EUROOPAN YHTEISÖJEN KOMISSIO

Bryssel 30.3.2009
KOM(2009) 149 lopullinen

KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE, NEUVOSTOLLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE SEKÄ ALUEIDEN KOMITEALLE

elintärkeiden tietoinfrastruktuureiden suojaamisesta

”Euroopan suojaaminen laajoilta tietoverkkohyökkäyksiltä ja -häiriöiltä: valmiuden, turvallisuuden ja sietokyvyn parantaminen”

{SEC(2009) 399}
{SEC(2009) 400}

(komission esittämä)

KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE, NEUVOSTOLLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE SEKÄ ALUEIDEN KOMITEALLE

elintärkeiden tietoinfrastruktuureiden suojaamisesta

”Euroopan suojaaminen laajoilta tietoverkkohyökkäyksiltä ja -häiriöiltä: valmiuden, turvallisuuden ja sietokyvyn parantaminen”

1. JOHDANTO

Tieto- ja viestintäteknologia (TVT) on yhä kiinteämpi osa jokapäiväistä elämäämme. Jotkin TVT-järjestelmät, -palvelut, -verkot ja -infrastruktuurit (jäljempänä ’TVT-infrastruktuurit’) muodostavat olennaisen osan Euroopan taloudesta ja yhteiskunnasta. Niillä joko tarjotaan keskeisiä hyödykkeitä ja palveluja tai ne muodostavat alustan muille elintärkeille infrastruktuureille. Näitä pidetään yleisesti elintärkeinä tietoinfrastruktuureina (CII)[1] siksi, että niiden toiminnan keskeytymisellä tai vaurioitumisella olisi vakavia vaikutuksia yhteiskunnan välttämättömille toiminnoille. Viimeaikaisia esimerkkejä ovat laajat tietoverkkohyökkäykset Viroon vuonna 2007 ja merenalaisten kaapelien katkeaminen vuonna 2008.

Maailman talousfoorumi arvioi vuonna 2008, että elintärkeiden tietoinfrastruktuurien laajan toimintahäiriön todennäköisyys seuraavan 10 vuoden kuluessa on 10–20 prosenttia. Toimintahäiriö voisi maailmanlaajuisesti aiheuttaa noin 250 miljardin dollarin kustannukset[2].

Käsillä olevassa tiedonannossa painotetaan ennaltaehkäisyä, valmiutta ja tietoisuutta, ja siinä määritellään sarja välittömiä toimenpiteitä elintärkeiden tietoinfrastruktuurien turvallisuuden ja sietokyvyn parantamiseksi. Painotus on linjassa neuvoston ja Euroopan parlamentin pyynnöstä käynnistetyn keskustelun kanssa. Tässä keskustelussa on pohdittu verkko- ja tietoturvapolitiikan haasteita ja painopisteitä sekä tarkoituksenmukaisimpia keinoja niiden ratkaisemiseksi EU:n tasolla. Ehdotetut toimet täydentävät toimia, joilla ehkäistään ja torjutaan elintärkeisiin tietoinfrastruktuureihin kohdistuvia rikoksia ja terroritekoja ja saatetaan niiden tekijät oikeudelliseen edesvastuuseen. Lisäksi ne tarjoavat synergiaetuja verkko- ja tietoturvan alan nykyisen ja tulevan EU:n tutkimustoiminnan sekä alan kansainvälisen toiminnan kanssa.

2. POLIITTINEN KONTEKSTI

Tällä tiedonannolla kehitellään eurooppalaista politiikkaa turvallisuuden ja luottamuksen lujittamiseksi tietoyhteiskunnassa. Jo vuonna 2005 komissio tähdensi, että on pikaisesti ryhdyttävä koordinoimaan toimia sidosryhmien luottamuksen rakentamiseksi sähköisiä viestintäverkkoja ja -palveluja kohtaan[3]. Tätä varten se vahvisti turvallisen tietoyhteiskunnan

---

1 Elintärkeille tietoinfrastruktuureille ehdotetaan määritelmää asiakirjassa KOM(2005) 576 lopullinen.

2 *Global Risks 2008.*

3 KOM(2005) 229.

strategian[4] vuonna 2006. Strategian keskeiset elementit, kuten TVT-infrastruktuurien turvallisuus ja sietokyky, vahvistettiin neuvoston päätöslauselmassa 2007/068/01. Sen omaksuminen ja toteutus sidosryhmien keskuudessa vaikuttaa kuitenkin vajavaiselta. Lisäksi tämä strategia vahvistaa Euroopan verkko- ja tietoturvaviraston (ENISA) taktista ja operatiivista roolia. Virasto perustettiin vuonna 2004 tehtävänään varmistaa verkko- ja tietoturvan korkea taso ja toimivuus yhteisössä sekä kehittää verkko- ja tietoturvakulttuuria EU:n kansalaisia, kuluttajia, yrityksiä ja hallintoja hyödyttävällä tavalla.

