Teksti **Jari Lindholm** Kuvat **Markus Pentikäinen**

Yhteys poikki

Jättimäinen kyberhyökkäys voisi lamauttaa Suomen, sillä valtio ei ole huolehtinut varautumisesta.

Elokuun puolivälissä, sodan raivotessa Kaukasuksella, toimittaja **Jevgeni Morozov** päätti tehdä kokeen.

Morozov halusi selvittää, kuinka helposti tavallinen venäläinen voisi liittyä internetissä syntyneeseen vapaaehtoisten kansalaisten kyberarmeijaan, jonka tavoitteena oli jumiuttaa Georgian verkkosivut samaan aikaan, kun heidän maansa panssarit jyrisivät kohti Tbilisiä.

”Tehtäväni oli yksinkertainen”, Morozov kirjoitti myöhemmin *Slate*-verkkolehdessä. ▶

”Halusin kokeilla, kuinka paljon vahinkoa minun kaltaiseni ihminen, joka on kaukana Kremlistä fyysisesti ja poliittisesti, voisi aiheuttaa Georgian tietoverkoille toimimalla omin päin, pelkän läppärin ja nettiyhteyden avulla.”

Morozov ryhtyi toimeen.

Blogeista ja keskustelufoorumeilta hän löysi ohjeita, joiden avulla pystyi muuttamaan tietokoneensa kyberaseeksi. Hän oppi luomaan yksinkertaisen tiedoston, joka pani hänen koneensa lataamaan georgialaisia sivustoja yhä uudelleen. Hän myös löysi ohjelman, jolla saattoi käynnistää yhden miehen nettihyökkäyksen hiirtä klikkaamalla.

Morozovista tuli virtuaalisissi vajaassa tunnissa.

Hän ei koskaan oikeasti liittynyt kyberarmeijaan, mutta tuhannet muut liittyivät.

Mukana oli pinttyneitä verkkorikollisia ja tavallisia, isänmaallisen raivon kiihdyttämiä venäläisiä. Käytössä oli sekä kadunmiesten koti-pc:itä että virusten avulla siepattuja ”orjakoneita”, joilla vain päivää aiemmin oli jaeltu Viagra-roskapostia.

Nämä digitaaliset tykinputket tulittivat samanaikaisesti kaikkia internetsivustoja, joiden osoitteessa oli Georgian tunnus, .ge.

Georgia ei voinut hyökkäykselle mitään. Presidentin, parlamentin, ulkoministeriön ja korkeimman oikeuden sivut kaatuivat. Seuraavina olivat vuorossa keskusvaalilautakunta, kulttuuriministeriö ja turvallisuusneuvosto.

Sitten vimma kohdistui sanomalehtiin, televisiokanaviin ja verkkojulkaisuihin.

Maailmassa tehdään joka päivä keskimäärin 1 300 palvelunestohyökkäystä.

Näillä internetpalveluihin ja verkkotoimintoihin kohdistetuilla massaiskuilla kiristetään yleensä rahaa yrityksiltä tai esitellään hyökkääjän taitoja.

Yhä useammin niillä myös ajetaan poliittisia päämääriä. Burman hallitusta on syytetty opposition web-sivujen kaatamisesta. Irakissa sunnit ovat sotkeneet šiiajohtajan sivuja. Äärі-islamistien kansainväliset nettifoorumit kaatuivat hiljan tuntemattomien hyökkääjien höykytyksessä.

Yhteensä erilaisia palvelunestohyökkäyksiä on tehty puolentoista vuoden aikana lähes miljoona.

Tyypillisiä seurauksia ovat toistaiseksi olleet harmi ja nöyryytys. Esimerkiksi toukokuussa 2007 hyökkäykset Yleisradion, Suomen Tietotoimiston, Suomi24-keskustelufoorumin ja Viestintäviraston sivuille pääsivät näkyvästi otsikoihin, mutta yhteiskunnalle niistä ei ollut vaaraa.

Katastrofi on kuitenkin vain ajan kysymys.

