KIRJALLINEN KYSYMYS 150/2000 vp

Echelon-vakoilujärjestelmä ja tiedonsiirron suojaaminen

Eduskunnan puhemiehelle

Kylmän sodan jälkeen puheet kansakuntien toisiaan kohtaan harjoittamasta vakoilusta vaikenivat. Tiedossa on ollut, että vakoilutoiminta on jatkunut, mutta keskustelu vakoilun mittavuudesta ja seurauksista on vaiennut. Monille Euroopan parlamentin edustajille ja meille muille kuuntelijoille tuli täytenä yllätyksenä Duncan Campbellin 23.2.2000 esittelemä raportti Echelon-vakoilujärjestelmästä ja sen toiminnasta.

Echelon-vakoilujärjestelmän avulla Yhdysvallat, englanninkieliset maat liittolaisinaan, pystyy hankkimaan tietoa Euroopan yrityksistä ja kansalaisista murtamalla järjestelmällisesti salausohjelmia, valvomalla Internetiä ja kuuntelemalla puhelimia. Järjestelmän kautta sanotaan kulkevan miljardeja viestejä tunnissa puhelujen, faksien ja sähköpostien muodossa. Suodatusjärjestelmä on tehokas. Tarpeelliset viestit fakseista ja Internetistä poimitaan hakusanojen avulla. Vakoilun taustaorganisaationa on Yhdysvaltojen kansallinen turvallisuusvirasto NSA, jonka väitetään etsivän tietoa, joka kiinnostaa ulkomailla kauppaa käyviä amerikkalaisia yrityksiä.

Echelon-vakoilujärjestelmän tarkkailuasemat ovat EU-rajojen ulkopuolella mm. Uudessa-Seelannissa, Australiassa, Kanadassa ja Japanissa. Tämän vuoksi vakoilua ei voida estää. Olisi kuitenkin tärkeää pohtia, miten suojaamme tiedonsiirron tarpeeksi hyvin. Kyse on myös kansalaisten perusoikeuksiin kuuluvan tietosuojan rikkomisesta.

On järkyttävää, että tällaisten vakoilujärjestelmien olemassaolosta vaietaan. Kukaan ei ole kiinnittänyt Echelonin olemassaoloon mitään huomiota, vaikka vakoilujärjestelmän on tiedetty toimineen jo kauan. Vakoilusta ja salakuuntelusta arvioidaan koituvan miljardien markkojen vuotuiset tappiot eurooppalaisille yrityksille. EU:ssa on raportin myötä herätty: sekä ministerineuvosto että komissio antavat lausuntonsa Echelonista maaliskuussa Euroopan parlamentille.

Edellä olevan perusteella ja valtiopäiväjärjestyksen 37 §:n 1 momenttiin viitaten esitämme kunnioittavasti valtioneuvoston asianomaisen jäsenen vastattavaksi seuraavan kysymyksen:

Mitä hallitus aikoo tehdä sen eteen, että tiedonsiirto suojattaisiin hyvin jo kansallisella tasolla Echelon-vakoilujärjestelmältä ja

miten hallitus tulee tiedottamaan omista tiedoistaan EU:hun ja Suomeen kohdistuvan vakoilun laajuudesta?

Helsingissä 25 päivänä helmikuuta 2000

Arto Seppälä /sd
Ville Itälä /kok

Eduskunnan puhemiehelle

Valtiopäiväjärjestyksen 37 §:n 1 momentissa mainitussa tarkoituksessa Te, Rouva puhemies, olette toimittanut valtioneuvoston asianomaisen jäsenen vastattavaksi kansanedustaja Arto Seppälän /sd ym. näin kuuluvan kirjallisen kysymyksen KK 150/2000 vp:

> *Mitä hallitus aikoo tehdä sen eteen, että tiedonsiirto suojattaisiin hyvin jo kansallisella tasolla Echelon-vakoilujärjestelmältä ja*
>
> *miten hallitus tulee tiedottamaan omista tiedoistaan EU:hun ja Suomeen kohdistuvan vakoilun laajuudesta?*

Vastauksena kysymykseen esitän kunnioittaen seuraavaa:

Signaalitiedustelua (sigint, signal intelligence) ovat harjoittaneet useat valtiot jo vuosikymmeniä. Ilmiö ei siis ole uusi. Yhdestä tällaisesta signaalitiedustelujärjestelmästä, anglo-amerikkalaisesta Echelonista, on keskusteltu jo muutama vuosi sitten Euroopan parlamentissa. Vaikkei Echelon olekaan ainoa signaalitiedustelua tai kommunikaatiotiedustelua (comint, communications intelligence) harjoittava organisaatio, on se todennäköisesti laajin lajissaan. Mainittakoon, että myös naapurimaassamme Venäjällä toimii FAPSI-niminen signaalitiedustelupalvelu, jonka palveluksessa on noin 54 000 työntekijää.

