Tiedustelupalvelujärjestelmän yhteensopivuus unionin oikeuden kanssa

7.2.1. Yhteensopivuus EY:n oikeuden kanssa

Valtion turvallisuutta ja rikosten torjuntaa palvelevat toiminnot ja toimenpiteet eivät periaatteessa kuulu EY:n perustamissopimuksen sääntelyalaan. Euroopan yhteisö voi rajoitetun toimivallan periaatteen mukaisesti toimia vain niissä asioissa, joissa sillä on vastaavat toimivaltuudet. Niinpä se jätti johdonmukaisesti mainitut alueet Euroopan yhteisön perustamissopimukseen, erityisesti sen 95 artiklaan (entiseen 100a artiklaan) perustuvien tietosuojadirektiivien soveltamisalan ulkopuolelle. Direktiiviä 59/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta[4] sekä direktiiviä 97/66/EY henkilötietojen käsittelystä ja yksityisyyden suojasta televiestinnän alalla[5] ei sovelleta missään tapauksessa käsittelyyn[6] / toimiin[7]; joka koskee / jotka koskevat yleistä turvallisuutta,

[1] Vrt. edellä luku 1, 1.3.
[2] Vrt. luku 2.
[3] Vrt. luvut 5, 5.6 ja 5.8.
[4] EYVL L 281, 1995, s. 31.
[5] EYVL L 24, 1998, s. 1.
[6] Direktiivin 95/46 3 artiklan 2 kohta.
[7] Direktiivin 97/66 1 artiklan 3 kohta.

puolustusta, valtion turvallisuutta (myös valtion taloudellista hyvinvointia, kun käsittelyoperaatio on sidoksissa valtion turvallisuutta koskeviin kysymyksiin) tai rikosoikeuden alalla tapahtuvaa valtion toimintaa. Sama muotoilu otettiin tällä hetkellä parlamentin käsittelyssä olevaan ehdotukseen Euroopan parlamentin ja neuvoston direktiiviksi henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla.[1] Jäsenvaltion osallistuminen valtion turvallisuutta palvelevaan sieppausjärjestelmään ei siten voi olla ristiriidassa tietosuojadirektiivien kanssa.

Toiminta ei myöskään voi olla ristiriidassa EY:n perustamissopimuksen 286 artiklan kanssa, jossa tietosuojadirektiivien soveltamisala ulotetaan yhteisön toimielinten ja elinten tietojenkäsittelyyn. Sama koskee asetusta 45/2001 yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.[2] Tätäkin asetusta sovelletaan vain, kun elimet toimivat EY:n perustamissopimuksen puitteissa.[3] Väärinkäsitysten välttämiseksi korostettakoon tässä kohdin nimenomaan, ettei mikään taho ole missään vaiheessa väittänyt yhteisön toimielinten tai laitosten osallistuneen sieppausjärjestelmään eikä esittelijällä ole myöskään mitään viitteitä sellaisesta.

7.2.2. Yhteensopivuus muun EU-oikeuden kanssa

Osaston V (yhteinen ulko- ja turvallisuuspolitiikka) ja osaston VI (poliisiyhteistyö ja oikeudellinen yhteistyö rikosasioissa) alalla ei ole EY-direktiiveihin verrattavia tietosuojamääräyksiä. Euroopan parlamentti on useasti viitannut siihen, että tässä kohden vallitsee erittäin suuri toiminnan tarve.[4]

Ihmisten perusoikeuksien ja perusvapauksien suoja taataan näillä aloilla vain Euroopan unionista tehdyn sopimuksen 6 ja 7 artiklalla, erityisesti 6 artiklan 2 kohdalla, jossa unioni sitoutuu kunnioittamaan perusoikeuksia sellaisina kuin ne taataan Euroopan ihmisoikeussopimuksessa ja sellaisina kuin ne ilmenevät jäsenvaltioiden yhteisessä valtiosääntöperinteessä. Sen lisäksi, että perusoikeudet ja erityisesti Euroopan ihmisoikeussopimus sitovat jäsenvaltioita (ks. jäljempänä luku 8), tästä syntyy myös unionille velvollisuus noudattaa perusoikeuksia lainsäädännössä ja hallinnossa. Koska EU:n tasolla ei kuitenkaan toistaiseksi ole säädöstä televiestinnän valvonnasta turvallisuus- tai tiedustelupalvelutarkoituksiin[5], kysymys Euroopan unionista tehdyn sopimuksen 6 artiklan 2 kohdan rikkomisesta ei toistaiseksi nouse esiin.

---

[1] KOM (2000) 385 lop., EYVL C 365, s. 223.

[2] Asetus (EY) N:o 45/2001, EYVL L 8, 2001, s. 1.

[3] Asetuksen 3 artiklan 1 kohta; vrt. myös johdanto-osan kappale 15 "Kun yhteisöjen toimielimet ja elimet käsittelevät henkilötietoja tämän asetuksen soveltamisalaan kuulumattomien, erityisesti Euroopan unionista tehdyn sopimuksen V ja VI osastossa tarkoitettujen toimien toteuttamiseksi, yksilöiden perusoikeuksien ja -vapauksien suojelu varmistetaan noudattamalla Euroopan unionista tehdyn sopimuksen 6 artiklan määräyksiä."

[4] Vrt. esim. päätöslauselma neuvoston ja komission toimintasuunnitelmasta parhaista tavoista panna täytäntöön Amsterdamin sopimuksen määräykset vapauteen, turvallisuuteen ja oikeuteen perustuvan alueen toteuttamisesta (13844/98 - C4-0692/98 - 98/0923(CNS)), EYVL C 219, 30.7.1999, s. 61-.

[5] Telekuuntelun alalla on tällä hetkellä kaksi EU:n säädöstä, joilla kummallakaan ei säädellä kuuntelun sallimista:
– neuvoston päätöslauselma, annettu 17 päivänä tammikuuta 1995, laillisen telekuuntelun kansainvälisistä edellytyksistä (EYVL C 329, 4.11.1996), jonka liitteeseen sisältyvät laillista telekuuntelua koskevat tekniset edellytykset nykyaikaisissa televiestintäjärjestelmissä.
– neuvoston säädös, annettu 29 päivänä toukokuuta 2000, Euroopan unionista tehdyn sopimuksen 34 artiklan mukaisen yleissopimuksen tekemisestä keskinäisestä oikeusavusta rikosasioissa Euroopan unionin jäsenvaltioiden välillä (EYVL C 197, 2000, s. 1, 17 f artikla), jossa säädetään, millä edellytyksillä oikeusavun tulee olla rikosasioissa mahdollista telekuuntelun alalla. Kuunneltavien henkilöiden oikeuksia ei rajoiteta tällä mitenkään, koska jäsenvaltio, jossa kuunneltava on, voi aina kieltäytyä oikeusavusta, mikäli kyseisen valtion kansallinen lainsäädäntö ei sitä salli.

7.3. Kysymys yhteensopivuudesta, jos järjestelmää käytetään väärin talousvakoiluun

Jos jokin jäsenvaltio tukisi muun muassa kilpailuvakoilua harjoittavaa sieppausjärjestelmää antamalla omat tiedustelupalvelunsa sen käyttöön tai antamalla vieraiden tiedustelupalvelujen käyttää omaa aluettaan kyseiseen tarkoitukseen, se rikkoisi todellakin EY:n oikeutta. Jäsenvaltiot ovat nimittäin Euroopan yhteisön perustamissopimuksen 10 artiklan nojalla sitoutuneet laajaan lojaaliuteen ja erityisesti pidättymään kaikista toimenpiteistä, jotka ovat omiaan vaarantamaan sopimuksen tavoitteiden saavuttamista. Vaikkei televiestinnän sieppaus tapahtuisikaan oman maan talouden hyväksi (tämä muuten olisi verrattavissa valtiontukeen ja rikkoisi siten EY:n perustamissopimuksen 87 artiklaa) vaan kolmansien maiden hyväksi, kyseinen toiminta olisi periaatteellisessa ristiriidassa EY:n perustamissopimuksen perustana olevan yhteismarkkinoiden periaatteen kanssa, koska se merkitsisi kilpailun vääristymistä.

Lisäksi tällainen menettely rikkoisi esittelijän mielestä televiestinnän alaa koskevaa tietosuojadirektiiviä[1], koska direktiivien sovellettavuus on ratkaistava toiminnallisten eikä organisatoristen näkökohtien perusteella. Tämä ilmenee paitsi soveltamisalan sanamuodosta myös lain hengestä. Jos tiedustelupalvelut käyttävät kapasiteettiaan talousvakoiluun, niiden toiminta ei palvele turvallisuutta tai rikostentorjuntaa vaan on vieraantunut tarkoituksestaan ja kuuluu siten kokonaan direktiivin soveltamisalaan. Direktiivin 5 artiklassa kuitenkin velvoitetaan jäsenvaltiot varmistamaan viestinnän luottamuksellisuus, erityisesti niiden on "kiellettävä se, että muut kuin käyttäjät voisivat … kuunnella, salakuunnella, tallentaa tai muulla tavalla siepata tai valvoa viestejä". Poikkeuksia saa 14 artiklan mukaan tehdä vain silloin, kun se on välttämätöntä valtion turvallisuuden, maanpuolustuksen tai rikosten torjunnan turvaamiseksi. Koska talousvakoilu ei oikeuta poikkeuksiin, olisi yhteisön oikeutta siinä tapauksessa rikottu.

7.4. Tulos

Yhteenvetona voidaan todeta, että nykyisessä oikeudellisessa tilanteessa Echelonin kaltainen tiedustelupalvelujärjestelmä ei voi olla ristiriidassa unionin oikeuden kanssa, koska sillä ei ole sellaisia kosketuskohtia unionin oikeuteen, joiden vuoksi järjestelmä ei olisi yhteensopiva sen kanssa. Tämä pätee kuitenkin vain siinä tapauksessa, että järjestelmää käytetään todellakin vain valtion turvallisuuden palvelemiseen. Jos sitä sen sijaan käytetään ulkomaisten yritysten vastaiseen kilpailuvakoiluun, syntyy ristiriita EY:n oikeuden kanssa. Jos jokin jäsenvaltio osallistuisi siihen, se rikkoisi yhteisön oikeutta.

[1] Direktiivi 97/66 EY, EYVL L 24, 1998, s. 1.

8. Tiedustelupalvelun harjoittaman viestinnän kuuntelun yhdenmukaisuus yksityisyyttä koskevan perusoikeuden kanssa

8.1. Viestinnän kuuntelu puuttumisena yksityisyyttä koskevaan perusoikeuteen

Viestinnän kuuntelu ja myös tiedustelupalvelujen harjoittama tietojen hankinta tähän tarkoitukseen[1] merkitsee aina vakavaa puuttumista henkilön yksityisyyteen. Valtion harjoittama rajaton kuuntelu on sallittua vain "poliisivaltiossa". Sitä vastoin EU:n jäsenvaltioissa, joissa demokratia on vakiintunutta, pidetään kiistatta välttämättömänä, että valtion elimet ja tiedustelupalvelut kunnioittavat yksityiselämää. Tämä on yleensä kirjattu jäsenvaltioiden perustuslakeihin. Yksityisyydellä on siten erityinen suoja, ja tähän oikeuteen puuttumiseen annetaan mahdollisuus vain oikeushyväharkinnan jälkeen suhteellisuusperiaatetta noudattaen.

Ongelmat tiedostetaan myös Echelon-valtioissa. Annetuilla suojamääräyksillä pyritään kuitenkin suojaamaan omien kansalaisten yksityisyyttä, joten Euroopan kansalaiset eivät niistä yleensä hyödy. Siksi Yhdysvaltain sähköisen valvonnan ehtoja koskevissa määräyksissä valtion toimivaa tiedustelupalvelua koskevia etuja ei aseteta vastakkain tehokkaan yleisen perusoikeusturvan kanssa vaan "Yhdysvaltain kansalaisten" tarpeellisen yksityisyyden suojan kanssa.[2]

8.2. Yksityisyyden suoja kansainvälisissä sopimuksissa

Yksityisyyden merkitys perusoikeutena on otettu huomioon lukuisissa kansainvälisen oikeuden sopimuksissa.[3] Maailmanlaajuisista sopimuksista on mainittava erityisesti kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus[4], joka solmittiin vuonna 1966 YK:ssa ja jonka 17 artikla takaa yksityisyyden suojan. Yleissopimuksen kansainvälisoikeudellisia rikkomuksia koskevista kysymyksistä päättävän, 41 artiklan mukaan perustetun yleisen ihmisoikeusvaliokunnan päätöksiin ovat yhtyneet kaikki Echelon-valtiot silloin, kun kyseessä ovat olleet muiden valtioiden esittämät kanteet. Yhdysvallat ei ole kuitenkaan allekirjoittanut lisäpöytäkirjaa[5], jolla laajennettiin ihmisoikeusvaliokunnan toimivaltaa käsittämään yksityisen kansalaisen vetoomuksia, joten yksityisillä henkilöillä ei ole mahdollisuutta kääntyä ihmisoikeusvaliokunnan puoleen Yhdysvaltain rikkoessa yleissopimusta.

---

[1] Saksan liittotasavallan perustuslakituomioistuin (BVerfG), liittotasavallan 1 perustuslakioikeus 2226/94, 14.7.1999, reunanumero 187. Sen mukaan oikeuden rikkomista on [...] jo itse tietojen keruu, jos viestintää kerätään liittotasavallan tiedustelupalvelun käyttöön ja jos se muodostaa perustan myöhemmälle vertailulle etsittävien käsitteiden kanssa.

[2] Vrt. Yhdysvaltain kongressille helmikuun 2000 lopussa laadittua raporttia "Legal Standards for the Intelligence Community in Conducting Electronic Surveillance", http://www.fas.org/irp/nsa/standards.html, jossa viitataan lakiin nimeltä Foreign Intelligence Surveillance Act (FISA), painettu seuraavissa: U.S.C. 50 osaston 36 luvun 1801 § ja seur. ja Exec. Order -asetus nro 12333, 3 C.F.R. 200 (1982), painettu seuraavassa: U.S.C. 50 osaston 15 luvun 401 § ja seur. , http://www4.law.cornell.edu/uscode/50/index.html.

[3] Ihmisoikeuksien julistuksen 12 artikla; Yhdistyneiden kansakuntien kansalaisoikeuksia ja poliittisia oikeuksia koskevan yleissopimuksen 17 artikla; EU:n perusoikeuskirjan 7 artikla, Euroopan ihmisoikeussopimuksen 8 artikla; OECD:n neuvoston suositus tietojärjestelmien turvallisuutta koskevista suuntaviivoista, hyväksytty 26./27.11.1993 C(92) 188/lopull.; yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä tehdyn Euroopan neuvoston yleissopimuksen 7 artikla; vrt. STOA:n toimeksiannosta julkaisemaan tutkimukseen Development of surveillance tehnology and risk of abuse of economic information; Vol 4/5: The legality of the interception of electronic communications: A concise survey of the principal legal issues and instruments under international, European and national law (Chris Elliot), october 1999, 2.

[4] Kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus, jonka Yhdistyneiden kansakuntien yleiskokous hyväksyi 16. 12. 1966.

[5] Opitional Protocol to the International Covenant on civil and Political Rights, jonka Yhdistyneiden kansakuntien yleiskokous hyväksyi 16.12.1966.

EU:n tasolla on yritetty toteuttaa erityinen eurooppalainen perusoikeusturva laatimalla Euroopan unionin perusoikeuskirja. Perusoikeuskirjan 7 artiklassa, jonka otsikkona on yksityis- ja perhe-elämän kunnioittaminen, mainitaan jopa erikseen viestinnän kunnioittaminen.[1] Tämän lisäksi 8 artiklassa mainitaan henkilötietosuoja. Tämä olisi suojannut yksilöitä niissä tapauksissa, joissa heidän tietojaan käsitellään (automaattisesti tai ei-automaattisesti). Kuuntelussa on yleensä kyse tästä, muissa sieppaustilanteissa peräti aina.

Perusoikeuskirjaa ei ole toistaiseksi sisällytetty sopimukseen. Se sitoo siis ainoastaan kolmea elintä, jotka ovat sitoutuneet Nizzan Eurooppa-neuvoston yhteydessä annettuun juhlalliseen julistukseen, eli neuvostoa, komissiota ja Euroopan parlamenttia. Esittelijän tietämyksen mukaan yksikään näistä elimistä ei ole sekaantunut tiedustelupalvelutoimintaan. Vaikka perusoikeuskirjasta tulee täysivoimainen sen jälkeen, kun se on sisällytetty sopimukseen, on syytä huomata, että sen soveltamisalaa on rajoitettu. Perusoikeuskirjan 51 artiklan mukaisesti perusoikeuskirja koskee "unionin toimielimiä ja laitoksia… sekä jäsenvaltioita ainoastaan silloin, kun ne soveltavat unionin oikeutta". Perusoikeuskirja tulisi näin muodoin kyseeseen ainoastaan välineenä, jolla kielletään kilpailun vääristymistä aiheuttavat valtiontuet (ks. luku 7.3).

Ainoa kansainvälisesti tehokas keino kattavan yksityisyyden suojan takaamiseksi on Euroopan ihmisoikeussopimus.

8.3. Euroopan ihmisoikeussopimuksen säädökset

8.3.1. Euroopan ihmisoikeussopimuksen merkitys Euroopan unionissa

Perusoikeuksia koskeva suoja, joka sisältyy Euroopan ihmisoikeussopimukseen, on erityisen merkittävä, koska kaikki EU:n jäsenvaltiot ovat hyväksyneet sopimuksen ja se määrittää siten yhtenäisen eurooppalaisen suojatason. Sopimusvaltiot ovat sitoutuneet kansainvälisen oikeuden nojalla takaamaan Euroopan ihmisoikeussopimuksessa määritellyt oikeudet sekä noudattamaan Strasbourgissa toimivan Euroopan ihmisoikeustuomioistuimen päätöksiä. Euroopan ihmisoikeustuomioistuin voi tutkia, ovatko kulloinkin voimassa olevat kansalliset säädökset yhdenmukaiset Euroopan ihmisoikeussopimuksen kanssa. Jos sopimusvaltiot rikkovat ihmisoikeuksia, ne voidaan tuomita ja velvoittaa maksamaan korvauksia. Euroopan ihmisoikeussopimuksen merkitys on lisääntynyt myös siksi, että Euroopan yhteisöjen tuomioistuin on pyytänyt sitä toistuvasti mukaan päätöksentekoon tutkiessaan lakeja jäsenvaltioiden yleisten oikeusperiaatteiden valossa. Lisäksi Amsterdamin sopimuksella vahvistettiin EY:n perustamissopimuksen 6 artiklan 2 kohdan mukainen EU:n velvoite kunnioittaa perusoikeuksia sellaisena kuin ne on taattu Euroopan ihmisoikeussopimuksessa.

[1] Perusoikeuskirjan mukaan jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja viestintäänsä kohdistuvaa kunnioitusta.

8.3.2. Euroopan ihmisoikeussopimuksen antaman suojan laajuus alueen ja henkilöiden kannalta

Euroopan ihmisoikeussopimuksessa taatut oikeudet ovat yleisiä ihmisoikeuksia eivätkä ne siksi ole sidottuja kansalaisuuteen. Ne on myönnettävä jokaiselle henkilölle, joka kuuluu sopimusvaltioiden lainkäyttövallan piiriin. Tämä merkitsee, että ihmisoikeuksia on joka tapauksessa noudatettava koko valtion alueella ja paikalliset poikkeukset merkitsisivät sopimuksen rikkomista. Sen lisäksi ne ovat kuitenkin voimassa myös sopimusvaltioiden alueen ulkopuolella, jos valtio on siellä julkisen vallan harjoittajana. Euroopan ihmisoikeussopimuksen takaamat oikeudet sopimusvaltioon nähden kuuluvat siten myös valtion alueen ulkopuolella oleville henkilöille, jos sopimuksen allekirjoittanut valtio puuttuu heidän yksityisyyden suojaansa alueensa ulkopuolella[1].

Viimeksi mainittu seikka on tässä erityisen tärkeä, koska perusoikeuksia koskeviin ongelmiin televiestinnän kuuntelun alueella liittyy se erityispiirre, että kuuntelusta vastaava valtio ja kuunneltava voivat olla eri alueilla ja varsinainen salakuunteluprosessi voi tapahtua eri paikassa. Tämä koskee erityisesti kansainvälistä viestintää ja mahdollisesti myös kansallista viestintää, jos tiedot kulkevat ulkomailla olevia kaapeleita pitkin. Kun kyse on ulkomaantiedustelupalvelusta, tämä on jopa tyypillinen tilanne. On myös mahdollista, että tietoja tiedustelupalvelun pyytämästä valvonnasta luovutetaan edelleen muille valtioille.

8.3.3. Televiestinnän kuuntelun luvallisuus Euroopan ihmisoikeussopimuksen 8 artiklan nojalla

Euroopan ihmisoikeussopimuksen 8 artiklan 1 kohdan nojalla "jokaisella […] oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta." Puhelujen ja televiestinnän suojaamista ei tosin nimenomaan mainita, mutta Euroopan ihmisoikeustuomioistuimen oikeuskäytännön mukaan ne sisältyvät ihmisoikeussopimuksen 8 artiklan mukaisen suojan käsitteisiin "yksityiselämä" ja "kirjeenvaihto".[2] Perusoikeussuoja ei tällöin kata ainoastaan viestinnän sisältöä vaan myös ulkoisten puhelutietojen rekisteröinnin. Vaikka tiedustelupalvelu rekisteröi ainoastaan sellaisia tietoja kuin yhteyden ajankohdan ja keston tai valitun numeron ja muita vastaavia tietoja, kyseessä on tällöinkin yksityisyyden suojaan puuttuminen.[3]

[1] Vrt. EGMR Loizidou/Türkei, 23.3.1995, Z 62 lisätodisteineen "...the concept of 'jursidiction' under this provision is not restricted to the national territory of the High Contracting Parties.[...] responsibility can be involved because of acts of their authorities, whether performed within or outside national boundaries, which produce effects outside their own territory", missä viitataan teokseen Euroopan ihmisoikeustuomioistuin, Drozd ja Janousek, 26.6.1992, Z 91. vrt. tarkemmin Jacobs, The European Convention on Human Rights (1996), 21 ja seur.

