TULEVAISUUSVALIOKUNNAN LAUSUNTO 1/2013 vp

Valtioneuvoston selvitys (UTP) valtioneuvoston periaatepäätöksestä Suomen kyberturvallisuusstrategiasta

Ulkoasiainvaliokunnalle

JOHDANTO

Vireilletulo

Ulkoasiainvaliokunta on 8 päivänä helmikuuta 2013 lähettänyt valtioneuvoston selvityksen valtioneuvoston periaatepäätöksestä Suomen kyberturvallisuusstrategiasta (UTP 2/2013 vp) tulevaisuusvaliokunnalle mahdollisia toimenpiteitä varten.

Asiantuntijat

Valiokunnassa ovat olleet kuultavina
- turvallisuusjohtaja Timo Härkönen, valtioneuvoston kanslia
- pääsihteeri Aapo Cederberg, puolustusministeriö
- erityisasiantuntija Yrjö Benson, valtiovarainministeriö
- toimitusjohtaja Ilkka Kananen, Huoltovarmuuskeskus
- professori Aki-Mauri Huhtinen, Maanpuolustuskorkeakoulu
- professori Rauno Kuusisto, puolustusvoimat
- ylitarkastaja Pertti Haaksluoto, suojelupoliisi
- asiantuntija Hannu Kauppinen
- tutkimusjohtaja Mikko Hyppönen, F-Secure Oyj
- johtaja Reima Päivinen, Fingrid Oyj
- yritysturvallisuusjohtaja Juha Härkönen, Fortum Oyj
- asiantuntijapäällikkö Jussi Snellman, OP-Pohjola-ryhmä
- johtaja Timo Heimo, Ruokakesko Oy
- Director of Cyber Security, Doctor of Military Science Jarno Limnéll, Stonesoft Corporation
- johtava asiantuntija Mika Linna, Finanssialan Keskusliitto.

VALIOKUNNAN KANNANOTOT

Perustelut

Suomen kyberturvallisuusstrategia

Tulevaisuusvaliokunta pitää Suomen kyberturvallisuusstrategiaa melko onnistuneena. Strategia tunnistaa keskeiset kybertoimintaympäristön muutokset, ja visio on oikeansuuntainen.

Kyberturvallisuusstrategian tavoitteena on lisätä toimijoiden yhteistä ymmärrystä kyberturvallisuudesta, käynnistää koko yhteiskunnan kattava varautuminen ja suunnittelu, lisätä kykyä yhteiskunnan elintärkeiden toimintojen turvaamiseen, vahvistaa puolustuskykymme uskottavuutta sekä kehittää Suomen kybertoimintaympäristöstä kansallinen kilpailuetu.

Vision toteuttaminen moninapaistuvassa ja nopeasti muuttuvassa globaalissa toimintaympäristössä on vaikea tehtävä. Yhteistyötä tarvitaan. Mikään lukuisista toimijoista ei voi yksin hallita kyberfyysisen toimintaympäristön kokonaisuutta. Myös kansalaisten osaamisella ja asenteilla on merkittävä rooli kyberturvallisuuden ylläpitämisessä ja edistämisessä.

Uhkiin varautumista vaikeuttaa niiden moninaisuus: tekniset viat, onnettomuudet, ilkivalta, rikollisuus, terrorismi, vakoilu ja jopa kybersodat. Määritelmästä riippuen kyberuhkiin varautumisella on liittymäpintaa myös elektroniseen sodankäyntiin, informaatiosodankäyntiin, psykologiseen vaikuttamiseen, avainhenkilövaikuttamiseen, strategiseen viestintään, harhauttamiseen, informaatioturvallisuuteen ja maineen hallintaan.

Kyberuhkiin varautuminen, niiden torjunta ja iskuista palautuminen edellyttävät hyvää koordinaatiota ja ohjeistusta. Toisaalta ohjeistus ja koordinaatio voivat samaan aikaan muodostaa myös uuden uhan: jo pelkästään avoimesti saatavilla olevat puhelinnumerot voivat paljastaa iskujen tekijöille turvallisuusviranomaisten organisaatiohierarkian.

Vaikka kyberturvallisuusstrategiassa korostuvat uhkakuvat, niin kybertoimintaympäristö on samaan aikaan myös mahdollisuus kestävälle kasvulle. Parhaimmassa tapauksessa kyberturvallisuudessa hankittu maine ja luottamus voivat tukea myös muuta tuotantoa ja vientiä blokkiutuvassa ja moninapaistuvassa maailmassa.

Tämän perusteella tulevaisuusvaliokunta keskittyy lausunnossaan erityisesti seuraaviin teemoihin:

1. julkisen ja yksityisen sektorin yhteistyö,
2. kansainvälinen yhteistyö,
3. kansalaisten rooli kyberturvallisuudessa,
4. kyberosaamisen kehittäminen,
5. kriisinsietokyky ja
6. kybertoimintaympäristön liiketoimintamahdollisuudet.

