Euroopan talous- ja sosiaalikomitean lausunto aiheesta ”Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa”

COM(2013) 48 final — 2013/0027 (COD)

(2013/C 271/25)

Esittelijä: **Thomas McDONOGH**

Neuvosto päätti 21. helmikuuta 2013 ja Euroopan parlamentti 15. huhtikuuta 2013 Euroopan unionin toiminnasta tehdyn sopimuksen 114 artiklan nojalla pyytää Euroopan talous- ja sosiaalikomitean lausunnon aiheesta

Ehdotus – Euroopan parlamentin ja neuvoston direktiivi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa

COM(2013) 48 final – 2013/0027 (COD).

Asian valmistelusta vastannut ”liikenne, energia, perusrakenteet, tietoyhteiskunta” -erityisjaosto antoi lausuntonsa 30. huhtikuuta 2013.

Euroopan talous- ja sosiaalikomitea hyväksyi 22.–23. toukokuuta 2013 pitämässään 490. täysistunnossa (toukokuun 22. päivän kokouksessa) seuraavan lausunnon. Äänestyksessä annettiin 163 ääntä puolesta ja 1 vastaan 5:n pidättyessä äänestämästä.

1. **Päätelmät ja suositukset**

1.1 Komitea panee merkille ehdotetun direktiivin, joka olisi nähtävä äskettäin julkaistuun Euroopan unionin kyberturvallisuusstrategiaan ([1]) liittyvässä laajemmassa yhteydessä. Strategiassa hahmotellaan kattava visio verkko- ja tietoturvasta, jotta varmistetaan, että digitaalitalous voi kasvaa turvallisesti samalla kun edistetään eurooppalaisia vapauden ja demokratian arvoja.

1.2 ETSK on tyytyväinen ehdotettuun direktiiviin, jotta varmistetaan verkko- ja tietoturvan yhteinen korkea taso koko EU:ssa. Verkko- ja tietoturvan yhdenmukaistaminen ja hallinta unionin tasolla ovat olennaisen tärkeitä digitaalisten sisämarkkinoiden loppuunsaattamisen ja sisämarkkinoiden moitteettoman toiminnan kannalta kokonaisuudessaan. Komitea on komission tavoin huolissaan valtavasta vahingosta, jota taloudelle ja EU:n kansalaisten hyvinvoinnille voi aiheutua verkko- ja tietoturvan häiriöstä. Ehdotettu direktiivi ei kuitenkaan vastaa komitean odotuksia vahvasta lainsäädännästä tässä erittäin tärkeässä kysymyksessä.

1.3 Komitea on erittäin pettynyt siihen, että useat jäsenvaltiot eivät ole edistyneet verkko- ja tietoturvan tehokkaassa toteuttamisessa kansallisella tasolla. ETSK on huolissaan lisääntyneistä riskeistä, joita tämä tilanne aiheuttaa kansalaisille, sekä tilanteen kielteisistä vaikutuksista digitaalisten sisämarkkinoiden loppuunsaattamiseen. Kaikkien jäsenvaltioiden olisi viipymättä hoidettava verkko- ja tietoturvaa koskevat täyttämättä jääneet velvoitteensa.

1.4 Tämä puutteellinen edistyminen on luomassa uuden digitaalisen kuilun verkko- ja tietoturvassa pitkälle edistyneiden jäsenvaltioiden eliittiryhmän ja vähemmän edistyneiden jäsenvaltioiden välille. Tällainen kuilu heikentää verkko- ja tietoturvaan liittyvää luottamusta ja yhteistyötä unionitasolla, ja jollei siihen puututa pikaisesti, se voi aiheuttaa jäsenvaltioiden erilaisista valmiuksista johtuvia häiriöitä sisämarkkinoilla.