[2] Vrt. Euroopan ihmisoikeustuomioistuin, Klass ym., 6.9.1978, Z 41.

[3] Vrt. Euroopan ihmisoikeustuomioistuin, Malone, 2.8.1984, Z 83 ja seur; samoin Davy, B/Davy/U, Aspekte staatlicher Informationssammlung und Art 8 MRK, JBl 1985, 656.

Perusoikeutta ei ihmisoikeussopimuksen 8 artiklan 2 kohdan mukaan myönnetä rajoituksetta. Yksityisyyden kunnioittamisen perusoikeuteen voidaan puuttua, jos siihen on kansallisen lainsäädännön mukainen oikeusperusta.[1] Tämän lainsäädännön tulee olla yleisesti saatavilla ja sen seurauksien ennakoitavissa.[2]

Jäsenvaltiot eivät voi vapaasti päättää tilanteista, joissa perusoikeuksiin voidaan puuttua. Euroopan ihmisoikeussopimuksen 8 artikla sallii ne vain 2 kohdassa luetelluissa tarkoituksissa. Näitä ovat varsinkin kansallinen turvallisuus, yleinen rauha ja järjestys, rangaistavien toimien estäminen mutta myös maan taloudellinen hyvinvointi[3], joka ei kuitenkaan oikeuta talousvakoilua, koska tähän lasketaan ainoastaan "demokraattisessa yhteiskunnassa tarpeellinen" perusoikeuksiin puuttuminen. Jokaisen puuttumistilanteen kohdalla tulee valita lievin tavoitteen saavuttamiseen soveltuva keino, minkä lisäksi väärinkäyttö on pystyttävä estämään riittävän varmasti.

8.3.4. Euroopan ihmisoikeussopimuksen 8 artiklan vaikutus tiedustelupalvelujen toimintaan

Nämä yleiset periaatteet merkitsevät tiedustelupalvelujen toiminnan perustuslainmukaisuuden kannalta seuraavaa: Jos kansallisen turvallisuuden varmistamiseksi näyttää tarpeelliselta antaa tiedustelupalveluille lupa televiestinnän sisällön tai vähintään yhteystietojen sieppaamiseen, sen on perustuttava kansallisiin oikeussäännöksiin ja asiaa koskevien määräysten on oltava yleisesti saatavilla. Toiminnan seurausten tulee olla henkilön ennakoitavissa, mutta erityiset salassapitovaatimukset on kuitenkin otettava huomioon. Siten tuomioistuin on todennut eräässä tuomiossaan, joka koskee työntekijöiden salaisen valvonnan 8 artiklan mukaisuutta kansalliseen turvallisuuteen liittyvillä aloilla, että tässä erikoistapauksessa ennakoitavuusvaatimus ei voi olla sama kuin muilla aloilla.[4] Tuomioistuin vaati kuitenkin tässäkin yhteydessä, että oikeussäännöksistä on joka tapauksessa käytävä ilmi, missä oloissa ja millä ehdoilla valtio saa salaa ja siten mahdollisesti vaarallisella tavalla puuttua yksityisyyden suojaan.[5]

Tiedustelupalvelujen toiminnan ihmisoikeuksien mukaisuutta arvioitaessa on otettava huomioon, että vaikka kansallinen turvallisuus on peruste myöntää lupa yksityisyyden suojaan puuttumiseen, asiassa on Euroopan ihmisoikeussopimuksen 8 artiklan 2 kohdan mukaan sovellettava suhteellisuusperiaatetta: Kansallinen turvallisuuskin antaa oikeuden yksityisyyden suojaan puuttumiseen vain silloin, kun se on demokraattisessa yhteiskunnassa välttämätöntä. Euroopan ihmisoikeustuomioistuin on tässä yhteydessä ilmoittanut yksiselitteisesti, että valtion etuja kansallisen turvallisuutensa turvaamisessa tulee punnita vertaamalla siihen, miten vaikeaa on henkilön yksityisyyden kunnioittamiseen liittyviin etuihin puuttuminen.[6] Yksityisyyden

[1] Euroopan ihmisoikeustuomioistuimen oikeuskäytännön mukaan (erityisesti Sunday Times, 26.4.1979, Z 46 alkaen, Silver ym., 25.3.1983, Z 85 ja seur.) 8 artiklan käsite "law" ei tarkoita ainoastaan lakeja muodollisessa merkityksessä vaan myös lakiastetta alhaisempia oikeuden määräyksiä, mahdollisesti jopa kirjoittamatonta oikeuskäytäntöä. Edellytyksenä on kuitenkin aina, että se on säännöksen alaisten henkilöiden ennakoitavissa, missä olosuhteissa tällainen puuttuminen on mahdollista. Vrt. Wessley, Das Fernmeldegeheimnis – ein unbekanntes Grundrecht? ÖJZ 1999, 491 ff, 495.

[2] Silver ym., 25.3.1983, Z 87 f.

[3] Euroopan ihmisoikeustuomioistuin hyväksyi "taloudellisen hyvinvoinnin" perusteeksi tapauksessa, jossa oli kyse julkisten korvausmaksujen osoittamisen kannalta merkittävien lääketieteellisten tietojen luovuttamisesta M.S./Ruotsi, 27.8.1997, Z 38; samoin tapauksessa, jossa oli kyse Alankomaiden karkottamasta henkilöstä, joka eli sosiaalitukien varassa sen jälkeen, kun hänen oleskelulupansa perusteen voimassaolo oli lakannut. Ciliz/Niederlande, 11.7.2000, Z 65.

[4] Euroopan ihmisoikeustuomioistuin, Leander, 26.3.1987, Z 51.

[5] Euroopan ihmisoikeustuomioistuin, Malone, 2.8.1984, Z 67.

[6] Euroopan ihmisoikeustuomioistuin, Leander, 26.3.1987, Z 59, Sunday Times, 26.4.1979, Z 46 ja seur.

suojaan puuttumiset eivät tosin rajoitu välttämättä tarpeellisiin, mutta ei riitä, että ne ovat vain hyödyllisiä tai toivottavia[1]. Käsitys, että kaiken televiestinnän kuuntelu olisi paras suoja järjestäytynyttä rikollisuutta vastaan, olisi Euroopan ihmisoikeussopimuksen 8 artiklan vastainen silloinkin, kun se olisi luvallista kansallisten oikeusäännösten nojalla.

Lisäksi tiedustelupalvelutoiminnan erityisluonne edellyttää salassapitoa ja sitten erityistä etujen punnitsemista, minkä vuoksi vastaavasti on sallittava suuremmat valvontamahdollisuudet. Tuomioistuin on nimenomaan korostanut, että salaiseen valvontajärjestelmään kansallisen turvallisuuden varmistajana sisältyy riski, että se demokratian puolustamisen varjolla heikentää demokratiaa tai jopa tuhoaa sen, ja että sen vuoksi tarvitaan asianmukaiset ja tehokkaat takuut tällaista väärinkäyttöä vastaan.[2] Tiedustelupalvelujen lainmukainen toiminta on siksi perustuslain mukaista vain silloin, kun Euroopan ihmisoikeussopimuksen sopimusvaltio on luonut riittävät valvontajärjestelmät ja muut takuut väärinkäytön varalta. Tuomioistuin toi Ruotsin tiedustelupalvelun toiminnan yhteydessä esiin, että se pitää erityisen tärkeänä kansanedustajien läsnäoloa poliisin valvontaelimissä samoin kuin oikeusministeriön, parlamentin oikeusasiamiehen ja parlamentin oikeusasioiden valiokunnan suorittamaa valvontaa. Tässä valossa vaikuttaa arveluttavalta, että Ranskassa, Kreikassa, Irlannissa, Luxemburgissa ja Espanjassa ei ole omia tiedustelupalvelujen parlamentaarisia valvontaelimiä[3] eikä niissä myöskään tunneta pohjoismaiden parlamenttien oikeusasiamiehiin verrattavaa valvontajärjestelmää.[4] Esittelijä pitää siksi tervetulleina Ranskan kansalliskokouksen puolustusvaliokunnan pyrkimyksiä perustaa valvontavaliokunta,[5] varsinkin, kun Ranskalla on käytössään teknisesti ja maantieteellisesti huomattava tiedustelupalvelukapasiteetti.

8.4. Velvollisuus valppauteen vieraiden tiedustelupalvelujen toiminnan varalta

8.4.1. Euroopan ihmisoikeussopimuksen 8 artiklan kiertäminen muiden valtioiden tiedustelupalveluja käyttämällä on kiellettyä

Kuten edellä perusteellisesti selostettiin, sopimusvaltioita koskevat tietyt ehdot, joiden täyttyessä niiden tiedustelupalvelujen toiminta on ihmisoikeussopimuksen 8 artiklan mukaista. On selvää, että tiedustelupalvelut eivät vapaudu näistä velvoitteista turvautumalla muiden tiedustelupalvelujen toimintaan, joita koskevat vähemmän tiukat säännökset. Muuten laillisuusperiaate ja siihen liittyvät saatavuuden ja ennakoitavuuden osa-alueet ja Euroopan ihmisoikeustuomioistuimen oikeussäännöstön sisältö menettäisivät merkityksensä.

Tämä merkitsee ensinnäkin, että tietojen vaihto tiedustelupalvelujen kesken on sallittua vain rajoitetusti. Tiedustelupalvelu voi pyytää tietoja toiselta tiedustelupalvelulta vain silloin, kun ne voidaan hankkia sellaisin ehdoin, jotka oma kansallinen oikeussäännöstö sallii. Lain sallimaa toimintasädettä ei saa laajentaa sopimuksilla muiden tiedustelupalvelujen kanssa. Samoin tiedustelupalvelu voi työskennellä vieraalle tiedustelupalvelulle sen ohjeiden mukaan vain, jos se

[1] Euroopan ihmisoikeustuomioistuin, Silver ym., 24.10.1983, Z 97.
[2] Euroopan ihmisoikeustuomioistuin, Leander, 26.3.1987, Z 60.
[3] Esittelijä on tietoinen siitä, että Luxemburgissa ja Irlannissa ei ole ulkomaantiedustelupalvelua eivätkä ne harjoita kansainvälistä tiedustelua. Erityisen valvontaelimen vaatimus koskee tässä tapauksessa ainoastaan kotimaassa tapahtuvaa tiedustelupalvelutoimintaa.
[4] Katso lisätietoja tiedustelupalvelun valvontatilanteesta jäsenmaissa luvusta 9.
[5] Vrt. lakiehdotukseen "Proposition de loi tendant à la création de délégations parlementaires pour le renseignement" ja kansanedustaja Arthur Paechtin tähän liittyvään raporttiin N° 1951 Assmeblée nationale, 11. lainsäädäntöjakso, rekisteröity 23. marraskuuta 1999.

on vakuuttunut siitä, että toiminta on oman kansallisen oikeussäännöstön mukaista. Vaikka tiedot olisi tarkoitettu toisen valtion käyttöön, oikeussäännöstön alaisen henkilön lainvastainen yksityisyyden suojaan puuttuminen on joka tapauksessa perustuslain vastaista.

Lisäksi Euroopan ihmisoikeussopimuksen sopimusvaltiot eivät saa sallia muiden maiden tiedustelupalvelujen toimintaa alueellaan, jos on aihetta olettaa, että niiden toiminta ei täytä Euroopan ihmisoikeussopimuksen vaatimuksia.[1]

8.4.2. Seuraukset Euroopan ulkopuolisten tiedustelupalvelujen sallitulle toiminnalle Euroopan ihmisoikeussopimuksen sopimusvaltioiden alueella

8.4.2.1. Euroopan ihmisoikeustuomioistuimen asiaa koskeva oikeuskäytäntö

Hyväksymällä Euroopan ihmisoikeussopimuksen sopimusvaltiot ovat sitoutuneet siihen, että niiden riippumattomuus on sidoksissa perusoikeuksien tarkasteluun. Ne eivät voi päästä tästä velvoitteesta luopumalla riippumattomuudestaan. Nämä valtiot ovat edelleen vastuussa omasta alueestaan ja niillä on velvoitteensa eurooppalaisen oikeussäännöstön alaisia henkilöitä kohtaan myös silloin, kun tiedustelupalvelutoimintaan liittyvää valtaa käyttää toinen valtio. Euroopan ihmisoikeustuomioistuin on sittemmin vahvistanut pysyväksi oikeuskäytännöksi sopimusvaltioiden velvollisuuden toteuttaa soveliaita toimia yksityisyyden suojaamiseksi, niin että yksityiset henkilöt (!) eivät rikkoisi Euroopan ihmisoikeussopimuksen 8 artiklaa. Tämä pätee myös horisontaalisella tasolla, jolloin yksilöä vastassa ei ole valtio vaan toinen henkilö.[2] Jos valtio sallii toisen valtion tiedustelupalvelun toiminnan alueellaan, suojaustarve on huomattavasti suurempi, koska tällöin valta on toisella viranomaisella. Tässä yhteydessä vaikuttaa loogiselta pitää lähtökohtana, että valtion on valvottava, että sen alueella tapahtuva tiedustelupalvelutoiminta on ihmisoikeuksien mukaista.

8.4.2.2. Seuraukset asemille

Saksan Bad Aiblingissa Amerikan Yhdysvaltojen käyttöön on annettu oma alue ainoastaan satelliittien vastaanottamista varten. Ison-Britannian Menwith Hillissä maaston käyttö sallitaan samaan tarkoitukseen. Jos amerikkalainen tiedustelupalvelu kuuntelisi näillä asemilla yksityisten tai yritysten ei-sotilaallista viestintää, joka on peräisin Euroopan ihmisoikeussopimuksen allekirjoittaneesta valtiosta, Euroopan ihmisoikeussopimuksen mukainen valvontavelvollisuus tulisi voimaan. Tämä tarkoittaa käytännössä, että Saksalla ja Yhdistyneellä kuningaskunnalla on Euroopan ihmisoikeussopimuksen sopimusvaltioina velvollisuus varmistua siitä, että amerikkalaisen tiedustelupalvelun toiminta on perusoikeuksien mukaista. Tämä korostuu siksikin, että kansalaisjärjestöjen ja lehdistön edustajat ovat jo useita kertoja ilmaisseet huolensa NSA:n toiminnasta.

[1] Vrt. myös Yernault, "Echelon" et l'Europe. La protection de la vie privée face à l'espionnage des communications, Journal des tribunaux, Droit Européen 2000, 187 ja seur.
[2] Euroopan ihmisoikeustuomioistuin, Abdulaziz, Cabales ja Balkandali, 28.5.1985, Z 67; X ja Y/Alankomaat, 26.3.1985, Z 23; Gaskin vs Yhdistynyt kuningaskunta 7.7.1989, Z 38; Powell ja Rayner, 21.2.1990, Z 41.

8.4.2.3. Vaikutukset toisen valtion toimeksiannosta tehtävään kuunteluun

Tiedustelupalvelu GCHQ:n antamien tietojen mukaan Ison-Britannian Morwenstow'ssa siepataan yhteistyössä NSA:n kanssa siviiliviestintää tarkoin sen ohjeita noudattaen ja välitetään viestintä raakamateriaalina Yhdysvalloille. Myös toimeksiannosta kolmansille osapuolille tehtäviä töitä koskee velvollisuus tarkistaa, että toimeksianto on perusoikeuksien mukainen.

8.4.2.4. Erityinen huolellisuusvelvollisuus sopimuksen ulkopuolisten maiden tapauksessa

Kun on kyse Euroopan ihmisoikeussopimuksen sopimusvaltioista, voidaan tietyssä määrin vastavuoroisesti olettaa, että myös toinen valtio noudattaa Euroopan ihmisoikeussopimusta. Näin on ainakin silloin, kun Euroopan ihmisoikeussopimuksen sopimusvaltiolle ei ole todistettu, että se toimisi järjestelmällisesti ja jatkuvasti Euroopan ihmisoikeussopimuksen vastaisesti. Yhdysvallat on valtio, joka ei ole allekirjoittanut Euroopan ihmisoikeussopimusta eikä myöskään sitoutunut siihen verrattavaan valvontajärjestelmään. Sen tiedustelupalvelujen toiminta on erittäin tarkoin säädeltyä, kun on kyse Yhdysvaltain kansalaisista tai henkilöistä, jotka oleskelevat laillisesti Yhdysvalloissa. NSA:n toimintaan ulkomailla sovelletaan kuitenkin erilaisia säädöksiä, joista huomattavan monet ovat luokiteltuja eivätkä siksi yleisesti saatavilla. Lisäksi tässä yhteydessä on huolestuttavaa, että vaikka tiedustelupalvelu on edustajainhuoneen ja senaatin valiokunnan valvonnan alainen, nämä valiokunnat osoittavat vain vähäistä mielenkiintoa NSA:n ulkomailla harjoittamaa toimintaa kohtaan.

Näyttää siksi perustellulta vedota Saksaan ja Englantiin, jotta ne ottaisivat vakavasti Euroopan ihmisoikeussopimuksen tuomat velvoitteensa ja tulevaisuudessa sallisivat NSA:n tiedustelupalvelutoimet alueellaan vain, jos ne ovat Euroopan ihmisoikeussopimuksen mukaisia. Tässä yhteydessä on otettava huomioon kolme päänäkökohtaa.

1. Euroopan ihmisoikeussopimuksen mukaan yksityisyyden suojaan voidaan puuttua vain sellaisten säädösten nojalla, jotka ovat yleisesti saatavilla ja joiden seuraukset ovat yksilön ennakoitavissa. Tämä vaatimus täyttyy vain, jos Yhdysvallat ilmoittaa Euroopan kansalaisille, millä tavalla ja missä olosuhteissa tiedustelua tehdään. Jos ilmoitetut tavat ja ehdot eivät ole Euroopan ihmisoikeussopimuksen mukaisia, asiaa koskevat säännökset on mukautettava eurooppalaiseen suojatasoon.

2. Euroopan ihmisoikeussopimuksen mukaan yksityisyyden suojaan puuttuminen ei saa olla kohtuutonta, ja on valittava lievin keino. Euroopan kansalaisen kannalta Euroopassa tapahtuva yksityisyyden suojaan puuttuminen on arvioitava lievemmäksi kuin Amerikan taholta tuleva, koska vetoaminen kansallisiin oikeusasteisiin on mahdollista vain ensimmäisessä tapauksessa.[1] Siksi yksityisyyden suojaan puuttumisen tulee mahdollisuuksien mukaan tapahtua joko Saksan tai Englannin taholta, johdonmukaisesti kuitenkin siltä taholta, jossa syytteeseenpano tapahtuu. Yhdysvallat on yrittänyt toistuvasti tehdä televiestinnän kuuntelun oikeutetuksi moittimalla eurooppalaisia korruptiosta ja lahjonnasta.[2] Yhdysvalloille on huomautettu, että kaikissa EU:n valtioissa on toimiva rikosoikeusjärjestelmä. Jos tästä on epäilystä, Yhdysvaltain tulee jättää oikeuskäsittely vastapuolen huoleksi. Ellei epäilystä ole, kuuntelu on katsottava kohtuuttomaksi, siksi ihmisoikeuksien vastaiseksi ja kielletyksi. Euroopan ihmisoikeussopimuksen mukaiseksi

[1] Tämä vastaa myös Euroopan ihmisoikeussopimuksen 13 artiklaa, jonka mukaan loukatulle annetaan oikeus tehokkaaseen oikeussuojakeinoon kansallisten oikeusasteiden edessä.
[2] Woolsey (entinen CIA:n johtaja), Why America Spies on its Allies, The Wall Street Journal Europe, 22.3.2000, 31.

toiminta on siis katsottava vain silloin, kun Yhdysvallat harjoittaa ainoastaan sellaista kuuntelua, joka on tarpeen sen kansallisen turvallisuuden takaamiseksi mutta luopuu kuuntelusta, jolla pyritään rikosten selvittämiseen.

3. Kuten edellä jo todettiin, Euroopan ihmisoikeustuomioistuin edellytti perusoikeuksien noudattamista koskevassa oikeuskäytännössään, että käytössä on riittävät valvontajärjestelmät ja takeet väärinkäyttöä vastaan. Tämä merkitsee sitä, että Yhdysvaltain Euroopan maaperältä käsin toteuttama televiestinnän kuuntelu on ihmisoikeuksien mukaista vain, jos Yhdysvallat luo vastaavat tehokkaat valvontajärjestelmät niitä tapauksia varten, joissa se sieppaa sieltä käsin viestintää kansallisen turvallisuutensa takaamiseksi, tai jos NSA Euroopan maaperällä toimiessaan sitoutuu noudattamaan vastaanottajamaan (eli Saksan tai Ison-Britannian) valvontajärjestelmän sääntöjä.

Vain näissä kolmessa kohdassa esitetyn vaatimuksen täyttyessä voidaan taata, että Yhdysvaltain menettely televiestinnän sieppaamisessa on Euroopan ihmisoikeussopimuksen mukaista ja että Euroopan ihmisoikeussopimuksella taattu yhtenäinen suojataso Euroopassa voidaan säilyttää.

9. Onko Euroopan unionin kansalaisilla riittävä suoja tiedustelupalvelujen toimintaa vastaan?

9.1. Tiedustelupalvelujen toiminnalta suojaaminen: kansallisten parlamenttien tehtävä

Tiedustelupalvelujen toiminta saattaa tulevaisuudessa olla yhteisen ulko- ja turvallisuuspolitiikan eräs osatekijä, mutta toistaiseksi asiaa koskevia EU-tason säännöksiä ei vielä ole,[1] joten tiedustelupalvelujen toiminnalta suojaamisen muodot määräytyvät yksinomaan kansallisten oikeusjärjestysten perusteella.