Lähtökohtia

Suomen kyberturvallisuusstrategiassa kuvataan kyberturvallisuuden visio, toimintamalli ja strategiset linjaukset. Strategiassa painottuu kyberturvallisuuden johtaminen ja kansallinen koordinaatio. Vuoden 2013 aikana laaditaan lisäksi kansallinen toimeenpano-ohjelma, joka tulee sisältämään eri hallinnonalojen ja toimijoiden valmisteluvastuulle tulevat käytännön toimenpiteet.

Lisäksi osoitetaan erillinen lisämääräraha Kyberturvallisuuskeskuksen rakentamiseen ja toimintaan. Lisämäärärahan suuruus suunnitellaan osana yhteistä toimeenpanosuunnitelmaa. Kyberturvallisuuskeskukselle luodaan 24/7-toimintakyky, mikä alustavan arvion mukaan edellyttää noin kymmenen henkilötyövuoden ja noin miljoonan euron lisäresursseja.

> Tulevaisuusvaliokunta kiirehtii kyberturvallisuusstrategian toimeenpano-ohjelman laatimista ja kannattaa Kyberturvallisuuskeskuksen perustamista. Kyberturvallisuuskeskukselle on myös taattava riittävä rahoitus.

Tietoverkkojen toimintavarmuus on välttämätöntä modernin tietoyhteiskunnan toiminnalle. Kriittisiin yrityksiin ja tuotantoon kohdistuvat kyberuhat muodostavat siksi merkittävän riskin.

Haitanteko, rikollisuus, tiedustelu ja operaatiot tietoverkossa ovat lisääntyneet merkittävästi. Uusien haittaohjelmien määrä ei koskaan ennen ole ollut näin suuri. Suomen hallintoon ja elinkeinoelämään kohdistui vuonna 2010 yli kaksi miljoonaa järjestelmähaavoittuvuuksien hyväksikäyttöyritystä tai murtoyritystä.

Monet kyberuhat (kuten esimerkiksi virukset, huijaukset, identiteettivarkaudet ja palvelunestohyökkäykset) ovat yleisesti tunnettuja, ja niihin on jo torjuntamenetelmänsä. Viime vuosina avoimissa verkoissa on kuitenkin esiintynyt yhä enemmän ammattimaisesti kohdennettuja ja räätälöityjä hyökkäyksiä, joiden torjuminen on erittäin vaikeaa. Hyökkäyksiin on osallistunut valtiollisia toimijoita, ja hyökkäykset ovat kohdistuneet myös teollisuus- ja kiinteistöautomaatioon sekä erilaisten ohjausprosessien tietojärjes-

telmiin. Ongelmien ennakoidaan tulevaisuudessa kasvavan entisestään, koska yhä useampi laite on yhteydessä verkkoon ja on sitä kautta myös mahdollisen kyberhyökkäyksen kohteena.

Valtaosa nykyisistä haittaohjelmatapauksista voidaan luokitella taloudellista hyötyä tavoitteleviksi. Nämä virukset liittyvät joko roskapostin lähettämiseen, salasanojen sekä luottokortti- ja henkilötietojen kalasteluun, hajautettuihin palvelunestohyökkäyksiin tai tietovarkauksiin. Kansalaisten näkökulmasta tyypillisiä ongelmia ovat haittaohjelmat, jotka sisältävät näppäimistönauhurin. Näppäimistönauhuri nauhoittaa saastuneella koneella kaiken, mitä käyttäjä koneellaan naputtelee, ja lähettää sen haittaohjelman tekijälle. Näin käyttäjän salasanat ja sähköpostit päätyvät vääriin käsiin. Suurin ongelma on kuitenkin henkilötiedot ja luottokorttinumerot, jotka käyttäjä syöttää tehdessään ostoksia verkkokaupassa. Suomessa nähdään jatkuvasti tapauksia, joissa haittaohjelmilla viedyillä luottokorttinumeroilla on tehty petoksia. Kyberrikollisuuden kuluttajille aiheuttamat menetykset ovat noin 85 miljardia euroa vuodessa.

Tunnetuimpia vakoiluohjelmia ovat Flame (2012) ja Red October (2013), jotka on suunniteltu seuraamaan ja tallentamaan koneen käyttäjän toimintaa ja varastamaan tiedostoja. Ohjelmat kykenevät varastamaan tiedostoja ja sähköposteja, seuraamaan Skype-puheluita ja ylipäätään kaikkea, mitä ihmiset tietokoneillaan tekevät. Ne voivat levitä USB-tikuissa ja suljetuissa lähiverkoissa ja kohdistuvat myös älypuhelimiin. Pekingissä havaittiin vuonna 2012 laajamittainen, ulkomaisiin toimittajiin kohdistunut kybervakoilu.

