Euroopan unionin neuvosto

Bryssel, 17. toukokuuta 2021
(OR. en)

8640/21

Toimielinten välinen asia:
2020/0359(COD)

LIMITE

CYBER 138
JAI 523
DATAPROTECT 125
TELECOM 194
MI 332
CSC 190
CSCI 78

ILMOITUS

Lähettäjä:	Puheenjohtajavaltio
Vastaanottaja:	Pysyvien edustajien komitea / Neuvosto
Asia:	Ehdotus EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVIKSI toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta – Tilanneselvitys

Tämä selvitys on laadittu puheenjohtajavaltion vastuulla. Se ei rajoita yksittäisten jäsenvaltioiden mahdollisuutta tuoda esiin erityisiä näkökohtia tai lisäkannanottoja. Siinä selvitetään asiakohdassa mainittua ehdotusta koskevaa tähänastista työtä neuvoston valmisteluelimissä ja esitetään tilannekatsaus ehdotuksen käsittelyyn. Neuvostoa pyydetään panemaan merkille tämä tilannekatsaus.

I JOHDANTO

1. Komissio antoi 16. joulukuuta 2020 ehdotuksen direktiiviksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa (tarkistettu verkko- ja tietoturvadirektiivi)[1]. Sen tarkoituksena on korvata nykyinen verkko- ja tietoturvadirektiivi[2]. Direktiiviehdotus oli yksi niistä toimenpiteistä, joita esitettiin EU:n kyberturvallisuusstrategiassa digitaaliselle vuosikymmenelle[3] tarkoituksena vahvistaa häiriönsietokykyä kyberuhkia vastaan ja varmistaa, että kansalaiset ja yritykset voivat hyötyä luotettavista digitaaliteknologioista.

2. SEUT 114 artiklaan perustuvan ehdotuksen tarkoituksena on parantaa julkisten ja yksityisten toimijoiden, toimivaltaisten viranomaisten ja yleensäkin koko unionin häiriönsietokykyä ja kykyä vastata uhkiin. Ehdotuksessa laajennetaan huomattavasti nykyisen verkko- ja tietoturvadirektiivin soveltamisalaa, käsitellään toimitusketjujen turvallisuutta, tiukennetaan asetettavia kyberturvallisuusvaatimuksia ja sujuvoitetaan raportointivelvoitteita. Samalla otetaan käyttöön tiukempia valvontatoimenpiteitä ja täytäntöönpanon tiukempaa valvontaa. Se sisältää lisäksi säännöksiä, joissa käsitellään kyberturvallisuuskriisien hallintaan liittyvää, kansallisella ja unionin tasolla toteutettavaa tiedonvaihtoa ja yhteistyötä. Ehdotuksessa käsitellään myös verkkotunnusten rekisteröintitietoja sisältävien tietokantojen sääntelyä.

---

1 Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta, COM(2020)823 final.

2 Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa.

3 Asiak. 14133/20.

3. Euroopan parlamentissa ehdotuksen käsittelystä vastaa teollisuus-, tutkimus- ja energiavaliokunta, ja lausuntonsa siitä antavat ulkoasiainvaliokunta, sisämarkkina- ja kuluttajansuojavaliokunta, liikenne- ja matkailuvaliokunta ja kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunta. Ehdotuksen esittelijä on Bart Groothuis (Renew, Alankomaat). Puheenjohtajavaltio Portugali kävi 29. tammikuuta 2021 ehdotuksesta epävirallisen näkemysten vaihdon teollisuus-, tutkimus- ja energiavaliokunnan esittelijän kanssa. Sisämarkkina- ja kuluttajansuojavaliokunnan lausunnon esittelijän Morten Lokkegaardin (Renew, Tanska) edustajien kanssa puheenjohtajavaltio oli yhteydessä 12. huhtikuuta 2021. Teollisuus-, tutkimus- ja energiavaliokunnan yksikönpäällikön ja muiden toimihenkilöiden kanssa puheenjohtajavaltio Portugali kävi 16. huhtikuuta 2021 epävirallisen näkemysten vaihdon. Esittelijä esitteli 3. toukokuuta 2021 mietintöluonnoksensa teollisuus-, tutkimus- ja energiavaliokunnassa[4].