Kansallisilla parlamenteilla on tässä kaksitahoinen tehtävä: lainsäätäjinä ne tekevät ratkaisut tiedustelupalvelujen toiminnan sisällöstä ja valtuuksista sekä tiedustelupalvelutoiminnan valvonnan muodoista. Kuten edellisessä luvussa on yksityiskohtaisesti selvitetty, televiestinnän valvonnan sallittavuutta koskevia määräyksiä antaessaan parlamenttien on toimittava Euroopan ihmisoikeussopimuksen 8 artiklan asettamissa rajoissa. Tämä merkitsee, että määräysten on oltava välttämättömiä ja suhteellisia ja niiden seurausten yksilön kannalta ennakoitavissa. Lisäksi on luotava valvontaviranomaisten valtuuksia vastaavat asianmukaiset ja tehokkaat kontrollimekanismit.

Useimmissa valtioissa kansallisilla parlamenteilla on aktiivinen rooli myös valvontaviranomaisina, koska toimeenpanovallan valvonta (ja siten myös tiedustelupalvelujen valvonta) on lakien säätämisen ohella toinen parlamenttien "klassisista" tehtävistä. Valvonnan muodot EU:n jäsenvaltioissa poikkeavat kuitenkin hyvin paljon toisistaan. Useissa valtioissa on rinnakkain parlamentaarisia ja parlamentin ulkopuolisia elimiä.

9.2. Kansallisten viranomaisten valvontatoimia koskevat valtuudet

Valtio saa yleensä harjoittaa kuuntelua oikeustutkintaan, sisäisen rauhan ja järjestyksen takaamiseen ja valtion (ulkoiseen) turvallisuuteen[2] liittyvistä syistä.

Televiestintäsalaisuuden saa murtaa kaikissa jäsenvaltioissa oikeustutkinnan toimittamiseksi, mikäli epäilyt todellisen henkilön tekemästä (usein ankaran rangaistuksen alaisesta, siis erityisen vakavasta) rikoksesta ovat riittävät. Asiaan puuttumiseksi tarvittavat painavat syyt edellyttävät tällöin yleensä oikeuden lupaa[3]. Kuuntelun kestosta, sen valvonnasta ja tietojen hävittämisestä on annettu tarkat ohjeet.

Sisäisen turvallisuuden ja järjestyksen takaamiseksi konkreettisen rikosepäilyn ollessa kyseessä valtion harjoittama tiedonhankinta ulotetaan tapauskohtaisissa tutkimuksissa laajemmalle. Ääriryhmien tai kumouksellisten liikkeiden, terrorismin ja järjestäytyneen rikollisuuden varhaista tunnistamista varten kansallinen lainsäädäntö sallii tietojen hankkimisen myös määrätyistä henkilöistä tai ryhmistä. Asiaan vaikuttavien tietojen keruu ja analysointi on tällöin erityisten sisäisten tiedustelupalvelujen tehtävänä.

---

[1] Vrt. luku 7.

[2] Myös Euroopan ihmisoikeussopimuksen 8 artiklan 2 kohdan mukaan nämä tunnustetaan perusteiksi puuttua yksityisyyteen. Vrt. edellä kohta 8.3.2.

[3] Yhdistyneen kuningaskunnan oikeus poikkeaa tästä: siellä lupia koskevat päätökset tekee ministeri (Secretary of State) (Regulation of Investigatory Powers Act 2000, Section 5 (1) ja (3) (b).

Tärkeä osa kuuntelutoimista on itse asiassa valtion turvallisuuspalvelun toimintaan kuuluvaa kuuntelua. Ulkomaita koskevien merkityksellisten tietojen käsittely, arviointi ja esittäminen kuuluvat yleensä erityisen ulkomaantiedustelupalvelun[1] tehtäviin. Kuuntelun kohteena eivät tavallisesti ole konkreettiset yksittäiset henkilöt, vaan pikemminkin tietyt alueet tai taajuudet. Ulkomaantiedustelupalvelun käytössä olevien keinojen ja oikeudellisten valtuuksien lisäksi esiintyy monenlaisia muita toimia, jotka ulottuvat puhtaasti sotilaallisesta lyhytaalloilla tapahtuvasta radiotiedustelusta kaikenlaisten ulkomaihin suuntautuvien televiestintäyhteyksien valvontaan. Monissa jäsenvaltioissa televiestinnän kuuntelu puhtaasti tiedustelupalvelutarkoituksiin on kokonaan kielletty,[2] toisissa jäsenvaltioissa se on sallittu ministerien antaman määräyksen perusteella[3] – eräissä tapauksissa ehtona on riippumattoman komission lupa[4] –, eräiden viestintämuotojen osalta se on sallittu jopa ilman mitään rajoitusta[5]. Monien ulkomaantiedustelupalvelujen suhteellisen suuret valtuudet johtuvat siitä, että niiden tavoitteena on ulkomaisen viestinnän kuuntelu ja sen vuoksi niiden toiminta koskettaa vain pientä osaa omista oikeusalamaisista, jolloin asiaan liittyvä huoli on oleellisesti vähäisempi.

9.3. Tiedustelupalvelujen valvonta

Tehokas ja kattava valvonta on erityisen tärkeää ensinnäkin siksi, että tiedustelupalvelut tekevät työtään salassa ja niiden työ ulottuu pitkälle aikavälille, toisin sanoen henkilöt ovat kuuntelun kohteina usein pitkän aikaa tai (oikeudellisesta tilanteesta riippuen) he eivät saa lainkaan tietää kuuntelusta. Toiseksi valvonta on tärkeää siksi, että kuuntelutoimet kohdistuvat usein suurehkoihin, löyhästi rajattuihin henkilöryhmiin, jolloin valtio voi erittäin nopeasti saada haltuunsa hyvin suuren määrän henkilökohtaisia tietoja.

Kaikkia valvontaelimiä – kokonaan niiden muodosta riippumatta – koskee luonnollisesti ongelma, että tiedustelupalvelujen erityisluonteen vuoksi ei useinkaan ole todettavissa, annetaanko kaikki tiedot todella elinten käyttöön vai jätetäänkö osa antamatta. Määräysten antamisessa on sen vuoksi oltava erittäin huolellisia. Periaatteessa voidaan lähteä siitä, että, valvonta on tehokasta ja niin ollen kuuntelutoimien laillisuus on laajalti taattu silloin, kun televiestinnän valvonnan määrääminen on rajattu ylimmän hallintotason tehtäväksi, kun sen toteuttamiseen vaaditaan oikeuden etukäteen myöntämä lupa ja kun riippumaton elin valvoo myös toimien toteuttamista. Lisäksi demokratiapoliittisesta ja oikeusvaltioperiaatteen toteutumisen näkökulmasta tarkastellen on toivottavaa, että vallanjaon periaatteen mukaisesti parlamentaarinen elin valvoo tiedustelupalvelujen toimintaa kokonaisuutena.

Saksassa tämä on toteutunut pääosin. Siellä telekuunteluun liittyviä toimia koskevat määräykset antaa asiasta vastaava liittohallituksen ministeri. Erittäin kiireellisiä tapauksia lukuun ottamatta asiasta on ennen toimiin ryhtymistä ilmoitettava erityiselle riippumattomalle, määräyksiä vapaasti noudattavalle komissiolle ("G 10 -komissio"[6]), joka päättää toimen tarpeellisuudesta ja sallittavuudesta. Silloin, kun Saksan ulkomaantiedustelupalvelulle BND:lle voidaan antaa oikeus

[1] Ulkomaantiedustelupalvelujen toiminnasta on perusteellinen esitys luvussa 2.
[2] Koskee Itävaltaa ja Belgiaa.
[3] Koskee Isoa-Britanniaa (Regulation of Investigatory Powers Act, Section 1) ja langallisen viestinnän osalta Ranskaa (Art 3 une 4 Loi 91-646 du 10 Juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications).
[4] Koskee Saksaa, laki kirje-, posti- ja televiestintäsalaisuuden rajoittamisesta (Laki perustuslain 10 artiklan soveltamisesta). Lain 9 § mukaan komissiolle on tehtävä ilmoitus ennen toimeenpanoa (lukuun ottamatta erittäin kiireellisiä tapauksia).
[5] Koskee langatonta viestintää Ranskassa (Art 20 Loi 91-646 du 10 Juillet 1991, loi relative au secret des correspondances émises par la voie des télécommunications).
[6] Vrt. perusteellinen esitys seur. lähteessä: Die Parlamentarische Kontrolle der Nachrichtendienste in Deutschland, tilanne 9.9.2000, julkaisija Saksan liittopäivät, PKGr:n sihteeristö.

kuunnella langatonta televiestintää suodattamalla sitä hakusanoja käyttäen, komissio päättää myös luvallisista hakusanoista. G 10 -komission tehtävänä on myös valvoa laissa määrätyn ilmoituksen antamista asianomaisille sekä BND-tiedustelupalvelun hankkimien tietojen hävittämistä.

Lisäksi Saksassa on parlamentin valvontaelin (PKGr)[1], johon kuuluu yhdeksän kansallisen parlamentin jäsentä ja joka valvoo Saksan kaikkien kolmen tiedustelupalvelun toimintaa. PKGr:llä on oikeus tutustua asiakirjoihin, kuulla tiedustelupalvelujen työntekijöitä, vierailla tiedustelupalveluissa ja saada tietoja. Tietojen antamisesta voidaan kieltäytyä vain silloin, kun kieltäytyminen on välttämätöntä tietojen käyttöoikeuteen liittyvistä pakottavista syistä, ulkopuolisten yksityisyyden suojan vuoksi tai jos on kysymys asioista, jotka kuuluvat toimeenpanoelinten vastuun ydinalueisiin. PKGr:n neuvottelut ovat salaisia, ja jäsenet ovat myös virasta erottuaan salassapitovelvollisia. PKGr antaa vaalikauden puolivälissä ja lopussa Saksan liittopäiville kertomuksen valvontatoiminnasta.

Näin laaja ja käytännössä aukoton tiedustelupalvelujen valvonta on kuitenkin poikkeus jäsenvaltioissa.

Esimerkiksi Ranskassa[2] tarvitaan pääministerin lupa vain sellaisiin kuuntelutoimiin, jotka edellyttävät kaapelin salakuuntelua. Erityisesti tätä varten perustetulle komissiolle (Commission nationale de contrôle des interceptions de sécurité), jonka jäseninä ovat yksi kansalliskokousedustaja ja yksi senaattori, kuuluu vain näitä koskeva valvonta. Ministerin tai hänen edustajansa anomaa kuuntelutoimea koskeva lupa toimitetaan komission puheenjohtajalle, joka voi laillisuusepäilystapauksessa saattaa asian komission käsiteltäväksi. Komissio antaa sen jälkeen suosituksensa, ja jos epäillään rikosoikeudellisesti merkittävää lainrikkomusta, komissio ilmoittaa asiasta yleiselle syyttäjälle. Kansallisten etujen puolustamiseksi toimitettavaa kuuntelua, johon sisältyy radioliikenteen kuuntelua ja siis myös satelliittien kautta hoidettavaa viestintää, eivät koske mitkään rajoitukset eikä niitä siten myöskään valvo mikään komissio.

Ranskan tiedustelupalvelujen työtä ei valvo muiltakaan osin mikään erityinen parlamentin valvontavaliokunta. Asiaa kuitenkin valmistellaan parhaillaan. Kansalliskokouksen puolustusvaliokunta on jo hyväksynyt asiaa koskevan ehdotuksen[3] mutta täysistuntokeskustelua ei ole vielä toistaiseksi käyty.

Yhdistyneessä kuningaskunnassa kaikkeen maassa harjoitettuun viestinnän kuunteluun tarvitaan ministeritason (Secretary of State) lupa. Lain muotoilu jättää kuitenkin epäselväksi, kuuluisiko myös kohdistamaton, laaja-alainen viestinnän sieppaus hakusanojen tutkintaa varten asetuksessa "Regulation of Investigatory Powers Act 2000" (RIP) käytetyn käsitteen "interception" (sieppaus) alaan, jos aineistoa ei tutkita Britannian alueella, vaan niin sanottu raakamateriaali välitetään ulkomaille ilman tutkintaa. RIP 2000 -asetuksen määräysten noudattamista valvovat (jälkikäteen) pääministerin nimittämät valtuutetut (Commissioners), jotka ovat virassa olevia tai entisiä korkeamman asteen tuomareita. Salakuuntelutoimista vastaava valtuutettu (Interception Commissioner) valvoo salakuuntelulupien antamista ja avustaa salakuuntelutoimia koskevien valitusten tutkimisessa. Tiedustelupalveluvaltuutettu (Intelligence Service Commissioner) valvoo

[1] Laki liittovaltion tiedustelupalvelun valvonnasta (PKGrG), annettu 17. kesäkuuta 1999 BGBl I 1334, hyväksytyssä muodossa.
[2] Loi 91-646 du 10 Juillet 1991, loi relative au secret des correspondances émises par la voie des t´lécommunications.
[3] Vrt. asiasta laadittu lakiehdotus "Proposition de loi tendant à la création de délégations parlementaires pour le renseignement", ja kansalliskokousedustaja Arthur Paechtin raportti, N° 1951 Assmeblée nationale, 11. vaalikausi, kirjattu 23. marraskuuta 1999.

tiedustelu- ja turvallisuuspalvelujen toimintaa koskevia lupia ja avustaa näitä palveluja koskevien valitusten tutkimisessa. Erityinen oikeusistuin (Investigatory Powers Tribunal), jonka puheenjohtajana on korkeamman asteen tuomari, tutkii kaikki salakuuntelutoimia ja tiedustelupalvelujen toimintaa koskevat valitukset.

Parlamentaarista valvontaa hoitaa tiedustelu- ja turvallisuusasioiden valiokunta (Intelligence and Security Committee, ISC),[1] joka valvoo kaikkien kolmen siviilitiedustelupalvelun (MI5, MI6 ja GCHQ) toimintaa. Sen tehtäviin kuuluu erityisesti menojen ja hallinnon tarkastus sekä turvallisuuspalvelun, tiedustelupalvelun ja GCHQ:n toimintatapojen valvonta. Valiokuntaan kuuluu yhdeksän ylä- ja alahuoneen jäsentä, joista kukaan ei saa olla ministeri. Muiden valtioiden valvontavaliokunnista, jotka yleensä valitsee tai nimittää parlamentti tai parlamentin puhemies, nämä eroavat sikäli, että valiokunnat nimittää pääministeri neuvoteltuaan asiasta ensin oppositiojohtajan kanssa.

Jo nämä esimerkit osoittavat, että suojataso on hyvin vaihteleva. Parlamentaarisen valvonnan osalta esittelijä haluaisi korostaa, että tiedustelupalvelujen valvonnassa erityiset valvontavaliokunnat ovat erittäin tärkeitä. Niiden etuna päävaliokuntiin nähden on, että tiedustelupalvelujen luottamus niitä kohtaan on vahvempi, koska niiden jäsenet ovat salassapitovelvollisia eivätkä niiden istunnot ole julkisia. Lisäksi niille on myönnetty erityistehtävänsä hoitamiseen erityiset oikeudet, mikä on välttämätöntä tiedustelualaan liittyvän toiminnan valvomiseksi.

Ilahduttavaa on, että EU:n jäsenvaltioiden enemmistö on asettanut tiedustelupalvelujen valvojaksi erityisen parlamentaarisen valvontavaliokunnan. Belgiassa[2], Tanskassa[3], Saksassa[4], Italiassa[5], Alankomaissa[6] ja Portugalissa[7] on parlamentin valvontavaliokunta, joka vastaa sekä sotilastiedustelupalvelun että siviilitiedustelupalvelun valvonnasta. Yhdistyneessä kuningaskunnassa[8] erityinen valvontavaliokunta valvoo ainoastaan siviilitiedustelupalveluita – joilla tosin on oleellisesti suurempi merkitys –, sotilastiedustelupalvelua valvoo normaali puolustusvaliokunta. Itävallassa[9] tiedustelupalvelun kahta haaraa varten on kaksi eri valvontavaliokuntaa, joiden toiminta on järjestetty samalla tavalla ja joilla on samat oikeudet.

[1] Intelligence services act 1994, Section 10.
[2] Comité permanent de contrôle des services de renseignements et de sécurité, Comité permanent R, Loi du 18 juillet 1991 /IV, organique du contrôle des services de police et de renseignements.
[3] Udvalget vedrørende efterretningstjenesterne, Lov om etablering af et udvalg om forsvarets og politiets efterretningstjenester, lov 378 af 6/7/88.
[4] Parlamentin valvontaelin (PKGr), laki liittovaltion tiedustelupalvelutoiminnan valvonnasta (PKGrG), annettu 17. kesäkuuta 1999 BGBl I 1334, hyväksytyssä muodossa.
[5] Comitato parlamentare, L. 24 ottobre 1977, n. 801, art. 11, Istituzione e ordinamento dei servizi per le informazioni e la sicurezza e disciplina del segreto di Stato.
[6] Tweede-Kamercommissie voor de Inlichtingen- en Veiligheidsdiensten, 17. Reglement van orde van de Tweede Kamer der Staten-General, Art. 22.
[7] Conselho de Fiscalização dos Serviços de Informações (CFSI), laki 30/84, annettu 5. syyskuuta 1984, muutettu lailla 4/95, annettu 21. helmikuuta 1995, lailla 15/96, annettu 30. huhtikuuta 1996 ja lailla 75-A/97, annettu 22. heinäkuuta 1997.
[8] Intelligence and Security Committee (ISC), intelligence services act 1994, Section 10.
[9] Parlamentin valvontavaliokunnat: Der Ständige Unterausschuss des Landesverteidigungsausschusses zur Überprüfung von nachrichtendienstlichen Maßnahmen zur Sicherung der militärischen Landesverteidigung, Der Ständige Unterausschuss des Ausschusses für innere Angelegenheiten zur Überprüfung von Maßnahmen zum Schutz der verfassungsmäßigen Einrichtungen und ihrer Handlungsfähigkeit, lain B-VG 52a artikla, työjärjestyslain (Geschäftsordnungsgesetz) 1975 32b §§ ja seur.

Pohjoismaissa, Suomessa[1] ja Ruotsissa[2], parlamentaarinen valvonta kuuluu riippumattoman, parlamentin valitseman oikeusasiamiehen tehtäviin. Ranskassa, Kreikassa, Irlannissa, Luxemburgissa ja Espanjassa ei ole erityisiä parlamentin valiokuntia. Näissä maissa varsinaiset valiokunnat hoitavat valvontatehtävät osana yleistä parlamentaarista toimintaa.

9.4. Tilanteen arviointi Euroopan kansalaisten kannalta

Tilanne Euroopassa näyttää Euroopan kansalaisten kannalta epätyydyttävältä. Televiestinnän kuunteluun annettujen valtuuksien laajuus vaihtelee suuresti. Sama koskee valvontavaliokuntia. Kaikilla tiedustelupalvelutoimintaa harjoittavilla jäsenvaltioilla ei ole riippumattomia, parlamentaarisia valvontaelimiä ja niillä tarvittavia valvontavaltuuksia. Yhtenäisestä suojatasosta ollaan kaukana.

Eurooppalaisesta näkökulmasta tilanne on erittäin valitettava, koska asia ei koske kovinkaan paljon näiden maiden omia kansalaisia, jotka voivat vaikuttaa suojatasoon äänestyskäyttäytymisellään. Haitalliset vaikutukset koskettavat ennen kaikkea muiden maiden kansalaisia, koska ulkomaantiedustelupalvelujen toiminta suuntautuu luonnostaan ulkomaihin. Ulkomaisten järjestelmien kohteena yksittäinen henkilö on suhteellisen suojaton, ja suojelutarve on tällöin vielä suurempi. Ei myöskään sovi unohtaa, että tiedustelupalvelujen erityisluonteen vuoksi Euroopan unionin kansalaiset voivat olla samanaikaisesti usean tiedustelupalvelun toiminnan kohteena. Yhtenäinen, demokraattisten periaatteiden mukainen suojaustaso olisi tällöin toivottava. Tässä yhteydessä olisi myös harkittava, kuinka laajasti tätä alaa koskevat tietosuojamääräykset olisivat EU:n tasolla toteuttamiskelpoisia.

Lisäksi kysymys Euroopan kansalaisten suojelusta tulee aivan uuteen valoon, kun jäsenvaltioiden tiedustelupalvelujen yhteistyö osana yhteistä turvallisuuspolitiikkaa käynnistyy. Silloin eurooppalaisten unionin toimielinten on annettava riittävät suojelua koskevat säännökset. Euroopan parlamentin tehtävä oikeusvaltioperiaatteen puolustajana on vaatia, että sillä on silloin demokraattisesti valtuutettuna elimenä vastaava valvontaoikeus. Euroopan parlamentin tehtävänä on tällöin myös luoda edellytykset, joilla voidaan taata, että erittäin arkaluonteiset tiedot ja muut salaiset asiakirjat käsitellään luottamuksellisesti erityisesti tähän tarkoitukseen perustetussa valiokunnassa, jonka jäsenet ovat salassapitovelvolliset. Vain mainittujen ehtojen täyttyessä on realistista ja perusteltua vaatia näitä valvontaoikeuksia silloin, kun tiedustelupalvelujen on tarkoitus olla toimivassa yhteistyössä – joka on ehdottoman välttämätöntä vakavasti otettavan yhteisen turvallisuuspolitiikan kannalta.

[1] Oikeusasiamies, oikeusperusta poliisin (SUPO) osalta: poliisilaki 493/1995 33 § ja laki pakkokeinolain 5 a luvun muuttamisesta 366/1999 15 §, asevoimien osalta: poliisilaki 493/1995 33 § ja laki poliisin tehtävien suorittamisesta puolustusvoimissa 1251/1995 5 §.

[2] Rikspolisstyrelsens ledning, Förordning (1989:773) med instruktion för Rikspolisstyrelsen (asetus (1989:773) kansallisesta poliisiviranomaisesta).