Vuonna 2008 verkko- ja tietoturvaviraston toimeksiantoa jatkettiin sellaisenaan maaliskuuhun 2012[5]. Samalla neuvosto ja Euroopan parlamentti kehottivat jatkamaan keskustelua verkko- ja tietoturvan tulevaisuudesta ja eurooppalaisen toiminnan yleisestä suuntaamisesta verkko- ja tietoturvan parantamiseksi. Komissio järjesti tämän keskustelun tueksi viime maaliskuussa internetissä julkisen kuulemisen[6], jonka tulokset julkistetaan piakkoin.

Tässä tiedonannossa kaavaillut toimet suoritetaan Euroopan elintärkeiden infrastruktuurien suojaamisohjelman (EPCIP)[7] alaisuudessa ja sen rinnalla. Yksi EPCIP-ohjelman keskeisistä elementeistä on Euroopan elintärkeiden infrastruktuurien määrittämisestä ja nimeämisestä annettu direktiivi[8,9], jossa TVT-toimiala yksilöidään yhdeksi tulevaisuuden painopistealueista. Toinen EPCIP-ohjelman tärkeä elementti on elintärkeiden infrastruktuurien varoitusjärjestelmä (CIWIN)[10].

Sääntelyn osalta komissio on ehdottanut sähköisten viestintäverkkojen ja -palvelujen sääntelyjärjestelmän uudistamista[11]. Uudistus tuo mukanaan turvallisuutta ja koskemattomuutta koskevia uusia säännöksiä. Säännöksillä pyritään ennen muuta tehostamaan operaattoreiden velvoitteita varmistaa asianmukainen reagointi tunnistettuihin riskeihin, taata palvelujen tarjonnan jatkuvuus ja ilmoittaa tietoturvaloukkauksista[12]. Tämä lähestymistapa edistää yleistä tavoitetta eli elintärkeiden tietoinfrastruktuurien turvallisuuden ja sietokyvyn parantamista. Euroopan parlamentti ja neuvosto tukevat yleisesti ottaen näitä säännöksiä.

Tässä tiedonannossa ehdotetuilla toimilla täydennetään poliisi- ja oikeusyhteistyön nykyisiä ja tulevia toimia TVT-infrastruktuureihin kohdistuvien rikosten ja terroritekojen ehkäisemiseksi ja torjumiseksi ja niiden tekijöiden saattamiseksi oikeudelliseen edesvastuuseen. Tällaisia toimia on kaavailtu muun muassa neuvoston puitepäätöksessä tietojärjestelmiin kohdistuvista hyökkäyksistä[13] ja sen suunnitellussa ajantasaistamisessa[14].

Tässä aloitteessa otetaan huomioon NATO:n toimet tietoverkkojen yhteisessä puolustamisessa, eli sen perustamat yksiköt *Cyber Defence Management Authority* ja *Cooperative Cyber Defence Centre of Excellence*.

---

4 KOM(2006) 251.
5 Asetus (EY) N:o 1007/2008.
6 http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464
7 KOM(2006) 786 lopullinen.
8 Direktiivi 2008/114/EY.
9 http://register.consilium.europa.eu/pdf/fi/08/st16/st16862.fi08.pdf
10 KOM(2008) 676 lopullinen.
11 KOM(2007) 697, KOM(2007) 698 ja KOM(2007) 699.
12 Puitedirektiivin 13 artikla.
13 2005/222/YOS.
14 KOM(2008) 712.

Myös kansainvälisen politiikan kehittyminen otetaan huomioon, erityisesti G8-maiden vahvistamat elintärkeiden tietoinfrastruktuurien suojaamisperiaatteet[15], YK:n yleiskokouksen päätöslauselma 58/199 *Creation of a global culture of cybersecurity and the protection of critical information infrastructures* sekä äskettäinen OECD:n suositus elintärkeiden tietoinfrastruktuurien suojaamisesta.

3. MISTÄ ON KYSYMYS

3.1. Elintärkeät tietoinfrastruktuurit ovat olennaisia EU:n talouden ja yhteiskunnan kasvulle

TVT-toimialan ja TVT-infrastruktuurien taloudellinen ja yhteiskunnallinen merkitys korostuu innovointia ja talouskasvua koskevissa äskettäisissä raporteissa. Näitä ovat i2010-ohjelman puoliväliarviointi[16], Ahon ryhmän raportti[17] ja EU:n vuosittaiset talouskatsaukset[18]. OECD korostaa TVT:n ja internetin merkitystä taloudellisen suorituskyvyn ja yhteiskunnallisen hyvinvoinnin parantamisessa ja yhteiskuntien paremmissa valmiuksissa parantaa kansalaisten elämänlaatua maailmanlaajuisesti[19]. Se myös suosittelee sellaisia politiikkoja, jotka lujittavat luottamusta internet-infrastruktuuriin.

TVT-toimiala on elintärkeä yhteiskunnan kaikille lohkoille. Yritysmaailma on siitä riippuvainen sekä suorien myyntitulojen että sisäisten prosessien tehostamisen kautta. TVT on innovoinnin kriittinen komponentti, ja se edustaa lähes 40:ä prosenttia tuottavuuden kasvusta[20]. TVT on myös jo kiinteä osa julkishallintojen työtä: sähköisen hallinnon palveluja on otettu käyttöön kaikilla tasoilla, samoin kuin uudempia innovatiivisia sovelluksia terveydenhuollon, energian ja poliittisen osallistumisen alalla. Tämän johdosta julkinen sektori on erittäin riippuvainen TVT:stä. Mutta myös kansalaiset käyttävät yhä enemmän TVT:tä arkielämässään: elintärkeiden tietoinfrastruktuurien turvallisuuden parantaminen lisäisi kansalaisten luottamusta TVT:tä kohtaan, varsinkin kun henkilötietojen ja yksityisyyden suoja paranisivat.