4. Euroopan talous- ja sosiaalikomitea antoi lausuntonsa 28. huhtikuuta 2021[5].

5. Pysyvien edustajien komitea päätti 3. helmikuuta 2021 kuulla ehdotuksesta Euroopan alueiden komiteaa[6]. Euroopan alueiden komitea ei ole toistaiseksi antanut lausuntoaan.

6. Euroopan tietosuojavaltuutettu antoi lausuntonsa 11. maaliskuuta 2021[7].

7. Eurooppa-neuvosto pyysi 26. helmikuuta 2021 antamassaan julkilausumassa[8] lainsäätäjiä edistämään ripeästi työtä etenkin tarkistetun verkko- ja tietoturvadirektiivin osalta.

---

4 2020/0359(COD).
5 TEN/730-EESC-2020.
6 5573/21.
7 Lausunto 5/2021 aiheesta "the Cybersecurity Strategy and the NIS 2.0 Directive".
8 https://www.consilium.europa.eu/fi/press/press-releases/2021/02/26/statement-of-the-members-of-the-european-council-25-26-february-2021/

8. EU:n kyberturvallisuusstrategiasta digitaaliselle vuosikymmenelle 22. maaliskuuta 2021 antamissaan päätelmissä[9] neuvosto totesi, että unionin kyberturvallisuutta koskeva kattava ja horisontaalinen lähestymistapa on tärkeä, ja tunnusti samalla täysimääräisesti jäsenvaltioiden toimivallan ja tarpeet, samoin kuin jatkuvan teknisen avun ja yhteistyön merkityksen jäsenvaltioiden valmiuksien kehittämisessä. Kyberuhkiin liittyvän toimintaympäristön kehityksen huomioon ottaen neuvosto pani merkille verkko- ja tietoturvadirektiiviin perustuvan uuden ehdotuksen direktiiviksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja muistutti tukevansa kansallisten kyberturvallisuuskehysten vahvistamista ja yhdenmukaistamista sekä jäsenvaltioiden välistä jatkuvaa yhteistyötä. Lisäksi neuvosto korosti tarvetta yhdenmukaistaa ja jäsennellä alakohtaista lainsäädäntöä tällä alalla.

II KÄSITTELY NEUVOSTON VALMISTELUELIMISSÄ

9. Neuvostossa ehdotusta tarkastellaan kyberkysymysten horisontaalisessa työryhmässä. Komissio esitteli työryhmän epävirallisessa videoneuvottelussa 17. joulukuuta 2020 uuden kyberturvallisuusstrategian ja ehdotuksen verkko- ja tietoturvadirektiivin tarkistamiseksi. Kattavampi komission esittely ehdotuksesta kuultiin 12. tammikuuta 2021.

10. Kyberkysymysten horisontaalisen työryhmän epävirallisessa videoneuvottelussa 19. tammikuuta 2021 puheenjohtajavaltio Portugali selvitti työmenetelmäänsä tarkistetusta verkko- ja tietoturvadirektiivistä käytäviä keskusteluja varten. Puheenjohtajavaltion suunnitelmiin kuului ehdotuksen huolellinen läpikäynti, jossa otettaisiin huomioon tarkistettuun direktiiviin sisältyvät merkittävät uudistukset ja jonka yhteydessä valtuuskunnat voisivat esittää huomautuksiaan ja kysymyksiään kirjallisesti, minkä jälkeen komissio esittäisi selvennyksiä.

[9] 6722/21.