Kybersotaa todennäköisempi uhkakuva on painostus ja sotaa alempi kyberkonflikti. Tämäkään uhkakuva ei ole pelkästään teoreettinen: kaikilla viime aikojen kansallisilla ja kansainvälisillä konflikteilla on ollut poikkeuksetta myös kyberrintamansa. Esimerkiksi Viron pronssisoturipatsas-mellakoiden yhteydessä vuonna 2007 tapahtui kyberhyökkäys, joka kaatoi Viron keskeisiä tietojärjestelmiä. Yli kaksi viikkoa jatkuneet hyökkäykset kohdistuivat muun muassa sanomalehtien, pankkien ja valtion verkkosivuille. Iskut olivat palvelunestohyökkäyksiä, joissa ei pyritty murtautumaan palvelimille vaan pelkästään ylikuormittamaan ne keinotekoisesti aiheutetun tietoliikenneruuhkan avulla. Selvitäkseen hyökkäyksistä Viro joutui sulkemaan itsensä kansainvälisen internetliikenteen ulkopuolelle. Viron iskujen jälkeen Suomessakin jouduttiin puolustautumaan kyberiskuja vastaan. Kohteina Suomessa olivat mm. Yleisradio, STT, Eniro ja Suomi24.fi.

Myös arabimaista tuli runsaasti hyökkäyksiä tanskalaisia sivustoja vastaan vuoden 2005 pilakuvajupakan aikana. Irakin sodan aloituspäivänä 2003 satoja yhdysvaltalaisia ja brittiläisiä verkkosivustoja sotkettiin liittouman vastaisilla iskulauseilla. Jo Kosovon kriisin aikana (1990-luvun lopussa) nähtiin yksittäisten tahojen tekemiä verkkohyökkäyksiä.

Kybersodassa voidaan toimia myös sosiaalisen median kautta, kuten vuoden 2011 tapahtumat Pohjois-Afrikassa ja Venäjällä sekä hiljattain myös Gazan kriisin yhteydessä ovat osoittaneet. Sosiaalisessa mediassa ja ylipäätään mediayhteiskunnassa oleellista eivät ole vain faktat, vaan myös se, millaisen merkityksen faktat saavat ihmisten välisessä vuorovaikutuksessa. Suurin osa internetissä olevasta tiedosta liikkuu ilman minkäänlaista tiedon eheyden tarkistusta tai alkuperän varmistamista. Siten internetissä on helppoa manipuloida isojenkin massojen saamaa tietoa ilman, että sitä huomataan. Ihmisten mielipiteet polarisoituvat asenteiden ääripäihin normaalien mielipiteiden kadotessa.

Venäjän kyberpuolustuskonsepti sisältää ajatuksen kyberturvallisuusjoukoista tarvittaessa myös toisen valtion alueella. US Cyber Command puolestaan koordinoi USA:n kykyä ja toimintavalmiutta, jolla voidaan varmistaa Yhdysvaltojen ja sen liittolaisten toimintavapaus kyberavaruudessa ja kiistää sen käyttö vastustajilta. USA:lla arvioidaan olevan noin 10 000 kybersotilasta. Kiinan kyberpuolustusstrategia perustuu elektronisen sodankäynnin ja tietoverkko-operaatioiden samanaikaiseen käyttöön vastustajan elintärkeitä informaatiojärjestelmiä vastaan. Strategian mukaan näitä keinoja käytetään konfliktien alkuvaiheessa ja mahdollisesti en-

naltaehkäisevästi. Tavoitteena on toteuttaa lamauttavia iskuja johtamisjärjestelmään, samalla kun käytetään ohjuksia, ilmahyökkäyksiä ja erikoisjoukkojen iskuja fyysisiin kohteisiin ja laitteisiin. Kiinalla arvioidaan olevan jopa 160 000 kybersotilasta.

> Tulevaisuusvaliokunta katsoo, että kyberuhkan kasvu ei vähennä perinteistä, fyysisen iskun uhkaa. Kyberasetta voidaan käyttää myös fyysisen iskun valmisteluun ja strateginen infrastruktuuri voidaan kyberaseista huolimatta kaataa edelleen myös fyysisellä iskulla. Siksi kyberturvallisuusstrategiassa tulisi huomioida myös tietojärjestelmien yms. strategisen infrastruktuurin turvaaminen fyysisiltä iskuilta.

Esimerkiksi ydinaseiden käytettävyys on lisääntynyt kyberulottuvuuden myötä. Ydinaseista muodostetulla likaisella pommilla voidaan lamauttaa koko kyberulottuvuus ajallisesti ja paikallisesti käyttäen sähkömagneettista pulssia.