10. Suojautuminen talousvakoilua vastaan

10.1. Talous vakoilukohteena

Taloudellista toimintaa harjoittavassa yrityksessä on salassapidon kannalta kolmenlaista tietoa. Yhteen ryhmään kuuluvat tiedot, joita pyritään nimenomaan **levittämään mahdollisimman paljon**. Tähän kuuluvat tiedot yrityksen tuotteista (esimerkiksi tuotteiden ominaisuuksista ja hinnoista) sekä mainonnan tavoin toimivat tiedot, jotka vaikuttavat yrityksestä annettavaan kuvaan.

Toiseen ryhmään kuuluvat tiedot, joita **ei suojella eikä myöskään aktiivisesti levitetä**, koska niillä ei ole mitään yhteyttä yrityksen kilpailutilanteeseen. Näitä tietoja ovat esimerkiksi yrityksen henkilöstön retken päivämäärä, henkilöstöruokalan ruokalista tai käytössä olevien telekopiokoneiden merkki.

Kolmantena ryhmänä ovat tiedot, joita **estetään joutumasta muiden tietoon**. Tietoja suojataan paitsi kilpailijoilta myös valtiolta – silloin kun yritys ei halua noudattaa lakeja (esimerkiksi vero- ja kauppasaartosäännöksiä). Suojausta esiintyy eriasteisena. Jyrkin muoto on ehdoton salassapito, joka voi koskea esimerkiksi ennen patenttihakemuksen jättämistä hallussa olevia tutkimustuloksia tai varusteluteollisuuden tuotantoa[1].

Vakoilulla tarkoitetaan nyt käsiteltävänä olevassa tapauksessa yrityksessä salaisina pidettyjen tietojen hankintaa. Jos vakoilija on kilpailuasemassa oleva yritys, puhutaan **kilpailuvakoilusta** (yritysvakoilusta, teollisuusvakoilusta). Jos vakoilun harjoittajana on valtion tiedustelupalvelu, puhutaan **talousvakoilusta.**

10.1.1. Vakoilun kohteet eriteltyinä

Talousvakoilussa oleelliset strategiset tiedot voidaan jaotella toiminnan alojen tai yrityksen eri osa-alueiden mukaan.

10.1.1.1. Toiminnan alat

On aivan selvää, että erityisesti seuraavia aloja koskevat tiedot ovat erittäin kiinnostavia: biotekniikka, geenitekniikka, lääketieteellinen tekniikka, ympäristötekniikka, suurtehotietokoneet, ohjelmistot, optoelektroniikka, kuvantunnistus- ja signaalitekniikka, tietokoneiden muistit, teollinen keramiikka, suurtehometalliseokset, nanoteknologia. Luettelo ei ole täydellinen ja lisäksi se muuttuu teknisen kehityksen myötä. Näillä aloilla vakoilu on ennen kaikkea tutkimustulosten tai erityisten tuotantotekniikkojen varastamista.

10.1.1.2. Yrityksen osa-alueet

Vakoilun kohteina ovat luonnollisesti tutkimus ja kehitys, ostotoiminnot, henkilökunta, tuotanto, jakelu, myynti, markkinointi, tuotantolinjat sekä rahoitukseen liittyvät asiat. Usein näiden tietojen merkitystä ja tärkeyttä aliarvioidaan (ks. 10.1.4).

[1] Informationen für geheimschutzbetreute Unternehmen, BMWI 1997.

10.1.2. Kilpailuvakoilu

Yrityksen strateginen asema markkinoilla riippuu tilasta, jossa yritys on tutkimukseen ja kehitykseen, tuotantomenetelmiin, tuotantolinjoihin, rahoitukseen, markkinointiin, myyntiin, jakeluun, ostotoimintoihin ja työvoimaan nähden[1]. Sitä koskevat tiedot kiinnostavat kaikkia kilpailijoita erityisen paljon, koska niiden avulla saadaan tietää yrityksen suunnitelmista ja heikoista puolista ja voidaan siten käynnistää strategiset vastatoimet.

Osa näistä tiedoista on julkisia. Alalla on erityisiä konsulttiyrityksiä, jotka tekevät täysin laillisissa rajoissa kilpailija-analyysejä. Näihin yrityksiin kuuluu maineikkaita yhtiöitä kuten saksalainen Roland & Berger. Käsite "Competitive Intelligence" on nykyisin Yhdysvalloissa liikkeenjohdon perustyökaluja[2]. Lukuisista erillisistä tiedoista saadaan ammattimaisesti yhdistettynä selkeä tilannekuva.

Laillisen ja rangaistavan kilpailuvakoilun erottaa toisistaan tietojen hankinnassa käytettävien keinojen valinta. Rikolliseksi katsottava toiminta alkaa vasta silloin, kun käytetyt keinot ovat voimassa olevan oikeusjärjestyksen mukaan rangaistavia – analyysien laatiminen sinänsä ei ole rangaistavaa. Kilpailijoita erityisesti kiinnostaviin tietoihin pääsy pyritään tietysti estämään, ja näitä tietoja voi hankkia vain lainvastaisin keinoin. Käytettävät tekniikat ovat samanlaisia kuin luvussa 2 kuvaillut yleiset vakoilumenetelmät.

Kilpailuvakoilun laajuudesta ei ole tarkkoja tietoja. Erittäin suuri osa tapauksista ei tule julkisuuteen, kuten ei perinteisessä vakoilussakaan. Kumpikin osapuoli (vakoilija ja uhri) pyrkii välttämään julkisuutta. Vakoilun kohteeksi joutuminen on aina haitaksi yrityksen imagolle, eikä vakoilijoiden toimintojen julkitulo ole tietenkään heidän etunsa mukaista. Sen vuoksi vakoilutapauksia viedään vain harvoin oikeuskäsittelyyn.

Lehdistössä esiintyy kuitenkin toistuvasti raportteja kilpailuvakoilusta. Esittelijä on lisäksi keskustellut aiheesta eräiden suurten saksalaisyritysten turvallisuuspäälliköiden[3] ja amerikkalaisten ja eurooppalaisten yhtiöiden johtajien kanssa. Yhteenvetona voidaan todeta, että kilpailuvakoilua esiintyy, mutta se ei vaikuta päivittäiseen toimintaan.

10.2. Talousvakoilun aiheuttamat vahingot

Koska suuri osa kilpailuvakoilu- ja talousvakoilutapauksista ei tule julkisuuteen, niiden aiheuttamien vahinkojen laajuudesta ei voida esittää tarkkoja lukuja. Lisäksi on otettava huomioon, että joissakin tapauksissa on edullista esittää luvut mahdollisimman suurina. Turva-alan yritysten ja vakoiluntorjuntaa harjoittavien tiedustelupalveluiden edun mukaista on ymmärrettävästi sijoittaa vahinkoarvio realistisesti mahdollisen asteikon yläpäähän. Tästä huolimatta luvut antavat asiasta jonkinlaisen käsityksen.

Max Planck -instituutti arvioi jo vuonna 1988 talousvakoilun Saksassa aiheuttamat vahingot vähintään 8 miljardiksi Saksan markaksi[4]. Saksan turva-alan konsulttiyritysten liiton

[1] M.F.Porter, Competitive Strategy.
[2] Hummelt, Roman, Wirtschaftsspionage auf dem Datenhighway, Hanserverlag, München 1997.
[3] Yksityiskohtaiset tiedot ja nimet eivät ole julkisia.
[4] IMPULSE, 3/97, s.13 ja seur.

puheenjohtaja ilmoitti asiantuntijoihin tukeutuen luvuksi 15 miljardia Saksan markkaa vuodessa. Euroopan poliisien ammattijärjestöjen puheenjohtaja Hermann Lutz arvioi vahinkojen olevan 20 miljardia Saksan markkaa vuodessa. FBI[1] ilmoittaa vuosina 1992–1993 Amerikan taloudelle kilpailija- ja talousvakoilusta aiheutuneeksi vahingoksi 1,7 miljardia USA:n dollaria. Yhdysvaltain edustajainhuoneen tiedustelupalveluiden valvontavaliokunnan entisen puheenjohtajan mukaan menetykset ovat 100 miljardia USA:n dollaria. Ne ovat aiheutuneet saamatta jääneistä tilauksista ja ylimääräisistä tutkimus- ja kehityskustannuksista. Tästä on seurannut kuuden miljoonan työpaikan menetys vuosien 1990 ja 1996 välisenä aikana.[2]

Periaatteessa vahinkojen tarkan määrän tunteminen ei ole välttämätöntä. Valtiolla on velvollisuus toteuttaa poliisin ja vakoiluntorjuntaviranomaisten kanssa kilpailija- ja talousvakoilua estäviä toimia. Tämä velvollisuus sillä on kansantaloudellisen vahingon suuruudesta riippumatta. Myöskään yritysten tietosuojaa ja omia vakoiluntorjuntatoimia koskevissa ratkaisuissa kokonaisvahinkoluvut eivät ole käyttökelpoinen perusta. Jokaisen yrityksen on laskettava itse tietovarkauksien aiheuttaman vahingon mahdollinen enimmäismäärä, arvioitava esiintymistodennäköisyys ja verrattava niin syntyneitä lukuja turvallisuusjärjestelyjen kustannuksiin. Todellinen ongelma ei ole vahinkojen kokonaismäärää koskevien lukujen puuttuminen. Ongelma on pikemminkin siinä, että suuryrityksiä lukuun ottamatta tällaisia kustannus-hyöty-laskelmia ei juurikaan tehdä ja siten turvallisuus laiminlyödään.

10.3. Kuka vakoilee?

Merkittäviä toimeksiantajia yrityksiin kohdistuvassa vakoilussa ovat tilintarkastusyhtiö Ernst Young LLP:n[3] tekemän tutkimuksen mukaan kilpailijat (39 %), asiakkaat (19 %), alihankkijat (9 %) ja tiedustelupalvelut (7 %). Vakoilijoina ovat omat työntekijät, yksityiset vakoiluyritykset, maksetut hakkerit tai tiedustelupalveluiden ammattilaiset[4].

10.3.1. Omat työntekijät (sisäpiiririkkeet)

Tutkittu kirjallisuus, valiokunnassa kuultujen asiantuntijoiden asiasta antamat tiedot ja esittelijän keskustelut turvallisuuspäällikköjen ja vakoiluntorjuntaviranomaisten kanssa osoittavat yhtäpitävästi, että suurin vakoiluriski piilee pettyneissä ja tyytymättömissä työntekijöissä. Yrityksen työntekijöinä he pääsevät käsiksi tietoihin suoraan, tekevät palveluksia rahasta ja vakoilevat liikesalaisuuksia toimeksiantajilleen.

Suuria riskejä liittyy myös työpaikan vaihtoon. Nykyisin ei tarvitse kopioida pinoittain paperia tärkeiden tietojen viemiseksi ulos yrityksestä. Tiedot voidaan tallentaa huomaamatta levykkeille ja ottaa ne työpaikan vaihdon yhteydessä mukaan käytettäväksi uuden työnantajan palveluksessa.

[1] Congressional Statement, L.J.Freech, Director FBI, 9.5.1996.
[2] Robert Lyle, Radio Liberty/Radio fre Europe, 10. helmikuuta 1999.
[3] Computerzeitung, 30.11.1995, s. 2.
[4] R. Hummelt, Spionage auf dem Datenhighway, München 1997, s. 49 ja seur.

10.3.2. Yksityiset vakoiluyritykset

Vakoilutietojen hankintaan erikoistuneiden yritysten määrä kasvaa jatkuvasti. Näissä yrityksissä työskentelee myös tiedustelupalvelujen entisiä työntekijöitä. Yritykset toimivat usein sekä turvallisuusalan konsulttiyrityksinä että etsivätoimistoina ja ne hankkivat tietoja toimeksiantojen pohjalta. Yleensä käytetyt menetelmät ovat laillisia, mutta myös laittomia menetelmiä käyttäviä yrityksiä on.

10.3.3. Hakkerit

Hakkerit ovat tietokoneasiantuntijoita, jotka voivat tietojensa avulla hankkia pääsyn tietoverkkoihin. Hakkeritoiminnan alkuaikoina asialla olivat tietokoneharrastajat, jotka huvittelivat tietokonejärjestelmien turvajärjestelyjä murtamalla. Nykyisin sekä tiedustelupalveluiden palveluksessa että vapailla markkinoilla on sopimushakkereita.

10.3.4. Tiedustelupalvelut

Kylmän sodan loputtua tiedustelupalvelujen tehtävät ovat muuttuneet. Uusia tehtäväalueita ovat kansainvälinen järjestäytynyt rikollisuus ja talouden toimintaan liittyvät asiat (ks. luku 10.5).

10.4. Miten vakoilu toimii?

Vakoiluntorjuntaviranomaisten ja suurten yritysten turvallisuuspäälliköiden mukaan talousvakoilussa käytetään kaikkia tiedustelupalvelujen tavanomaisia menetelmiä ja välineitä (ks. luku 2.4). Yrityksillä on kuitenkin usein avoimempia rakenteita kuin sotilaallisilla tai tiedustelupalvelua harjoittavilla laitoksilla tai valtionhallinnolla. Talousvakoiluun liittyy sen vuoksi lisäksi seuraavia riskejä:

– Työntekijöiden hankkiminen on yksinkertaisempaa, koska yritysturvallisuuden mahdollisuudet eivät ole verrattavissa vakoiluntorjuntaviranomaisten mahdollisuuksiin.

– Työpaikan liikkuvuus johtaa siihen, että tärkeitä tietoja kuljetetaan kannettavan tietokoneen mukana. Talousvakoilun vakiotekniikkaan kuuluu, että hotellihuoneeseen murtautumisen jälkeen varastetaan kannettava tietokone tai kopioidaan sen kovalevy.

– Murtautuminen tietoverkkoihin onnistuu helpommin kuin turvallisuudestaan tarkoissa valtion laitoksissa, koska juuri pienissä ja keskisuurissa yrityksissä turvallisuustietoisuus ja turvajärjestelyt eivät ole läheskään yhtä tehokkaat.

– Samoista syistä paikan päällä tapahtuva kuuntelu (ks. luku 3.2) on yrityksissä yksinkertaisempaa.

Kerättyjä tietoja tutkittaessa ilmenee, että talousvakoilu keskittyy pääasiassa itse yritykseen tai liikkuvaan työpaikkaan. Tämä johtuu siitä, että halutut tiedot eivät muutamaa poikkeusta lukuun ottamatta (ks. luku 10.6) ole löydettävissä salakuuntelemalla kansainvälisiä televiestintäverkkoja.

10.5. Valtioiden harjoittama talousvakoilu

10.5.1. Tiedustelupalvelujen harjoittama strateginen talousvakoilu

Kylmän sodan loppumisen jälkeen tiedustelupalveluilta vapautui kapasiteettia, jota nyt käytetään muilla aloilla. Yhdysvallat on ilmoittanut avoimesti, että osa sen tiedustelupalvelutoiminnasta kohdistuu myös talouden alaan. Tähän kuuluu esimerkiksi talouspakotteiden noudattamisen valvonta, aseiden ja niin sanottujen kaksikäyttötuotteiden toimittamista koskevien sääntöjen noudattamisen valvonta, raaka-ainemarkkinoiden kehityslinjat ja kansainvälisten rahoitusmarkkinoiden tapahtumat. Esittelijän tietojen mukaan tästä alueesta eivät ole kiinnostuneita pelkästään Yhdysvaltain tiedustelupalvelut. Asiaa ei myöskään kritisoida mitenkään runsaasti.

10.5.2. Tiedustelupalvelut kilpailuvakoilun agentteina

Kritiikkiä esitetään silloin, kun valtiollisia tiedustelupalveluita käytetään väärin hankkimaan oman valtion alueella oleville yrityksille vakoilulla etuja kansainvälisessä kilpailussa. Tässä voidaan erottaa kaksi tapausta.[1]

10.5.2.1. Tekniikan huipulla olevat valtiot

Pitkälle kehittyneet teollisuusvaltiot voivat ilman muuta hyötyä teollisuusvakoilusta. Tietyn alan kehitysvaiheen vakoilun ansiosta voidaan käynnistää omiin ulkomaisiin taloussuhteisiin liittyviä ja tukipoliittisia toimia, joiden avulla joko saatetaan oma teollisuus kilpailukykyisemmäksi tai säästetään tukia. Toisena painopisteenä voi olla suuria tilauksia koskevien yksityiskohtien hankkiminen (ks. 10.6).

10.5.2.2. Teknisesti vähemmän edistyneet valtiot

Osa näistä valtioista pyrkii hankkimaan teknistä taitotietoa, jonka avulla ne voisivat saattaa omaa teollisuuttaan lähemmäs muiden maiden tasoa ilman kehityskustannuksia ja lisenssimaksuja. Lisäksi pyritään saamaan haltuun tuotemalleja ja valmistustekniikoita sekä saavuttamaan alhaisemman palkkatason ansiosta edullisesti valmistettujen tuotejäljennösten avulla kilpailukykyisyys maailmanmarkkinoilla. On osoitettu, että Venäjän tiedustelupalveluille on annettu tällainen tehtävä. Venäjän federaation lakikokoelman ulkomaantiedustelua koskevassa laissa nro 5 nimenomaan mainitaan taloudellisten ja tieteellis-teknisten tietojen hankinta tiedustelupalvelujen tehtävänä.

Toiset näistä valtioista (esimerkiksi Iran, Irak, Syyria, Libya, Pohjois-Korea, Intia ja Pakistan) pyrkivät hankkimaan tietoja kansallisia varusteluohjelmiaan varten ennen kaikkea ydinteknologian ja biologisten ja kemiallisten aseiden alalta. Toinen osa näiden tiedustelupalvelujen toimintaa on pitää yllä peitefirmoja, joiden kautta kaksikäyttötuotteiden ostot hoidetaan epäilyjä herättämättä.

[1] Erään vakoiluntorjuntaa harjoittavan tiedustelupalvelun esittelijälle antama tieto, lähde suojattu.

10.6. Soveltuuko Echelon teollisuusvakoiluun?

Kansainvälisen teleliikenteen strategisella kuuntelulla voidaan saada kilpailuvakoilun kannalta merkittäviä tietoja vain satunnaisina löytöinä. Yrityksiä koskevat luottamukselliset tiedot pidetään käytännössä yleensä itse yrityksissä, joten **kilpailuvakoilussa tietoja saadaan ennen kaikkea työntekijöiden** tai solutettujen henkilöiden avulla tai tunkeutumalla sisäisiin tietoverkkoihin. Kilpailuvakoilussa viestinnänkuuntelujärjestelmää voidaan käyttää vain silloin, kun luottamukselliset tiedot kulkevat yrityksen ulkopuolelle kaapeleita pitkin tai radioyhteyden (satelliittien) välityksellä. Tämä on aina tilanne seuraavissa kolmessa tapauksessa:

– yritykset, jotka toimivat kolmella aikavyöhykkeellä niin että osavuositulokset lähetetään Euroopasta Amerikkaan ja edelleen Aasiaan
– monikansallisten konsernien videokokoukset, joissa käytetään V-Sat- tai kaapeliyhteyttä
– neuvottelut tärkeistä sopimuksista työmaalla (esimerkiksi tehdaslaitoksia, televiestinnän perusrakenteita tai uusia liikennejärjestelmiä rakennettaessa) ja kun sieltä käsin on saatava keskusteluyhteys yritykseen.

Jos yritykset eivät näissä tapauksissa suojaa viestintäänsä, kilpailijoiden vakoilijat saavat tätä viestintää sieppaamalla käyttöönsä arvokkaita tietoja.

10.7. Julkaistut tapaukset

Lehdistössä ja alan kirjallisuudessa on käsitelty eräitä talouden alan tai kilpailijoiden vakoilutapauksia. Eräitä lähteitä on hyödynnetty ja tiedot on koottu oheiseen taulukkoon. Taulukossa ilmoitetaan asianosaiset, tapauksen ajankohta, sekä yksityiskohtaiset tiedot asiasisällöstä, tavoitteista ja seurauksista.

On huomiota herättävää, että yhdestä ja samasta tapauksesta on saatettu kertoa hyvin eri tavoin. Esimerkkinä voidaan mainita Enercon-tapaus, jossa "tekijäksi" ilmoitetaan NSA, Yhdysvaltojen talousministeriö tai valokuvia ottaneet kilpailijat.