Echelon-järjestelmässä on kyse elektroniseen tiedusteluun perustuvasta järjestelmästä, jonka perusta luotiin jo kylmän sodan alkuvaiheessa vuonna 1947. Se oli tuolloin suunnattu Neuvostoliittoa ja sen satelliittivaltioita vastaan. Järjestelmässä mukana olevat valtiot ovat Yhdysvallat, Yhdistyneet Kuningaskunnat, Kanada, Uusi-Seelanti ja Australia. Nykymuotoinen Echelon perustettiin edellä tarkoitetun yhteistyön pohjalle 1970-luvun puolivälissä, jolloin sitä käytettiin pääasiassa poliittisen ja sotilaallisen tiedon keräämiseen Varsovan liiton suunnitelmista. Nykyisiin mittoihinsa se kasvoi kylmän sodan viimeisinä vuosina. Sittemmin Echelonin käyttötarkoitus on suuntautunut myös ei-sotilaallisiin kohteisiin, kuten terrorismiin, huumekauppaan ja rahanpesuun. Viime aikoina on Echelonin lisäksi epäilty liittyvän myös Yhdysvaltain harjoittamaan taloudelliseen tiedusteluun.

Sähköisessä muodossa liikkuu nykyisin paljon tietoa, myös hyvin luottamuksellistakin aineistoa, josta ei haluta antaa sivullisille tietoja. Tämän aineiston vuotaminen sivullisten käsiin voi aiheuttaa merkittäviä vahinkoja. Tällaisten tietojen sieppaamisen riski on merkittävän suuri. Tietojen suojaamisessa ovat sähköisten kommunikaatiovälineiden käyttäjät itse avainasemassa. Heidän tulisi omassa toiminnassaan ottaa kuuntelun riski huomioon. Riittävän vahvojen, testattujen salausten käyttö on ehdoton edellytys tietoturvan takaamiseksi. Varma tapa välttää nämä riskit on käyttää viestinnässä luotettavia ei-sähköisiä kuriiri- tai postitusyhteyksiä.

Suomella on hyvin toimivat viranomaissuhteet Euroopan unionin (EU) valtioihin myös turvallisuuskysymyksissä. Suojelupoliisi antaa vuosikertomuksissaan ja muissa valtionhallinnon sisäisissä raporteissa tietoja näistä riskeistä. Hallitus antaa luonnollisesti tarvittaessa tietoja eduskunnalle näistä keskusteluista samoin kuin myös Suomeen tai muuhun EU:n jäsenvaltioon mahdollisesti kohdistuvasta vakoilusta.

Ennalta estävä turvallisuustyö on yksi suojelupoliisin lakisääteiseen toimialaan kuuluvista tehtävistä ja myös yksi olennainen suojelupoliisin

käytännön toiminnan osa. Ennalta estävää turvallisuustyötä suojelupoliisi toteuttaa muun muassa siten, että se informoi yrityksiä ja viranomaisia uhkakuvista, harjoittaa ohjaus- ja neuvontatoimintaa sekä antaa erityistä asiantuntija-apua muun muassa tietoturvallisuuteen, yritysvakoiluun, tietovuotoihin, tietojen suojaamiseen sekä henkilöstöturvallisuuskysymyksiin liittyen. Viime vuosina toimintaa on suunnattu erityisesti huipputeknologiayrityksiin ja tutkimuslaitoksiin. Toiminnassa on korostettu etenkin maailmanlaajuisen tietojärjestelmien verkottumisen ja informaatioteknologian kehittymisen sekä toisaalta merkittävästi lisääntyneen tieteellis-taloudellis-teknisen tiedustelutoiminnan mukanaan tuomia uhkatekijöitä ja tietoturvallisuusriskejä. Lähtökohtana toiminnassa on eri organisaatioiden informoiminen ajankohtaisista tietoturvallisuuteen liittyvistä teknisistä ynnä muista kysymyksistä, jotta eri organisaatioissa voitaisiin tältä pohjalta sisäisesti varautua mahdollisiin uhkatekijöihin sekä suunnitella tietoturvallisuusstrategia ja sen mukaiset käytännön järjestelyt asianmukaisella tavalla. Tarvittaessa voidaan antaa myös konsulttiapua näissä kysymyksissä. Vastuu tietojen ja tietojärjestelmien suojaamisesta ja sen käytännön toteutuksesta on kuitenkin luonnollisesti aina yrityksillä ja viranomaisilla itsellään.