Julkisen ja yksityisen sektorin yhteistyö

Kybertoimintaympäristöön liittyvä käsitteistö on vielä hajanaista ja puutteellista. Toimijoita on paljon ja sitä myöten myös tietoturvatapahtumien havaitsemis-, valvonta- ja reagointikyky on sektorikohtaista ja laadultaan epätasaista. Prosessit, vastuut ja ohjeistukset yhteiskuntaa laajasti koskettavan kyberkriisin johtamisessa ja selvittämisessä vaativat siksi selkiinnyttämistä ja harjoittelua.

> Tulevaisuusvaliokunta kannattaa kyberturvallisuusstrategiassa esitettyjä tavoitteita kyberuhkaan liittyvän kansallisen koordinaation ja tilannekuvan kehittämiseksi.

Viranomaisten välisen yhteistyön ja tilannekuvan kehittäminen ja ylläpitäminen edellyttävät asiantuntijoiden mukaan myös tarkennuksia luottamuksellisen tiedon jakamiseen sekä joitakin lainsäädännöllisiä muutoksia.

> Tulevaisuusvaliokunta kiirehtii kyberturvallisuuden koordinaatioon ja tilannekuvan ylläpitämiseen liittyvien lainsäädännöllisten kehittämistarpeiden selvittämistä.

Kyberuhka voi toteutuessaan vaikuttaa laaja-alaisesti elintärkeisiin toimintoihimme. Esimerkkinä uhasta on käytetty nk. viiden minuutin sotaa:

1. Ensimmäisen minuutin aikana pysäytetään pankkien välinen maksuliikenne.
2. Toisen minuutin aikana pysäytetään pääosa julkisesta liikenteestä ja merkittävä osa yksityisautoista.
3. Kolmannen minuutin aikana sekoitetaan elintarviketoimitusten logistiikkajärjestelmät.
4. Neljännen minuutin aikana katkaistaan tärkeimmät tietoliikenneyhteydet tai hidastetaan niitä merkittävästi.
5. Viidennen minuutin aikana epästabiloidaan sähkönsiirron kantaverkko ja aiheutetaan maanlaajuinen black-out.

Tätä kuvitteellista skenaariota ei aluksi pidetty asiantuntijapiireissä kovinkaan todennäköisenä. Oletettavasti itäeurooppalaistahot pääsivät kuitenkin vuonna 2012 Alankomaissa 150 000 tietokoneeseen. Näistä koneista ryöstettiin 750 GB tietoja yhteiskunnan elintärkeiden toimintojen infrastruktuurista. Tietomurron kohteina oli tuhansia organisaatioita muun muassa ministeriöistä, aluehallinnosta, sairaaloista ja vesihuollosta. Varastetuilla tiedolla olisi todennäköisesti voitu halvaannuttaa koko maa. Tämän jälkeen kokonaisvaltaiseen kyberuhkaan (viiden minuutin sodan kaltaiseen skenaarioon) on suhtauduttu aiempaa vakavammin.

Toinen runsaasti huomiota saanut tapaus on puolestaan eräiden arvioiden mukaan lännen suunnalta alkunsa saanut Stuxnet (2010). Stuxnet oli täsmäohjattu kyberase, jolla onnistuttiin merkittävästi hidastamaan Iranin uraaninrikastamisohjelmaa. Se ei levinnyt tietoverkon välityksellä, vaan haittaohjelma vietiin perille USB-tikulla suljettuun järjestelmäympäristöön. Uutta oli myös se, että isku toteutettiin teolli-

suusautomaation ohjelmoitavan piirikortin välityksellä.

Tapaus osoitti kyberaseen tehokkuuden: haluttu vaikutus saatiin aikaiseksi sadasosalla siitä hinnasta mitä sotilaallinen isku olisi maksanut, ja ilman ihmisuhreja. Siksi Stuxnetin katsotaan käynnistäneen uuden kyberaikakauden, jossa siirrytään hakkerismista kohti hyvin organisoituja ja korkeatasoista teollisuusautomaatio-osaamista vaativia operaatioita, joissa osapuolina ovat valtiot tai suuret organisaatiot. Vastaavanlaisia piirikortteja on miljoonia erimerkkisiä ja mitä moninaisimmissa laitteissa joka maassa, myös asejärjestelmissä, ja näiden piirikorttien sisäinen tietosuoja on huono. Strategisessa infrastruktuurissa, kuten esimerkiksi energialaitoksissa sekä myös julkishallinnon tietojärjestelmissä, on käytössä jopa kymmeniä vuosia vanhoja ohjelmistoja. Mitä vanhempi järjestelmä on, sitä haavoittuvampi se on myös kyberuhkalle, sillä suojauksen taso on järjestelmän rakentamisvaiheessa asetettu silloisten vaatimusten tasolle.

> Tulevaisuusvaliokunta kiirehtii julkishallinnon sekä muiden huoltovarmuuden kannalta keskeisten toimijoiden tietojärjestelmien ohjelmistojen ja tietoturvan päivittämistä ajan tasalle.