Tapaus	Kuka	Milloin	Mitä	Miten	Tavoite	Seuraukset	Lähde
Air France	DGSE	vuoteen 1994 asti	liikematkustajien keskustelut	Air Francen 1. luokan matkustamoista löytyi kuuntelulaitteita – lentoyhtiö esitti julkisen anteeksipyynnön	tiedonhankinta	ei mainittu	"Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“, Arno Schütze, 1/
Airbus	NSA	1994	Airbusin ja saudiarabialaisen lentoyhtiön tiedonvaihto lentokonekaupasta	neuvottelukumppanien faksien ja puhelujen sieppaus	tiedon välittäminen edelleen amerikkalaisille kilpailijoille Boeingille ja McDonnell Douglasille	amerikkalaiset saivat 6 miljardin dollarin kaupan	"Antennen gedreht“, Wirtschaftswoche Nr. 46 / 9. marraskuuta 2000
Airbus	NSA	1994	6 miljardin dollarin arvoinen sopimus Saudi-Arabian kanssa eurooppalaisen Airbus-yhtymän lahjusten paljastuminen	Eurooppalaisen Airbus-yhtymän ja Saudi-Arabian lentoyhtiön / hallituksen faksien ja puhelujen sieppaus viestintäsatelliiteilla	lahjonnan paljastaminen	Airbusin amerikkalainen kilpailija McDonnell Douglas sai kaupan	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, Duncan Campbell
BASF	myyntimies	ei mainittu	BASF-yrityksen (kosmetiikka-osasto) ihovoiteen raaka-aineen tuotantomenetelmän kuvaus	ei mainittu	ei mainittu	ei seurauksia, koska joutui kiinni	"Nicht gerade zimperlich“, Wirtschaftswoche Nr. 43 / 16. lokakuuta 1992
Saksan talous-ministeriö	CIA	1997	Saksan talousministeriön tietoja high tech -tuotteista	vakoojan käyttö	tiedonhankinta	vakoojan yritys paljastui ja hänet karkotettiin	"Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“, Arno Schütze, 1/98
Saksan talous-ministeriö	CIA	1997	Berliiniläisen Mykonos-oikeusjutun taustoja, Hermes-luottoja viennille Iraniin, ansa high tech -tuotteita Iraniin toimittaville saksalaisille yrityksille	USA:n lähettiläälksi naamioitunut CIA-vakooja käy ystävällismielisiä keskusteluja arabialueesta (erityisesti Iranista) vastaavan osaston johtajan kanssa talousministeriössä	tiedonhankinta	ei mainittu Virkamies ottaa yhteyttä Saksan turvallisuusviranomaisiin, jotka ilmoittavat amerikkalaisille CIA:n operaation olevan epätoivottu. CIA-vakooja "vedettiin pois".	"Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste“, Landesamt für Verfassungsschutz Baden-Württemberg, Stuttgart, tilanne: 1998
Dasa	Venäjän tiedustelu-palveluita	1996 – 1999	müncheniläisen aseteknologian yrityksen puolustusteknologiaan liittyvien asiakirjojen myynti ja luovutus (SZ / 30.05.2000: aseteollisuuden yhtymä Dasa Ottobrunnissa)	tehtävään värvätty kaksi saksalaista	tiedonhankinta ohjuksista ja asejärjestelmistä (panssari- ja ilmatorjunta)	SZ / 30.05.2000: "(...) petos ei ollut sotilaalliselta kannalta "erityisen vakava". Tuomioistuin toteaa, että tämä koskee myös taloudellisia vahinkoja."	"Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Bonn, huhtikuu 2001 "Haftstrafe wegen Spionage für Russland“, SDZ / 30. toukokuuta 2000
kauppa-saarto	BND	noin 1990	kauppasaarrolla suojatun tekniikan viennin aloittaminen uudelleen	teleliikenteen kuuntelu	laittoman ase- ja teknologiasiirron paljastaminen	ei erityisiä seurauksia, toimituksia ei estetä	"Maulwürfe in Nadelstreifen", Andreas Förster, s. 110

			Libyaan (mm. Siemens)				

Tapaus	Kuka	Milloin	Mitä	Miten	Tavoite	Seuraukset	Lähde
Enercon	tuulivoima-asiantuntija Olden-burgista ja Kenetechin työntekijä	ei mainittu	Aurichissa toimivan Enercon-yrityksen tuulivoimala	ei mainittu	ei mainittu	ei mainittu	"Anmerkungen zur Sicherheitslage der deutschen Wirtschaft“, ASW; Bonn, huhtikuu 2001
Enercon	NSA	ei mainittu	itäfriisiläisen insinöörin Aloys Wobbenin sähköntuotantoon kehittämä tuulipyörä	ei mainittu	Wobbenin teknisten tietojen toimittaminen yhdysvaltalaiselle yritykselle	yhdysvaltalainen yritys patentoi Wobbenin tuulipyörän; yhdysvaltalainen asianajotoimisto nostaa kanteen Wobbenia vastaan (patenttioikeuden loukkaus)	"Aktenkrieger“, SZ, 29. maaliskuuta 2001
Enercon	Kenetech Windpower Corp -yritys Yhdys-valloista	1994	high tech -tuulivoimalan tärkeitä yksityiskohtia (kytkentälaitteista levyihin)	valokuvia	tulokseen johtanut patenttimenettely USA:ssa	Enercon GmbH panee jäihin suunnitelmat uusien markkinoiden hankkimisesta Yhdysvalloista	"Sicherheit muss künftig zur Chefsache werden“, HB / 29. elokuuta 1996
Enercon	insinööri W. Olden-burgista ja Kenetech-yritys Yhdys-valloista	maalisk. 1994	Enerconin tuuligeneraattori tyyppiä E-40	insinööri W. toimittaa tutkimustuloksia, Kenetechin työntekijä valokuvaa laitosta ja elektronisia yksityiskohtia	Kenetech: etsii todisteita myöhemmälle (1995) patentinloukkauskanteelle Enerconia vastaan Enercon: yrityssalaisuuksia koskevan tiedon laiton hankinta Erään TV-toimittajan väitetään kuulleen NSA:n entiseltä työntekijältä, että amerikkalaiset ovat toimittaneet Enerconista yksityiskohtaisia tietoja Echelonin kautta Kenetechille.	ei mainittu	"Klettern für die Konkurrenz“, SZ 13. lokakuuta 2000
Enercon	Kenetech Windpower	ennen 1996	tietoja Enerconin tuulivoimalasta	Kenetechin insinöörit valokuvaavat laitosta	Kenetech rakentaa samanlaisen laitoksen	Enercon voittaa kiistan; vakoilijoita vastaan nostetaan syyte; arvioidut tappiot: useita satoja miljoonia D-markkoja	"Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“, Arno Schütze, 1/98
Japanin kauppa-ministeriö	CIA	1996	neuvottelut yhdysvaltalaisten autojen tuontikiintiöistä Japanin markkinoilla	Japanin kauppaministeriön atk-järjestelmään murtautuminen	USA:n neuvottelijan Mickey Kantorin halutaan suostuvan alhaisimpaan tarjoukseen	Kantor hyväksyy alhaisimman tarjouksen	"Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“, Arno Schütze,

							1/98
japanilaiset autot	USA:n hallitus	ei mainittu	neuvottelut japanilaisten luksusautojen tuonnista tietoja japanilaisten autojen päästöstandardeista	COMINT, ei annettu tarkempia tietoja	tiedonhankinta	ei tietoa	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, Duncan Campbell

Tapaus	Kuka	Milloin	Mitä	Miten	Tavoite	Seuraukset	Lähde
López	NSA	ei mainittu	VW:n ja Lópezin videokonferenssi	sieppaus Bad Aiblingista	tiedon toimittaminen General Motorsille ja Opelille	syyttäjänviraston väitetään saaneen sieppauksen avulla "erittäin tarkkoja todisteita" tutkintaa varten	Saksan armeijan kapteeni Erich Schmidt-Eenboom, lähde: "Wenn Freunde spionieren“ www.zdf.msnbc.de/news/54637.asp?cp1=1
López	López ja kolme työtoveria	1992–1993	tutkimukseen, suunnitteluun, valmistukseen ja ostoon liittyviä papereita ja tietoja (Espanjan-tehtaaseen liittyviä asiakirjoja, erilaisten mallisarjojen kustannustietoja, projektitutkimuksia, osto- ja säästöstrategioita)	aineiston keruu	General-Motorsin asiakirjojen käyttö VW:ssä	Oikeusjutun jälkeen yritykset sopivat tuomioistuimen ulkopuolella. López eroaa 1996 VW:n johtajan tehtävästä, VW erottaa 1997 kolme muuta Lópezin ryhmän työntekijää, maksaa 100 miljoonaa dollaria GM/Opelille (väitetysti asianajokuluja) ja hankkii GM/Opelilta 7 vuoden ajan varaosia yhteensä 1 miljardin dollarin arvosta	"Wirtschaftsspionage. Die gewerbliche Wirtschaft im Visier fremder Nachrichtendienste“, Landesamt für Verfassungsschutz Baden-Württemberg, Stuttgart, tilanne: 1998
López	NSA	1993	José Ignacio Lópezin ja VW:n johtajan Ferdinand Piëchin videokonferenssi	videokonferenssin kopioiminen ja toimittaminen General Motorsille (GM)	suojata GM:n yrityssalaisuuksia Amerikassa, jotka López halusi toimittaa edelleen VW:lle (hintaluetteloita, salaisia suunnitelmia uudesta autotehtaasta ja uudesta pikkuautosta)	López joutuu kiinni, rikosprosessi keskeytetään 1998 sakkojen maksamisen vuoksi, NSA:sta ei tietoja	"Antennen gedreht“, Wirtschaftswoche Nr.46 / 9. marraskuuta 2000 "Abgehört“, Berliner Zeitung, 22. tammikuuta 1996 "Die Affäre López ist beendet“, Wirtschaftsspiegel, 28. heinäkuuta 1998 "Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“, Arno Schütze, 1/98
Los Alamos	Israel	1988	Kaksi Israelin ydintutkimusohjelman työntekijää murtautuu Los Alamosin ydinaselaboratorion keskustietokoneeseen	tietomurto	tietojen hankkiminen USA:n uusista ydinaseiden sytyttimistä	ei erityisiä seurauksia, sillä hakkerit pakenevat Israeliin, missä toinen pidätetään vähäksi aikaa, yhteydestä Israelin salaiseen palveluun ei virallisesti puhuta	"Maulwürfe in Nadelstreifen", Andreas Förster, s. 137
salakuljetus	BND	70-luku	atk-laitteiden salakuljetus DDR:ään	ei mainittu	itäblokkiin suuntautuvat teknologiasiirron paljastaminen	ei erityisiä seurauksia, toimituksia ei estetä	"Maulwürfe in Nadelstreifen", Andreas Förster, s. 113

Tapaus	Kuka	Milloin	Mitä	Miten	Tavoite	Seuraukset	Lähde
TGV	DGSE	1993	Siemensin kustannuslaskelmat tilaus suurnopeusjunien toimittamisesta Etelä-Koreaan	ei mainittu	alhaisemman tarjouksen esittäminen	ICE-valmistaja menettää tarjouksen Alcatel-Alsthomille	"Wirtschaftsspionage: Was macht eigentlich die Konkurrenz?“, Arno Schütze, 1/98
TGV	tuntematon	1993	AEG:n ja Siemensin kustannuslaskelmat, jotka koskevat valtion tilausta Etelä-Koreassa suurnopeusjunien toimittamisesta	Siemens väittää, että sen puhelin- ja faksiyhteyksiä Soulin toimipisteessä on kuunneltu	neuvotteluetu brittiläis-ranskalaiselle kilpailijalle GEC Alsthomille	Asiakas päättää valita GEC Alsthomin tarjouksen, vaikka saksalaisten tarjous oli ensin parempi	"Abgehört“, Berliner Zeitung, 22. tammikuuta 1996
Thomson-Alcatel vs. Raytheon	CIA/ NSA	1994	Amazonasin alueen satelliittivalvontaa koskevan brasilialaisen miljarditilauksen myöntäminen ranskalaiselle Thomson-Alcatelille (1,4 miljardia dollaria)	tarjouskilpailun voittajan (Thomson-Alcatel, FR) viestintäliikenteen kuuntelu	korruption paljastaminen (lahjusten maksaminen)	Clinton valittaa asiasta Brasilian hallitukselle; USA:n hallituksen vaatimuksesta sopimus myönnetään amerikkalaiselle Raytheon-yritykselle	"Maulwürfe in Nadelstreifen", Andreas Förster, s. 91
Thomson-Alcatel vs. Raytheon	USA:n kauppa-ministeriö "näki vaivaa"	1994	neuvottelut miljardihankkeesta, joka koskee Brasilian sademetsän tutkavalvontaa	ei mainittu	tarjouksen saaminen	ranskalaisen yhtymät Thomson CSF ja Alcatel menettävät tilauksen amerikkalaiselle Raytheon-yritykselle	"Antennen gedreht“, Wirtschaftswoche Nr.46 / 9. marraskuuta 2000
Thomson-Alcatel vs. Raytheon	NSA Department of Commerce		neuvottelut miljardihankkeesta (1,4 miljardia dollaria) Amazonasin alueen valvonnasta (SIVA) Brasilian valintalautakunnan lahjonnan paljastaminen Campbellin huomautus: Raytheon toimittaa varusteita Sugar Grovessa olevalle sieppausasemalle	Thomson-CSF:n ja Brasilian välisten neuvottelujen salakuuntelu ja tulosten toimittaminen Raytheon-yhtiölle	lahjonnan paljastaminen tarjouksen saaminen	Raytheon saa sopimuksen	“Development of Surveillance Technology and Risk of Abuse of Economic Information, Vol 2/5 10 1999 STOA, Duncan Campbell http://www:raytheon.com/sivam/contract.html
Thyssen	BP	1990	miljoonatilaus kaasun- ja öljynporauksesta Pohjanmerellä	Tarjouskilpailun voittajan (Thyssen) faksien sieppaus	korruption paljastaminen	BP vaatii Thyssenilta vahingonkorvauksia	"Maulwürfe in Nadelstreifen", Andreas Förster, s. 92
VW	tuntematon	"viime vuosina"	ei mainittu	mm. maakumpuun kiinnitetty infrapunakamera, joka välittää kuvia radioteitse	tiedon hankkiminen uusista tuloksista	VW ilmoittaa satojen miljoonien menetyksistä	"Sicherheit muss künftig zur Chefsache werden“, HB / 29. elokuuta 1996
VW	tuntematon	1996	VW:n testirata Ehra-Lessienissä	piilokamera	tietoja VW:n uudesta mallista	ei mainittu	"Auf Schritt und Tritt“ Wirtschaftswoche Nr. 25, 11. kesäkuuta 1998

10.8. Talousvakoilulta suojeleminen

10.8.1. Oikeudellinen suoja

Yrityssalaisuuksien varastaminen on luokiteltu kaikkien teollisuusmaiden oikeuskäytännössä rangaistavaksi teoksi. Kansallisen suojan taso vaihtelee kuten muissakin rikoslainsäädännön piiriin kuuluvissa asioissa. Langetettavat rangaistukset ovat kuitenkin yleensä selvästi lievempiä kuin sotilassalaisuuksien vakoilutapauksissa. Useissa tapauksissa on tosin kiellettyä vakoilla ainoastaan kotimaassa toimivaa kilpailevaa yritystä, kun taas ulkomailla sijaitsevan yrityksen vakoilua ei ole kielletty. Tämä pätee myös Yhdysvalloissa.

Asiaa koskevissa laeissa kielletään - tiivistetysti ilmaisten - teollisuusyritysten harjoittama keskinäinen vakoilu. On kyseenalaista, rajoittavatko lait myös kansallisten tiedustelupalvelujen toimintaa. Tiedustelupalveluilla kun on yleensä niiden perustamisesta annettujen lakien mukaisesti oikeus siepata tietoja.

Jos tiedustelupalvelut taas antavat vakoilun avulla hankitut tiedot yksittäisten yritysten käyttöön, kyseessä on rajatapaus. Yleensä tämä ei kuuluisi enää tiedustelupalveluille laeilla myönnettyjen erityisvaltuuksien piiriin. Erityisesti EU:n alueella tietojen luovuttaminen merkitsisi Euroopan talousyhteisöstä tehdyn sopimuksen loukkaamista (ks. luku…).

Tästä huolimatta yrityksen olisi kuitenkin erittäin vaikea hyödyntää oikeudellista suojaansa vetoamalla tuomioistuimeen. Viestien sieppaamisesta ei jää jälkiä tai oikeudessa näytöksi kelpaavia todisteita.

10.8.2. Talousvakoilun muut esteet

Valtiot ovat hyväksyneet, että tiedustelupalvelut toimivat myös talouden alalla hankkiakseen yleisiä strategisia tietoja. Tätä herrasmiessopimusta rikotaan kuitenkin räikeästi, jos kilpailijoita vakoillaan oman teollisuuden eduksi. Valtio, jonka kyetään pitävästi osoittamaan syyllistyneen moiseen, joutuisi pahoihin poliittisiin ongelmiin. Tämä koskisi myös ja erityisesti juuri Yhdysvaltojen kaltaista maailmanmahtia, jonka poliittisen johtoaseman oikeutusta tapaus vahingoittaisi pahasti. Keskitason mahdeilla saattaisi pikemminkin olla varaa joutua oikeuteen, maailmanmahdilla taas ei.

Poliittisten ongelmien ohella olisi otettava myös huomioon käytännön näkökohta siitä, mille yrityksille kilpailijoita vakoilemalla saadut tiedot voitaisiin luovuttaa. Lentokonetuotannon alalla vastaus on helppo, koska koko maailmassa on ainoastaan kaksi suurta tarjoajaa. Muissa tapauksissa yksittäisen toimijan suosiminen on erittäin vaikeaa, jos tarjoajia on useampi eivätkä ne ole valtion omistuksessa. Jos kanssakilpailijoiden tarjouksia koskevat yksityiskohtaiset tiedot luovutetaan yhdelle yritykselle kansainvälisen tarjouskilpailun yhteydessä, olisi kenties vielä ajateltavissa, että vakoilun avulla hankitut tiedot toimitettaisiin kaikille oman maan kilpailijoille. Tämä pätee erityisesti tapauksiin, joissa hallituksen antama tuki on jokseenkin samalla tapaa kaikkien kansallisten kilpailijoiden saatavilla, kuten Yhdysvaltojen Advocacy Center-tapaukseen. Patentoimisilmoituksen jättämiseen vääjäämättä johtavissa teknologiavarkaustapauksissa taas yritysten yhdenvertainen kohtelu ei enää olisi loogisesti mahdollista.

Asia muodostuisi suureksi ongelmaksi erityisesti Amerikan poliittisessa järjestelmässä. Sikäläisten politiikkojen vaalikampanjointi on pitkälti riippuvainen teollisuuden vaalipiireissä tekemistä lahjoituksista. Jos julkisuuteen pääsisi tietoja yhdestä ainoasta tapauksesta, jossa tiedustelupalvelut olisivat suosineet yksittäisiä yrityksiä, poliittinen järjestelmä täyttyisi syytöksistä. CIA:n entinen pääjohtaja totesi valiokunnan edustajien kanssa käymässään keskustelussa, että Yhdysvaltojen kongressi sekoaisi tällaisesta tapauksesta. Sattuvasti sanottu!

10.9. Yhdysvallat ja talousvakoilu

10.9.1. Amerikkalaisten virallinen kanta talousvakoiluun

CIA:n entinen pääjohtaja Woolsey ja tiedustelupalveluja valvovan edustajainhuoneen valiokunnan puheenjohtaja Porter Goss esittivät keskusteluissa seuraavan tiivistetyn kannan:

1. Yhdysvallat valvoo kansainvälistä teleliikennettä hankkiakseen yleisiä tietoja talouden kehityksestä, kaksikäyttötuotteiden toimittamisesta ja saartojen noudattamisesta.

2. Yhdysvallat valvoo kohdennetusti yksittäisten yritysten viestintää sopimusten myöntämistä koskevien menettelyjen yhteydessä estääkseen yhdysvaltalaisten yritysten etuja vahingoittavasta lahjonnasta aiheutuvan markkinoiden vääristymisen.

Amerikkalaisten yritysten harjoittama lahjonta on kielletty lailla ja tilintarkastajat ovat velvollisia ilmoittamaan havaitsemistaan lahjusten maksamisista. Jos viestintää valvottaessa kävisi ilmi julkisiin tarjouksiin liittyvää lahjontaa, Yhdysvaltojen lähettiläs ottaisi yhteyttä kyseisen maan hallitukseen. Lahjuksia tarjonneille amerikkalaisyrityksille taas ei tiedotettaisi asiasta suoraan.

10.9.2. Advocacy Center -keskuksen asema Yhdysvaltain viennin tukemisessa

10.9.2.1. Advocacy Center-keskuksen tehtävät

Yhdysvaltojen kauppaministeriön alaisuuteen kuuluva Advocacy Center on presidentti Clintonin käynnistämän ja Bushin jatkaman kansallisen vientistrategian kulmakivi. Vuonna 1993 perustettu keskus on auttanut satoja amerikkalaisyrityksiä hankkimaan ulkomailla toteutettavia julkisia sopimuksia. Keskus yhdistää Yhdysvaltojen hallituksen resurssit yksittäisalojen asiantuntijoista lähetystöjen talousattaseoihin ja aina Valkoiseen taloon saakka.

10.9.2.2. Keskuksen toimintamenetelmät

Itse keskuksessa työskentelee ainoastaan pieni 12 työntekijän joukko (tiedot saatu 6.2.2001). Keskus palvelee yrityksiä viennin edistämisen alalla toimivien Yhdysvaltain hallinnon viranomaisten tukipisteenä. Se tekee työtä yrityksille syrjimättä, mutta se toimii selkeiden sääntöjen mukaisesti ja tukee ainoastaan Yhdysvaltain kansallisen edun mukaisia hankkeita. Tästä syystä toimitettujen tuotteiden on oltava arvoltaan vähintään 50 prosenttisesti peräisin Yhdysvalloista.

10.9.2.3. Keskusta koskevat avoimet kysymykset

Yhdysvaltojen hallitus ei suostunut järjestämään valiokunnan jäsenten ja keskuksen välisiä kaavailtuja keskusteluja. Tästä syystä kahdesta epäilyä herättävästä asiasta ei päästy puhumaan:

a. valiokunnalla on hallussaan asiakirjoja, jotka näyttävät osoittavan, että CIA on osallistunut keskuksen työskentelyyn,

b. keskus myöntää Internet-sivuillaan, että se yhdistää 19 Yhdysvaltain hallinnon viraston resurssit. Eräässä toisessa yhteydessä yksilöidään kuitenkin ainoastaan 14 virastoa. Tämä antaa aihetta kysyä, miksi viiden viraston nimeä ei ole julkistettu.

10.10. Tietokoneverkkojen turvallisuus

Tiedot toimitetaan myöhemmin.

10.11. Riskien aliarviointi

Tiedot toimitetaan myöhemmin

10.11.1. Suuryritykset

10.11.2. Pk-yritykset

10.11.3. Euroopan toimielimet

10.11.4. Tutkimuslaitokset

11. Suojautuminen salauksen avulla

11.1. Viestien salauksen tarkoitus ja toimintaperiaate

11.1.1. Viestien salauksen tarkoitus

Viestiä lähetettäessä on aina olemassa riski, että viesti joutuu asiattoman käsiin. Jos tällaisessa tilanteessa halutaan estää ulkopuolista saamasta selville viestin sisältö, viestistä on tehtävä sellainen, ettei hän pysty lukemaan tai kuuntelemaan sitä, eli viesti on salattava. Sotilas- ja diplomatian aloilla on siksi jo pitkään käytetty salaustekniikoita.[1]

Viimeisten 20 vuoden aikana viestien salauksen merkitys on lisääntynyt, koska yhä suurempi osa viestinnästä on mennyt ulkomaille eikä oma valtio ole enää pystynyt suojelemaan kirje- ja sähkesalaisuutta siellä. Sen lisäksi oman valtion laajentuneet tekniset mahdollisuudet viestinnän lailliseen kuunteluun/tallentamiseen ovat kasvattaneet huolestuneiden kansalaisten suojauksen tarvetta. Kaiken lisäksi rikollisten lisääntynyt mielenkiinto tietojen laittomaan käyttöön ja väärentelyyn on käynnistänyt turvatoimet (esim. pankkialalla).