Valtiovarainministeriö on asettanut helmikuun 18 päivänä 2000 jaoston valmistelemaan salauskäytäntöjä koskevaa valtionhallinnon tietoturvallisuussuositusta. Jaostossa on Pääesikunnan, sisäasiainministeriön, ulkoasiainministeriön, valtiovarainministeriön ja Telehallintokeskuksen edustus. Jaoston toimikausi päättyy 30 päivänä marraskuuta 2000. Jaoston tehtävänä on määritellä riittävät salauskäytännöt sekä viranomaisten sisäiseen ja viranomaisten väliseen että viranomaisen ja kansalaisen tai muun asiakkaan väliseen yhteydenpitoon. Tehtävänä on suosittaa, mitkä salauskäytännöt ovat riittäviä erityyppisten tietojen, asiakirjojen ja sähköpostiviestien käsittelyyn eri käsittelyvaiheissa. Lisäksi tehtävänä on selvittää, millaisia ohjelmistoja salauksen hoitamiseen on tarjolla sekä laatia tietoturvallisuussuositus, jonka avulla voidaan parantaa tietoturvallisuuden tasoa yhtenäistämällä salauskäytäntöjä ja salaustekniikan käyttöä valtionhallinnossa.

Salauskäytäntöjen ja salaustekniikan yleistyessä viranomaisten välisessä sähköisessä tiedonsiirrossa ottanevat teleoperaattorit yleisemminkin käyttöön standardoituja salauskäytäntöjä myös yksityisen sektorin välisessä tiedonsiirrossa, jolloin esimerkiksi Echelon-järjestelmän signaalitiedustelu voidaan estää.

Helsingissä 21 päivänä maaliskuuta 2000

Sisäasiainministeri Kari Häkämies

Till riksdagens talman

I det syfte 37 § 1 mom. riksdagsordningen anger har Ni, Fru talman, till vederbörande medlem av statsrådet översänt följande av riksdagsman Arto Seppälä /sd m.fl. undertecknade skriftliga spörsmål SS 150/2000 rd:

> *Vad ämnar regeringen göra för att dataöverföringen redan på nationell nivå skall skyddas väl mot Echelon-spaningssystemet och*
>
> *hur ämnar regeringen informera om sina egna uppgifter om omfattningen av det spionage som riktas mot Finland och EU?*

Som svar på detta spörsmål får jag vördsamt anföra följande:

Många stater har utövat signalspaning (sigint, signal intelligence) redan i årtionden. Det är alltså inget nytt fenomen. Ett av dessa system för signalspaning, det anglo-amerikanska Echelon, har redan för några år sedan diskuterats i Europaparlamentet. Även om Echelon inte är den enda organisation som utövar signalspaning eller kommunikationsspaning (comint, communications intelligence), är den sannolikt den största i sitt slag. Det bör även nämnas att i vårt grannland Ryssland fungerar en signalspaningstjänst vid namn FAPSI, som har ca 54 000 personer i sin tjänst.

Echelon är ett system som baserar sig på elektronisk spaning och vars grund lades redan i början av det kalla kriget 1947. Då var det riktat mot Sovjetunionen och dess satellitstater. De stater som är med i systemet är Förenta staterna, Förenade kungariket, Kanada, Nya Zeeland och Australien. Echelon i dess nuvarande form grundades på basis av detta samarbete i mitten av 1970-talet, varvid det användes i huvudsak för att samla politisk och militär information om Warszawapaktens planer. Sin nuvarande omfattning fick systemet under det kalla krigets sista år. Senare har användningen av Echelon varit inriktad även på icke-militära mål som terrorism, narkotikahandel och penningtvätt. På sista tiden har Echelon dessutom misstänkts vara förknippat med den ekonomiska underrättelse som Förenta staterna bedriver.