1.5 ETSK katsoo, kuten se on tuonut esiin aiemmissa lausunnoissaan ([2]), että varovaiset ja vapaaehtoiset toimet eivät ole riittäviä ja että tarvitaan jäsenvaltioihin kohdistuvia voimakkaita sääntelyllisiä velvoitteita, jotta varmistetaan verkko- ja tietoturvan yhdenmukaistaminen, hallinta ja täytäntöönpano Euroopan tasolla. Valitettavasti ETSK:n täytyy todeta, että tässä tarkasteltava ehdotus direktiiviksi ei tarjoa tarvittavaa selkeää ja lujaa lainsäädäntöä. Komitea uskoo, että tarvittavan yhteisen korkean verkko- ja tietoturvan tason varmistamiseksi asetus olisi jäsenvaltioille asetettuine, huolellisesti määriteltyine velvoitteineen direktiiviä tehokkaampi.

1.6 Huolimatta Euroopan komission aikomuksesta antaa delegoituja säädöksiä, jotta varmistetaan yhtenäiset olosuhteet direktiivin eräiden osien täytäntöönpanoa varten, komitea katsoo, että ehdotetusta säädöksestä puuttuu standardeja, selkeitä määritelmiä ja ehdottomia velvoitteita, minkä vuoksi jäsenvaltioille jää aivan liian paljon liikkumavaraa tulkitessaan keskeisiä elementtejä ja siirtäessään ne osaksi kansallista lainsäädäntöä. Komitea toivoo, että ehdotuksessa esitettäisiin paljon tarkempia standardien, vaatimusten ja menettelyjen määritelmiä, joita jäsenvaltioiden, viranomaisten, markkinatoimijoiden ja keskeisten internettoiminnan mahdollistavien tahojen on noudatettava.

([1]) ”Avoin, turvallinen ja vakaa verkkoympäristö”, JOIN(2013) 1.

([2]) ETSK:n lausunnot aiheista ”Elintärkeiden tietoinfrastruktuureiden suojaaminen”, EUVL C 255, 22.9.2010, s. 98 ja ”Direktiivi tietojärjestelmiin kohdistuvista hyökkäyksistä”, EUVL C 218, 23.7.2011, s. 130.

1.7 Jotta vahvistetaan verkko- ja tietoturvaa käsittelevän politiikan muotoilua ja täytäntöönpanoa EU:ssa, komitea kehottaa perustamaan ilmailualan keskusviranomaisen (EASA) ([3]) kaltaisen EU-tason verkko- ja tietoturvaviranomaisen. Tällainen elin laatisi standardeja ja valvoisi verkko- ja tietoturvan kaikkien elementtien täytäntöönpanoa koko unionissa turvallisten päätelaitteiden ja käytäntöjen sertifioinnista aina verkko- ja tietoturvan toteuttamiseen saakka.

1.8 ETSK on erittäin tietoinen kyberturvallisuuden ja tietosuojan lisääntyneistä riskeistä, jotka johtuvat pilvipalvelujen käyttöönotosta ([4]) Euroopassa. Komitea kehottaa nimenomaan sisällyttämään ehdotettuun säädökseen turvallisuutta koskevia erityisiä lisävaatimuksia ja -velvoitteita pilvipalvelujen tarjonnan ja käytön osalta.

1.9 Asianmukaisen vastuuvelvollisuuden varmistamiseksi verkko- ja tietoturvan alalla säädöksessä olisi selvennettävä, että toimijoilla, joilla on ehdotetun direktiivin nojalla velvoitteita, olisi oikeus pitää ohjelmistojen ja laitteistojen toimittajia vastuussa kaikista tuotteidensa tai palveluidensa vioista, jotka vaikuttavat suoraan verkko- ja tietoturvapoikkeamiin.

1.10 ETSK kehottaa jäsenvaltioita kiinnittämään erityistä huomiota siihen, että pienten ja keskisuurten yritysten (pk-yritysten) verkko- ja tietoturvaa koskevat tiedot ja kyberturvallisuuteen liittyvät taidot paranevat. Komitea myös kiinnittää komission huomion ”hakkerikilpailujen” menestykseen Yhdysvalloissa ([5]) ja eräissä jäsenvaltioissa ([6]) sekä tarpeeseen lisätä tietoisuutta kyberturvallisuudesta ja kouluttaa verkko- ja tietoturvan ammattilaisten seuraava sukupolvi.