Sähköisen ja automaattisen viestinnän (sähkeen, puhelimen, radion, kaukokirjoittimen, faksin ja internetin) keksimisen myötä viestien lähettämisestä tuli paljon yksinkertaisempaa ja verrattomasti nopeampaa. Tämän haittana oli, että ei ollut minkäänlaista **teknistä** suojaa kuuntelua/tallentamista vastaan ja kuka tahansa sopivat laitteet omistava saattoi sekaantua viestintään, jos hän pääsi käsiksi viestiä kuljettavaan viestintävälineeseen. Kuuntelusta ei jää ammattitaitoisesti suoritettuna lainkaan tai juuri lainkaan jälkiä. Näin ollen viestien salaus sai aivan uuden merkityksen. Pankkisektori alkoi ensimmäisenä sähköisen rahaliikenteen myötä käyttää siihen liittyvän viestinnän suojaukseen viestien salausta. Talouden lisääntyvän kansainvälistymisen myötä silläkin alalla alettiin ainakin osittain suojata viestintää salauksella. Kun täysin suojaton viestintä Internetin välityksellä tuli yleiseen käyttöön, kasvoi myös yksityishenkilöiden tarve suojata viestintäänsä kuuntelulta.

Tämän kertomuksen yhteydessä herää siis kysymys, onko viestinnän salaukseen olemassa edullisia, lain sallimia, riittävän turvallisia ja helppokäyttöisiä menetelmiä, joiden ansiosta olisi mahdollista itse suojautua kuuntelua vastaan.

11.1.2. Viestien salauksen toimintaperiaatteet

Viestien salauksen periaatteena on, että selvästä tekstistä tehdään salaista tekstiä, niin että se ei merkitse mitään tai merkitsee jotain muuta kuin alunperin. Sisäpiirin jäsenet voivat kuitenkin muuttaa sen takaisin alkuperäiseen muotoonsa. Viestin salauksella voidaan esim. muuttaa kirjainten järjestystä järkevästä järjettömäksi, niin ettei viestiä ymmärrä kukaan ulkopuolinen.

Tähän käytetään tiettyä menetelmää (salausalgoritmia), joka perustuu kirjainten vaihtamiseen (transpositioon) ja/tai kirjainten korvaamiseen (substituutioon). **Salausmenetelmää** (algoritmia) ei nykyään pidetä salassa. Päinvastoin: hiljattain järjestettiin maailmanlaajuinen julkinen tarjouskilpailu, joka koski uutta maailmanlaajuista talouselämän käyttöön tarkoitettua salausstandardia. Tämä koskee myös tietyn salausalgoritmin toteutusta laitteen osana esim. salausfaksissa.

[1] Tähän liittyviä todisteita on jo antiikin ajalta, esim. spartalaisten käyttämä skytale 5. vuosisadalla jKr.

Varsinainen salaisuus on niin sanottu **avain.** Asiasisältö selviää parhaiten esimerkillä tutulta alueelta. Oven lukkojen toimintatavat ovat yleensä julkisesti tunnettuja jo siksikin, että niille on myönnetty patentti. Oven yksilöllinen suojaus on tulosta siitä, että tietylle lukkotyypille voi olla olemassa useita erilaisia avaimia. Juuri näin toimii myös tietojen salaus: **yleisesti tunnetulla salausmenetelmällä** (algoritmilla) voidaan pitää salassa **monia** erilaisia viestejä erilaisten, asianosaisten **salassa pitämien** yksilöllisten avainten ansiosta.

Yllä käytettyjen käsitteiden selventämiseen voidaan käyttää esimerkkinä "Caesarin salausmenetelmää". Rooman hallitsija Caesar salasi viestejä niin, että hän yksinkertaisesti korvasi jokaisen kirjaimen sillä kirjaimella, joka seurasi kolmea kirjainta myöhemmin aakkosjärjestyksessä, eli A:n D:llä, B:n E:llä jne. Sanasta **ECHELON** tulee tällöin sana **HFKHORQ. Salausalgoritmi** koostuu siis tässä tapauksessa **kirjainten siirtämisestä** aakkosten sisällä, ja konkreettinen **avain** on ohje siirtyä **kolmella kirjaimella aakkosissa!** Sekä salaus että salauksen avaaminen tapahtuu samalla tavalla: siirtämällä kirjaimia 3 kirjaimen verran. Näin ollen kyseessä on symmetrinen menetelmä. Nykyään tällainen menetelmä ei suojaa viestiä sekuntiakaan!

Hyvässä salauksessa menetelmä voi hyvin olla yleisesti tunnettu, ja silti salausta voidaan pitää turvallisena. Tällöin vaatimuksena on kuitenkin, että avainvalikoima on niin suuri, että kaikkien avainten kokeileminen (niin sanottu **brute force attack**) ei ole mahdollista kohtuullisessa ajassa tietokoneidenkaan avulla. Toisaalta avainten paljous ei yksin riitä takaamaan salauksen varmuutta, jos salausmenetelmän tuloksena saadaan salateksti, joka sisältää merkkejä koodin selvittämistä varten (esim. tiettyjen kirjaimien kasautuminen).[1] Caesarin salausmenetelmä ei ole kummankaan ominaisuuden kannalta turvallinen salausmenetelmä. Yksinkertaisen korvauksen avulla menetelmä voidaan selvittää nopeasti jo siksi, että kussakin kielessä eri kirjaimien yleisyys vaihtelee. Sitä paitsi on vain 25 siirtomahdollisuutta eli vain 25 avainta, koska aakkosissa on vain 26 kirjainta. Vastustaja voi hyvin nopeasti saada sopivan avaimen yksinkertaisesti kokeilemalla ja selvittää tekstin.

Seuraavassa pyritään selventämään sitä, millainen turvallisen järjestelmän tulisi olla.

11.2. Salausjärjestelmien turvallisuus

11.2.1. Yleistä salauksen turvallisuuden käsitteestä

Jos salausjärjestelmältä vaaditaan, että sen tulee olla "turvallinen", tällä voidaan tarkoittaa kahta eri asiaa. Ensinnäkin voidaan vaatia, että se on ehdottoman turvallinen, eli että viestin selvittäminen avainta tietämättä on mahdotonta ja että tämä mahdottomuus voidaan todistaa matemaattisesti. Toiseksi voidaan tyytyä siihen, että koodia ei voida murtaa nykyisellä tekniikalla, jolloin saavutetaan turvallisuus ajanjaksolla, joka on huomattavasti pidempi kuin "kriittinen" aika, jonka ajan viestin tulee pysyä salaisena.

11.2.2. Absoluuttinen varmuus: one-time pad

[1] Vrt. myös Leiberich, Vom diplomatischen Code zur Fallfürfunktion - Hundert Jahre Kryptographie in Deutschland, Spektrum der Wissenschaft, kesäkuu 1999, 26–.

Absoluuttisen varmoja järjestelmiä on toistaiseksi vain yksi: one-time pad. Tämä järjestelmä kehitettiin ensimmäisen maailmansodan loppupuolella[1], mutta sitä käytettiin myöhemmin Moskovan ja Washingtonin välisessä kriisikaukokirjoittimessa. Toimintaperiaatteena on avain, joka sisältää täysin sattumanvaraisesti keskenään vaihdettuja kirjaimia, niin että kirjainten vaihtotapa ei toistu. Lähettäjä ja vastaanottaja salaavat viestin näiden kirjainrivien avulla ja hävittävät avaimen heti, kun sitä on käytetty ensimmäisen kerran. Koska avaimen sisällä ei ole sisäistä järjestystä, salausanalyytikon on mahdotonta murtaa koodi. Tämä voidaan osoittaa jopa matemaattisesti.[2]

Tämän menetelmän haittana on, että ei ole helppoa valmistaa suuria määriä tällaisia sattumanvaraisia avaimia[3] ja että avainten jakaminen turvallisella tavalla on vaikeaa ja epäkäytännöllistä. Siksi tätä menetelmää ei käytetä yleisessä yritysten välisessä viestinnässä.

11.2.3. Tekniikan tasoa vastaava suhteellinen varmuus

11.2.3.1. Koneiden käyttö salausten avaamiseen ja laatimiseen

Jo ennen one-time padin keksimistä kehitettiin salausmenetelmiä, joilla saatiin aikaan suuri määrä avaimia ja joiden tuottamat salaiset tekstit sisälsivät mahdollisimman vähän säännönmukaisuuksia ja tarjosivat siksi tuskin lainkaan lähtökohtia salausanalyysille. Jotta näitä menetelmiä saataisiin luotua riittävän nopeasti käytännön sovelluksiin, salaukseen ja salausten avaamiseen kehitettiin koneita. Vaikuttavin näistä oli varmaankin ENIGMA[4], jota Saksa käytti toisessa maailmansodassa. Englannin Bletchley Parkissa koottu joukko salauksen avauseksperttejä onnistui selvittämään ENIGMAn salausmenetelmän erityisten koneiden, niin sanottujen "pommien" avulla. Sekä ENIGMA että "pommi" olivat mekaanisia koneita.

11.2.3.2. Tietokoneen käyttö viestien salauksessa

Tietokoneen keksiminen toimi uranuurtajana salaustieteelle, koska sen tehokkuus mahdollistaa yhä monimutkaisempien järjestelmien käytön. Vaikka tämä ei muutakaan salauksen perusperiaatteita, järjestelmiin tuli kuitenkin tiettyjä uudistuksia. Ensinnäkin salausjärjestelmien mahdollinen monimutkaisuusaste moninkertaistui, koska mekaaninen toteutettavuus ei enää rajoittanut sitä. Lisäksi salausprosessin nopeus lisääntyi huomattavasti.

Tietokoneet käsittelevät tietoa digitaalisesti binäärilukujen avulla. Jälkimmäisellä tarkoitetaan, että informaatio ilmaistaan kahdesta eri merkistä (0 ja 1) muodostuvina jonoina. Luku 1 merkitsee fysiikassa sähköistä jännitettä tai magnetisointia ("valo päällä"), 0 jännitteen tai magnetisoinnin poisjäämistä ("valo pois päältä"). Tämän ohella on kehittynyt ASCII[5]-järjestelmän mukainen standardointi, jossa jokainen kirjain esitetään seitsemänkirjaimisella

[1] Sen otti käyttöön majuri Joseph Mauborgne, Yhdysvaltain armeijan salauksen tutkimusosaston johtaja. Vrt. Singh, Geheime Botschaften (1999), 151.
[2] Vrt. Singh, Geheime Botschaften (1999), 151–.
[3] Vrt. Wobst, Abenteuer Kryptologie[2] (1998), 60.
[4] Enigman kehitti Arthur Scherbius, ja se patentoitiin vuonna 1928. Se muistutti tietyllä tavalla kirjoituskonetta, koska siinä oli näppäimistö, jonka avulla syötettiin luettava teksti. Pistokelevyn ja pyörivän telan avulla teksti salattiin tietyn ohjeen mukaan, ja salaus avattiin samalla koneella koodikirjojen avulla.
[5] American Standard Code for Information Interchange.

numeroiden 0 ja 1 yhdistelmällä[1]. Siksi teksti näkyy numeroista 0 ja 1 koostuvana numerorivinä, ja kirjainten sijasta salataan numeroita.

Tässä voidaan käyttää sekä transpositiota (vaihtoa) että substituutiota (korvaamista). Substituutiota voidaan käyttää esimerkiksi lisäämällä avain mielivaltaisen numerorivin muodossa. Binäärisen matematiikan sääntöjen mukaan kahden yhtä suuren luvun summa on nolla (eli 0 +0=0 ja 1 +1=0), kun taas kahden eri luvun summa on yksi (0+1=1). Yhteenlaskulla aikaansaatava uusi salattu numerojono on siis binäärinen jono, jota voidaan joko käsitellä edelleen digitaalisesti tai joka saadaan uudelleen luettavaan muotoon vähentämällä lisätty avain.

Tietokoneiden avulla voidaan vahvoja salausalgoritmeja käyttäen luoda salattuja tekstejä, jotka eivät tarjoa käytännössä lainkaan mahdollisuuksia salausanalyysille. Näin salauksen avausyritys on mahdollinen enää ainoastaan kokeilemalla kaikki mahdolliset avaimet. Mitä pidempi avain on, sitä pahemmaksi kompastuskiveksi muodostuu selvittämiseen tarvittava aika tehokkaimmillakin tietokoneilla. On siis saatavana menetelmiä, joita voidaan pitää varmoina nykyisellä tekniikan tasolla.

11.2.4. Standardointi ja turvallisuuden tahallinen rajoittaminen

Tietokoneiden yleistyessä 1970-luvulla salausjärjestelmien standardointi kävi yhä tärkeämmäksi, koska vain siten yritykset voivat turvallisesti kommunikoida liikekumppaniensa kanssa ilman kohtuuttomia kustannuksia. Ensimmäisenä standardointiin pyrittiin Yhdysvalloissa.

Voimakasta salausta voidaan käyttää myös epärehellisiin tarkoituksiin, tai käyttäjä voi olla mahdollinen vihollinen sodassa; salauksella voidaan myös vaikeuttaa sähköistä vakoilua tai tehdä se mahdottomaksi. Siksi NSA vaati, että valittaisiin talouselämälle riittävän turvallinen salausstandardi, jonka se itse kuitenkin pystyisi selvittämään erikoisen teknisen varustuksensa avulla. Tämän vuoksi avaimen pituus rajoitettiin 56 bittiin. Tämä mahdollistaa enintään 100 000 000 000 000 000 avaimen käytön[2]. Marraskuun 23. päivänä 1976 otettiin todellakin käyttöön Horst Feistelin niin sanottu Lucifer-Chiffre **56-bittisenä versiona**, jonka virallinen nimi oli Data Encryption Standard (DES). Siitä tuli Yhdysvaltojen virallinen salausstandardi neljännesvuosisadan ajaksi.[3] Myös Euroopassa ja Japanissa tätä standardia alettiin käyttöä varsinkin pankkialalla. DES-standardien algoritmia ei vastoin eri tiedotusvälineissä esitettyjä väitteitä ole toistaiseksi onnistuttu selvittämään, mutta nyt on jo laitteita, jotka ovat riittävän tehokkaita kaikkien avainten kokeilemiseksi ("brute force attack"). Triple-DES-standardia, jolla on 112-bittinen avain, voidaan sitä vastoin edelleen pitää varmana. DES-standardin seuraaja AES (Advanced Encryption Standard) on eurooppalainen menetelmä[4], joka luotiin nimellä Rijndael Belgian Leuvenissa. **Se on nopea ja sitä voidaan pitää varmana, koska siinä luovuttiin avaimen pituusrajoituksista.** Tämä johtui Yhdysvaltojen salauspolitiikan muuttumisesta (katso kohtaa 11.1.4.)

Standardointi merkitsi yrityksille salauksen huomattavaa yksinkertaistumista. Ongelmana oli kuitenkin edelleen avainten jakelu.

---

[1] A = 1000001, B= 1000010, C= 1000011, D= 1000100, E = 1000101, jne.
[2] Tämä luku koostuu binäärisessä muodossa 56 nollasta ja ykkösestä Vrt. Singh, Geheime Botschaften (1999), 03.
[3] Vrt. Singh, Geheime Botschaften (1999), 302–.
[4] Sen kehittivät kaksi belgialaista Louvainin katolisen yliopiston kryptografia, Joan Daemen ja Vincent Rijmen.

11.3. Ongelmana turvallinen avainten jakelu/luovutus

11.3.1. Epäsymmetrinen salaus: public key -menetelmä

Niin kauan kuin järjestelmä toimii yhdellä avaimella, jota käytetään sekä salaukseen että salauksen avaamiseen (symmetrinen salaus), järjestelmän käyttö on hankalaa, kun viestintäkumppaneita on paljon. Avain on nimittäin luovutettava jokaiselle uudelle viestintäkumppanille **etukäteen** niin, etteivät ulkopuoliset voi saada sitä selville. Tämä on käytännössä vaikeaa talouselämässä ja yksityishenkilöillekin mahdollista vain yksittäisissä tapauksissa.

Ratkaisun tähän tarjoaa epäsymmetrinen salaus: salaukseen ja salauksen selvittämiseen ei käytetä samaa avainta. Viesti salataan avaimella, jonka jokainen voi tuntea, niin sanotulla **yleisavaimella**. Menetelmä toimii kuitenkin kuin yksisuuntainen katu: tekstiä ei voi muuttaa takaisin luettavaan muotoon yleisavaimella. Siksi jokainen, joka haluaa saada salatun viestin, voi lähettää viestintäkumppanilleen yleisavaimensa myös epävarmaa reittiä viestin salausta varten. Näin saadun viestin salauksen avaamiseen käytetään toista avainta, **yksityistä avainta,** joka pidetään salassa ja jota ei lähetetä.[1] Parhaiten tätä menetelmää valaisee vertaus riippulukkoon: jokainen voi napsauttaa sellaisen lukon kiinni ja siten sulkea arkun varmasti, mutta avaaminen onnistuu vain siltä, joka omistaa oikean avaimen.[2] Yleisavain ja yksityinen avain liittyvät toisiinsa; yksityistä avainta ei kuitenkaan voi selvittää yleisavaimen perusteella.

Ron Rivest, Adi Shamir ja Leonard Adleman keksivät epäsymmetrisen salausjärjestelmän, jossa käytetään heidän mukaansa nimettyä RSA-menetelmää. Yksisuuntaiseen toimintoon (niin sanottuun lattialuukkutoimintoon) käytetään yleisavaimen osana kahden erittäin suuren jaottoman luvun tuloa. Sillä salataan luettava teksti. Salauksen avaus onnistuu vain, jos tietää molempien käytettyjen jaottomien lukujen arvot. Ei kuitenkaan ole matemaattista menetelmää, jonka avulla kahden jaottoman luvun kertominen voitaisiin kääntää niin, että kertolaskun tuloksesta voitaisiin laskea alkuperäiset jaottomat luvut. Toistaiseksi tämä onnistuu vain järjestelmällisesti kokeilemalla. Siksi menetelmä on nykyisellä tietämyksen tasolla varma, kunhan valitaan riittävän suuret jaottomat luvut. Ainoa riski on, että joku loistava matemaatikko keksisi joskus nopeamman tavan tekijöiden jakamiseen. Tähän saakka kukaan ei kuitenkaan ole pystynyt tähän suuresta vaivannäöstä huolimatta.[3] Monet jopa väittävät, että ongelmaa ei voi ratkaista, mutta tarkkoja todisteita tästä ei ole toistaiseksi esitetty.[4]

Yleisavaimen avulla toteutettava salaus vaatii kuitenkin symmetriseen menetelmään (esim. DES) verrattuna paljon enemmän tietokoneen laskuaikaa tai nopeiden suurtietokoneiden käyttöä.

[1] Idean epäsymmetrisestä salauksesta yleisavainmenetelmän muodossa ovat kehittäneet Whitfield Diffie ja Martin Hellmann.
[2] Singh, Geheime Botschaften (1999), 327.
[3] Vrt. Buchmann, Faktorisierung großer Zahlen, Spektrum der Wissenschft 2 1999, 6–.
[4] Vrt. Singh, Geheime Botschaften (1999), 335–.

11.3.2. Yleisavaimella tapahtuva salaus yksityishenkilöille

Jotta yleisavainmenetelmä saataisiin laajempaan käyttöön, Phil Zimmerman keksi yhdistää laskennallisesti suuritöisen yleisavainmenetelmän nopeampaan symmetriseen menetelmään. Itse viesti salataan Zürichissä kehitetyllä symmetrisellä IDEA-menetelmällä, kun taas symmetrisen salauksen avain välitetään samanaikaisesti yleisavainmenetelmällä. Zimmermann laati käyttäjäystävällisen ohjelman nimeltä Pretty Good Privacy, joka loi tarvittavat avaimet ja suoritti salauksen napin painalluksella (tai hiiren napsautuksella). Ohjelma vietiin Internetiin, mistä jokainen voi ladata sen omalle koneelleen. PGP:n osti lopulta amerikkalainen yritys nimeltä NAI, mutta yksityishenkilöt saavat sen edelleen käyttöönsä maksutta.[1] Aiemmista versioista julkaistiin lähdeteksti, joten voidaan olettaa, että ansoja ei ole rakennettu. Uusimman, erityisen käyttäjäystävällisellä graafisella käyttöliittymällä varustetun PGP 7 -version lähdetekstejä ei valitettavasti enää julkaista.

On kuitenkin olemassa vielä toinen Open PGP -standardin toteutustapa: GnuPG. GnuPG tarjoaa samat salausmenetelmät kuin PGP ja on myös yhteensopiva PGP:n kanssa. Se on kuitenkin ilmainen ohjelma, jonka lähdekoodi on tunnettu ja jota voi käyttää ja levittää kuka tahansa. Saksan liittotasavallan talous- ja teknologiaministeriö on tukenut GnuPG:n reititystä Windowsille ja graafisen käyttöliittymän kehittämistä, mutta se ei valitettavasti ole vielä täysin valmis. Esittelijän tietojen mukaan se on kuitenkin työn alla.

Lisäksi on vielä OpenPGP:n kanssa kilpailevia standardeja, kuten S/MIME, jota monet sähköpostiohjelmat tukevat. Esittelijän tiedossa ei kuitenkaan ole ilmaisversioita siitä.