11. Kyberkysymysten horisontaalisessa työryhmässä keskusteltiin lisäksi tarkistetun verkko- ja tietoturvadirektiivin vuorovaikutuksesta alakohtaisen lainsäädännön, kuten kriittisten toimijoiden häiriönsietokykyä koskevan direktiivin ja rahoitusalan digitaalista häiriönsietokykyä koskevan asetuksen, kanssa. Komissio (muuttoliike- ja sisäasioiden pääosasto) esitteli uutta ehdotusta kriittisten toimijoiden häiriönsietokykyä koskevaksi asetukseksi ja toi siinä yhteydessä esiin pääkohdat ehdotuksen vuorovaikutuksesta tarkistetun verkko- ja tietoturvadirektiivin kanssa. Kyberkysymysten horisontaalisen työryhmän kokouksissa käsiteltiin myös yhteyksiä rahoitusalan digitaalista häiriönsietokykyä koskevaan asetusehdotukseen tarkastelemalla tausta-asiakirjaa, jonka oli laatinut kyseisestä ehdotuksesta käytävistä neuvotteluista vastaavan finanssipalvelutyöryhmän puheenjohtaja, sekä epävirallista asiakirjaa, jonka kolme jäsenvaltiota esitti finanssipalvelutyöryhmän puitteissa verkko- ja tietoturvaviranomaisten ja kansallisen toimivaltaisen viranomaisen välisestä vastaavuudesta rahoitusalan digitaalista häiriönsietokykyä koskevan asetuksen yhteydessä. Kyberkysymysten horisontaalisen työryhmän puheenjohtaja selvitti lisäksi pelastuspalvelutyöryhmän kokouksessa tarkistetun verkko- ja tietoturvadirektiivin käsittelyn tilannetta. Puheenjohtajavaltio piti kyberkysymysten horisontaalisen työryhmän säännöllisesti ajan tasalla pelastuspalvelutyöryhmän ja finanssipalvelutyöryhmän käsittelemien asioiden yhteydessä käydyistä, tähän ehdotukseen liittyvistä keskusteluista. Puheenjohtajavaltio toi jälleen esiin, että kansallisella tasolla tarvitaan tiivistä koordinointia niiden eri ministeriöiden kesken, joiden toimialaan nämä säädökset pääasiassa kuuluvat.

12. Kyberkysymysten horisontaalinen työryhmä aloitti 2. ja 9. helmikuuta 2021 pidetyissä epävirallisissa videoneuvotteluissa ehdotuksen tarkastelun kahdesta ensimmäisestä artiklasta (direktiivin kohde ja soveltamisala) sekä liitteistä I ja II. Kyberkysymysten horisontaalisen työryhmän 2. helmikuuta pidetyssä kokouksessa komissio ja verkko- ja tietoturva-alan yhteistyöryhmän puheenjohtaja selvittivät asian käsittelyn tilannetta verkko- ja tietoturva-alan yhteistyöryhmässä, mukaan lukien sen roolia verkko- ja tietoturvadirektiivin täytäntöönpanon helpottamisessa. Tuossa kokouksessa Euroopan unionin kyberturvallisuusviraston (ENISA) pääjohtaja esitteli lisäksi viraston työohjelmaa, muun muassa tietoja verkko- ja tietoturvaan liittyviä investointeja koskevasta ENISAn tutkimuksesta ja viraston roolia tukemassa jäsenvaltioita ja EU:n toimielimiä verkko- ja tietoturvadirektiiviin liittyvän toimintapolitiikan ja ohjeistuksen täytäntöönpanossa. Näissä kokouksissa käytiin perusteellisia keskusteluja soveltamisalasta ja esitettiin kysymyksiä oikeasuhteisuudesta.

13. Kyberkysymysten horisontaalisen työryhmän 22. helmikuuta 2021 pidetyssä kokouksessa komissio esitteli vaikutustenarvioinnin verkko- ja tietoturvadirektiivin tarkistamisesta. Lisäksi jatkettiin ehdotuksen käsittelyä tarkastelemalla 3 ja 4 artiklaa (vähimmäistason yhdenmukaistaminen ja määritelmät).

14. Ehdotuksen alustavaa arviointia jatkettiin kyberkysymysten horisontaalisen työryhmän kokouksessa 2. maaliskuuta 2021 käymällä laajoja keskusteluja 5 artiklasta, joka koskee kansallisia kyberturvallisuusstrategioita, sekä 6 artiklasta, joka koskee komission kokouksessa seikkaperäisesti esittelemiä koordinoitua haavoittuvuuden ilmaisemista ja Euroopan haavoittuvuusrekisteriä.

15. Keskusteluja jatkettiin kyberkysymysten horisontaalisen työryhmän 9. maaliskuuta 2021 pidetyssä kokouksessa tarkastelemalla 7–11 artiklaa, jotka koskevat kyberturvallisuuden kriisinhallintapuitteita, kansallisia toimivaltaisia viranomaisia ja tarkistetun verkko- ja tietoturvadirektiivin mukaisia keskitettyjä yhteyspisteitä, tietoturvaloukkauksiin reagoivia ja niitä tutkivia yksiköitä (CSIRT) sekä niitä koskevia vaatimuksia, tehtäviä ja kansallisen tason yhteistyötä.