1.11 Koska on tärkeää, että kaikki jäsenvaltiot noudattavat verkko- ja tietoturvamääräyksiä koko EU:ssa, ETSK kehottaa komissiota harkitsemaan, miten monivuotisen rahoituskehyksen varoja voitaisiin kohdentaa verkko- ja tietoturvamääräysten noudattamiseen, jotta autettaisiin taloudellista tukea tarvitsevia jäsenvaltioita.

1.12 Verkko- ja tietoturvateknologioiden tutkimuksen, kehittämisen ja innovoinnin rahoituksen olisi oltava keskeinen painopiste tutkimuksen ja innovoinnin Horisontti 2020 -puiteohjelmassa, jotta Eurooppa voi pysyä mukana nopeasti muuttuvassa verkkouhkien maailmassa.

1.13 Jotta selvennetään, millä toimijoilla on ehdotetun säädöksen nojalla lakisääteisiä velvollisuuksia, ETSK toivoo, että kukin jäsenvaltio velvoitettaisiin julkaisemaan sähköinen luettelo kaikista niistä toimijoista, joita direktiivin mukaiset riskinhallinta- ja raportointivaatimukset koskevat. Tällainen avoimuus ja julkinen vastuuvelvollisuus lisäisi luottamusta ja edistäisi säännösten noudattamista.

1.14 Komitea kehottaa komissiota kiinnittämään huomiota moniin aiempiin lausuntoihinsa, joissa käsitellään verkko- ja tietoturvaa ja otetaan kantaa turvallisen tietoyhteiskunnan ja elintärkeiden infrastruktuureiden suojaamisen tarpeeseen ([7]).

2. **Komission ehdotuksen pääkohdat**

2.1 Ehdotus verkko- ja tietoturvadirektiiviksi julkaistiin yhdessä asiakirjan ”Euroopan unionin kyberturvallisuusstrategia” kanssa. Strategian tavoitteena on vahvistaa tietojärjestelmien sietokykyä, vähentää verkkorikollisuutta, vahvistaa EU:n kansainvälistä verkkotoimintapolitiikkaa ja verkkopuolustusta, kehittää kyberturvallisuuteen liittyviä teollisia ja teknologisia voimavaroja sekä samalla edistää perusoikeuksia ja muita EU:n keskeisiä arvoja.

2.2 Verkko- ja tietoturvassa on kyse internetin ja muiden yhteiskuntamme toimintaa tukevien verkkojen, tietojärjestelmien ja niihin liittyvien palveluiden suojaamisesta. Verkko- ja tietoturva on keskeinen sisämarkkinoiden moitteettoman toiminnan kannalta.

2.3 Verkko- ja tietoturvaan sovellettava puhtaasti vapaaehtoinen lähestymistapa, jota EU on tähän mennessä noudattanut, ei suojele riittävästi verkko- ja tietoturvariskeiltä. Tämänhetkiset verkko- ja tietoturvavalmiudet eivät riitä vastaamaan nopeasti muuttuviin uhkiin eivätkä varmistamaan korkeatasoista ja yhtenäistä suojaa kaikissa jäsenvaltioissa.

([3]) Euroopan lentoturvallisuusvirasto: http://easa.europa.eu/

([4]) ETSK:n lausunnot aiheista ”Tietotekniikan resurssipalvelut (*cloud computing*) Euroopassa”, EUVL C 24, 28.1.2012, s. 40 ja ”Pilvipalvelujen potentiaali käyttöön Euroopassa, EUVL C 76, 14.3.2013, s. 59.

([5]) http://www.nytimes.com/2013/03/25/technology/united-states-wants-to-attract-hackers-to-public-sector.html?pagewanted=all&_r=0

