Electronic Frontier Finland
PL 239
00101 HELSINKI

25.3.2009
LAUSUNTO

ASIA: VNS 1/2009 vp Suomen turvallisuus- ja puolustuspolitiikka 2009

1 Johdanto

Turvallisuus- ja puolustuspolitiikka liittyy Electronic Frontier Finlandin alaan vain siltä osin kuin se koskettaa tietotekniikkaa ja ihmisoikeuksia, ja rajoitumme tässä lausunnossa niihin.

Lyhyenä yhteenvetona voidaan todeta, että vaikka selonteossa tulee moneen kertaan esille yhteiskunnan yhä kasvava riippuvuus erilaisista tietoteknisistä järjestelmistä ja niiden mahdollisen lamaantumisen aiheuttamat ongelmat, siinä ei kiinnitetä riittävästi huomiota niiden erityispiirteisiin.

Erityisesti sisäpiiriläisten tai pikkurikollisia merkittävämmillä voimavaroilla varustettujen hyökkääjien nimenomaan tietoteknisille järjestelmille aiheuttamia riskejä ei ole nostettu esille.

Selonteossa todetaan aivan oikein, että ”sähköisten viestintä- ja tietojärjestelmien rakenteet mahdollistavat niiden käytön rikollisiin tarkoituksiin sekä vaikuttamisen yhteiskunnan elintärkeisiin toimintoihin myös maamme rajojen ulkopuolelta”, mutta huoltovarmuuteen liittyvät riippuvuudet tietojärjestelmien toimittajista jäävät kuitenkin mielestämme liian vähälle huomiolle.

Vielä vähemmän huomiota selonteossa saavat vaarat, joita voi aiheutua viranomaisten omaan käyttöön laadittujen järjestelmien joutumisesta kokonaan tai osittain vääriin käsiin tai kun niistä vuotaa arkaluontoista, väärinkäytöksille altista tietoa.

2 Eritasoisten tilanteiden ristiriitaiset turvallisuusuhat

Selonteossa ei nosteta selvästi esille sitä tietoteknisille turvajärjestelmille luonteenomaista piirrettä, että keinot, jotka tehoavat hyvin heikkoihin vastustajiin, saattavat kääntyä suorastaan haitallisiksi suuremmilla resursseilla varustetun vastapuolen kanssa.

Teoreettisena ääritapauksena voidaan ajatella koko järjestelmän joutumis-

ta vääriin käsiin esimerkiksi maan joutuessa miehitetyksi, ja järjestelmien arviointia siinäkin tapauksessa voisi pitää hyödyllisenä ajatuskokeena. Tätä skenaariota emme tässä kuitenkaan analysoi sen enempää.

Monessakin merkittävän todennäköisenä pidettävässä kriisitilanteessa sen sijaan on mahdollista, että joku merkittävillä resursseilla varustettu toimija — terroristi- tai rikollisjärjestö, monikansallinen yritys tai jopa valtio — voisi yrittää vaikuttaa Suomen poliittiseen päätöksentekoon, lainsäädäntöön, vaaleihinkin, käyttäen hyväkseen tietoteknisten järjestelmiemme heikkouksia. Joitakin mahdollisia uhkaskenaarioita on hahmoteltu alempana.

Pienimuotoisemman, normaalioloissa tapahtuvan tietoverkkorikollisuuden aiheuttamat uhat ovat luonteeltaan joissakin suhteissa selvästi edellisestä eroavia ja helpommin perinteisen poliisitoiminnan keinoin torjuttavissa. Tietotekniikka tarjoaa myös monia olennaisesti uusia mahdollisuuksia, mutta niiden käyttöönotossa pitäisi olla varovainen ja arvioida etukäteen niiden skaalautuvuutta ja vaarallisuutta poikkeustilanteissa. Poliisin tietoteknisissä valmiuksissa ja resursseissa ja niiden ajan tasalla pitämisessä on joka tapauksessa paljon parantamisen varaa.

3 Riippuvuus ulkopuolisista toimijoista

Selonteossa todetaan oivaltavasti, että "Yritysten kansainvälisen omistuksen lisääntyminen vaikuttaa varautumisen järjestelyihin" ja toisaalla, että "Sotilasliittoon kuulumattomana maana Suomi ei voi käyttää sotilaallisen puolustuksensa suunnittelun perusteena ulkopuolelta saatavaa sotilaallista tukea."