Suurin yksittäiseen valtioon kohdistunut hyökkäys tapahtui vain 85 kilometrin päässä Suomesta.

Kun vironvenäläiset olivat kimpaantuneet Tallinnan *Pronssisoturi*-patsaan siirtämisestä 26. huhtikuuta 2007, alkoi kolme viikkoa kestänyt nettihyökkäys, johon osallistui sekä venäläisiä hakkereita että tavallisia kansalaisia.

Aluksi kohteina olivat sivustot, joiden toimivuus oli useimmille samantekevää: parlamentti, puolustusministeriö, poliisi, puolueet. Mutta tilanne synkkeni nopeasti.

”Kohteiksi joutuivat muun muassa teleoperaattoreiden verkot ja pankkien taustajärjestelmät”, sanoo tietoturvayhtiö F-Securen tutkimuspäällikkö **Mikko Hyppönen**.

”Hyökkäykset alkoivat lähestyä kriittistä infrastruktuuria. Sellaisen pitäisi olla irti julkisesta verkosta. Virossa osa oli ja osa ei.”

Kyberiskujen henkinen vaikutus oli väkevä.

”Meidän virolaiset kollegamme ovat moneen kertaan teroittaneet, että oli täysin yhdentekevää, olivatko presidentin www-sivut nurin”, sanoo Viestintäviraston CERT-FI-tietoturvayksikön päällikkö **Erka Koivunen**.

”Mutta kun online-maksaminen muuttui mahdottomaksi, ihmisiltä hyytyi hymy.”

Massiivinen kyberhyökkäys olisi turmiollisin maalle, joka on siirtänyt elintärkeät toimintonsa verkkoon.

Tällainen maa on esimerkiksi Suomi.

Laaja isku ei halvaannuttaisi pelkästään julkisia internetsivustoja vaan pahimmassa tapauksessa kaupat, tavarankuljetuksen, sähkönjakelun ja sairaalat.

Lähi-Alepasta ei saisi maitoa, koska kassat olisivat pimeinä. Eikä myymälään saapuisi täydennystä, koska keskusvarastoissa ei automatisoinnin jälkeen ole henkilökuntaa, joka kiipeäisi itse hakemaan tavaran hyllyltä.

Sairaaloissa ei pystyttäisi lukemaan potilastietoja eikä kirjoittamaan reseptejä. Lääkärit eivät saisi röntgenkuvia auki työasemillaan, koska yhteydet teleyritysten palvelimilla sijaitseviin kuvavarastoihin olisivat poikki.

Puhelinluuria olisi turha hamuta, sillä puhelutkin kulkevat datapaketteina bittiavaruudessa. Kännykät saattaisivat toimia – paitsi jos isku olisi kohdistunut matkapuhelinverkon keskuksiin, jotka tietenkin ovat verkossa.

Kauhunäky kuulostaa huikealta.

Silti asiantuntijat eivät ole valmiita sivuuttamaan sitä pelkkänä tieteisfantasiana.

”Riskit ovat suuret”, sanoo teleoperaattori TDC:n teknologiajohtaja **Jorma Mellin**.

”Suomessa on tietotaitoa ja tunnemme vaarat, mutta kyllä me olemme erittäin haavoittuvia.”

Vaikka yhteiskunnalle kriittiset toiminnot on internetissä suljettu niin sanottuihin virtuaalisiin yksityisverkkoihin, niiden liikenne kulkee samoissa kaapeleissa samojen laitteiden läpi kuin julkisen internetin datavirta. Erilliset koneet ovat eilispäivän luksusta, johon ei kustannussäästöjen maailmassa ole paluuta, Mellin sanoo.

”Samoihin tilaajakeskittimiin kytketään kuluttajia, yrityksiä tai vaikka joku sairaala. Jos kotien laajakaistayhteyksissä on vakava häiriö, kaikkien muidenkin liikenne on vaarassa häiriintyä.”

F-Securen Hyppösen mukaan Suomessa on toistaiseksi osattu melko hyvin huolehtia tärkeiden verkkojen suojaamisesta.