([6]) http://www.bbc.co.uk/news/technology-17333601

([7]) ETSK:n lausunto aiheesta ”Turvallisen tietoyhteiskunnan strategia”, EUVL C 97, 28.4.2007, s. 21.
ETSK:n lausunto aiheesta ”Elintärkeiden tietoinfrastruktuureiden suojaaminen”, EUVL C 255, 22.9.2010, s. 98.
ETSK:n lausunto aiheesta ”ENISA-asetus”, EUVL C 107, 6.4.2011, s. 58.
ETSK:n lausunto aiheesta ”Yleinen tietosuoja-asetus”, EUVL C 229, 31.7.2012, s. 90.
ETSK:n lausunto aiheesta ”Tietojärjestelmiin kohdistuvat hyökkäykset”, OJ C 218, 23.7.2011, s. 130.
ETSK:n lausunto aiheesta ”Sähköiset transaktiot sisämarkkinoilla”, EUVL C 351, 15.11.2012, s. 73.
ETSK:n lausunto aiheesta ”EU:n pilvipalvelustrategian valmistelu”, EUVL C 76, 14.3.2013, s. 15.
ETSK:n lausunto aiheesta ”Pilvipalvelujen potentiaali käyttöön Euroopassa”, EUVL C 76, 14.3.2013, s. 59.

2.4 Jäsenvaltioiden valmiudet ja varautumistaso vaihtelevat nykyisin hyvin paljon, mikä johtaa verkko- ja tietoturvaan sovellettavien lähestymistapojen hajanaisuuteen eri puolilla EU:ta. Koska verkot ja järjestelmät ovat yhteenliitettyjä, EU:n yleinen verkko- ja tietoturva heikentyy sellaisten jäsenvaltioiden takia, joissa turvataso on riittämätön. Tämä tilanne vaikeuttaa myös luottamuksen luomista vertaisryhmien välille, mikä on ennakkoedellytys yhteistyölle ja tiedonvaihdolle. Näin ollen yhteistyötä harjoitetaan vain niiden vähemmistönä olevien jäsenvaltioiden kesken, joissa valmiustaso on korkea.

2.5 Direktiivin, joka perustuu Euroopan unionin toiminnasta tehdyn sopimuksen 114 artiklaan, tavoitteena on helpottaa digitaalisten sisämarkkinoiden loppuunsaattamista ja moitteetonta toimintaa siten, että

— toteutetaan verkko- ja tietoturvan yhteinen vähimmäistaso jäsenvaltioissa ja lisätään siten yleistä varautumistasoa ja reagointikykyä

— parannetaan verkko- ja tietoturvaan liittyvää yhteistyötä EU:n tasolla rajat ylittävien turvapoikkeamien ja -uhkien torjumiseksi

— luodaan riskinhallintakulttuuri ja parannetaan tietojen vaihtoa yksityisen ja julkisen sektorin välillä.

2.6 Ehdotetussa direktiivissä asetetaan muun muassa seuraavia oikeudellisia vaatimuksia:

a) Jokaisen jäsenvaltion on hyväksyttävä kansallinen verkko- ja tietoturvastrategia ja nimettävä verkko- ja tietojärjestelmien turvallisuudesta vastaava kansallinen toimivaltainen viranomainen, jolla on riittävät taloudelliset ja henkilöstövoimavarat, jotta se voi ehkäistä ja käsitellä verkko- ja tietoturvariskejä ja -poikkeamia ja reagoida niihin.

b) Jäsenvaltioiden ja komission on luotava yhteistyömekanismi voidakseen antaa toisilleen varhaisvaroituksia turvariskeistä ja -poikkeamista, tehdäkseen yhteistyötä ja järjestääkseen säännöllisiä vertaisarviointeja.

c) Tietyntyyppisten toimijoiden on koko EU:ssa otettava käyttöön riskinhallintamenetelmiä ja raportoitava kansallisille toimivaltaisille viranomaisille keskeisissä palveluissaan ilmenevistä merkittävistä turvapoikkeamista. Toimijoita, joita nämä vaatimukset koskevat, ovat tiettyjen alojen (pankki- ja rahoituspalveluiden, liikenteen, energia-alan ja terveydenhuollon) elintärkeiden tietoinfrastruktuureiden ylläpitäjät, tietoyhteiskunnan palvelut (etenkin pilvipalvelut, sähköisen kaupankäynnin alustat, internetvälitteiset maksupalvelut, hakukoneet, sovelluskaupat ja verkkoyhteisöpalvelut) mahdollistavat toimijat ja julkishallinnon tahot.

2.7 Jäsenvaltioiden on saatettava direktiivi osaksi lainsäädäntöään viimeistään 18 kuukauden kuluttua siitä kun neuvosto ja Euroopan parlamentti ovat hyväksyneet direktiivin (todennäköisesti joskus vuonna 2014).