16. Kyberkysymysten horisontaalisen työryhmän 17. maaliskuuta 2021 pidetyssä ylimääräisessä kokouksessa käsiteltiin yhteistyötä käsittelevään III lukuun kuuluvia 12–16 artiklaa, jotka koskevat verkko- ja tietoturvan yhteistyöryhmää, CSIRT-verkostoa, Euroopan kyberkriisien yhteysorganisaatioiden verkostoa (EU-CyCLONe), raporttia kyberturvallisuuden tilasta unionissa sekä vertaisarviointeja. Erityisesti näistä artikloista esitettiin kysymyksiä ja selvennyksiä. Kokouksessa tarkasteltiin myös hallinnointia koskevaa 17 artiklaa, ja Europolin Euroopan verkkorikostorjuntakeskuksen (EC3) ehkäisy- ja valistusyksikön päällikkö selvitti lainvalvontaviranomaisten kantaa tarkistettuun verkko- ja tietoturvadirektiiviin.

17. Kyberkysymysten horisontaalisen työryhmän kokouksessa 24. maaliskuuta 2021 tarkasteltiin kyberturvallisuusriskien hallinta- ja raportointivelvoitteita käsittelevään IV lukuun kuuluvia 18 artiklaa (kyberturvallisuusriskien hallintatoimenpiteet), 19 artiklaa (kriittisiä toimitusketjuja koskevat EU:n koordinoidut riskinarvioinnit) ja 20 artiklaa (raportointivelvoitteet). Näistä 20 artiklan katsotaan kuuluvan tarkistetun verkko- ja tietoturvadirektiivin keskeisiin säännöksiin.

18. Kyberkysymysten horisontaalisen työryhmän kokouksessa 14. huhtikuuta 2021 tarkasteltiin 21 artiklaa (eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käyttö), 22 artiklaa (standardointi) ja 23 artiklaa (verkkotunnusten ja rekisteröintitietojen tietokannat) samoin kuin 24 ja 25 artiklaa (lainkäyttövalta ja rekisteröinti). Lisäksi kokouksessa keskusteltiin tietojenvaihtoa koskevasta V luvusta sekä valvontaa ja täytäntöönpanoa koskevasta VI luvusta. Jäsenvaltiot esittivät lukuisia huomautuksia ja kysymyksiä 29 ja 30 artiklasta niiden laajuuden ja yksityiskohtaisuuden vuoksi. Artikloista edellinen koskee valvontaa ja täytäntöönpanoa keskeisten toimijoiden ja jälkimmäinen tärkeiden toimijoiden osalta. Seikkaperäisiä huomautuksia ja kysymyksiä esitettiin myös hallinnollisia sakkoja koskevasta 31 artiklasta, henkilötietojen tietoturvaloukkaukseen johtavia rikkomisia koskevasta 32 artiklasta ja seuraamuksia koskevasta 33 artiklasta. Jäsenvaltiot pyysivät myös selvennystä keskinäistä avunantoa koskevaan 34 artiklaan.

19. Kyberkysymysten horisontaalinen työryhmä sai artiklojen läpikäynnin päätökseen 19. huhtikuuta pidetyssä kokouksessaan, jossa tarkasteltiin siirtymä- ja loppusäännöksiä koskevaa VII lukua (35–43 artikla).

20. Kokouksessaan 28. huhtikuuta 2021 kyberkysymysten horisontaalinen työryhmä tarkasteli johdanto-osaa ja sai näin koko ehdotuksen läpikäynnin päätökseen. Kyseessä oli ensimmäinen Portugalin puheenjohtajakaudella järjestetty kyberkysymysten horisontaalisen työryhmän fyysinen kokous, jossa käsiteltiin tarkistettua verkko- ja tietoturvadirektiiviä. Komissio oli esittänyt aiemmin 15. helmikuuta 2021 johdanto-osan kappaleiden ja asiaankuuluvien artiklojen vastaavuustaulukon.

21. Kyberkysymysten horisontaalinen työryhmä kävi kokouksessaan 5. toukokuuta 2021 alustavan näkemysten vaihdon ehdotuksen työstämisen aloittamiseksi. Käsittelyn edistämiseksi puheenjohtajavaltio on päättänyt, että laadintaprosessi aloitetaan käsittelemällä tarkistetun verkko- ja tietoturvadirektiivin vuorovaikutusta alakohtaisen lainsäädännön kanssa. Päätös perustui ehdotuksen läpikäynnin yhteydessä kyberkysymysten horisontaalisessa työryhmässä käytyihin keskusteluihin sekä siihen, että jäsenvaltiot olivat jo määritelleet tuon kysymyksen tärkeäksi, ottaen huomioon sitä koskeva erityismaininta EU:n kyberturvallisuusstrategiasta digitaaliselle vuosikymmenelle 22. maaliskuuta 2021 annetuissa neuvoston päätelmissä. Jäsenvaltioita on pyydetty toimittamaan tätä koskevia konkreettisia tekstiehdotuksia 14. päivään toukokuuta 2021 mennessä.