”Mutta kyllä tilanne on luisumassa avoimempaan suuntaan. Pahaa pelkään, että kymmenen vuoden kuluttua Suomessakin kaikki riippuu siitä, että netti toimii.”

Myös Viestintäviraston turvallisuuspäällikkö **Jani Arnell** tunnistaa uhan.

”Voimme joutua tilanteeseen, jossa paljon verkottunut, yhteiskunnallisesti kriittinen toimija saadaan saarrettua palvelunestohyökkäyksellä, tai sen järjestelmät joutuvat sellaiseen kuntoon, että se ei pysty antamaan palvelua.”

Pystyisikö innokkaiden nettiamatöörien armeija siis iskemään ulkomailta suomalaisen tietoyhteiskunnan hermoon?

TDC:n Mellinillä on vastaus valmiina.

”Olen vakuuttunut, että pystyisi.”

Onko Suomi varautunut tällaiseen uhkaan?

Haastattelukierros valtionhallinnossa tuottaa yksimielisen vastauksen: kyllä – ja hyvin.

Suomalaisten virkamiesten mukaan maamme suhtautuu tietoturvauhkiin vakavasti, toimii johdonmukaisesti niiden torjumiseksi ja on muutenkin tietoteknisesti valveutunut.

”Me olemme Euroopassa yksi niitä harvoja valtioita, jotka ovat oikeasti panostaneet tähän asiaan”, sanoo viestintäneuvos **Kari Ojala** liikenne- ja viestintäministeriöstä.

”Suomessa on tele- ja tietoverkot järjestetty sillä tavalla, että meillä ei pääse käymään ollenkaan samalla tavalla kuin Virossa.”

Samaa mieltä on Huoltovarmuuskeskuksen apulaisjohtaja **Veli-Pekka Kuparinen**.

”Kansainvälisessä vertailussa varautumisemme taso on hyvä. Meillä on sellainen kulttuuri, että kun annamme ohjeita, niitä noudatetaan, vaikkei olisi sanktioitakaan.”

Suomen vahvuus on, että keskeiset viranomaiset tuntevat toisensa, sanoo valtiovarainministeriön neuvotteleva virkamies **Mikael Kiviniemi**, joka vetää Valtionhallinnon tietoturvallisuuden johtoryhmää VAHTIa.

”Haluan tehdä yhden asian hyvin selväksi: yhteistyö toimii nykyisillä toimivaltuuksilla erittäin hyvin.”

Tarkempi tutustuminen tietoyhteiskunnan kriisivalmiuteen paljastaa kuitenkin jotain muuta: sekasorron.

Ministeriöt, laitokset ja kunnat valvovat itse itseään. Ulkoistaminen on villiä ja vapaata. Yhteisiä standardeja ei ole, lainsäädäntö ei ulotu tietoturvaan, eikä asioista tietävillä viranomaisilla ole valtuuksia huolehtia, että kaikki on kunnossa.

Ydinkysymykseen – olemmeko turvassa kyberhyökkäyksiltä – ei kukaan pysty vakuuttavasti vastaamaan. Yhdelläkään virallisella taholla ei yksinkertaisesti ole tilanteesta kokonaiskuvaa.

Periaatteessa näin ei pitäisi olla. Asiantuntijoista ei nimittäin ole pulaa.

Keskeinen tietoturvaviranomainen on työ- ja elinkeinoministeriön alaisuudessa toimiva Huoltovarmuuskeskus, jonka tehtävänä on turvata kansakunnan välttämättömät toiminnot kriisien aikana.

Huoltovarmuuskeskus ei huolehdi pelkästään elintarvikehuollosta ja energiansaannista vaan myös tietoyhteiskunnan toimivuudesta. Laitos tarjoaa turvallista palvelinkonetilaa valtion organisaatioille ja ”huoltovarmuuskriittisikси” luokitelluille yksityisille firmoille, kuten pankeille ja kaupan keskusliikkeille. Se on myös rahoittanut internetliikenteen kannalta olennaisia yhdysliikennepisteitä.