3. **Yleistä**

3.1 Internetin ja digitaaliyhteiskunnan kasvu vaikuttaa syvällisesti jokapäiväiseen elämään. Kun riippuvuutemme internetistä lisääntyy, vapautemme, hyvinvointimme ja elämänlaatumme riippuvat kuitenkin yhä enemmän vahvasta verkko- ja tietoturvasta: jos internet ei toimi eivätkä esimerkiksi sähköiset potilastiedot ole saatavilla hätätilanteessa, ihmisiä voi kuolla. Elintärkeä tietoinfrastruktuuri on Euroopassa yhä uhatumpi, eikä verkko- ja tietoturvatasomme ole riittävän hyvä.

3.2 Europolin johtaja totesi viime vuonna, että hän on ”hyvin huolissaan laajalti perusteettomasta luottamuksesta internetin loukkaamattomuuteen” ([8]). Kuulemme usein rikollisten, terroristien tai vieraiden valtioiden keskeisiin perusrakenteisiin kohdistamista uusista verkkohyökkäyksistä. Kohteet eivät useinkaan raportoi hyökkäyksistä, koska ne pelkäävän maineensa menettämistä. Viime viikkoina on kuitenkin havaittu Euroopan internetinfrastruktuuriin ([9]) ja pankkijärjestelmiin ([10]) kohdistuneita hyökkäyksiä, jotka ovat olleet liian haitallisia peiteltäviksi. Eräässä raportissa ([11]) on arvioitu, että vuonna 2011 Alankomaissa tehtiin 92 miljoonaa verkkohyökkäystä ja Saksassa 82 miljoonaa. Yhdistyneen kuningaskunnan hallitus arvioi, että vuonna 2011 maassa tehtiin 44 miljoonaa verkkohyökkäystä, joiden kustannukset taloudelle olivat lähes 30 miljardia euroa ([12]).

3.3 EU:n neuvosto käsitteli vuonna 2007 verkko-. ja tietoturvaongelmaa Euroopassa ([13]). Siitä lähtien noudatettu poliittinen lähestymistapa ([14]) on kuitenkin pääasiassa tukeutunut jäsenvaltioiden vapaaehtoiseen toimintaan, ja vain jäsenvaltioiden vähemmistö on ryhtynyt tehokkaisiin toimiin. Komitea panee merkille, että monet jäsenvaltiot eivät edelleenkään ole julkaisseet kansallista kyberturvallisuusstrategiaa eivätkä laatineet kansallista verkkoturvallisuuspoikkeamavarautumissuunnitelmaa. Eräät jäsenvaltiot eivät ole vielä perustaneet tietotekniikan kriisiryhmää (CERT-ryhmää) eivätkä edelleenkään ratifioineet verkkorikollisuutta koskevaa Euroopan neuvoston yleissopimusta ([15]).

([8]) http://forumblog.org/2012/05/what-if-the-internet-collapsed/
([9]) http://www.nytimes.com/2013/03/27/technology/internet/online-dispute-becomes-internet-snarling-attack.html?pagewanted=all&_r=0
([10]) http://www.dutchnews.nl/news/archives/2013/04/online_retailers_demand_banks.php
([11]) http://www.securelist.com/en/analysis/204792216/Kaspersky_Security_Bulletin_Statistics_2011
([12]) *UK Cyber Security Strategy – Landscape Review*: http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf
([13]) Neuvoston päätöslauselma 2007/C 68/01.
([14]) COM(2006) 251 final ja COM(2009) 149 final.
([15]) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