Asiantuntijoiden mukaan kyberturvallisuusstrategiassa on huomioitu erittäin hyvin julkisen sektorin keskeiset tarpeet ja kehittämiskohteet. Merkittävä osa yhteiskunnan toiminnan kannalta kriittisestä infrastruktuurista on kuitenkin yksityisen sektorin toimijoiden vastuulla. Tämä on todettu myös kyberturvallisuusstrategiassa. Siksi strategian onnistunut toteuttaminen edellyttää tiivistä yksityisen ja julkisen sektorin yhteistoimintaa ja tietojenvaihtoa.

Kokonaisturvallisuuden kannalta elintärkeitä toimintoja ovat muun muassa valtion johtaminen, kansainvälinen toiminta, Suomen puolustuskyky, sisäinen turvallisuus, talouden ja infrastruktuurin toimivuus, väestön toimeentuloturva ja toimintakyky sekä henkinen kriisinkestävyys. Viron vuoden 2007 kokemuksista opittiin se, että julkishallinnon tietojärjestelmiin hyökkääminen ei lamaannuta kansakuntaa. Huomattavasti suurempia uhkakuvia liittyy tieto- ja energiajärjestelmien lamaantumiseen.

> Tulevaisuusvaliokunta korostaa yksityisen sektorin ja strategisen infrastruktuurin ensisijaista roolia kyberturvallisuuden kehittämisessä. On pyrittävä entistä parempaan julkisen ja yksityisen sektorin yhteistyöhön kyberuhkien torjunnassa. Eräs keino kehittää monialaisten toimijoiden yhteistyötä on harjoittelu.

Esimerkiksi Virossa on käytössä Kyberkaitse. Kyberkaitse harjoittelee määräajoin kyberhyökkäämistä Viron kriittistä infrastruktuuria vastaan. Näitä joukkoja on käytetty myös NATO:n kyberharjoituksissa, joissa Suomikin oli aktiivisessa roolissa mukana vuonna 2012. Viro perusti Kyberkaitsen vuoden 2007 kyberhyökkäyksistä toivuttuaan ja sai Tallinaan sittemmin myös NATOn kybersuorituskykyjen osaamisen kehittämiskeskuksen (CCDCOE). Suomella on tähän kehittämiskeskukseen hyvät suhteet, ja Suomi ja Ruotsi on kutsuttu sen liitännäisjäseniksi.

Kaupan ja teollisuuden uhkamalleissa korostuvat häiriöt logistiikassa, tietojärjestelmissä ja energian tuotannossa. Syitä häiriöille voivat olla muun muassa ilkivalta, rikollisuus, onnettomuudet, tekniset viat ja luonnon ääri-ilmiöt. Teollisuuden ja kaupan edustajien mielestä yksityisen sektorin ja strategisen infrastruktuurin kyberriskeihin varautuminen tulisikin kytkeä osaksi toimijoiden normaalia varautumista, koska varautumismenettelyt ovat samankaltaisia useissa eri häiriöissä. Kyberhyökkäyksen, vesivahingon, tulipalon tai esimerkiksi myrskyn aiheuttaman tieto- ja/tai energiaverkon toimintahäiriön vaikutukset ja seuraukset ovat samanlaisia. Siksi kyberuhkiin varautuminen tulisi liittää yritysten normaaleihin varojärjestelmiin. Erillisten varojärjestelmien rakentaminen aiheuttaa monimutkaistumista, ylimääräistä työtä ja tarpeettomia kustannuksia.

> Tulevaisuusvaliokunnan mielestä kyberriskeihin varautumista on harjoiteltava ja kehitettävä osana toimijoiden normaalia riskivarautumista.

Kyberfyysisen toimintaympäristön tulevaisuuden kannalta merkittävä kehitystrendi on arjen tietoyhteiskunnan kehittyminen. Tämän trendin seurauksena yhä useammalla laitteella ja tavaralla on älyominaisuuksia ja ne voivat olla etäluettavia tai muilla tavoin yhteydessä verkkoon. Stuxnet (2010), Flame (2012) ja Red October (2013) ovat esimerkkejä haittaohjelmista, jotka on suunnattu tätä uutta infrastruktuuria ja toimintaympäristöä silmällä pitäen. Ne voivat toimia suljetuissa lähiverkoissa, teollisuuden ja erilaisten laitteiden piirikorteissa ja myös älypuhelimissa. Näiden laitteiden tietoturvaominaisuudet eivät ole samalla tasolla kuin tietokoneiden. Ongelmia voi aiheuttaa jo pelkästään verkossa olevan tiedon oikeudellinen asema ja käyttö: minkä maan lainsäädäntöä esimerkiksi noudatetaan internetin globaaleissa verkkopalveluissa ja palvelupilvissä?