22. Portugalin puheenjohtajakaudella ehdotusta on esitelty ja käyty läpi 17:ssä kyberkysymysten horisontaalisen työryhmän kokouksessa. Muutamat jäsenvaltiot ovat esittäneet käsittelyn yhteydessä tarkasteluvaraumia ehdotukseen kokonaisuudessaan tai joihinkin sen osiin.

23. Puheenjohtajavaltio katsoo, että tarkistetun verkko- ja tietoturvadirektiivin huolellisen läpikäynnin ansiosta jäsenvaltiot ovat saaneet komissiolta yksityiskohtaisia selvityksiä tarkistettuun direktiiviin tehdyistä perustavanlaatuisista muutoksista ja samalla tilaisuuden tuoda esiin tärkeimmät ehdotukseen liittyvät epäilyksenaiheensa ja siten auttaa ja järkevöittää tulevaa työtä, jotta yleisnäkemys saataisiin muodostettua asianmukaisessa aikataulussa.

III ASIASISÄLTÖ

24. Samalla kun kyberkysymysten horisontaalisen työryhmän keskusteluissa on yleisesti ottaen suhtauduttu myönteisesti tarkistettuun verkko- ja tietoturvadirektiiviin, jäsenvaltiot ovat tuoneet esiin keskeisiä kysymyksiä ja epäilyksenaiheita, joita olisi pohdittava ehdotuksesta käytävissä neuvotteluissa.

25. Yksi keskusteluissa usein esillä olleista aiheista koskee tarkistetun verkko- ja tietoturvadirektiivin ja alakohtaisen lainsäädännön välistä vuorovaikutusta. Tähänastisissa keskusteluissa huomattava enemmistö jäsenvaltioista on todennut, että ehdotetun tarkistetun verkko- ja tietoturvadirektiivin on ehdottomasti katsottava muodostavan kyberturvallisuuden horisontaalisen kehyksen EU:ssa ja että sitä olisi käytettävä perusnormina kaiken asiaankuuluvan alakohtaisen lainsäädännön vähimmäistasoiselle yhdenmukaistamiselle.

26. Laajalti on kyseenalaistettu myös tarkistetun verkko- ja tietoturvadirektiiviin soveltamisalan huomattava laajentaminen: se, missä laajuudessa keskeiset ja tärkeät toimijat kuuluvat direktiivin soveltamisalaan, jäsenvaltioiden velvollisuus määritellä keskeiset ja tärkeät toimijat, seuraukset, joita aiheutuu kansallisten toimivaltaisten viranomaisten valmiuksiin valvoa näitä toimijoiden luetteloita, liitteiden yksityiskohtaiset erityismäärittelyt siitä, mitkä keskeiset ja tärkeät toimijat kuuluvat soveltamisalaan, esimerkiksi elintarvike- ja liikennealan laaja mukaanotto riippumatta siitä, mikä niiden merkitys on asiaankuuluvalla alalla, yhtenäisen kynnystason (size-cap) käyttöönoton rajoitukset erityisesti, kun on kyse toimijoista, jotka tarjoavat useampaa kuin yhtä palvelua, tai pienistä ja mikroyrityksistä, joilla on merkittäviä keskinäisiä riippuvuussuhteita muiden palvelujen kanssa, mikä johtaa ketjureaktiovaikutuksiin.

27. Jotkin jäsenvaltiot ovat myös ottaneet esiin sen, että yhtenäisen kynnystason kriteeri on ainoa arviointiperuste, jolla määritellään direktiivin soveltamisalaan luettavat keskeiset ja tärkeät toimijat. Ne pitävät parempana – kumulatiivisesti sovellettuna – riskiperusteista arviointitapaa tai kansallisella tasolla käyttöön otettavia laadullisia lisäkriteereitä. Komission selkeän kannan mukaan yhtenäisen kynnystason kriteeri on paras mahdollinen – vaikkei kenties ihanteellinen – arviointiväline, jolla voidaan puuttua nykyisestä verkko- ja tietoturvadirektiivistä johtuvaan määrittelymenettelyn tehottomuuteen ja välttää siten tulevan välineen soveltamisen hajanaisuus.