3.4 Kymmenen jäsenvaltiota, jotka ovat erittäin edistyneitä verkko- ja tietoturva-asioissa, ovat perustaneet Euroopan valtiollisten tietotekniikan kriisiryhmien yhteenliittymän (EGC) tehdäkseen tiivistä yhteistyötä verkko- ja tietoturvan ja poikkeamiin reagoinnin aloilla. EGC:n jäseneksi ei tällä hetkellä voi liittyä: muut heikommin edistyneet 17 jäsenvaltiota ja uudelleen muodostettu CERT-EU ([16]) on nykyisin suljettu tämän eliittiryhmän ulkopuolelle. Uusi digitaalinen kuilu on avautumassa verkko- ja tietoturvassa erittäin edistyneiden ja muiden jäsenvaltioiden välille. Jollei tätä kuilua kurota umpeen, verkko- ja tietoturvan erot jäytävät digitaalisten sisämarkkinoiden ydintä ja rajoittavat luottamuksen, yhdenmukaisuuden ja yhteentoimivuuden kehittämistä. Ilman päättäväisiä toimia erittäin edistyneiden ja heikommin edistyneiden jäsenvaltioiden välinen kuilu todennäköisesti kasvaa, mikä aiheuttaisi eri maiden välisistä valmiuseroista johtuvia sisämarkkinoiden häiriöitä.

3.5 Kyberturvallisuusstrategian onnistuminen ja ehdotetun verkko- ja tietoturvadirektiivin tehokkuus riippuvat vahvasta verkko- ja tietoturvateollisuudesta Euroopassa sekä verkko- ja tietoturvaan liittyvää erityistaitoa omaavien työntekijöiden riittävästä määrästä. ETSK panee tyytyväisenä merkille, että ehdotetussa direktiivissä viitataan jäsenvaltioiden tarpeeseen investoida verkko- ja tietoturvaan liittyviin opetus-, valistus- ja koulutusohjelmiin. Komitea kehottaa kuitenkin kaikkia jäsenvaltiota toteuttamaan erityistoimia, jotta pk-sektoria informoidaan, valistetaan ja tuetaan kyberturvallisuuteen liittyvissä asioissa. Suurten yritysten on helppo hankkia tarvitsemansa osaaminen, mutta pk-yritykset tarvitsevat tukea.

3.6 ETSK on valmis tekemään yhteistyötä Euroopan verkko- ja tietoturvaviraston (ENISA) kanssa verkko- ja tietoturvan edistämiseksi verkkoturvallisuuskuukauden aikana myöhemmin vuonna 2013. Kun ajatellaan kyberturvallisuusstrategian ja verkko- ja tietoturvaa käsittelevän direktiivin tavoitetta kehittää turvallisuuden huomioon ottavaa kulttuuria kaikkialla unionissa ja lisätä verkko- ja tietoturvan edellyttämien taitojen tasoa, komitea kiinnittää komission huomion teinien keskuudessa järjestettyihin hankkerikilpailuihin, jotka ovat huomattavasti edistäneet valveutumista erinäisissä jäsenvaltioissa ja Yhdysvalloissa.

3.7 Komitea on tyytyväinen myös siihen, että kyberturvallisuusstrategiassa sitoudutaan rahoittamaan verkko- ja tietoturvaan keskittyvää tutkimus-, kehittämis- ja innovointitoimintaa.

3.8 Pilvipalvelujen kasvu synnyttää monia uusia riskejä, jotka on otettava huomioon kyberturvallisuudessa. Verkkorikollisten käytössä on nykyisin esimerkiksi valtava laskentateho suhteellisen alhaisin kustannuksin, ja tuhansien yritysten tiedot on nykyisin tallennettu keskitettyihin tietokantoihin, jotka ovat alttiita kohdennetuille hyökkäyksille. ETSK on suosittanut verkkojen sietokyvyn parantamista pilvipalvelujen yhteydessä ([17]).

([16]) CERT-EU on EU:n toimielinten, virastojen ja muiden elinten perustama pysyvä tietotekniikan kriisiryhmä.

([17]) ETSK:n lausunnot aiheista ”Tietotekniikan resurssipalvelut (*cloud computing*) Euroopassa”, EUVL C 24, 28.1.2012, s. 40 ja ”Pilvipalvelujen potentiaali käyttöön Euroopassa”, EUVL C 76, 14.3.2013, s. 59.

3.9 Komitea on aiemmin kehottanut ottamaan vapaaehtoiselta pohjalta käyttöön verkkokaupassa sovellettavan eurooppalaisen sähköisen henkilötunnisteen nykyisten kansallisten järjestelmien täydennykseksi. Tällainen järjestelmä tehostaisi petosten torjuntaa, lisäisi talouden toimijoiden välistä luottamusta, alentaisi palveluntarjontaan liittyviä kustannuksia, parantaisi palveluiden laatua ja tarjoaisi kansalaisille parempaa suojaa.