11.3.3. Tulevat menetelmät

Kvanttisalausmenetelmät voivat tuottaa tulevaisuudessa aivan uusia näkökulmia turvalliseen avainten luovutukseen. Sillä varmistetaan, että kuuntelu avaimen luovutuksen yhteydessä huomattaisiin. Jos lähetetään polarisoituja fotoneja, niiden polarisaatiota ei voida tutkia sitä muuttamatta. Salakuuntelijat datakaapelin varrella havaitaan silloin varmasti. Tällöin käytettäisiin vain avainta, jota ei ole kuunneltu. Kokeissa on jo onnistuttu siirrossa 48 kilometrin matkalla lasikuitukaapelia pitkin ja yli 500 metrin matkalla ilmassa.[2]

11.4. Salaustuotteiden turvallisuus

Keskusteltaessa salausmenetelmien todellisesta turvallisuudesta on myös yhä uudelleen väitetty, että amerikkalaisissa tuotteissa on ansoja. Otsikoissa on esiintynyt mm. Excel, josta väitetään, että eurooppalaisessa versiossa avaimen puolikas esiintyy avoimesti tiedoston otsikossa. Tiedotusvälineiden huomiota on herättänyt myös Microsoft, koska eräs hakkeri löysi ohjelmaan kätketyn "NSA-avaimen", minkä Microsoft luonnollisesti kiisti jyrkästi. Koska Microsoft ei ole julkistanut lähdekoodia, jokainen tätä koskeva väite on pelkkää arvailua. PGP:n ja GnuPG:n aiempien versioiden osalta tällainen porsaanreikä voidaan kuitenkin melkoisen varmasti sulkea pois, koska niiden lähdekoodi on julkistettu.

[1] Tietoja ohjelmasta löytyy osoitteesta www.pgpi.com.
[2] Kvanttisalausjärjestelmistä vrt. Wobst, Abenteuer Kryptographie[2] (1998), 234–.

11.5. Salaus ristiriidassa valtion intressien kanssa

11.5.1. Salauksen rajoitusyritykset

Monet valtiot ovat toistaiseksi kieltäneet salausohjelmien tai salauslaitteiden käytön ja tekevät poikkeuksista luvanvaraisia. Tällä ei tarkoiteta diktatuureja kuten Kiinaa, Irania tai Irakia. Myös demokraattisissa valtioissa salausohjelmien tai -koneiden käyttöä tai myyntiä on rajoitettu laeilla. Viestintä pitäisi suojata asiattomien yksityishenkiöiden lukemiselta, mutta valtiolla pitäisi olla silti mahdollisuus lailliseen salakuunteluun tarvittaessa. Viranomaisten teknisen etumatkan menettäminen pitäisi korvata lakisääteisillä kielloilla. Niinpä Ranska on viime aikoihin saakka kieltänyt yleisesti salauksen käytön ja myöntänyt yksittäisiä salauslupia. Saksassa keskusteltiin joitakin vuosia sitten myös salauksen rajoittamisesta ja avaimen luovutuspakosta. Yhdysvalloissa on tämän sijasta aiemmin rajoitettu avaimen pituutta.

11.5.2. Turvallisen salauksen vaikutus sähköiseen kaupankäyntiin

Nykyisin nämä yritykset lienevät jo kaikki epäonnistuneet. Valtion mielenkiintoa salauksen avausmahdollisuuksiin ja siten luettaviin teksteihin ei nimittäin laimenna vain yksityisyyden säilyttämistä koskeva oikeus vaan myös selvät taloudelliset edut. Sähköinen kaupankäynti ja sähköinen rahaliikenne ovat nimittäin riippuvaisia turvallisesta Internet-viestinnästä. Jos sitä ei voida taata, nämä tekniikat ovat tuhoon tuomittuja, koska asiakkaiden luottamus olisi menetetty. Tämä yhteys selittää muutoksen esimerkiksi Yhdysvaltojen ja Ranskan salauspolitiikassa.

Mainittakoon tässä yhteydessä, että sähköinen kaupankäynti edellyttää turvallisia salausmenetelmiä kahdessa mielessä: paitsi viestien salaukseen, myös liikekumppanin varmaan tunnistukseen. Sähköinen allekirjoitus voidaan nimittäin toteuttaa käyttämällä yleisavainmenetelmää käännetyssä järjestyksessä: salaukseen käytetään yksityistä avainta ja salauksen selvittämiseen yleisavainta. Tämä salaustapa vahvistaa allekirjoituksen alkuperäisyyden. Kuka tahansa voi vakuuttua sen aitoudesta käyttämällä henkilön yleisavainta, mutta itse allekirjoitusta ei voi jäljitellä. Myös tämä toiminto on sisällytetty käyttäjäystävällisesti PGP:hen.

11.5.3. Ongelmia liikematkoilla

Joissakin valtioissa liikeasioissa matkustavat eivät saa käyttää salausohjelmia mukana pitämissään kannettavissa tietokoneissa. Tämä estää kokonaan oman yrityksen kanssa käytävän viestinnän suojauksen tai mukana olevien tietojen suojauksen tunkeutumista vastaan.

11.6. Salaukseen liittyviä käytännön kysymyksiä

Etsittäessä vastausta siihen, kenen ja missä olosuhteissa kannattaisi käyttää salausta, tuntuu oikealta erottaa toisistaan yksityishenkilöt ja yritykset.

Yksityishenkilöiden osalta on sanottava suoraan, että faksien ja puheluiden salaaminen salauspuhelimella tai -faksilla ei oikeastaan ole mahdollista. Ei vain siksi, että näiden laitteiden hankintakustannukset ovat suhteellisen suuret, vaan myös koska niiden käytettävyys edellyttää, että keskustelukumppanilla on myös käytössään vastaavat laitteet, mikä lienee todella harvinaista.

Sitä vastoin jokainen voi ja jokaisen tulisi salata sähköpostiviestinsä. Usein väitetään, ettei ole salaisuuksia eikä salaus siksi ole tarpeen, mutta tähän on todettava, että emmehän yleensä lähetä kirjallisia viestejä postikortteina. Salaamaton sähköpostiviesti ei kuitenkaan ole mitään muuta kuin kirje ilman kuorta. Sähköpostien salaus on turvallista ja suhteellisen ongelmatonta. Internetissä on jo käyttäjäystävällisiä järjestelmiä, kuten PGP/GnuPG, joita tarjotaan yksityishenkilöiden käyttöön jopa ilmaiseksi. Valitettavasti ohjelmat eivät ole vielä riittävän yleisessä käytössä. Olisi toivottavaa, että julkinen sektori näyttäisi hyvää esimerkkiä ja ryhtyisi itse käyttämään standardien mukaista salausta, jotta salausjärjestelmät tulisivat tutuiksi.

Yritysten osalta tulisi ehdottomasti huolehtia siitä, että luottamuksellisia tietoja lähetetään vain varmistettuja viestintäreittejä pitkin. Tämä vaikuttaa itsestään selvältä ja onkin varmaan silloin, kun kyse on suurista yrityksistä, mutta nimenomaan pienissä ja keskisuurissa yrityksissä yrityksen sisäisiä tietoja lähetetään usein sähköpostitse salaamattomina, koska ongelmasta ei olla toistaiseksi tietoisia. Olisi toivottavaa, että toimialajärjestöt ja kauppakamarit pyrkisivät entistä ahkerammin levittämään tietoa tästä asiasta. Tosin sähköpostien salaaminen on vain yksi turvallisuusnäkökohta monien joukossa eikä varsinkaan hyödytä mitään, jos tiedot annetaan muiden käyttöön jo ennen salaamista. Tämä merkitsee sitä, että koko työympäristö on turvattava, eli käytettyjen tilojen turvallisuus on taattava ja valvottava fyysistä pääsyä toimistoihin ja tietokoneisiin. Myös tietojen luvaton käyttö verkon välityksellä on estettävä sopivien palomuurien avulla. Erityisen vaaran tässä suhteessa muodostaa sisäisen verkon ja Internetin yhdistäminen. Jos turvallisuus otetaan vakavasti, tulisi myös käyttää ainoastaan sellaisia käyttöjärjestelmiä, joiden lähdekoodi on julkinen ja tarkistettu, koska vain silloin voidaan varmuudella sanoa, mitä tiedoille tapahtuu. Yrityksillä on siis runsaasti tehtävää turvallisuuden alalla. Markkinoilla on jo lukuisia yrityksiä, jotka tarjoavat turvallisuusneuvontaa ja -sovelluksia kohtuullisin hinnoin, ja kysynnän myötä myös tarjonta lisääntyy jatkuvasti. Lisäksi on kuitenkin toivottava, että toimialajärjestöt ja kauppakamarit tarttuvat näihin ongelmiin, jotta erityisesti pienet yritykset huomaisivat turvallisuusongelmien tärkeyden, ja tukevat kattavan suojajärjestelmän suunnittelua ja soveltamista.

12. EU:n ulkosuhteet ja tiedusteluaineiston keruu

12.1. Johdanto

Kun Maastrichtin sopimus hyväksyttiin vuonna 1991, yhteinen ulko- ja turvallisuuspolitiikka (YUTP) luotiin perusmuodossaan Euroopan unionin uudeksi politiikan välineeksi. Kuusi vuotta myöhemmin Amsterdamin sopimus loi lisärakennetta YUTP:lle ja antoi mahdollisuuden yhteistä puolustusta koskeviin aloitteisiin Euroopan unionin sisällä säilyttäen samalla nykyiset liittoutumat. Helsingissä joulukuussa 1999 kokoontunut Eurooppa-neuvosto käynnisti Euroopan turvallisuus- ja puolustusaloitteen Amsterdamin sopimuksen pohjalta ja pitäen mielessään Kosovon kokemukset. Tällä aloitteella pyritään luomaan vuoden 2003 toiseen puoliskoon mennessä monikansalliset joukot, joihin kuuluisi noin 50 000–60 000 sotilasta. Tällaisen monikansallisen armeijan olemassaolo tekee itsenäisen tiedustelukapasiteetin kehittämisestä välttämätöntä. Nykyisen WEU:n tiedustelukapasiteetin yksinkertainen integrointi ei riitä tähän tarkoitukseen. Entistä laajempaa, nykyiset yhteistyömuodot reilusti ylittävää yhteistyötä jäsenvaltioiden tiedusteluelinten välillä ei voida välttää.

Yhteisen turvallisuus- ja yhteistyöpolitiikan edelleenkehittäminen ei kuitenkaan ole ainoa tekijä, joka laajentaa unionin tiedustelupalvelujen yhteistyötä entisestään. Euroopan unionin entistä laajempi taloudellinen integraatio edellyttää myös entistä tiiviimpää yhteistyötä tiedusteluaineiston keruun alueella. Yhdistynyt eurooppalainen talouspolitiikka edellyttää yhtenäistä käsitystä taloudellisesta todellisuudesta Euroopan unionin ulkopuolisessa maailmassa. Yhtenäinen kanta kauppaneuvotteluissa maailman kauppajärjestön WTO:n sisällä tai kolmansien maiden kanssa edellyttää neuvottelukannan yhteistä suojelua. Euroopan vahvat teollisuudenalat tarvitsevat yhteistä suojausta Euroopan unionin ulkopuolelta tulevaa taloudellista vakoilua vastaan.

Lopuksi on korostettava, että unionin toisen pilarin edelleenkehittämisen ja unionin toiminnan sisäpolitiikan ja oikeuden aloilla tulee myös johtaa entistä laajempaan yhteistyöhön tiedustelupalvelujen välillä. Etenkään yhteinen taistelu terrorismia, laitonta asekauppaa, ihmiskauppaa ja rahanpesua vastaan ei ole mahdollista ilman tiedustelupalvelujen tehokasta yhteistyötä.

12.2. Yhteistyömahdollisuudet EU:n sisällä

12.2.1. Nykyinen yhteistyö

Vaikka tiedustelupalvelut ovat jo pitkään luottaneet vain itse hankkimiinsa tietoihin ja suhtautuneet kenties jopa epäilevästi muihin tiedustelupalveluihin Euroopan unionin sisällä, palvelujen välinen yhteistyö on jo alkanut vähitellen lisääntyä. Ahkeraa yhteydenpitoa esiintyy NATO:n ja WEU:n puitteissa ja Euroopan unionin sisällä. Vaikka NATO:n puitteissa toimivat tiedustelupalvelut ovatkin yhä voimakkaasti riippuvaisia Yhdysvaltojen paljon kehittyneemmästä toiminnasta alalla, WEU:n satelliittikeskuksen rakentaminen Torrejoniin (Espanjaan) ja WEU:n päämajan tasoisen tiedusteluosaston perustaminen ovat tehneet Euroopan toiminnasta tällä alalla entistä itsenäisempää.

12.2.2. Yhteisen eurooppalaisen tiedustelupolitiikan edut

Käynnissä olevien kehityskulkujen lisäksi on korostettava, että yhteisellä eurooppalaisella tiedustelupolitiikalla on objektiivisia etuja. Näitä etuja voidaan kuvata seuraavasti.

12.2.2.1. Ammatilliset edut

Ensinnäkin salaista ja julkista materiaalia on tarjolla aivan liikaa, jotta sitä kaikkea pystyttäisiin keräämään, analysoimaan ja arvioimaan Länsi-Euroopassa yhdessä ainoassa virastossa tai kahdenkeskisen sopimuksen perusteella. Tiedustelupalveluihin kohdistuvat vaatimukset vaihtelevat puolustusvoimien tiedustelusta kolmansien maiden sisäisen ja kansainvälisen talouspolitiikan seurantaan ja järjestäytyneen rikollisuuden ja huumeiden salakuljetuksen vastaista taistelua tukevaan tiedusteluun. Vaikka yhteistyötä tehtäisiin vain aivan perustasolla eli avoimista lähteistä tulevan tiedon keruussa (OSINT), yhteistyön tulokset olisivat jo erittäin tärkeitä Euroopan unionin politiikan kannalta.

12.2.2.2. Budjettiedut

Viime aikoina tiedusteluaineiston keruuseen tarkoitettuja varoja on leikattu, ja joissakin tapauksissa ne pienenevät edelleen. Samaan aikaan tiedon ja siksi myös tiedustelun tarve on lisääntynyt. Yhteistyö on näiden pienennettyjen budjettien vuoksi mahdollista ja pitkällä aikavälillä myös kannattavaa. Kun rahaa on niukasti, yhteistoiminta kiinnostaa varsinkin teknisten välineiden hankinnassa ja ylläpidossa ja myös kerätyn tiedusteluaineiston arvioinnissa. Laajempi yhteistyö lisää tiedusteluaineiston keruun tehokkuutta.

12.2.2.3. Poliittiset edut

Periaatteessa kerätyn tiedosteluaineiston tavoitteena on antaa hallituksille mahdollisuus parempaan ja paremmin perusteltuun päätöksentekoon. Euroopan unionin tasolla tapahtuva entistä tehokkaampi poliittinen ja taloudellinen yhdentyminen edellyttää, että tiedusteluaineistoa on käytettävissä Euroopan tasolla ja että se myös perustuu useampaan kuin yhteen ainoaan lähteeseen.

12.2.3. Loppuhuomautukset

Nämä objektiiviset edut antavat vain kuvan yhteistyön kasvavasta merkityksestä Euroopan unionin sisällä. Ennen jokainen kansallisvaltio vastasi yksin ulkoisesta turvallisuudestaan, sisäisestä järjestyksestään, kansansa hyvinvoinnista ja kulttuuri-identiteetistään. Nyt Euroopan unioni on omaksumassa monilla aloilla roolin, joka ainakin täydentää kansallisvaltion roolia. Ei ole mahdollista, että tiedustelupalvelut olisivat viimeinen ja ainoa alue, johon Euroopan yhdentyminen ei vaikuttaisi.

12.3. Euroopan unionin tasoa laajempi yhteistyö

Toisesta maailmansodasta lähtien yhteistyötä tiedusteluaineiston keruun alalla ei ensin tehty Euroopan tasolla vaan enemmänkin Atlantin valtameren yli. Yhdistyneen kuningaskunnan ja Yhdysvaltojen välille on jo aiemmin osoitettu syntyneen hyvin läheiset suhteet tiedusteluaineiston keruun alalla. Yhdysvallat on kuitenkin ollut ja on edelleen ehdottomasti hallitseva osapuoli myös armeijan tiedusteluaineiston keruun alalla NATO:n puitteissa ja laajemminkin. Tärkein kysymys on, heikentääkö kasvava eurooppalainen yhteistyö

tiedusteluaineiston keruun alalla vakavasti suhteita Yhdysvaltoihin vai voiko se jopa vahvistaa näitä suhteita. Miten EU:n ja Yhdysvaltojen suhteet kehittyvät uuden Bushin hallinnon aikana? Ja varsinkin, miten tämä Yhdysvaltojen ja Yhdistyneen kuningaskunnan välinen erityissuhde säilytetään näissä puitteissa?

Jotkut ovat sitä mieltä, että Iso-Britannian ja Yhdysvaltojen erityisen suhteen ja yhteisen ulko- ja turvallisuuspolitiikan edelleenkehittämisen ei tarvitse olla ristiriidassa keskenään. Toiset taas uskovat, että varsinkin tiedusteluaineiston keruu voi olla se seikka, joka pakottaa Yhdistyneen kuningaskunnan päättämään, onko sen kohtalona yhteistyö Euroopassa vai Atlantin yli. Iso-Britannian läheiset suhteet Yhdysvaltoihin (ja muihin UKUSA-sopimuksen osapuoliin) voivat vaikeuttaa entisestään tiedonvaihtoa muiden EU-maiden kesken – koska Iso-Britannia ei välttämättä ole niin kiinnostunut tiedonvaihdosta Euroopan tasolla ja koska sen kumppanit EU:ssa eivät välttämättä luota Iso-Britanniaan niin paljon. Samoin jos Yhdysvallat uskoo Iso-Britannian solmineen erityisiä yhteyksiä EU-kumppaneihinsa ja sen olevan osa erityistä eurooppalaista sopimusta, Yhdysvallat ei välttämättä enää niin mielellään kerro tietojaan Yhdistyneelle kuningaskunnalle. EU:n laajempi yhteistyö tiedusteluyhteistyön alueella voi siksi panna kovalle koetukselle Yhdistyneen kuningaskunnan yhteistyöhalun Euroopan kanssa ja EU:n yhdentymismahdollisuudet.

Nykyisissä olosuhteissa on kuitenkin erittäin epätodennäköistä, että äärimmäisen nopeakaan kehitys eurooppalaisten kumppanien välisessä yhteistyössä voisi lyhyellä tai pidemmälläkään aikavälillä "kuroa kiinni" Yhdysvaltojen teknistä etumatkaa. Euroopan unioni ei pysty luomaan kehittynyttä SIGINT-satelliittien, kuvankäsittelysatelliittien ja maa-asemien verkkoa. Euroopan unioni ei pysty lyhyellä aikavälillä luomaan erittäin kehittynyttä tietokoneverkkoa, jota tarvitaan kerätyn materiaalin valintaan ja arviointiin. Euroopan unioni ei ole varautunut tarjoamaan käyttöön tarvittavia varoja, jotta se muodostaisi todellisen vaihtoehdon Yhdysvaltojen tiedustelutoiminnalle. Siksi Euroopan unionin kannattaa jo tekniikan ja budjetin näkökulmasta säilyttää läheinen suhde Yhdysvaltojen kanssa tiedusteluaineiston keruun alueella. Suhteet Yhdysvaltoihin on kuitenkin tärkeää säilyttää myös poliittisemmasta näkökulmasta, ja niitä on tarvittaessa vahvistettava varsinkin yhteisessä taistelussa järjestäytynyttä rikollisuutta, terrorismia, huumeita ja asekauppaa sekä rahanpesua vastaan. Yhteinen tiedustelutoiminta on tarpeen yhteisen taistelun tukemiseksi. Entisessä Jugoslaviassa toteutettujen kaltaiset yhteiset rauhanturvatoimet edellyttävät Euroopan entistä aktiivisempaa osallistumista kaikilla toiminnan alueilla.

Toisaalta kasvavan eurooppalaisen tietoisuuden lisäksi tarvitaan kasvavaa eurooppalaista vastuuta. Euroopan unionista pitäisi tulla tasa-arvoisempi kumppani paitsi talouden myös puolustuksen alueella ja siksi myös tiedusteluaineiston keruun alalla. Itsenäisemmän eurooppalaisen tiedustelukapasiteetin ei siksi pitäisi katsoa olevan osoitus Atlantin yli yltävien suhteiden heikkenemisestä vaan sitä tulisi käyttää vahvistuksena vakiinnutettaessa Euroopan unionin asemaa tasa-arvoisempana ja pystyvämpänä kumppanina. Samaan aikaan Euroopan unionin on pyrittävä itsenäisesti suojelemaan talouttaan ja teollisuuttaan laittomia ja ei-tervetulleita uhkia kuten talousvakoilua, verkkorikollisuutta ja terroristien hyökkäyksiä vastaan. Toisaalta Atlantin yli yltävä ymmärtämys on tarpeen teollisuusvakoilun alueella. Euroopan unionin ja Yhdysvaltojen tulisi sopia siitä, mikä on sallittua ja mikä ei tällä alalla. Atlantin yli tehtävän yhteistyön vahvistamiseksi tällä alalla voitaisiin tehdä yhteinen aloite Maailman kauppajärjestön tasolla, jolloin järjestön mekanismeja voitaisiin käyttää oikeudenmukaisen talouskehityksen suojaamiseen kaikkialla maailmassa.