> Tulevaisuusvaliokunta korostaa, että Suomen on tutkittava ja selvitettävä tarkoin arjen tietoyhteiskuntaan liittyvät uudet kyberriskit ja -mahdollisuudet.

Kansainvälinen yhteistyö

Kybertoimintaympäristö on globaali. Siksi riskejä ei voi hallita eikä mahdollisuuksiin voida tarttua pelkästään kansallisella tasolla. Kyberfyysinen toimintaympäristö hankaloituu entisestään, mikäli jokainen valtio kehittää kyberturvallisuuteen omat ratkaisunsa.

Kansainvälisen yhteistyön tarve koskee muun muassa sähköverkkoa ja pankkijärjestelmää. 75 % Suomen sähköstä kulkee Fingridin verkossa, johon on suorat yhteydet Venäjältä, Ruotsista, Norjasta ja Virosta. Suomen energiaverkkoon voidaan vaikuttaa myös ulkomailla ja Suomen energiaverkkoon voidaan vastaavasti iskeä siksi, että iskun tekijä yrittää vaikuttaa jonkin muun maan, kuten esimerkiksi Venäjän tai Viron energiaverkkoon.

Koska nykyaikainen pankkitoiminta perustuu käytännössä täysin sähköisessä muodossa olevan tiedon pitkälle automatisoituun käsittelyyn, on tietojärjestelmien toimivuus olennaista kaikkien pankin keskeisten tehtävien hoidon kannalta. Yhtenäiseen euromaksualueeseen siirtymisen jälkeen merkittävä osa pankkiryhmien välisessä maksuliikenteessä tarvittavista järjestelmistä on yleiseurooppalaisia, kuten esimerkiksi maksujen selvitykseen käytetty EBA clearingin palvelu, sekä pankkien välisiin katteiden siirtoihin käytetty Euroopan keskuspankin Target2 -järjestelmä.

Suomen pankkijärjestelmään kohdistuvan iskun ei siis tarvitse kohdistua Suomeen, vaan jossakin muualla Euroopassa tai jopa toisella mantereella sijaitsevaan pankkien yhteiseen palvelukeskukseen.

> Tulevaisuusvaliokunta katsoo, että kansallista kyberturvallisuutta on kehitettävä yhteistyössä kansainvälisten verkostojen kanssa. Uhkia ei voida hallita pelkästään kansallisilla toimilla.

Merkittäviä yhteistyötahoja ovat esimerkiksi Tallinnassa sijaitseva NATO:n kybersuorituskykyjen osaamisen kehittämiskeskus (CCDCOE) ja European Network and Information Security Agency (ENISA).

Kansalaisten rooli kyberturvallisuudessa

Informaatio- ja viestintäteknologian nopean kehittymisen myötä erilaiset sähköiset palvelut ovat saatavissa ajasta ja paikasta riippumatta erilaisilla päätelaitteilla. Kansalaisten ja elinkeinoelämän tarpeista lähtevä tiedon monipuolinen jalostaminen ja hyödyntäminen ovat modernin tietoyhteiskunnan tärkeimpiä menestystekijöitä. Älypuhelimet ja langattomat verkkopalvelut ovat mahdollistaneet nk. esineiden internetin — toimintaympäristön, jossa kaikenlaiset esineet ja laitteet voivat olla yhteydessä toisiinsa, erilaisiin tietokantoihin ja pilvipalveluihin. Yhä useampi toiminto tapahtuu automaattisesti. Kyse ei ole pelkästään teknologian muutoksesta, vaan sosiaalisesta ja kulttuurisesta muutoksesta, joka näkyy myös ihmisten ja organisaatioiden rakenteissa, toimintamalleissa, elämäntavoissa ja arvoissa.

Kyberfyysinen toimintaympäristö ei rajoitu johonkin tiettyyn teknologiaan tai pelkästään

virtuaaliseen toimintaympäristöön eikä siinä ole kyse pelkästään hallinnon ja strategisen infrastruktuurin tietojärjestelmien turvallisuudesta, vaan modernin tietoyhteiskunnan kulttuurisista ja sosiaalisista ilmiöistä, jotka ovat syvästi kietoutuneet ihmisten yksilöllisiin elämäntapoihin. Tätä kokonaisuutta on vaikea hallita poliittisin keinoin. Kyberfyysinen toimintaympäristö on vain osittain julkishallinnon säädettävissä.

> Tulevaisuusvaliokunta korostaa, että kyberturvallisuutta on tarkasteltava ennen kaikkea yhteiskunnallisena, kulttuurisena ja sosiaalisena ilmiönä eikä pelkästään teknologisina ratkaisuina.