3.2. Elintärkeiden tietoinfrastruktuurien riskit

Ihmisten tekemien hyökkäysten, luonnonkatastrofien tai teknisten häiriöiden aiheuttamia riskejä ei useinkaan ymmärretä täysin ja/tai analysoida riittävästi. Niinpä sidosryhmät eivät ole tarpeeksi tietoisia riskeistä voidakseen toteuttaa tehokkaita turva- ja vastatoimia.

Tietoverkkohyökkäykset ovat kehittyneisyydessään nousseet ennennäkemättömälle tasolle. Yksinkertaisista kokeiluista on tullut taidonnäytteitä, joita tehdään voitontavoittelumielessä tai poliittisista syistä. Eniten uutisoituja esimerkkejä yleisestä suuntauksesta ovat äskettäiset laajamittaiset tietoverkkohyökkäykset Viroon, Liettuaan ja Georgiaan. Virusten, matojen ja muiden haittaohjelmien valtava määrä, ns. botnet-verkkojen yleistyminen ja roskapostin jatkuva kasvu vahvistavat ongelman vakavuuden[21].

---

15 http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf

16 KOM(2008) 199 lopullinen.

17 http://ec.europa.eu/invest-in-research/pdf/2006_aho_group_report_fi.pdf

18 *EU Economy 2007 Review* http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf

19 http://www.oecd.org/dataoecd/1/29/40821707.pdf

20 http://epp.eurostat.ec.europa.eu/ – *Science and Technology/Information Society*.

21 KOM(2006) 688 lopullinen.

Riippuvaisuus elintärkeistä tietoinfrastruktuureista, niiden yhteenliitynnät maiden rajojen yli ja keskinäiset riippuvuudet muiden infrastruktuurien kanssa – puhumattakaan niiden haavoittuvuuksista ja uhkakuvista – korostavat tarvetta lähestyä niiden turvallisuutta ja sietokykyä systeemisestä näkökulmasta ja puolustuksen etulinjana häiriöitä ja hyökkäyksiä vastaan.

3.3. Elintärkeiden tietoinfrastruktuurien turvallisuus ja sietokyky luottamuksen lisääjinä tietoyhteiskunnassa

Jotta voitaisiin varmistaa TVT-infrastruktuurien maksimaalinen hyödyntäminen ja tietoyhteiskunnan taloudellisten ja yhteiskunnallisten mahdollisuuksien täysimääräinen toteuttaminen, kaikkien sidosryhmien on voitava kokea ne erittäin luotettaviksi. Tämä riippuu useista tekijöistä, joista tärkein on TVT-infrastruktuurien korkean tason turvallisuuden ja sietokyvyn varmistaminen. Eri komponenttien monimuotoisuus, avoimuus, yhteentoimivuus, käytettävyys, läpinäkyvyys, vastuukysymykset ja tarkastettavuus sekä kilpailu ovat keskeisiä vetureita turvallisuuden kehittämiselle ja turvallisuutta parantavien tuotteiden, prosessien ja palvelujen käyttöönoton edistämiselle. Kuten komissio on jo korostanut[22], kyseessä on jaettu vastuu: millään yksittäisellä sidosryhmällä ei ole keinoja yksin varmistaa kaikkien TVT-infrastruktuurien turvallisuutta ja sietokykyä ja suoriutua kaikista tähän liittyvistä velvollisuuksista.

Tällaisten vastuiden ottaminen vaatii riskinhallintalähestymistavan ja -kulttuurin omaksumista; on kyettävä reagoimaan tunnettuihin uhkiin ja ennakoimaan tuntemattomia, ilman ylilyöntejä ja jarruttamatta innovatiivisten palvelujen ja sovellusten markkinoille tuloa.

3.4. Euroopan haasteet

Kaikkien niiden toimien lisäksi ja täydennykseksi, jotka liittyvät elintärkeiden infrastruktuurien määrittämisestä ja nimeämisestä annetun direktiivin täytäntöönpanoon ja erityisesti TVT:n alakohtaisten kriteerien määritykseen, elintärkeiden tietoinfrastruktuurien turvallisuuden ja sietokyvyn parantaminen edellyttää useiden laajempien haasteiden ratkaisemista.

3.4.1. Kansallisten lähestymistapojen hajanaisuus ja koordinoimattomuus

Vaikka edessä olevilla haasteilla ja kysymyksillä on yhteisiä piirteitä, elintärkeiden tietoinfrastruktuurien turvallisuuden ja sietokyvyn parantamiseen tähtäävät toimet ja järjestelmät vaihtelevat eri jäsenvaltioissa. Sama koskee jäsenvaltioiden osaamis- ja valmiustasoa.