Keskeisten tietojärjestelmien riippuvuus yksittäisistä, usein ulkomaisista toimijoista ja suljetuista, oman tietoturva-auditoinnin ulottumattomiin jäämistä ohjelmistoista jää kuitenkin huomiotta. Pahimmassa tapauksessa voisi käydä niin, että pääsy omiin dokumentteihimme tai järjestelmiimme olisi katkaistavissa yhden ulkomaalaisen yrityksen päätöksellä ilman ennakkovaroitusta. Tämä pitäisi ottaa huomioon etenkin huoltovarmuutta arvioitaessa.

Kaikkien tärkeiden dokumenttien ja ohjelmien osalta tulisikin ottaa vaatimukseksi avointen, standardoitujen ja usean erimaalaisen toimittajan tukemien formaattien ja protokollien käyttö, ja vaatia tärkeimpien ohjelmistojen lähdekoodia itse auditoitavaksi.

4 Avoimuus vs. salaisuus

Tietoteknisten järjestelmien turvallisuutta arvioitaessa on tärkeää huomata, että joissakin asioissa salailu heikentää turvallisuutta. Erityisesti kryptografiaan perustuvissa menetelmissä tunnetusti tilanne on se, että vaikka käytettyjen *avainten* huolellinen salassapito on ensiarvoisen tärkeää, käytetyn

tekniikan julkisuus on lähes aina turvallisuutta parantava tekijä, Näin siksi, että mitä useampi tekniikan tuntee, sitä todennäköisemmin sen heikkoudet on löydetty ja korjattu, ja avainten vaihtaminen on aina paljon helpompaa kuin teknisten perusratkaisujen. Tässäkin yhteydessä on hyvä muistaa sisäpiiriläisten suuri osuus tietomurroissa.

5 Tietovuodot

Monet viranomaisten tietojärjestelmät sisältävät eri tavoin arkaluontoista tietoa: poliisin järjestelmät, potilastietojärjestelmät (hyvin houkuttelevia esimerkiksi kiristykseen sopivia uhreja etsiville), erilaiset biotietopankit, DNA- ja sormenjälkirekisterit, kaikki ihmisten liikkeitä rekisteröivät järjestelmät, valvontakamerat jne.

Mitään järjestelmää ei kuitenkaan voida suojata sataprosenttisesti. Esimerkkejä poliisinkin tietojärjestelmien vuodosta viime aikoina löytyy mm. Ruotsista ja Britanniasta, ja huippuviroissakin olevat ihmiset ovat alttiita kiristykselle ja lahjonnalle — lähes kaikki merkittävät tietomurrot ovat ainakin osittain sisäpiiriläisten tekemiä. Tehtiin tietojärjestelmien suojaamiseksi mitä tahansa, kriittisen tietovuodon todennäköisyys kasvaa aina suoraan suhteessa kerättävän ja säilytettävän tiedon määrään.

Siten pitäisi ottaa periaatteeksi välttää arkaluontoisten tietojen keräämistä alunperinkään enempää kuin on välttämätöntä.

Koska kaikilla tietoa käsittelevillä toimijoilla on luonnollinen taipumus luottaa itseensä liikaa ja kerätä tietoa ”varmuuden vuoksi” enemmän kuin oikeasti olisi tarpeen ja perusteltua, olisi parasta yleisensä linjana kallistua mieluummin liian vähän kuin liian paljon tiedon keruun suuntaan. Tämä koskee niin tiedonkeruumekanismeja kuin kerätyn tiedon tallentamistakin.

Silloin kun tietoa kuitenkin kerätään, toimenpiteet sen suojaamiseksi pitäisi tietenkin mitoittaa arvioiden sen arkaluontoisuutta ja vuotoherkkyyttä myös eritasoisissa poikkeusoloissa.

6 Terrorismi

Terrorismia vastutettaessa tulisi muistaa, että varsinainen vihollinen ei ole ne ihmiset, jotka terroria harjoittavat, vaan järjestelmän muutos, jota he yrittävät saada aikaan, ja puolustettavana eivät ole ne ihmiset, jotka nyt ovat vallassa, vaan vallitseva järjestelmä - jonka olennainen osa on vapaus ja ihmisoikeudet.

Raportissa todetaankin aivan oikein, että ”Ihmisoikeudet ovat oleellinen osa laajaa turvallisuuskäsitystä ja inhimillisen turvallisuuden toteutumista.”