Keskus on lisäksi varmistanut, ettei suurikaan katastrofi katkaise viranomaisten välistä tiedonkulkua. Tästä pitää huolen kaksi puhelinjärjestelmää, valtakunnallinen varaverkko 2V ja viranomaisradioverkko VIRVE, joita hallinnoi valtion omistama teleoperaattori Suomen Erillisverkot Oy.

Viranomaisverkot ovat julkishallinnossa harvinaisuus: niistä voi sanoa, että tapahtui mitä tahansa, ne todennäköisesti pysyvät pystyssä.

Huoltovarmuuskeskuksen työparina tietoyhteiskunnan suojelemisessa on liikenne- ja viestintäministeriön alainen Viestintävirasto, joka viestintämarkkinalain valtuuttamana valvoo teleyrityksiä.

Viraston tietoturvayksikkö CERT-FI taas on pari vuotta antanut Huoltovarmuuskeskuksen rahoituksella tietoturvaapua yksityisille yrityksille.

Näiden viranomaisten rinnalla toimii kirjava joukko edellisen hallituksen tietoyhteiskuntaohjelman poikimia virkamiesryhmittymiä, kuten Julkisen hallinnon tietohallinnon neuvottelukunta JUHTA, Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI, kuntien tietohallintoyhteistyötä vahvistava KuntaIT ja valtion tietoteknologiatoiminnan johtamisyksikkö ValtIT.

Kaiken taustalla on kaksi vuotta sitten julkistettu, puolustusministeriön johdolla laadittu 73-sivuinen hallituksen periaatepäätös *Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia*, joka luonnostelee elämää kriisiajan Suomessa.

Johto kuitenkin puuttuu.

Suomessa ei ole yhtään yksittäistä viranomaista, joka valvoisi, että yhteiskunnan kriittinen infrastruktuuri on asianmukaisesti tietosuojattu.

Sellainen ei ole Huoltovarmuuskeskus, joka voi vain ohjeistaa. Sellainen ei ole Viestintävirasto, joka voi käskyttää vain teleoperaattoreita. Sellainen ei ole myöskään valtiovarainministeriö, jonka tietoturvaohjeilla ei ole määräyksen voimaa.

Eikä valvontaan olisi lakiakaan. Viestintämarkkinalailla voidaan ohjata ainoastaan teleyritysten toimintaa. Ajatus erillisestä tietoturvalaista ei innosta ainakaan byrokraatteja.

Seuraus on maallikon näkökulmasta hämmentävä: kukin ministeriö toimii niin kuin parhaaksi katsoo, eikä kukaan tiedä varmasti, ovatko toimet tietoturvan kannalta riittävät. Yksityisestä sektorista tiedetään vielä vähemmän. ▶

”Kyllä me olemme erittäin haavoittuvia.”

Kukin ministeriö toimii niin kuin parhaaksi katsoo.

Viestintävirastossa asiaintilaa pidetään kummallisena.

”Koska rahoitusta ei ole järjestetty, teleyritykset ja huoltovarmuuskriittiset firmat ovat asiakkainamme etusijalla”, sanoo CERT-FIn päällikkö Koivunen.

”Emme ole koskaan saaneet Suomen valtiolta toimeksiantoa, että pitäkää huoli, että kansakunta on myös hallinnon puolelta suojattu.”

Elokuun lopussa, Georgian kybersodan vielä raivotessa, Suomen hallitus myönsi virallisesti, että tietoyhteiskunnan lamaantuminen on todellinen uhka.

Huoltovarmuuden tavoitteita koskevassa valtioneuvoston päätöksessä otettiin vahvasti kantaa yhteiskunnan tietotekniseen kriisivarautumiseen.

”Kriittisimmät ja keskeisimmät tietotekniikan varassa olevat yhteiskunnan toiminnot tulee tunnistaa ja niihin liittyvät tietojärjestelmäratkaisut ja -palvelut tulee varmistaa erilaisia vakavia häiriöitä ja poikkeusoloja kestävillä järjestelyillä”, määrättiin vähälle huomiolle jääneessä päätöksessä.