Kansallisiin ratkaisuihin perustuvan lähestymistavan vaarana on toimien hajanaisuus ja tehottomuus Euroopassa. Erilaiset kansalliset lähestymistavat ja järjestelmällisen valtioiden rajat ylittävän yhteistyön puute heikentävät huomattavasti kansallisten vastatoimien tehokkuutta. Tämä johtuu muun muassa elintärkeiden tietoinfrastruktuurien yhteenliitoksista, minkä vuoksi yhden maan elintärkeiden tietoinfrastruktuurien alhainen turvallisuustaso ja sietokyky voivat lisätä haavoittuvuutta ja riskejä muissa maissa.

Tällaisen tilanteen ratkaiseminen edellyttää eurooppalaisia toimia, joilla tuodaan lisäarvoa kansallisiin toimintamalleihin ja ohjelmiin nähden. Toimilla edistetään haasteiden

[22] KOM(2006) 251 lopullinen.

tiedostamista ja yhteistä ymmärtämistä, vauhditetaan yhteisten poliittisten tavoitteiden ja painopisteiden hyväksymistä, lujitetaan jäsenvaltioiden välistä yhteistyötä ja integroidaan kansallisia toimintamalleja eurooppalaisiin ja maailmanlaajuisiin toimintamalleihin.

3.4.2. Uuden eurooppalaisen hallintomallin tarve elintärkeitä tietoinfrastruktuureja varten

Elintärkeiden tietoinfrastruktuurien turvallisuuden ja sietokyvyn parantaminen sisältää omat hallinnolliset haasteensa. Vaikka jäsenvaltiot ovat viime kädessä vastuussa elintärkeitä tietoinfrastruktuureita koskevan politiikan määrittelystä, politiikan täytäntöönpano riippuu yksityisestä sektorista, joka omistaa tai hallitsee suurta osaa elintärkeistä tietoinfrastruktuureista. Toisaalta markkinoilla ei useinkaan ole riittäviä kannustimia, jotta yksityinen sektori investoisi elintärkeiden tietoinfrastruktuurien suojaamiseen tasolla, jota hallitukset yleensä odottaisivat.

Tämän hallinto-ongelman ratkaisemiseksi on kansallisen tason malliratkaisuksi noussut julkis-yksityisiä kumppanuuksia. Mutta vaikka yleisesti ollaan samaa mieltä siitä, että myös Euroopan tason julkis-yksityiset kumppanuudet olisivat toivottavia, sellaisia ei ole vielä ilmaantunut. Olennaiset sidosryhmät kattava Euroopan laajuinen hallintokehys, johon voisi vielä sisältyä Euroopan verkko- ja tietoturvaviraston laajennettu rooli, voisi edistää yksityisen sektorin osallistumista julkisen politiikan strategisten tavoitteiden sekä operatiivisten painopisteiden ja toimien määrittelyyn. Tällainen kehys kaventaisi kansallisen poliittisen päätöksenteon ja kentällä vallitsevan todellisuuden välistä kuilua.

3.4.3. Euroopan rajalliset ennakkovaroitus- ja reagointivalmiudet

Hallintomenetelmät ovat tosiasiallisesti tehokkaita ainoastaan siinä tapauksessa, että kaikilla osallisilla on käytettävissään luotettavaa tietoa, jonka pohjalta toimia. Tämä koskee erityisesti hallituksia, jotka viime kädessä ovat vastuussa kansalaisten turvallisuuden ja hyvinvoinnin varmistamisesta.

Verkkoturvan loukkausten valvontaan ja raportointiin liittyvät prosessit ja käytännöt poikkeavat kuitenkin suuresti toisistaan eri jäsenvaltioissa. Joillakin jäsenvaltioilla ei ole minkäänlaista katto-organisaatiota valvontapisteenä. Mikä tärkeämpää, jäsenvaltioiden välinen yhteistyö ja tiedon jakaminen verkkoturvan loukkauksiin liittyvän luotettavan ja vastatoimet mahdollistavan tiedon osalta vaikuttaa kehittymättömältä. Se on joko epävirallista tai rajoittuu kahdenväliseen tai rajoitettuun monenväliseen tiedonvaihtoon. Lisäksi on tiedostettava, että kriittisten tilanteiden simuloinnilla ja reagointivalmiuksien testeillä on strategista merkitystä elintärkeiden tietoinfrastruktuurien turvallisuuden ja sietokyvyn parantamisessa. Erityisesti olisi keskityttävä joustaviin strategioihin ja prosesseihin, joilla ratkotaan potentiaalisten kriisien ennakoimattomuutta. Tietoverkon turvallisuutta testaavat harjoitukset ovat EU:ssa kuitenkin vielä lapsenkengissä. Jäsenvaltiosta toiseen ulottuvia harjoituksia on hyvin rajallisesti. Kuten äskettäiset tapahtumat[23] osoittivat, keskinäinen avunanto on olennainen osa kunnollista reagointia elintärkeisiin tietoinfrastruktuureihin kohdistuvia laajoja uhkia ja hyökkäyksiä vastaan.