Viranomaisten luonnollinen reaktio terrorismin uhkaan on lisätä valvontaa ja rajoittaa väärinkäytölle alttiita kansalaisoikeuksia. Tämä on kuitenkin yksi terroristien nimenomaisista tavoitteista, koska he hyvin tietävät niiden yleensä kääntyvän alkuperäistä tarkoitusta vastaan. Monet terrorisminvastaiset toimet kun ovat tylppiä aseita, jotka osuvat myös sivullisiin, ja helposti tekevät näistäkin vihollisia. Samalla ne vahvistavat terroristien sisäistä motivaatiota.

Tämä koskee etenkin puuttumista sananvapauteen, myös ja etenkin tietoverkoissa. Ajatus terrorismisivujen suodattamiseen netistä voi tuntua ensi alkuun houkuttelevalta, mutta käytännössä siitä on enemmän haittaa kuin hyötyä, vaikkei edes välitettäisi sananvapaudesta periaatteena.

Terrorismiepäily ei saa muutenkaan yksilöiden kohdalla jyrätä ihmisoikeuksien yli, ihmisiä yksilöinä eikä kollektiivisesti ei saa leimata eikä pidättää mielivaltaisesti mielivaltaiseksi ajaksi, vaan syytön kunnes toisin todistetaan.

Terrorismin torjuntaa ei pidä rakentaa ikäänkuin kaikki ihmiset olisivat potentiaalisia terroristeja, joita viranomaisten pitää valvoa kaiken aikaa. Ihmisoikeudet ja kansalaisten vapaus toimia itsenäisesti ovat myös olennainen tekijä terrorisminkestävässä yhteiskunnassa, eivät vain haitta tehokkaan viranomaistoiminnan tiellä.

7 Tietoverkkorikollisuus

Tietoverkot ovat olennainen osa nyky-yhteiskunnan infrastruktuuria, aivan kuten tieverkko — ja aivan samalla tavalla niissä liikkuu rikollisia. Kaikkea tekniikkaa voi käyttää sekä hyvään että pahaan, eikä tietoverkkorikollisuutta saada millään teknisellä taikatempulla katoamaan yhtään helpommin kuin voidaan estää rikollisia ajamasta maanteillä.

Tietoverkkorikollisuudella on toki omat erityispiirteensä, ja poliisin osaamisen ja resurssien parantamista siltä osin tarvitaan. Selonteko mainitseekin, että poliisin suorituskykyä ja toimivaltuuksia kehitetään. Ennen kaikkea olisi syytä huolehtia siitä, että poliisiviranomaisilla on riittävästi resursseja ja teknologista tietotaitoa tietoverkoissa tapahtuvien rikosten tutkimiseen. Tämä voisi näkyä esimerkiksi lisäresursseina tietoverkkoihin keskittyneiden poliisien kouluttamisessa.

Olennaista on kuitenkin pitää mielessä, että tietoverkot ovat osa yhteiskuntaa ja niissä täytyy toimia samoilla pelisäännöillä kuin muussakin yhteiskunnassa. Toisin sanoen sama laki tietoverkoissa kuin kadulla.

8 Uhkaskenaarioita

Seuraavassa on hahmoteltu joidenkin tietoteknisiin järjestelmiin liittyviä uhkakuvia erityisesti jonkinasteisissa poikkeustilanteissa. Yksi miettimisen arvoinen piirre kaikissa on, kuinka monta ihmistä minkäkin hyökkäyksen toteuttamiseksi pitää lahjoa tai kiristää tai muuten saada houkuteltua mukaan.

Vaalit: jo kohtuullisilla resursseilla varustettu ulkopuolinen toimija voisi vaikuttaa Suomen vaaleihin tietoteknisten järjestelmien heikkouksien kautta. Ilmeisin esimerkki on sähköinen äänestys, jos sitä vielä käytetään: 2008 kunnallisvaaleissa kokeiltu järjestelmän olisi voinut kaapata hyvinkin pieni määrä ihmisiä (jopa ilman yhtään suomalaista salaliittolaista). Suomen vaalijärjestelmän erityispiirteet tekevät ongelmasta vielä paljon pahemman kuin esimerkiksi Yhdysvalloissa (jossa väärinkäytöksiä on paljastunutkin useita).