Mycket data överförs idag i elektronisk form, t.o.m. mycket konfidentiellt material, som man inte vill ge utomstående information om. Om sådant material läcker ut till utomstående kan det orsaka stora skador. Risken att sådan information fångas in är mycket stor. De som använder elektroniska kommunikationsmedel är själva i en nyckelposition när det gäller att skydda informationen. De borde i sin egen verksamhet beakta risken för avlyssning. En obestridlig förutsättning för att dataskyddet skall kunna garanteras är att tillräckligt säkra, testade krypteringar används. Ett säkert sätt att undvika dessa risker är att man i kommunikationen använder icke-elektroniska kurir- eller postförbindelser.

Finland har välfungerande relationer till myndigheterna i Europeiska unionens (EU) länder även när det gäller säkerhetsfrågor. Skyddspolisen ger i sina årsrapporter och i andra rapporter inom statsförvaltningen information om dessa risker. Regeringen ger naturligtvis vid behov uppgifter till riksdagen om dessa diskussioner liksom om spionage som eventuellt riktas mot Finland eller EU:s andra medlemsstater.

Det förebyggande säkerhetsarbetet är en av de uppgifter som hör till skyddspolisens lagstadgade verksamhetsfält och som även utgör en vä-

sentlig del av säkerhetspolisens praktiska verksamhet. Säkerhetspolisen utför det förebyggande säkerhetsarbetet bl.a. så att den informerar företag och myndigheter om hotbilder, utövar styrnings- och informationsverksamhet samt ger särskild experthjälp bl.a. i samband med datasäkerhet, företagsspionage, läckor, skydd av information samt personalsäkerhet. Under de senaste åren har verksamheten särskilt riktats till högteknologiföretag och forskningsanstalter. I verksamheten har i synnerhet betonats de hotfaktorer och risker i fråga om datasäkerheten som uppstår när t.ex. datasystemen globalt ansluts till nät och informationsteknologin utvecklas och å andra sidan i och med att den vetenskapliga, ekonomiska, och tekniska underrättelseverksamheten ökar märkbart. Utgångspunkten i verksamheten är att olika organisationer informeras om aktuella tekniska och andra frågor som hänför sig till datasäkerheten, för att olika organisationer på basis av denna information internt skall kunna förbereda sig för eventuella hotfaktorer och på ett ändamålsenligt sätt planera en datasäkerhetsstrategi och praktiska arrangemang i enlighet med den. Vid behov kan man även ge konsulthjälp beträffande dessa frågor. Ansvaret för skyddet av information och datasystem och för det praktiska förverkligandet av detta ligger naturligtvis alltid på företagen och myndigheterna själva.

Finansministeriet har den 18 februari 2000 tillsatt en delegation som skall bereda en datasäkerhetsrekommendation för statsförvaltningen gällande praxis för krypteringen. I delegationen finns representanter för Huvudstaben, inrikesministeriet, utrikesministeriet, finansministeriet och Teleförvaltningscentralen. Delegationens mandatperiod löper ut den 30 november 2000. Delegationens uppgift är att definiera vad som är en tillräcklig krypteringspraxis såväl i kontakter inom myndigheten som mellan myndigheter och i kontakter mellan myndigheter och medborgare eller andra klienter. Uppgiften är att visa hurdan krypteringspraxis är tillräcklig för behandling av olika typer av information, handlingar och e-postmeddelanden i olika behandlingsskeden. Dessutom har den till uppgift att utreda hurdan programvara det finns till buds för skötseln av krypteringen samt att göra upp en datasäkerhetsrekommendation, med hjälp av vilken man kan förbättra datasäkerheten genom att förenhetliga krypteringspraxis och användningen av krypteringsteknik i statsförvaltningen.

I och med att krypteringspraxis och krypteringstekniken blir vanligare i den elektroniska dataöverföringen myndigheter emellan torde teleoperatörerna ta i mera allmänt bruk en standardiserad krypteringspraxis även i dataöverföringen inom den privata sektorn, varvid t.ex. Echelonsystemets signalspaning kan förhindras.

Helsingfors den 21 mars 2000

Inrikesminister Kari Häkämies