4. **Erityistä**

4.1 Verkko- ja tietoturvaa käsittelevä komission direktiiviehdotus on valitettavasti liian varovainen eikä riittävän selkeä ja riippuu liiaksi jäsenvaltioiden itsesääntelystä. Standardien, selkeiden määritelmien ja pakollisten velvoitteiden puuttuminen etenkin direktiivin IV luvut jättää liikaa liikkumavaraa jäsenvaltioille säädöksen keskeisten elementtien tulkinnassa ja saattamisessa osaksi kansallista lainsäädäntöä. Asetus, jossa on määritelty selvästi pakolliset lakisääteiset velvoitteet jäsenvaltioille, olisi direktiiviä tehokkaampi.

4.2 Komitea panee merkille, että ehdotetun direktiivin 6 artiklan mukaan kunkin jäsenvaltion on nimettävä ”toimivaltainen viranomainen” seuraamaan ja edistämään direktiivin johdonmukaista soveltamista kaikkialla unionissa. Lisäksi komitea toteaa, että direktiivin 8 artiklassa säädetään ”yhteistyöverkostosta”, joka sille ja komissiolle uskottujen toimivaltuuksien turvin huolehtii yleiseurooppalaisesta johtamisesta, ohjauksesta ja tarvittaessa täytäntöönpanon valvonnasta jäsenvaltiotasoa myöten. ETSK katsoo, että EU:n olisi näiden hallinnointipuitteiden pohjalta harkittava Euroopan lentoturvallisuusviraston (EASA) kaltaisen EU-tason viranomaisen perustamista verkko- ja tietoturva-asioita varten. EASA laatii standardeja ja huolehtii turvallisuusvaatimusten noudattamisesta ja täytäntöönpanon valvonnasta ilmailualusten, lentoasemien ja lentoyhtiöiden toiminnan osalta.

4.3 Komitean kohdassa 4.2 ehdottama EU-tason verkko- ja tietoturvaviranomainen voisi tukeutua Euroopan verkko- ja tietoturvaviraston (ENISA), Euroopan standardointikomitean (CEN), tietotekniikan kriisiryhmien (CERT), Euroopan valtiollisten tietotekniikan kriisiryhmien yhteenliittymän (EGC) ja muiden vastaavien toimijoiden jo tekemään työhön. Tällainen viranomainen laatisi standardeja ja valvoisi verkko- ja tietoturvan kaikkien elementtien täytäntöönpanoa turvallisten päätelaitteiden ja käytäntöjen sertifioinnista aina verkko- ja tietoturvan toteuttamiseen saakka.

4.4 Koska jäsenvaltiot ovat hyvin riippuvaisia toisistaan varmistettaessa verkko- ja tietoturva koko unionissa ja koska verkko- ja tietoturvahäiriöistä voi aiheutua erittäin korkeita kustannuksia kaikille asianosaisille, ETSK toivoo, että lainsäädännössä sovittaisiin selvistä ja oikeasuhteisista seuraamuksista velvoitteiden laiminlyönneistä ja että seuraamukset yhdenmukaistetaan, jotta ne kuvastavat Euroopan laajuista vastuuta ja mahdollisesti aiheutettavan vahingon laajuutta paitsi kotimarkkinoilla myös kaikkialla unionissa. Säädöksen 17 artiklassa, jossa käsitellään seuraamuksia, annetaan yleisesti ottaen jäsenvaltioille liikaa harkintavaltaa päättää seuraamuksista eikä tarjota riittäviä suuntaviivoja, jotta voidaan ottaa huomioon rajatylittävät ja Euroopan laajuiset vaikutukset.