Vahvan eurooppalaisen ennakkovaroitus- ja reagointivalmiuden on perustuttava kansallisten/valtiollisten tietotekniikan kriisiryhmien (CERT) moitteettomaan toimintaan, ts. niillä on oltava yhtäläiset perusvalmiudet. Näiden elinten on toimittava kansallisina

[23] http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/

katalysaattoreina sidosryhmien intresseille ja valmiuksille julkisen politiikan toimien suuntaan (mukaan luettuina toimet, jotka liittyvät kansalaisille ja pk-yrityksille ulottuviin tiedonvälitys- ja hälytysjärjestelmiin) ja jotta saataisiin aikaan tuloksellista yhteistyötä ja tiedonvaihtoa rajojen yli. Tämä toiminta voisi tukea olemassa olevia organisaatioita, kuten *European Governmental CERTs Groupia* (EGC)[24].

3.4.4. Kansainvälinen yhteistyö

Internetin nousu yhdeksi keskeisistä elintärkeistä tietoinfrastruktuureista vaatii erityistä huomiota sietokyvyn ja vakauden suhteen. Internet on hajautetun ja monennetun luonteensa vuoksi osoittautunut erittäin vahvaksi infrastruktuuriksi. Sen ilmiömäinen kasvu on kuitenkin lisännyt sen fyysistä ja loogista monimutkaisuutta ja tuottanut runsaasti uusia palveluja ja käyttömuotoja, ja on perusteltua kyseenalaistaa internetin kyky kestää kasvavaa määrää häiriöitä ja hyökkäyksiä.

Internetin elementtien kriittisyydestä on esitetty eriäviä näkemyksiä, mikä osittain selittää sen, että jäsenvaltioiden kansainvälisillä foorumeilla esittämät kannat poikkeavat toisistaan ja asian tärkeydestä ollaan eri mieltä. Tämä voi haitata internetin uhkien kunnollista ehkäisemistä, niihin valmistautumista ja kykyä selvitä niistä. Esimerkiksi ennen siirtymistä IPv4-protokollasta IPv6-protokollaan olisi siirtymisen seurauksia arvioitava elintärkeiden tietoinfrastruktuurien turvallisuuden näkökulmasta.

Internet on maailmanlaajuinen ja erittäin hajautettu verkkojen verkosto, jonka ohjauskeskukset eivät välttämättä noudata kansallisia rajoja. Tämän vuoksi tarvitaan erityinen kohdennettu lähestymistapa sen sietokyvyn ja vakauden varmistamiseen. Lähestymistapa perustuu kahtalaiseen lähtökohtaan: ensinnäkin on saavutettava yleinen konsensus internetin sietokyvyn ja vakauden eurooppalaisista painopisteistä julkisen politiikan ja operatiivisen toteuttamisen näkökulmasta. Toiseksi on saatava kansainvälinen yhteisö mukaan kehittämään internetin sietokyvyn ja vakauden periaatteita, jotka heijastavat eurooppalaisia perusarvoja, kolmansien maiden ja kansainvälisten organisaatioiden kanssa käytävän strategisen vuoropuhelun ja yhteistyön puitteissa. Tämä toiminta perustuisi siihen, että internetin vakaus on tietoyhteiskuntahuippukokouksessa[25] tunnustettu olennaisen tärkeäksi asiaksi.

4. SEURAAVAT TOIMET: KOHTI EU:N TASON KOORDINOINTIA JA YHTEISTYÖTÄ

Ongelmalla on yhteisön laajuinen ja maailmanlaajuinen ulottuvuus, ja yhdennetty EU:n lähestymistapa elintärkeiden tietoinfrastruktuurien turvallisuuden ja sietokyvyn parantamiseen toisi lisäarvoa niin kansallisille ohjelmille kuin jäsenvaltioiden nykyisille kahden- ja monenvälisille yhteistyöhankkeillekin.

Viron tapahtumien jälkeen käyty poliittinen keskustelu toi esille, että vastaavankaltaisten hyökkäysten vaikutuksia voidaan rajoittaa ennalta ehkäisevin toimin ja koordinoimalla toimintaa itse kriisitilanteen aikana. Jäsennellympi, koko EU:n laajuinen tietojen ja hyvien käytäntöjen vaihto voisi helpottaa huomattavasti valtioiden rajat ylittävien uhkien torjuntaa.

On syytä vahvistaa nykyisiä yhteistyövälineitä, Euroopan verkko- ja tietoturvavirasto mukaan luettuna, ja luoda tarpeen mukaan uusia välineitä. Olennaista on, että valittu lähestymistapa

[24] http://www.egc-group.org/

[25] Tunisin tietoyhteiskuntahuippukokouksen asialista, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

kattaa laajan kirjon sidosryhmiä ja se toimii usealla tasolla. Toiminnan on oltava Euroopan laajuista, mutta siinä otetaan huomioon kansalliset vastuut ja täydennetään niitä.