28. Jotkin jäsenvaltiot ovat kyseenlaistaneet sen, onko sisämarkkinoiden oikeusperustan eli SEUT 114 artiklan perusteella mahdollista lukea viranomaiset tarkistetun direktiivin soveltamisalaan. Kolme jäsenvaltiota on pyytänyt neuvoston oikeudelliselta yksiköltä kirjallista lausuntoa tästä kysymyksestä. Lisäksi on kyseenalaistettu kriteerit, joilla viranomaistoimijat määritellään (yhteinen tilastollisten alueyksiköiden nimikkeistö NUTS).

29. Useat jäsenvaltiot ovat tuoneet keskusteluissa esiin kansalliseen turvallisuuteen liittyvät huolenaiheet ja sen, että käytännössä tarkistetun direktiivin soveltamisalan ulkopuolelle jätetään julkiset toimijat, jotka osallistuvat yleisen turvallisuuden, puolustuksen ja kansallisen turvallisuuden ylläpitoon.

30. Jäsenvaltiot ovat myös ottaneet esiin eri rakenteiden, verkostojen ja mekanismien väliset yhteydet ja mahdolliset päällekkäisyydet kyberturvallisuuden alalla EU:n tasolla. Tämä huolenaihe on liittynyt erityisesti Euroopan kyberkriisien yhteysorganisaatioiden verkoston (EU-CyCLONe) käyttöönottoon ja lisäksi sellaisten tulevien ehdotusten ja/tai aloitteiden ennakointiin kuin turvaoperaatiokeskusten verkoston perustaminen tai ehdotus yhteisestä kyberturvallisuusyksiköstä.

31. Vertaisarviointien osalta jotkin jäsenvaltiot ovat kyseenalaistaneet niiden pakollisuuden ja mekanismin, jolla määritellään niissä sovellettavat menetelmät, samoin kuin tiedonvaihdon luottamuksellisuuden ja tietojen saatavuuden, sekä korostaneet kyseisten arviointien tekemiseen saatavilla olevien resurssien vähäisyyttä erityisesti pienemmissä jäsenvaltioissa.

32. Toimitusketjujen turvallisuuden osalta ja varsinkin tarkistettua direktiiviä koskevan ehdotuksen 18 artiklassa määriteltyjen kyberturvallisuusriskien hallintatoimenpiteiden sekä 19 artiklassa tarkoitettujen kriittisiä toimitusketjuja koskevien EU:n koordinoitujen riskinarviointien osalta komissio on todennut harkitsevansa tässä vaiheessa kokonaisvaltaista lähestymistapaa, myös mahdollisia uusia horisontaalisia sääntöjä, tarkoituksena parantaa kaikkien sisämarkkinoille saatettujen tuotteiden ja niihin liittyvien palvelujen kyberturvallisuutta.

33. Kuten edellä todettiin, jäsenvaltiot ovat esittäneet lukuisia kysymyksiä koordinoidusta haavoittuvuuden ilmaisemisesta ja ENISAn perustamaksi aiotusta Euroopan haavoittuvuusrekisteristä. Komissio selvitti näitä kahta asiaa yksityiskohtaisesti ja totesi, että niitä kehitetään tämän alan nykyisten kansallisten ja kansainvälisten parhaiden käytäntöjen ja menettelyjen pohjalta.

34. Raportoinnin osalta jäsenvaltiot esittivät huomautuksia hallinnollisesta rasitteesta, siitä johtuvista vaikutuksista vastuukysymyksiin, ilmoittamiselle asetetusta 24 tunnin määräajasta ja raportoinnista, joka koskee merkittäviä kyberuhkia ja läheltä piti -tilanteita.

35. Moni jäsenvaltio on myös viitannut käytännön ja oikeudellisen tason pohdintoihin, jotka liittyvät eIDAS-asetuksen (asetus sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla) ja eurooppalaisen sähköisen viestinnän säännöstön asiaankuuluvien säännösten kumoamiseen, ja pyytänyt Euroopan komissiolta lisäselvennyksiä näihin seikkoihin.