Kansalaisilla on suuri merkitys kyberturvallisuuden tuottamisessa. Esimerkiksi valtaosa kaikesta sähköpostista on nykyään roskapostia — ja suurin osa siitä tulee saastuneiden kotikoneiden kautta. Myös suurin osa haittaohjelmista on suunnattu juuri kansalaisia vastaan ja niillä tavoitellaan taloudellista hyötyä joko huijauksilla tai salasanoja varastamalla. Siksi ihmisten asenteet, tavat ja tietoisuus vaikuttavat merkittävällä tavalla siihen, miten kyberturvallisuus toteutuu kotona ja työpaikoilla. Kotikoneiden virustentorjuntaohjelmien päivityksellä, USB-tikkujen käyttötavoilla ja harkinnalla internetissä ja sähköpostissa on suuri merkitys arjen kyberturvallisuuden toteutumisessa.

Maaliskuussa 2013 tehtiin kaikkien aikojen suurin palvelunestohyökkäys roskapostin suodattamiseen erikoistuneen yhdysvaltalaisen CloudFare-palveluntarjoajan SpamHaus-palvelinta vastaan. Hyökkääjät käyttivät hyväkseen internetin avoimia Resolver-nimipalvelimia, joita on yrityksillä ja operaattoreilla. Hyökkäykseen valjastettiin myös toista sataa suomalaista palvelinta. Roskapostin levittämisen ja palvelunestohyökkäyksen ytimen kuitenkin muodostivat miljoonat, haittaohjelmilla käyttöön kaapatut kotikoneet.

> Tulevaisuusvaliokunnan mielestä myös kansalaiset on saatava mukaan kyberturvallisuuden kehittämiseen ja kyberturvallisuudesta on tehtävä modernin suomalaisen arjen tietoyhteiskunnan kansalaistaito.

Kyberosaamisen kehittäminen

Kyberturvallisuusstrategiassa korostetaan organisoitumisen merkitystä, tilanteeseen sopeutumista, uusien kyvykkyyksien luomista, uudenlaisen toimintayhteisön luonteen ymmärtämistä, uudenlaisten tosiasioiden havaitsemista sekä päätöksentekokoneiston sovittamista uuteen toimintaympäristöön sopivaksi. Tämä kaikki yhteistyö ja tilannekuvan ylläpitäminen edellyttävät monialaisten toimijoiden ohjeistamista ja kouluttamista.

Kyberturvallisuus edellyttää korkealaatuista teknologista ja ohjelmistoalan osaamista. Tämä kyvykkyys edellyttää vahvaa panostusta myös alan koulutukseen, kehittämiseen ja tutkimukseen. Vaikka sosiaaliset ja kulttuuriset toimintamallit ja -rakenteet ovatkin kyberturvallisuusstrategian tässä vaiheessa jääneet vähemmälle huomiolle, niin jatkossa kyberturvallisuus vaatii osaajikseen yhä enemmän myös ei-teknisen koulutuksen saaneita henkilöitä.

Keskeistä on lisätä kyberturvallisuuden osaamista kaikilla tasoilla yrityksien ja organisaatioiden johdosta suorittavaan portaaseen ja aina kansalaisiin asti.

> Tulevaisuusvaliokunta korostaa, että kyberturvallisuusstrategian toteuttaminen edellyttää myös tutkimukseen, koulutukseen ja tuotekehitykseen panostamista.

Hyvä esimerkki kyberosaamisen tutkimuksesta ja koulutuksesta on Jyväskylän yliopiston jo vuonna 2011 aloittama laaja-alainen ohjelmisto- ja tietoliikennetekniikan informaatioturvallisuuden yliopistotasoinen koulutus.

Kriisinsietokyky

Korkein riskitaso on erilaisilla ulkoistetuilla toiminnoilla. Läntiset asevoimat kykenevät suojaamaan ja varmentamaan oman johtamisjärjestelmänsä, mutta ongelman muodostavat strategiset

kumppanit ja erilaiset asejärjestelmien teknologiset ja ylläpidolliset alihankkijatoimijat.

Esimerkiksi huipputeknologinen F-35-lentokone perustuu miljoonien tietokoneiden ohjaukseen ja ohjelmistojen päivitykseen. Kuinka voidaan varmistua, että ohjelmistoissa ei ole mitään takaportteja eikä dominovaikutusta pääse tapahtumaan? Koneen ohjaaminen tapahtuu kuten iPadin käyttäminen. Siksi hyökkääjän ei tarvitse ymmärtää kaikkea kohteena olevasta järjestelmästä, vaan riittää, että ymmärtää, miten järjestelmän saa häirittyä.

Lainsäädännöllä ei voida enää kontrolloida sen paremmin kansalaisyhteiskuntien sisäisiä kuin myöskään kansainvälisiä kyberuhkia. Riskejä ei voi kokonaan torjua. On hyväksyttävä myös se, että kyberuhat ovat jo potentiaalisina yhteiskunnan elintärkeissä toiminnoissa, ja oleellista niiden realisoituessa on saada elintärkeät toiminnot nopeasti palautettua normaaleiksi tai on oltava vaihtoehtoisia varajärjestelmiä.