On tarpeen ymmärtää toimintakenttä ja sen rajoitteet perusteellisesti. Yksi huolenaihe on esimerkiksi internetin hajautettu luonne, minkä vuoksi verkon reunasolmuja voidaan käyttää hyökkäyksen levittäjinä. Tähän perustuvat muun muassa botnet-verkot. Hajautettu luonne on toisaalta myös keskeinen vakauden ja sietokyvyn tekijä ja voi ongelmatilanteissa auttaa palauttamaan järjestelmän toimintakuntoon nopeammin kuin liian muodolliset ja hierarkkiset menettelyt. Niinpä julkista politiikkaa ja operatiivisia menettelyjä on analysoitava tarkasti ja tapauskohtaisesti.

Myös ajoitus on tärkeä. On selvää, että nyt on toimittava nopeasti ja luotava tarpeelliset elementit sellaisten puitteiden rakentamiseksi, joiden avulla voidaan vastata nykyisiin haasteisiin ja joista on hyötyä tulevaisuuden verkko- ja tietoturvastrategiassa.

Näiden haasteiden ratkaisemiseksi komissio ehdottaa viittä toimintalinjaa:

(1) Varautuminen ja ehkäisy: valmiuden varmistaminen kaikilla tasoilla;

(2) Havaitseminen ja vastatoimet: kunnollisten ennakkovaroitusmekanismien rakentaminen;

(3) Häiriöiden lieventäminen ja toimintakunnon palautus: EU:n elintärkeiden tietoinfrastruktuurien puolustusmekanismien vahvistaminen;

(4) Kansainvälinen yhteistyö: EU:n painopisteiden edistäminen kansainvälisellä tasolla;

(5) TVT-toimialan kriteerit: Euroopan elintärkeiden infrastruktuurien määrittämisestä ja nimeämisestä annetun direktiivin[26] täytäntöönpanon tukeminen.

5. TOIMINTASUUNNITELMA

5.1. Varautuminen ja ehkäisy

<u>Perusvalmiudet ja -palvelut yleiseurooppalaista yhteistyötä varten.</u> Komissio kehottaa jäsenvaltioita ja asianosaisia sidosryhmiä • määrittelemään – Euroopan verkko- ja tietoturvaviraston tuella – vähimmäistason kansallisten/valtiollisten CERT-ryhmien valmiuksille ja palveluille sekä vastatoimioperaatioille yleiseurooppalaisen yhteistyön tueksi; • varmistamaan, että kansalliset/valtiolliset CERT-ryhmät toimivat kansallisten varautumis-, tiedonvälitys-, koordinointi- ja vastatoimivalmiuksien keskeisenä komponenttina.

[26] Neuvoston direktiivi 2008/114/EY.

Tavoite: vuoden 2010 loppuun mennessä sovitaan vähimmäisnormeista; vuoden 2011 loppuun mennessä kansalliset/valtiolliset CERT-ryhmät toimivat moitteetta kaikissa jäsenvaltioissa.

Sietokykyä käsittelevä eurooppalainen julkis-yksityinen kumppanuus (EP3R). Komissio aikoo

- edistää julkisen ja yksityisen sektorin yhteistyötä turvallisuus- ja sietokykytavoitteissa, lähtökohtaisissa vaatimuksissa, hyvissä toimintamalleissa ja toimenpiteissä. EP3R keskittyy eurooppalaiseen ulottuvuuteen strategisesta (esim. hyvät toimintamallit) ja taktisesta/operatiivisesta (esim. teollinen käyttöönotto) näkökulmasta. EP3R:n tulisi pohjautua olemassa oleviin kansallisiin aloitteisiin ja täydentää niitä ja Euroopan verkko- ja tietoturvaviraston operatiivista toimintaa.

Tavoite: vuoden 2009 loppuun mennessä laaditaan etenemissuunnitelma ja yleinen suunnitelma EP3R:ää varten; EP3R perustetaan vuoden 2010 puoliväliin mennessä; EP3R tuottaa ensimmäiset tuloksensa vuoden 2010 loppuun mennessä.

Jäsenvaltioiden välinen eurooppalainen tiedonjakofoorumi. Komissio aikoo

- perustaa eurooppalaisen foorumin, jossa jäsenvaltiot voivat jakaa tietoa ja hyviä toimintamalleja liittyen elintärkeiden tietoinfrastruktuurien turvallisuuteen ja sietokykyyn. Foorumi hyötyisi muiden organisaatioiden ja erityisesti Euroopan verkko- ja tietoturvaviraston työn tuloksista.

Tavoite: foorumi käynnistetään vuoden 2009 loppuun mennessä; se tuottaa ensimmäiset tulokset vuoden 2010 loppuun mennessä.

5.2. Havaitseminen ja vastatoimet

Eurooppalainen tiedonjako- ja hälytysjärjestelmä (EISAS). Komissio tukee

- EISAS-järjestelmän kehittämistä ja käyttöönottoa. Järjestelmän toiminta ulottuu kansalaisiin ja pk-yrityksiin ja se perustuu kansallisiin ja yksityisen sektorin tiedonjako- ja hälytysjärjestelmiin. Komissio tukee taloudellisesti kahta täydentävää prototyyppihanketta[27]. Euroopan verkko- ja tietoturvavirastoa kehotetaan arvioimaan näiden hankkeiden ja muiden kansallisten aloitteiden tuloksia ja laatimaan etenemissuunnitelma EISAS-järjestelmän jatkokehitykselle ja käyttöönotolle.