”Keskeisissä valtakunnallisissa tieto- ja viestintäjärjestelmissä yksittäisen kohteen lamautuminen tai vaurio ei saa lamauttaa koko järjestelmää.”

Päätöksessä todettiin myös ykskantaan, ettei mitä tahansa saa ulkoistaa.

”Yhteiskunnan toimivuudelle kriittisiä tietojärjestelmiä suunniteltaessa ja rakennettaessa on varmistettava, että niihin liittyvän ohjauksen, ylläpidon, järjestelmähallinnan ja teknisen tuen osaaminen säilyy Suomessa tai ohjaus- ja hallintakyky on oltava mahdollista palauttaa Suomeen.”

Jos päätöstä todella ryhdyttäisiin soveltamaan Suomen julkishallinnossa, monen asian pitäisi muuttua.

Tähän asti ministeriöt ja niiden alaiset laitokset ovat budjettiensa puitteissa saaneet ulkoistaa tietojärjestelmiään oman mielensä mukaan.

Kukaan ei ole esimerkiksi määrännyt, etteikö järjestelmiä saisi hankkia firmalta, joka on siirtänyt asiakaspalvelunsa Intiaan.

Teoriassa on täysin mahdollista, että vaikkapa ulkoministeriössä – tai Joroisten kunnassa – yhteydet atk-tukeen katkeavat, jos Välimerellä troolari rikkoo tietoliikennekaapelin, kuten kävi tämän vuoden helmikuussa.

”Tilaajan kannalta on tärkeää, että alihankkijan palvelu on yhtä tietoturvallista kuin sopimuskumppanin”, sanoo Valtion tietoturvallisuuden johtoryhmää VAHTIa vetävä Mikael Kiviniemi.

Silti valvontaa ei ole: VAHTIsta vastaava valtiovarainministeriö ei voi kajota siihen, mitä firmoja muualla valtionhallinnossa käytetään.

”Emme puutu tuolla tavalla hankintoihin.”

Riskit on vain pakko hyväksyä, sanoo toinen pitkän linjan virkamies, Helsingin ja Uudenmaan sairaanhoitopiirin Husin valmiuspäällikkö **Pekka Koskinen**.

”Kun koko ajan puhutaan tilaaja-tuottajamallista ja kustannuspaineet ovat kovat, se ajaa ulkoistamaan. Jos meillä olisi tietojärjestelmistä huolehtimassa omaa henkilökuntaa niin kuin ennen, se tuntisi prosessit ja työyhteisön. Tämä on aika pitkälle murentunut.”

Viestintäviraston tietoturvayksikössä on laskeskeltu ulkoistamisen todellisia kustannuksia. Johtopäätökset ovat synkät: massiivisen kyberhyökkäyksen sattuessa ensimmäisinä kaatuvat palvelut, joiden rakentamisessa on mietitty pelkästään hintalappua.

”Jos verkkotoimintoja on ulkoistettu ajatuksella, että se on jollain ihmeellisellä tavalla halpaa ja nopeaa, varajärjestelyihin on todennäköisesti jätetty satsaamatta”, sanoo yksikön päällikkö Koivunen.

”Palveluntuottajan omistajana olevan japanilaisen sijoittajan tai amerikkalaisen eläkerahaston näkökulmasta on yksi hailee, onko Intiaan sijoitettu palvelinkeskus Suomessa olevan asiakkaan tavoitettavissa – saati että se olisi siirrettävissä takaisin Suomeen, jos joku kriisi sitä vaatii.”

Syyskuussa 2004 pahin tapahtui Tuusulassa.

Kunnan sisäiseen tietojärjestelmään pääsi Gaobot-niminen virus, joka tukehdutti verkkoliikenteen.

Toimeentulotukea ei pystytty maksamaan, koska sosiaalitoimiston koneet kaatuivat. Kirjastojen lainaustoiminta pysähtyi. Terveyskeskuksissa lääkärit eivät saaneet auki potilastietoja eivätkä voineet tarkistaa potilaidensa lääkityksiä, sillä työasemat olivat pimeinä.