> Tulevaisuusvaliokunnan mielestä Suomen tulee varautua myös kyber-kriisinsietokykyyn, häiriöistä palautumiseen ja toipumiseen sekä elintärkeiden toimintojen kykyyn sietää kyberturvallisuuden varsin erilaisia ja erimittaisia häiriötilanteita.

Myös tämä osaamistarve läpäisee koko yhteiskunnan: miten toivumme ja selviämme siitä, jos joudumme syystä tai toisesta pärjäämään jonkin aikaa ilman vettä, sähköä, valoa, rahaa, kaupasta ostettavaa ruokaa, julkista liikennettä, polttoaineita, lääkkeitä jne.?

Kybertoimintaympäristön liiketoimintamahdollisuudet

Suomella on pienenä, osaavana ja yhteistyökykyisenä maana erinomaiset edellytykset nousta kyberturvallisuuden osaajaksi. Meillä on vahva osaamisperusta sekä pitkät perinteet tiiviistä ja luottamuksellisesta yksityisen ja julkisen sektorin yhteistyöstä sekä myös hallinnonalojen välisestä yhteistyöstä. Infrastruktuuri ja hallinto ovat vakaita.

Kybertoimintaympäristö on uhkien lisäksi siis myös mahdollisuus ja voimavara. Turvallinen kybertoimintaympäristö lisää taloudellista aktiviteettia. Kyberturvallisuus on itsessään uusi ja vahvistuva liiketoiminnan alue, ja turvallinen toimintaympäristö myös parantaa Suomen kansainvälistä houkuttelevuutta investointikohteena.

Kybermaailmassa suuruus ja massa eivät enää ole hallitsevia kilpailukykytekijöitä, vaan menestys perustuu yhä enemmissä määrin osaamiseen. Vaikka suurvalloilla on huomattavat resurssit toimia myös kybertoimintaympäristössä, niin ne eivät kuitenkaan dominoi sitä kokonaan. Myös pienet toimijat, kuten Suomi, voivat hankkia huippuosaamista ja kehittyä kyberturvallisuuden monilla erikoisaloilla.

Hyvin kyberuhilta suojattu maa on turvallinen paikka sijoittaa tuotantoa. Mielenkiintoinen mahdollisuus liittyy myös Stuxnetin kaltaisten haittaohjelmien ja takaporttien aiheuttamaan kansainväliseen epäluuloon: voivatko erilaisten siviili- ja sotilaslaitteiden ostajat enää tulevaisuudessa luottaa siihen, ettei laitteissa ole kätkettyjä ominaisuuksia? Tämä globaalin epäluottamuksen ilmapiiri voi olla etu pienelle, tunnetusti puolueettomalle ja läpinäkyvälle ja vakaan hallinnon omaavalle Suomelle, jonka tuotteisiin kaikki voivat luottaa.

Kyberfyysisen toimintaympäristön suurimmat liiketoimintamahdollisuudet liittyvät siihen, miten kyberturvallisuus voidaan liittää lisäarvoksi strategiseen infrastruktuuriin ja sitä kautta yritysten liiketoimintaympäristöön sekä kaikkeen Suomessa valmistettuun teknologiaan. Kyberturvallisuudesta voidaan kehittää merkittävä vientituote.

Kyberturvallisuusstrategia ei vielä kykene avaamaan riittävästi kyberfyysiseen toimintaympäristöön liittyviä mahdollisuuksia.

> Tulevaisuusvaliokunta ehdottaa, että eri toimijat, yksityiset ja julkiset, laativat seuraavassa vaiheessa myös mahdollisuuksista lähtevän kyberstrategian.

Lausunto

Lausuntonaan tulevaisuusvaliokunta esittää,

että ulkoasiainvaliokunta ottaa edellä olevan huomioon.

Helsingissä 3 päivänä huhtikuuta 2013

Asian ratkaisevaan käsittelyyn valiokunnassa ovat ottaneet osaa

pj.	Päivi Lipponen /sd		Jaana Pelkonen /kok (osittain)
vpj.	Oras Tynkkynen /vihr		Juha Sipilä /kesk
jäs.	Mikko Alatalo /kesk		Stefan Wallin /r (osittain)
	Olli Immonen /ps (osittain)		Sinuhe Wallinheimo /kok
	Harri Jaskari /kok		Ville Vähämäki /ps
	Kalle Jokinen /kok	vjäs.	Jouko Jääskeläinen /kd
	Mikael Jungner /sd		Mika Niikko /ps.
	Markus Mustajärvi /vr		

Valiokunnan sihteerinä on toiminut

valiokuntaneuvos Paula Tiihonen
pysyvä asiantuntija Olli Hietanen.