36. Jäsenvaltiot ovat myös kyseenalaistaneet sen, että tarkistetussa verkko- ja tietoturvadirektiivissä siirretään komissiolle laajasti valtaa antaa delegoituja ja täytäntöönpanosäädöksiä. Tähän huolenaiheeseen liittyvät pohdinnat yhteydestä kyberturvallisuussäädökseen sertifioinnin osalta.

IV LOPUKSI

37. Puheenjohtajavaltio ilmaisee vilpittömän kiitollisuutensa komission omistautuneesta osallistumisesta huolellisen läpikäynnin vaiheessa, jossa komissio on pyrkinyt antamaan vastauksia ja selvennyksiä jäsenvaltioiden keskusteluissa esittämiin kysymyksiin ja huomautuksiin.

38. Puheenjohtajavaltio panee merkille myös jäsenvaltioiden sitoutumisen käytyyn menettelyyn, mistä oli osoituksena käsittelyn kuluessa esitetyt lukuisat yksityiskohtaiset huomautukset ja kysymykset. Puheenjohtajavaltio on täysin tietoinen jäsenvaltioiden merkittävistä toimista, joilla on koordinoitu asian käsittelyä kansallisella tasolla eri ministeriöiden välillä.

39. Edellä kuvattujen kyberkysymysten horisontaalisen työryhmän keskustelujen perusteella puheenjohtajavaltio katsoo, että ehdotetun verkko- ja tietoturvadirektiivin tietyt ratkaisevan tärkeät seikat eivät ole vielä riittävän valmiita, jotta niiden työstämisestä jäsenvaltioiden kesken käytävissä keskusteluissa voitaisiin edistyä tuloksellisesti. Sen vuoksi puheenjohtajavaltio arvelee, että ehdotuksen käsittelyssä voitaisiin edetä käsittelemällä kysymystä tarkistetun verkko- ja tietoturvadirektiivin vuorovaikutuksesta alakohtaisen lainsäädännön kanssa. Siten saataisiin myös tarvittavaa selvyyttä tarkistetun verkko- ja tietoturvadirektiivin ja muiden säädösten vastaavien asiaankuuluvien säännösten välillä. Viimeksi mainittuihin, parhaillaan ja/tai pian neuvoston valmisteluelimissä käsiteltäviin säädöksiin kuuluvat muun muassa rahoitusalan digitaalista häiriönsietokykyä ja kriittisten toimijoiden häiriönsietokykyä koskevat asetusehdotukset. On syytä muistaa, että vuorovaikutuskysymykseen liittyvien säädösten neuvotteluprosessit niistä vastaavissa neuvoston valmisteluelimissä ovat keskenään eri vaiheissa. Käsittelemällä kysymys vuorovaikutuksesta asiaankuuluvan alakohtaisen lainsäädännön kanssa heti tarkistetun verkko- ja tietoturvadirektiivin laadinnan alkuvaiheessa voitaisiin saada eri säädöksistä käytävät neuvottelut etenemään sujuvasti, riippumattomasti ja vakaalta pohjalta.

40. Nykyisen suunnitelman perusteella Portugalin puheenjohtajakaudella tulee kesäkuun loppuun 2021 mennessä käydyksi 19 kyberkysymysten horisontaalisen työryhmän kokousta, joissa on käsitelty tarkistettua verkko- ja tietoturvadirektiiviä. Puheenjohtajavaltio katsoo, että se on noudattanut täysin Eurooppa-neuvoston kokouksessaan 26. helmikuuta esittämää pyyntöä edistää ripeästi työtä tarkistetun verkko- ja tietoturvadirektiivin osalta. Tämän se on tehnyt järjestämällä tarkistetun direktiivin huolellisen ja mielestään tarpeellisen läpikäynnin ja käynnistämällä sen jälkeen laadintamenettelyn.

41. Puheenjohtajavaltio Portugali on sitoutunut työskentelemään tiiviisti seuraavan puheenjohtajavaltion Slovenian kanssa tarkoituksena helpottaa keskustelujen jatkamista kyberkysymysten horisontaalisessa työryhmässä ja varmistaa ehdotuksen käsittelyn sujuva eteneminen neuvostossa.

42. Edellä esitetyn perusteella pysyvien edustajien komiteaa ja neuvostoa pyydetään panemaan merkille edistyminen kyseessä olevan direktiiviehdotuksen tarkastelussa.