Tuusulan käyttämä tietoturvaohjelma ei tunnistanut virusta. Niinpä vian korjaaminen kesti kuusi päivää.

Voisiko näin käydä muuallakin?

Kukaan ei tiedä.

Kuntien itsehallinto takaa, että jokainen saa tehdä hankintansa halvimmalla mahdollisella tavalla.

Näin on syntynyt länsimaisittain harvinaisen vaikeakulkuinen tietojärjestelmien ryteikkö, jota edes ministeriöiden vastaavat virkamiehet eivät tunne.

”Lähtökohtana on, että kunta on vapaa valitsemaan itse palveluntarjoajansa”, sanoo tietohallintoyhteistyötä vahvistavan KuntaIT-hankkeen päällikkö **Antti Holmroos**.

”On kunnan kyvykkyydestä kiinni, osaako se vaatia korkeatasoisia turvallisuusratkaisuja.”

Onko siis mahdollista, että jossain päin Suomea elintärkeät tietojärjestelmät on hankittu paikalliselta pc-pajalta?

”Ehdottomasti se on mahdollista.”

Tilanne on sekavin siellä, missä tietoverkkokatastrofin seuraukset olisivat kohtalokkaimmat: terveydenhuollossa.

Kahden naapurikunnan terveyskeskuksilla saattaa olla eri tietojärjestelmä. Erikoissairaanhoidosta vastaavalla sairaanhoitopiirillä on lisäksi omansa. Mikään laki ei määrää, että systeemien on oltava yhteensopivia – tai turvallisia.

Kiertääkseen ongelman jotkut kunnat ovat perustaneet yhdessä tietohallintoyrityksiä, joiden on tarkoitus taata järjestelmien toimivuus.

Kokemukset ovat olleet ristiriitaisia. Esimerkiksi Pirkanmaan kuntien ja sairaanhoitopiirin omistama YT Tieto kaatui keväällä 2007, kun osa kunnista ei liittynytkään firman kehittämään aluetietojärjestelmään vaan jäi odottamaan kansallista potilastietoarkistoa, jonka pitäisi valmistua parin vuoden sisällä.

”Tiedän, että kenttä toivoo yksityiskohtaisia määräyksiä siitä, miten asiat pitäisi tehdä”, sanoo sosiaali- ja terveysministeriön erityisasiantuntija **Teemupekka Virtanen**, jolla on pitkä kokemus tietoturvaasioista virkamiehenä ja tutkijana.

”Eräs vaihtoehto olisi, että rakennettaisiin yksi järjestelmä, joka rahoitettaisiin julkisesti ja jaettaisiin ilmaiseksi samanlaisena kaikkiin sairaaloihin. Mutta se ei ole suomalainen tapa.”

Mikä sitten on suomalainen tapa?

Soittokierros paljastaa, että sellaista ei ole. Pelkästään Helsingin seudulla ja lähikunnissa järjestelmiä on yhtä monta kuin hankkijoita.

Esimerkiksi Helsingin ja Uudenmaan sairaanhoitopiiri Hus on ulkoistanut ahkerasti, muun muassa palvelininfrastruktuurinsa, mutta on ainakin omien sanojensa mukaan huolehtinut ratkaisujen turvallisuudesta.

”Ei meille ole tullut ohjeistusta ministeriöstä”, sanoo tietohallintojohtaja **Jari Renko**.

”Mutta omat tietoturvaperiaatteemme ovat tiukemmat kuin valtionhallinnon yleiset it-periaatteet.”

Porvoossa tietojärjestelmät on pidetty suurimmaksi osaksi omissa käsissä. Kriisin sattuessa kaupungin oma väki toimii nopeammin kuin vieras palveluntuottaja, uskoo tietohallintopäällikkö **Niko Lindberg**.

”Kun pitää viipaloida saastuneita osia irti verkosta, tarvitaan aggressiivisia toimia. Se on vaikeampaa, jos tekijänä on ulkopuolinen taho.”