Ehkä vähemmän ilmeinen mutta helpompi ja jo nyt realistinen keino olisi vaikuttaa vaalimainontaan netissä — sen merkitys kasvaa vaali vaalilta, ja jonkun vaalisivuston pimentäminen ratkaisevalla hetkellä vaikka vain muutaman päivän ajaksi voisi vaikuttaa vaalitulokseen hyvinkin paljon. Perinteisten palvelunestohyökkäysten (jollaisista on jo saatu esimakua mm. Virossa, kuten selonteossakin mainitaan) lisäksi nettisuodatusjärjestelmien (sekä valtiollisen että kirjastoissa yms käytettävien) väärinkäytön mahdollisuus on tässä ilmeinen.

Jotkin autojen ajoperustaista käyttömaksua varten suunnitellut järjestelmät ovat myös alttiita väärinkäytöksille. Kuinka arvokasta vieraan vallan asiamiehille tai terroristeille olisikaan ajantasainen tieto Suomen johtohenkilöiden liikkeistä? Tässä suhteessa turvallisiakin ajoperustaisia laskutustapoja on, mutta asiaan pitää kiinnittää huomiota ajoissa ja erityisesti välttää keräämästä turhaa tietoa vuotoalttiisiin keskusvarastoihin.

Teletunnistetiedot ovat myös rikollisia, etenkin kiristystä suunnittelevia, kiinnostavaa aineistoa. Satunnaisia tietovuotoja ei voi välttää jos tietoja ylipäänsä kerätään, mutta erityisesti nopeat ja automaattiset tavat tietojen saamiseen ovat vaarallisia. Poliisin pääsy tunnistetietoihin pitäisi järjestää tavalla, jossa ei luoteta pelkästään tietokoneisiin tai automaattisiin järjestelmiin.

Sama koskee jo aikaisemminkin mainittuja terveydenhuollon tietoja. Pelkästään potilaiden suostumuksen pyytäminen tietojen siirtoon ei auta paljoa, heidän ei voi olettaa pystyvän arvioimaan eri riskien suhdetta — joskushan tiedon nopea saaminen voi olla myös kriittinen edellytys oikealle hoidolle. Tietoturva pitäisi rakentaa järjestelmän perusominaisuudeksi ja analysoida ennakkoon myös mahdollisia voimakkaan hyökkääjän aiheuttamia uhkia.

Etäluettavien tunnisteiden (rfid-sirut) käyttö henkilötunnisteissa kuten passeissa aiheuttaa myös omat vaaransa. Esimerkiksi Suomessa nyt myönnettävien passien tekniikka on sellainen, että olisi helppoa tehdä laite, joka reagoi tietyn henkilön passin läheisyyteen ja vaikka räjäyttää pommin. (Tämä nimenomainen vaara olisi helppo poistaa vaihtamalla passien kansimateriaali.)

Erilaisten biotunnistetietojen käyttö on ongelmallista monilla tavoin. Esimerkiksi sormenjälkiään ei voi noin vain vaihtaa, ja tulevan passiuudistuksen myötä toteutettavaksi suunnitellun kaikkien passinhaltijoiden sormenjälkirekisterin mahdollisesta joutumisesta vääriin käsiin aiheutuvaa peruuttamatonta vahinkoa vastaan arvioituna siitä saatavan hyödyn pitäisi olle todella suuri, että se kannattaisi toteuttaa.

9 Yhteenveto

Valtioneuvoston selonteossa on sinänsä kiitettävästi huomattu tietotekniikan muodostuneen turvallisuudellekin olennaisen tärkeäksi. Liian vähälle huomiolle siinä kuitenkin mielestämme ovat jääneet ainakin seuraavat seikat:

- riippuvuus ulkopuolisista tietojärjestelmätoimittajista;
- viranomaisjärjestelmien haavoittuvuus etenkin merkittävillä resursseilla varustetun hyökkääjän edessä ja sisäpiiriläisiä vastaan; ja
- ihmisoikeuksien käytännöllinen merkitys ja vapaan kansalaistoiminnan tärkeys viranomaistoiminnan rinnalla.

Electronic Frontier Finland ry:n puolesta

Tapani Tarvainen
puheenjohtaja

Electronic Frontier Finland – EFFI ry on perustettu käyttäjien ja kansalaisten oikeuksien puolustamiseksi Internetissä. Yhdistys pyrkii vaikuttamaan muun muassa lainsäädäntöhankkeisiin sananvapaudesta, yksityisyydestä, tekijänoikeu- desta, tietokoneohjelmien patentoinnista ja ei-toivotusta sähköisestä viestinnässä Suomessa ja Euroopassa. Lisätietoja EFFIn kotisivulta osoitteesta `http://www.effi.org/`.