12.4. Loppuhuomautukset

Euroopan unionin yhteisen tiedustelukapasiteetin jatkokehittämistä tulisi pitää tarpeellisena ja väistämättömänä. Samalla tulisi kuitenkin säilyttää Euroopan kansalaisen yksityisyyden suojan peruslähtökohdat. Yhteistyötä kolmansien maiden ja etenkin Yhdysvaltojen kanssa tulisi pitää yllä ja hyvin luultavasti vahvistaa. Tämä ei välttämättä tarkoita, että Euroopan SIGINT-toiminnot tulisi automaattisesti integroida itsenäiseen Euroopan unionin ECHELON-järjestelmään tai että Euroopan unionin tulisi liittyä täysjäseneksi nykyiseen UKUSA-sopimukseen. Kuitenkin asianmukaisen eurooppalaisen vastuun kehittämistä tiedusteluaineiston keruun alueella tulee harkita aktiivisesti. Yhdentynyt eurooppalainen tiedustelukapasiteetti edellyttää samalla eurooppalaista poliittista valvontajärjestelmää näiden virastojen toimien seuraamiseksi. On päätettävä, millä keinoilla arvioidaan tietoja ja tehdään poliittisia päätöksiä, jotka ovat seurausta tiedusteluraporttien analysoinnista. Tällaisen poliittisen valvontajärjestelmän ja siksi myös poliittisen tietoisuuden ja tiedusteluaineiston keruuprosessiin liittyvän vastuun puute olisi haitallista Euroopan yhdentymiskehitykselle.

13. Johtopäätökset ja suositukset

13.1. Alkuhuomautus

Tässä luvussa esitetään yhteenveto selvitystyön tuloksista ja mahdollisista johtopäätöksistä. Sitä ei tule ymmärtää lopullisena. Esittelijä haluaisi pikemminkin luoda työskentelyperustan poliittiselle keskustelulle, jota nyt on käytävä valiokunnassa. Tekstiä täytyy sen jälkeen muuttaa vielä kerran, jotta tämän keskustelun elementtejä voidaan sisällyttää siihen.

13.2. Johtopäätökset

Yksityistä ja talouselämän viestintää sieppaavan maailmanlaajuisen järjestelmän (Echelon-sieppausjärjestelmän) olemassaolo

Ei voida enää epäillä sitä, että on olemassa maailmanlaajuisesti toimiva viestintäsieppausjärjestelmä, jonka toimintaan osallistuvat Yhdysvallat, Yhdistynyt kuningaskunta, Kanada, Australia ja Uusi-Seelanti UKUSA-sopimuksen puitteissa. Käytettävissä olevien viitteiden perusteella vaikuttaa todennäköiseltä, että sen nimi on todellakin Echelon, tosin tällä on vain toissijainen merkitys. Tärkeää on, ettei sitä käytetä sotilaallisen, vaan yksityisen ja kaupallisen viestinnän sieppaamiseen.

Analyysi on osoittanut, ettei järjestelmän mahti voi olla läheskään niin suuri, kuin tiedotusvälineissä toisinaan oletetaan.

Sieppausjärjestelmän rajat

Järjestelmä perustuu satelliittiviestinnän maailmanlaajuiseen sieppaukseen. Kuitenkin vain hyvin pieni osa viestinnästä kulkee satelliittien kautta alueilla, joiden viestintätiheys on huomattavaa. Tämä merkitsee, että suurinta osaa viestinnästä ei voida siepata maa-asemien avulla vaan ainoastaan kaapeleita ja radioyhteyksiä salakuuntelemalla. Tutkimukset ovat kuitenkin osoittaneet, että Echelon-valtioilla on pääsy vain hyvin pieneen osaan kaapeli- ja radioyhteyksiin perustuvasta viestinnästä ja henkilöstökuluista johtuen ne voivat arvioida vain rajallista osaa viestinnästä.

Muiden sieppausjärjestelmien olemassaolon mahdollisuus

Koska viestinnän sieppaaminen on tiedustelupalvelujen yleisesti käyttämä vakoilukeino, myös muut valtiot voisivat pitää yllä vastaavanlaista järjestelmää, mikäli niillä on siihen riittävät taloudelliset ja maantieteelliset mahdollisuudet. Ranska pystyisi ainoana EU:n jäsenvaltiona pitämään jopa yksinään yllä maailmanlaajuista sieppausjärjestelmää ainakin maantieteellisten edellytysten puolesta merentakaisten alueidensa ansiosta. On viitteitä siitä, että myös Venäjä voisi pitää yllä senkaltaista järjestelmää.

Yhteensopivuus EU:n oikeuden kanssa

Arvioitaessa Echelonin kaltaisen järjestelmän yhteensopivuutta EU:n oikeuden kanssa on erotettava kaksi asiaa: Jos järjestelmää käytetään vain tiedustelupalvelutarkoituksiin, ristiriitaa EU:n oikeuden kanssa ei ole, koska valtion turvallisuutta palvelevat toiminnot eivät kuulu EY:n

perustamissopimuksen soveltamisalaan. Ne kuuluisivat Euroopan unionista tehdyn sopimuksen V osaston (YUTP) osastoon, mutta se ei toistaiseksi sisällä asiaa koskevia säädöksiä, joten kosketuskohdat puuttuvat. Jos järjestelmää sen sijaan käytetään kilpailuvakoiluun, järjestelmä on ristiriidassa jäsenvaltioiden välisen lojaliteettiperiaatteen sekä yhteismarkkinoiden ja vapaan kilpailun periaatteen kanssa. Jos jokin jäsenvaltio osallistuu siihen, se rikkoo EY:n oikeutta.

Tiedustelupalvelun harjoittaman viestinnän kuuntelun yhdenmukaisuus yksityisyyttä koskevan perusoikeuden kanssa (Euroopan ihmisoikeussopimuksen 8 artikla)

Kaikki viestinnän kuuntelu merkitsee voimakasta puuttumista ihmisen yksityisyyteen. Yksityisyyttä suojaavan Euroopan ihmisoikeussopimuksen 8 artiklassa sallitaan yksityisyyteen puuttuminen kansallisen turvallisuuden takaamiseksi, mikäli säädökset on kirjattu kansalliseen lainsäädäntöön ja ne ovat yleisesti saatavilla ja mikäli niissä säädetään, missä oloissa ja millä ehdoilla valtiovalta saa toteuttaa kyseisiä toimia. Yksityisyyteen puuttumisessa on noudatettava suhteellisuutta. Näin ollen siihen liittyvät hyötynäkökohdat on arvioitava. Ei riitä, että toimenpiteet olisivat yksinkertaisesti hyödyllisiä tai toivottavia.

Tiedustelupalvelujärjestelmä, jolla siepattaisiin mitä tahansa viestintää turvaamatta suhteellisuuden periaatteen noudattamista, ei olisi Euroopan ihmisoikeussopimuksen mukainen. Euroopan ihmisoikeussopimusta rikottaisiin myös siinä tapauksessa, että viestinnän kuuntelua säätelevällä säädöksellä ei ole oikeusperustaa, se ei ole yleisesti saatavilla tai se on muotoiltu niin, ettei sen kansalaisille aiheuttamia seurauksia voida ennakoida. Koska amerikkalaisten tiedustelupalvelujen ulkomailla suorittamaa toimintaa koskevat määräykset on useimmiten luokiteltu salaisiksi, on suhteellisuusperiaatteen noudattaminen vähintäänkin kyseenalaista. Tämä loukannee Euroopan ihmisoikeustuomioistuimen vahvistamia periaatteita oikeussuojan saatavuudesta ja ennakoitavuudesta. Vaikka Yhdysvallat ei ole Euroopan ihmisoikeussopimuksen osapuoli, jäsenvaltioiden on noudatettava sopimusta. Ne eivät voi välttää sopimuksesta aiheutuvia velvoitteitaan antamalla muiden maiden tiedustelupalvelujen, joita eivät sido yhtä tiukat määräykset, toimia alueellaan. Muutoin laillisuusperiaatteeseen sisältyvät oikeussuojan saatavuus ja ennakoitavuus menettäisivät merkityksensä ja Euroopan ihmisoikeustuomioistuimen oikeuskäytäntö vesittyisi.

Lisäksi tiedustelupalvelujen lainmukaisen toiminnan yhteensovittaminen perusoikeuksien kanssa vaatii riittäviä valvontajärjestelmiä vastapainoksi vaaralle, joka aiheutuu hallintokoneiston osan salaisesta toiminnasta. Ottaen huomioon, että Euroopan ihmisoikeustuomioistuin on nimenomaan korostanut tiedustelupalvelujen toiminnan tehokkaan valvontajärjestelmän merkitystä, tuntuu arveluttavalta, ettei kaikissa jäsenvaltioissa ole omia parlamentaarisia tiedustelupalvelujen valvontaelimiä.

Onko Euroopan unionin kansalaisilla riittävä suoja tiedustelupalvelujen toimintaa vastaan?

Euroopan unionin kansalaisten suoja riippuu yksittäisten jäsenvaltioiden oikeudellisesta tilanteesta, joka vaihtelee suuresti – kaikissa jäsenvaltioissa ei ole lainkaan parlamentaarisia valvontaelimiä –, joten voidaan tuskin puhua riittävästä suojasta. On Euroopan kansalaisten pääetujen mukaista, että kansallisilla parlamenteilla on virallisesti organisoitu erityinen valvontavaliokunta, joka valvoo tiedustelupalvelujen toimintaa. Sielläkin, missä valvontaelimiä on, niillä on suuri houkutus huolehtia enemmän kotimaantiedustelupalvelujen kuin

ulkomaantiedustelupalvelujen toiminnasta, koska yleensä vain ensin mainitut koskevat omia kansalaisia.

Jos tiedustelupalvelujen YUTP:n mukainen yhteistyö toteutuu, toimielinten on luotava riittävät Euroopan kansalaisia suojaavat määräykset.

Talousvakoilu

Ulkomaantiedustelupalvelujen tehtäväkenttään kuuluu, että ne ovat kiinnostuneita taloudellisista tiedoista, jotka koskevat esimerkiksi alakohtaista kehitystä, raaka-ainemarkkinoiden kehitystä, kauppasaartojen noudattamista, kaksikäyttötuotteiden toimitussääntöjen noudattamista jne. Näistä syistä kyseisiä yrityksiä usein valvotaan salakuunnellaan. Jos tiedustelupalvelut ryhtyvät kilpailuvakoilun välineiksi, niin että ne vakoilevat ulkomaisia yrityksiä hankkiakseen kilpailuetuja kotimaisille yrityksille, tilannetta ei voida hyväksyä. On esitetty useita väitteitä, joiden mukaan maailmanlaajuista sieppausjärjestelmää on käytetty tähän tarkoitukseen, mutta yhtään tapausta ei ole todistettu.

Yrityksiä koskevat luottamukselliset tiedot pidetään käytännössä yleensä itse yrityksissä, joten kilpailijavakoilussa tietoja saadaan ennen kaikkea työntekijöiden tai solutettujen henkilöiden avulla tai tunkeutumalla sisäisiin tietoverkkoihin. Kilpailijavakoilussa viestinnänkuuntelujärjestelmää voidaan käyttää vain silloin, kun luottamukselliset tiedot kulkevat yrityksen ulkopuolelle kaapeleita pitkin tai radioyhteyden (satelliittien) välityksellä. Tämä on aina tilanne seuraavissa kolmessa tapauksessa:

– yritykset, jotka toimivat kolmella aikavyöhykkeellä niin että osavuositulokset lähetetään Euroopasta Amerikkaan ja edelleen Aasiaan
– monikansallisten konsernien videokokoukset, joissa käytetään V-Sat- tai kaapeliyhteyttä
– neuvottelut tärkeistä sopimuksista työmaalla (esimerkiksi tehdaslaitoksia, televiestinnän perusrakenteita tai uusia liikennejärjestelmiä rakennettaessa) ja kun sieltä käsin on saatava keskusteluyhteys yritykseen.

Suojautumismahdollisuudet

Yritysten on turvattava koko työskentely-ympäristö ja suojattava kaikki viestintäkanavat, joilla välitetään luottamuksellisia tietoja. Euroopan markkinoilla on riittävästi kohtuuhintaisia salausjärjestelmiä. Myös yksityishenkilöitä on neuvottava salaamaan ehdottomasti sähköpostit. Salaamaton sähköposti on kuin ilman kirjekuorta lähetetty kirje. Internetissä on melko käyttäjäystävällisiä järjestelmiä, joita saa jopa ilmaiseksi yksityiskäyttöön.

Tiedustelupalvelujen yhteistyö EU:ssa

EU on sopinut tiedustelupalvelujen tietojenkeruun koordinoinnista itsenäisen turvallisuus- ja puolustuspolitiikan yhteydessä. EU:ssa toimivien tiedustelupalvelujen yhteistyö on toivottavaa, koska ensinnäkin yhteinen turvallisuuspolitiikka, johon ei sisällytettäisi tiedustelupalveluja, olisi järjenvastaista ja toiseksi yhteistyöllä saavutettaisiin monia ammatillisia, taloudellisia ja poliittisia etuja. Lisäksi tämä vastaisi paremmin ajatusta tasa-arvoisesta kumppanuudesta Yhdysvaltojen kanssa ja voisi sitoa kaikki jäsenvaltiot järjestelmään, joka olisi täysin Euroopan ihmisoikeussopimuksen mukainen. Silloin on luonnollisesti varmistettava, että Euroopan

parlamentilla on riittävät valvontaoikeudet. Euroopan parlamentti on laatimassa sisäisiä määräyksiä luottamuksellisten ja arkaluonteisten tietojen ja asiakirjojen saatavuudesta.

13.3. Suositukset

Kansalaisten ja yritysten suojaamista koskevien kansainvälisten sopimusten tekeminen ja muuttaminen

1. Euroopan neuvoston pääsihteeriä kehotetaan toimittamaan ministerikomitealle tutkimus siitä, olisiko aiheellista mukauttaa Euroopan ihmisoikeussopimuksen 8 artiklassa taattua yksityiselämän suojaa nykyaikaisiin viestintämenetelmiin ja kuuntelumahdollisuuksiin lisäpöytäkirjan avulla tai samalla, kun tietosuojasta annetaan sääntöjä tietosuojasta tehtyä yleissopimusta tarkistettaessa, edellyttäen että näin ei lasketa tuomioistuimen kehittämää oikeussuojan tasoa tai vähennetä uuteen kehitykseen mukautumisen edellyttämää joustavuutta;

2. Jäsenvaltioita kehotetaan luomaan eurooppalainen foorumi, jossa tarkistetaan kirje- ja viestintäsalaisuuden takaamista koskevia sääntöjä, ja sopimaan lisäksi yhteisestä tekstistä, jossa taataan yksityiselämän suoja, sellaisena kuin se on määriteltynä Euroopan unionin perusoikeuskirjan 7 artiklassa, kaikille Euroopan kansalaisille jäsenvaltioiden koko alueella ja lisäksi taataan, että tiedustelupalvelut noudattavat toiminnassaan perusoikeuksia ja kertomuksen 8 luvussa, erityisesti 8.3.4 kohdassa olevia, Euroopan ihmisoikeussopimuksesta johdettuja ehtoja;

3. Euroopan neuvoston jäsenvaltioita pyydetään tekemään lisäpöytäkirja, jossa mahdollistetaan Euroopan yhteisöjen liittyminen Euroopan ihmisoikeussopimukseen, tai harkitsemaan muita toimenpiteitä, joilla voidaan ratkaista Strasbourgin ja Luxemburgin tuomioistuinten oikeuskäytännön väliset ristiriidat;

4. YK:n pääsihteeriä kehotetaan pyytämään asiasta vastaavaa toimikuntaa esittämään ehdotuksia kansalaisoikeuksia ja poliittisia oikeuksia koskevan kansainvälisen yleissopimuksen yksityiselämän suojaa koskevan 17 artiklan mukauttamiseksi teknisiin uudistuksiin;

5. Yhdysvaltoja kehotetaan allekirjoittamaan kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälisen yleissopimus, jotta yleissopimuksella perustettu ihmisoikeuskomitea voi ottaa käsiteltäväksi Yhdysvaltoja vastaan nostettuja yksittäisten henkilöiden valituksia sopimuksen rikkomisesta; alalla toimivia amerikkalaisia kansalaisjärjestöjä, erityisesti ACLU:a (American Civil Liberties Union) ja EPIC:iä (Electronic Privacy Information Center) pyydetään painostamaan Yhdysvaltojen hallitusta asiassa;

Kansalliset lainsäädäntötoimet kansalaisten ja yritysten suojaamiseksi

6. Kaikkiin jäsenvaltioihin vedotaan, jotta nämä tarkistavat oman tiedustelupalveluja koskevan lainsäädäntönsä yhteensopivuuden perusoikeuksien kanssa;

7. Jäsenvaltiota kehotetaan pyrkimään sellaiseen yhteiseen suojan tasoon tiedustelupalvelujen toimintoihin nähden, joka vastaa jäsenvaltioiden suojan korkeinta

tasoa, koska ulkomaantiedustelupalvelun kohteena olevat kansalaiset ovat tavallisesti muiden valtioiden ja siten myös muiden jäsenvaltioiden kansalaisia;

8. EU:n toimielimiä kehotetaan, jos tiedustelupalvelujen YUTP:n mukainen yhteistyö toteutuu, luomaan riittävät Euroopan kansalaisia suojaavat määräykset; Euroopan parlamentti on luonnollisesti valvontaelin, jonka on osaltaan luotava tarvittavat edellytykset tämän erittäin herkän alueen valvonnalle, jotta tarvittavien valvontaoikeuksien vaatiminen olisi realistista ja perusteltua;

Erityiset oikeustoimet talousvakoilun torjumiseksi

9. Jäsenvaltioita kehotetaan pohtimaan, missä määrin talousvakoilua ja lahjontaa, jonka tarkoituksena on sopimusten hankkiminen, voitaisiin torjua yhteisön ja kansainvälisen oikeuden säännöksin, ja erityisesti, voitaisiinko WTO:ssa saada aikaan säännöt, joissa otetaan huomioon tällaisen toiminnan kilpailua vääristävä vaikutus siten, että tällaiset sopimukset todetaan mitättömiksi;

10. Jäsenvaltioita kehotetaan sitoutumaan yhteiseen yksiselitteiseen julistukseen, jonka mukaan ne pidättyvät toisiinsa kohdistuvasta talousvakoilusta, ja osoittamaan siten, että ne toimivat EY:n perustamissopimuksen hengen ja määräysten mukaisesti;

Toimet, jotka koskevat lainsäädännön soveltamista ja sen valvontaa

11. Kansallisiin parlamentteihin, joilla ei vielä ole omaa tiedustelupalveluja valvovaa parlamentaarista valvontaelintä, vedotaan, jotta ne perustaisivat sellaisen;

12. Tiedustelupalvelujen kansallisia valvontavaliokuntia pyydetään korostamaan voimakkaasti yksityisyyden suojaa käyttäessään niille myönnettyjä valvontavaltuuksia riippumatta siitä, onko kysymys omien kansalaisten, muiden EU:n kansalaisten vai yhteisön ulkopuolisten maiden kansalaisten valvonnasta;

13. Jäsenvaltioiden tiedustelupalveluja kehotetaan ottamaan tietoja vastaan toisilta tiedustelupalveluilta vain, jos voidaan todeta oman kansallisen lainsäädännön määrittämät edellytykset, koska jäsenvaltiot eivät voi vapauttaa itseään Euroopan ihmisoikeussopimuksesta aiheutuvista velvoitteista käyttämällä muita tiedustelupalveluja;

14. Saksaan ja Yhdistyneeseen kuningaskuntaan vedotaan, jotta ne salliessaan Yhdysvaltojen tiedustelupalvelujen edelleen kuunnella viestintää alueillaan asettavat ehdoksi sen, että kyseiset toiminnot ovat Euroopan ihmisoikeussopimuksen mukaisia, ts. että ne ovat suhteellisuusperiaatteen mukaisia, niiden oikeusperusta on tiedossa, niiden vaikutukset yksittäisiin ihmisiin ovat nähtävissä ja että niitä valvotaan tehokkaasti; koska ne vastaavat alueellaan tiedustelupalvelujen ihmisoikeuksien mukaisesta tai vain siedettävästä toiminnasta;

Toimet kansalaisten ja yritysten omaehtoisen suojelun edistämiseksi

15. Komissiota ja jäsenvaltioita kehotetaan kehittämään ohjelmia, jotka lisäävät kansalaisten ja yritysten tietoisuutta turvallisuusongelmista ja tarjoavat samalla käytännön apua kattavien suojajärjestelmien suunnitteluun ja toteutukseen;

16. Komissiota ja jäsenvaltiota pyydetään laatimaan sopivia toimia eurooppalaisen salaustekniikan ja -ohjelmien edistämiseksi, kehittämiseksi ja valmistamiseksi sekä ennen kaikkea tukemaan hankkeita, jotka tähtäävät sellaisten käyttäjäystävällisten salausohjelmien kehittämiseen, joiden lähdekoodi on julkinen;

17. Komissiota ja jäsenvaltioita kehotetaan edistämään ohjelmistohankkeita, joissa ohjelmistojen lähdekoodi julkistetaan, sillä vain näin voidaan taata, ettei ohjelmistoihin rakenneta "takaportteja" (ns. open source -ohjelmistot);

18. Unionin toimielimiin ja jäsenvaltioiden julkishallintoihin vedotaan sähköpostien järjestelmällisen salauksen käyttämiseksi, niin että salauksesta voisi pitkällä aikavälillä tulla normaali käytäntö;

Muut toimet

19. Yrityksiin vedotaan vakoilun torjumisesta vastaavien yksikköjen kanssa tehtävän yhteistyön lujittamiseksi, erityisesti ulkopuolisten talousvakoiluun tähtäävien hyökkäysten ilmoittamiseksi viranomaisille, jotta niiden tehokkuutta voidaan näin parantaa;

20. Komissiota kehotetaan antamaan ehdotus yritysten tietojen turvaamiseen liittyviä kysymyksiä käsittelevän eurooppalaisen neuvontaelimen perustamisesta, jonka tehtäviin kuuluu ongelmasta tiedottaminen ja käytännön apu;

21. Euroopan parlamenttia kehotetaan järjestämään Euroopan laajuinen konferenssi yksityiselämän suojaamisesta televalvonnalta, jotta eurooppalaisille, yhdysvaltalaisille ja muiden valtioiden kansalaisjärjestöille saadaan foorumi, jossa voidaan keskustella rajat ylittävistä ja kansainvälisistä näkökohdista sekä koordinoida toiminta-aloja ja menettelyjä.