Tuusulassa tilanne saattaa olla kohentunut vuoden 2004 virusfiaskon jälkeen – tai sitten ei.

Asiaa on mahdotonta selvittää, sillä kunnan tietohallintopäällikkö **Ali-Daniel Jokela** kieltäytyi haastattelusta.

Suomalaisen tietoyhteiskunnan suojaamisessa on käytetty hajautettua mallia. Ja se on pelkästään vahvuus.

Näin uskovat kaikki *Suomen Kuvalehden* haastattelemat virkamiehet.

”Jokainen operoi parhaan mahdollisen tiedon kanssa, ja kun yhteistyö pelaa, en näe siinä mitään huonoa”, sanoo liikenne- ja viestintäministeriön Ojala.

”Meillä on kyllä vastuut jaettu näistä asioista”, vakuuttaa Huoltovarmuuskeskuksen Kuparinen.

”Vahvuus on se, että kun ei ole keskitetty järjestelmiä, ne eivät ole ensisijaisesti haavoittuvia”, sanoo KuntaIT:n Holmroos.

Täysin toista mieltä on tuore tutkimus, jonka valtio itse on teettänyt.

Kesäkuussa valmistunut, valtiovarainministeriön ohjauksessa laadittu *Valtionhallinnon ICT-varautumisen esitutkimus* antaa murskaavan tuomion juuri niissä asioissa, jotka virkamiesten mielestä toimivat mainiosti.

Tutkimuksen mukaan tietoteknologiselle varautumiselle ”ei aseteta selkeästi velvoittavia vaatimuksia, jotka ulottuvat ministeriöistä virastoihin”. Lisäksi ”resursointi ei vastaa tavoitteita eikä vaikutuksia kyetä seuraamaan”.

Tutkimus listaa ammottavia aukkoja valtion kybervalmiuksissa:

Keskitetyt, velvoittavat ohjeet puuttuvat.

Nykyisten ohjeiden riittävyys on ”vakavissa erityistilanteissa epävarmaa”.

Ministeriöt asettavat itse itselleen vaatimukset ja valvovat niiden täyttämistä.

Ulkoistaminen on epäonnistunut, sillä ”palvelujentarjoajille ei ole asetettu riittäviä vaatimuksia varautumiseen liittyvien sopimusvelvoitteiden siirtämisestä alihankkijaverkostoonsa”.

Kaiken kaikkiaan suomalaisen tietoyhteiskunnan turvallisuus on epävarmalla pohjalla, tutkimus tiivistää.

”Tietovarantojen ja tietoliikenteen merkitys sähköisten palvelujen perustana on erittäin suuri, ja suojaamisessa on puutteita.” **SK**

Tutkimus listaa ammottavia aukkoja valtion kybervalmiuksissa.

Mikä palvelunesto?

Palvelunestohyökkäykseksi kutsutaan yritystä lamauttaa internetsivusto tai verkkopalvelu kuormittamalla sitä valtavalla määrällä keinotekoista liikennettä.

Hyökkäyksissä voi olla mukana jopa kymmeniätuhansia tietokoneita, jotka ovat joko normaalikäyttäjien hallinnassa tai heidän tietämättään virusten avulla haltuun otettuja ”orjia”.

Palvelunestohyökkäysten kohteita:

2002 Internetin osoitejärjestelmästä vastaavat juurinimipalvelimet.

2004 Google, Yahoo, Microsoft, Apple.

2007 Viro: ministeriöt, puolueet, pankit. Suomi: Yle, STT, Suomi24, Viestintävirasto.

Kesäkuu 2008 Elokuvatietokanta Internet Movie Database. Verkkokauppa Amazon.com.

Elokuu 2008 Georgia: ministeriöt, parlamentti oikeuslaitos, media.

Syyskuu 2008 Burman opposition sivut. Irakin šiiajohtajan Ali al-Sistanin sivut. Useat radikaalien islamistien keskustelufoorumit eri puolilla maailmaa. ■