Tavoite: prototyyppihankkeet saatetaan loppuun vuoden 2010 loppuun mennessä; vuoden 2010 loppuun mennessä laaditaan eurooppalaisen järjestelmän etenemissuunnitelma.

5.3. Häiriöiden lieventäminen ja toimintakunnon palautus

Kansalliset varautumissuunnitelmat ja harjoitukset. Komissio kehottaa jäsenvaltioita

[27] Terrorismin ja muiden turvallisuuteen liittyvien riskien ennalta ehkäisyä, torjuntavalmiutta ja niiden seurausten hallintaa koskevan erityisohjelman alaisuudessa: http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm.

- laatimaan kansallisia varautumissuunnitelmia ja järjestämään säännöllisiä harjoituksia laajamittaisiin verkkoturvaloukkauksiin reagoimisessa ja kriisitilanteiden hoitamisessa. Kansallisten/valtiollisten CERT/CSIRT-ryhmien tehtäväksi voidaan antaa kansallisten varautumissuunnitelmien, harjoitusten ja testauksen johtaminen, johon otetaan mukaan sekä yksityisen että julkisen sektorin sidosryhmiä. Euroopan verkko- ja tietoturvavirastoa kehotetaan tukemaan hyvien käytäntöjen vaihtoa jäsenvaltioiden välillä.

Tavoite: vuoden 2010 loppuun mennessä suoritetaan vähintään yksi kansallinen harjoitus jokaisessa jäsenvaltiossa.

Yleiseurooppalaiset harjoitukset laajojen verkkoturvaloukkausten varalle. Komissio aikoo

- tukea taloudellisesti yleiseurooppalaisia harjoituksia internetin turvaloukkausten varalta[28]. Tämä voi myös muodostaa operatiivisen pohjan yleiseurooppalaiselle osallistumiselle kansainvälisiin verkkoturvaloukkausten harjoituksiin, kuten yhdysvaltalaiseen *Cyber Storm* -harjoitukseen.

Tavoite: vuoden 2010 loppuun mennessä suunnitellaan ja toteutetaan ensimmäinen yleiseurooppalainen harjoitus; vuoden 2010 loppuun mennessä toteutetaan yleiseurooppalainen osallistuminen kansainvälisiin harjoituksiin.

Kansallisten/valtiollisten CERT-ryhmien yhteistyön lujittaminen. Komissio kehottaa jäsenvaltioita

- lujittamaan kansallisten/valtiollisten CERT-ryhmien yhteistyötä, myös tukemalla ja laajentamalla olemassa olevia yhteistyömekanismeja, kuten EGC:tä[29]. Euroopan verkko- ja tietoturvavirastoa kehotetaan ottamaan aktiivinen rooli kansallisten/valtiollisten CERT-ryhmien yleiseurooppalaisen yhteistyön edistämisessä ja tukemisessa. Pyrkimyksenä on parantaa valmiutta, lujittaa Euroopan kykyä reagoida verkkoturvaloukkauksiin ja torjua niitä sekä toteuttaa yleiseurooppalaisia (ja/tai alueellisia) harjoituksia.

Tavoite: vuoden 2010 loppuun mennessä kaksinkertaistetaan ECG:hen osallistuvien kansallisten elinten määrä; Euroopan verkko- ja tietoturvavirasto kehittää vuoden 2010 loppuun mennessä viitemateriaalia yleiseurooppalaisen yhteistyön tueksi.

5.4. Kansainvälinen yhteistyö

Internetin sietokyky ja vakaus. Tarkoituksena on toteuttaa kolmenlaista täydentävää toimintaa:

- Internetin pitkän aikavälin sietokyvyn ja vakauden eurooppalaiset painopisteet. Komissio aikoo johtaa Euroopan laajuista keskustelua, johon osallistuvat kaikki asianosaiset julkisen ja yksityisen sektorin sidosryhmät ja jossa määritellään EU:n painopisteet internetin pitkän aikavälin sietokyvyn ja vakauden suhteen.

Tavoite: vuoden 2010 loppuun mennessä määritellään EU:n painopisteet internetin kriittisten komponenttien ja kysymysten osalta.

[28] Ks. alaviite 27.
[29] Ks. alaviite 24.

- Internetin sietokyvyn ja vakauden periaatteet ja suuntaviivat (Euroopan taso). Komissio tulee tekemään yhteistyötä jäsenvaltioiden kanssa internetin sietokykyä ja vakautta koskevien suuntaviivojen määrittelyssä. Tarkoituksena on keskittyä muun muassa alueellisiin korjaaviin toimiin, keskinäistä avunantoa koskeviin sopimuksiin, koordinoituihin toimintakunnon palauttamis- ja jatkuvuusstrategioihin, kriittisten internet-resurssien maantieteelliseen jakautumiseen, teknisiin turvamenetelmiin internetin arkkitehtuurissa ja yhteiskäytännöissä sekä palvelujen ja datan toisintamiseen ja monimuotoisuuteen. Komissio rahoittaa jo DNS-järjestelmän sietokykyä tutkivaa työryhmää, jonka työ – muiden asiaan liittyvien hankkeiden ohella – auttaa konsensuksen rakentamisessa[30].