4.5 Tällä hetkellä valtiot ja elintärkeiden palveluiden tarjoajat eivät julkista turvallisuus- ja sietokykyhäiriöitä kuin pakon edessä. Tällainen avoimuuden puute heikentää Euroopan kykyä reagoida verkkouhkiin nopeasti ja tehokkaasti ja sen kykyä parantaa yleistä verkko- ja tietoturvaa vastavuoroisen oppimisen avulla. Komitea on erittäin tyytyväinen komission päätökseen säätää direktiivissä velvollisuudesta ilmoittaa kaikista merkittävistä verkko- ja tietoturvapoikkeamista. ETSK ei usko, että turvapoikkeamien vapaaehtoinen omatoiminen raportointi toimisi, sillä maineen menettämisen ja vastuuseen joutumisen pelko houkuttelee peittelemään häiriöitä.

4.6 Direktiivin 14 artiklassa, jossa tarkastellaan ilmoittamista, ei kuitenkaan määritellä, minkälaisia olisivat turvapoikkeamat, jotka ”vaikuttavat merkittävästi” turvallisuuteen, ja siinä annetaan asianomaisille elimille ja jäsenvaltioille liikaa harkintavaltaa päättää siitä, ilmoitetaan verkko- ja tietoturvapoikkeamista vai ei. Tehokas lainsäädäntö edellyttää yksiselitteisiä vaatimuksia. Koska ehdotettu direktiivi on liian epäselvä vaatimusten keskeisten määritelmien osalta, osapuolia ei voida pitää vastuussa säännösten rikkomisesta, kuten direktiivin 17 artiklassa säädetään.

4.7 Koska verkko- ja tietoturvan toteuttaminen on pitkälti yksityissektorin käsissä, on tärkeää edistää vankkaa luottamusta ja yhteistyötä kaikkien elintärkeistä tietoinfrastruktuureista ja -palveluista vastaavien yritysten kanssa. Komission vuonna 2009 käynnistämä sietokykyä käsittelevä eurooppalainen julkis-yksityinen kumppanuus (EP3R) on kiitoksen ja kannustuksen arvoinen. Komitea katsoo kuitenkin, että aloitetta tulee vahvistaa ja tukea sääntelyllisellä velvoitteella verkko- ja tietoturvasäädöksessä, jotta velvollisuutensa täyttämättä jättävät keskeiset toimijat voidaan pakottaa yhteistyöhön.

4.8 Kunkin jäsenvaltion olisi julkaistava tuomioistuimiaan varten sähköinen luettelo kaikista niistä toimijoista, joita ehdotetun direktiivin 14 artiklan mukaiset turvallisuusvaatimukset ja turvapoikkeamien ilmoittamisvelvoitteet koskevat. Tällainen avoimuus paitsi selventäisi sitä, millä tavoin kukin jäsenvaltio päättää soveltaa säädöksen 3 artiklan määritelmiä, myös auttaisi lisäämään luottamusta ja edistämään riskinhallintakulttuuria kansalaisten keskuudessa.

4.9 ETSK panee merkille, että ohjelmistojen kehittäjiin ja laitteistojen valmistajiin ei nimenomaan sovelleta direktiivin vaatimuksia, sillä ne eivät tarjoa tietoyhteiskunnan palveluja. Komitea katsoo kuitenkin, että ehdotetussa säädöksessä olisi todettava, että toimijat, joiden on noudatettava direktiivissä asetettuja velvoitteita, voivat valittaa ohjelmistojen ja laitteistojen toimittajille tuotteissa tai palveluissa havaituista puutteista, jotka vaikuttavat suoraan verkko- ja tietoturvapoikkeamiin.

4.10 Vaikka komissio arvioi, että ehdotetun verkko- ja tietoturvadirektiivin soveltamisen kustannukset ovat vuosittain noin 2 miljardia euroa, jotka jakautuvat Euroopassa julkisen ja yksityisen sektorin kesken, komitea katsoo, että eräiden talousvaikeuksissa olevien jäsenvaltioiden on vaikea löytää tarvittavia investointeja säännösten noudattamiseksi. On tutkittava, miten verkko- ja tietoturvasäännösten noudattamiseen voitaisiin antaa tukea monivuotisesta rahoituskehyksestä sekä erilaisista välineistä, kuten Euroopan aluekehitysrahastosta (EAKR) ja kenties sisäisen turvallisuuden rahastosta.

Bryssel 22. toukokuuta 2013

Euroopan talous- ja sosiaalikomitean puheenjohtaja

Henri MALOSSE