Tavoite: vuoden 2009 loppuun mennessä laaditaan eurooppalainen etenemissuunnitelma internetin sietokykyä ja vakautta koskevia periaatteita ja suuntaviivoja varten; vuoden 2010 loppuun mennessä sovitaan tällaisten periaatteiden ja suuntaviivojen ensimmäisestä luonnoksesta.

- Internetin sietokyvyn ja vakauden periaatteet ja suuntaviivat (maailmanlaajuinen taso). Komissio kehittelee yhdessä jäsenvaltioiden kanssa etenemissuunnitelmaa periaatteiden ja suuntaviivojen edistämiseksi maailmanlaajuisella tasolla. Tarkoitus on kehittää strategista yhteistyötä kolmansien maiden kanssa, erityisesti tietoyhteiskuntaa koskevien vuoropuhelujen merkeissä, yhtenä keinona maailmanlaajuisen konsensuksen rakentamiseen[31].

Tavoite: vuoden 2010 alkuun mennessä laaditaan etenemissuunnitelma vakautta ja sietokykyä koskeviin periaatteisiin ja suuntaviivoihin liittyvää kansainvälistä yhteistyötä varten; vuoden 2010 loppuun mennessä sovitaan kansainvälisesti tunnustettavien periaatteiden ja suuntaviivojen ensimmäisestä luonnoksesta keskusteltavaksi kolmansien maiden kanssa ja asiaan liittyvillä foorumeilla, kuten Internet Governance Forum -yhteistyössä.

Maailmanlaajuiset harjoitukset laajamittaistenilta internet-turvaloukkauksien hoitamista ja lieventämistä varten. Komissio kehottaa eurooppalaisia sidosryhmiä

- pohtimaan käytännöllistä tapaa laajentaa harjoituksia, joita järjestetään häiriöiden lieventämiseen ja toimintakunnon palauttamiseen liittyvän toimintalinjan alaisuudessa, maailmanlaajuiselle tasolle alueellisten varautumissuunnitelmien ja valmiuksien pohjalta.

Tavoite: komissio ehdottaa vuoden 2010 loppuun mennessä kehystä ja etenemissuunnitelmaa, joilla tuetaan Euroopan osallistumista maailmanlaajuisiin harjoituksiin laajojen internet-turvaloukkauksien hoitamista ja lieventämistä varten.

5.5. Euroopan elintärkeiden infrastruktuurien kriteerit TVT-toimialalla

TVT-toimialan erityiset kriteerit. Vuonna 2008 suoritetun valmistelutyön pohjalta komissio aikoo

[30] Ks. alaviite 27.
[31] KOM(2008) 588 lopullinen.

- yhteistyössä jäsenvaltioiden ja kaikkien asianosaisten sidosryhmien kanssa jatkaa kriteerien kehittämistä Euroopan elintärkeiden infrastruktuurien määrittämiseksi TVT-toimialalla. Tässä hyödynnetään tietoja, joita saadaan käynnisteillä olevasta selvityksestä[32].

Tavoite: komissio määrittelee vuoden 2010 puoliväliin mennessä kriteerit Euroopan elintärkeiden infrastruktuurien määrittämiseksi TVT-toimialalla.

6. PÄÄTELMÄT

Elintärkeiden tietoinfrastruktuurien turvallisuus ja sietokyky ovat puolustuksen eturintamassa toimintahäiriöitä ja hyökkäyksiä vastaan. Niiden parantaminen koko EU:ssa on olennaista, jos tietoyhteiskunnasta mielitään saada kaikki hyöty irti. Komissio ehdottaa tämän kunnianhimoisen tavoitteen saavuttamiseksi toimintasuunnitelmaa, jolla vahvistetaan Euroopan tason taktista ja operatiivista yhteistyötä. Näiden toimien onnistuminen riippuu siitä, kuinka tehokkaasti niissä pystytään hyödyntämään julkisen ja yksityisen sektorin toimintaa ja kuinka tiiviisti jäsenvaltiot, EU:n toimielimet ja sidosryhmät sitoutuvat ja osallistuvat niihin.

Aiheesta järjestetään 27.–28.4.2009 ministerikokous, jossa keskustellaan ehdotetuista aloitteista jäsenvaltioiden kanssa ja vahvistetaan näiden sitoumus osallistua eurooppalaisten verkko- ja tietoturvapolitiikan uudenaikaistamisesta ja lujittamisesta käytävään keskusteluun.

Koska elintärkeiden tietoinfrastruktuurien turvallisuuden ja sietokyvyn parantaminen on pitkän aikavälin tavoite, sitä koskevaa strategiaa ja toimenpiteitä on arvioitava säännöllisesti. Tämän vuoksi, ja koska tavoite on linjassa vuoden 2012 jälkeisestä EU:n verkko- ja tietoturvapolitiikasta käytävän yleisen keskustelun kanssa, komissio käynnistää vuoden 2010 loppupuolella tarkasteluprosessin, jossa arvioidaan ensimmäistä toimintavaihetta ja, tarpeen mukaan, yksilöidään ja ehdotetaan uusia toimia.

[32] Ks. alaviite 27.