Euroopa Liidu
Nõukogu

Brüssel, 17. mai 2021
(OR. en)

8640/21

Institutsioonidevaheline dokument: 2020/0359(COD)

LIMITE

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

MÄRKUS

Saatja:	Eesistujariik
Saaja:	Alaliste esindajate komitee / nõukogu
Teema:	Ettepanek: EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv (EL) 2016/1148 – Eduaruanne

Käesolev aruanne on koostatud eesistujariigi vastutusel ning ei mõjuta eri liikmesriikidele konkreetset huvi pakkuvaid teemasid ega nende edasist panust. Selles antakse ülevaade nõukogu ettevalmistavates organites seni tehtud tööst ning kirjeldatakse eespool nimetatud ettepaneku läbivaatamise seisu. Nõukogul palutakse aruanne teadmiseks võtta.

I. SISSEJUHATUS

1. Komisjon võttis 16. detsembril 2020 vastu direktiivi ettepaneku, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus (muudetud küberturvalisuse direktiiv, ehk „küberturvalisuse 2. direktiiv“),[1] et asendada praegune võrgu- ja infosüsteemide turvalisust käsitlev direktiiv („küberturvalisuse direktiiv“)[2]. Ettepanek on üks meetmetest, mis on ette nähtud ELi küberturvalisuse strateegias digikümnendi jaoks,[3] et suurendada küberohtudega seotud vastupidavusvõimet ning tagada, et kodanikud ja ettevõtjad saaksid kasutada usaldusväärset digitehnoloogiat.

2. ELi toimimise lepingu artiklil 114 põhineva ettepaneku eesmärk on täiendavalt suurendada avaliku ja erasektori üksuste, pädevate asutuste ja liidu kui terviku vastupidavusvõimet ja intsidentidele reageerimise suutlikkust. Ettepanekuga laiendatakse märkimisväärselt praeguse küberturvalisuse direktiivi kohaldamisala, käsitletakse tarneahelate turvalisust, tugevdatakse kehtestatud turvanõudeid ja ühtlustatakse aruandluskohustusi, kehtestades samal ajal rangemad järelevalvemeetmed ja jõulisema täitmise. Samuti sisaldab see sätteid küberkriiside ohjamist käsitleva teabe jagamise ja koostöö kohta liikmesriikide ja liidu tasandil. Ettepanekuga nähakse ette ka domeeninimede registreerimisandmete andmebaaside reguleerimine.

---

1 Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega tunnistatakse kehtetuks direktiiv (EL) 2016/1148, COM(2020)823 final.

2 Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus.

3 Dok 14133/20.

3. Euroopa Parlamendis vastutab ettepaneku eest tööstuse, teadusuuringute ja energeetikakomisjon (ITRE), kusjuures arvamuse esitavad väliskomisjon (AFET), siseturu- ja tarbijakaitsekomisjon (IMCO), transpordi- ja turismikomisjon (TRAN) ning kodanikuvabaduste, justiits- ja siseasjade komisjon (LIBE). Kõnealuse eelnõu raportöör on Bart Groothuis (Renew, Madalmaad). 29. jaanuaril 2021 pidas eesistujariik Portugal toimiku üle mitteametliku arvamuste vahetuse ITRE-komisjoni raportööriga. 12. aprillil 2021 suhtles eesistujariik IMCO-komisjoni arvamuse koostaja Morten Lokkegaardi (Renew, Taani) esindajatega. 16. aprillil pidas eesistujariik Portugal toimiku üle mitteametliku arvamuste vahetuse ITRE-komisjoni juhataja ja teiste administraatoritega. Raportöör esitas oma raporti projekti ITRE-komisjonile 3. mail 2021[4].

4. Euroopa Majandus- ja Sotsiaalkomitee võttis oma arvamuse vastu 28. aprillil 2021[5].

5. 3. veebruaril 2021 otsustas alaliste esindajate komitee konsulteerida ettepaneku osas Regioonide Komiteega[6]. Seni ei ole Regioonide Komitee oma arvamust esitanud.

6. Euroopa andmekaitseinspektor võttis oma arvamuse vastu 11. märtsil 2021[7].

7. Oma 26. veebruari 2021. aasta avalduses[8] kutsus Euroopa Ülemkogu kaasseadusandjaid üles jätkama kiiresti tööd, eelkõige seoses võrgu- ja infosüsteemide turvalisust käsitleva muudetud direktiiviga (küberturvalisuse 2. direktiiv).

---

4 2020/0359(COD).
5 TEN/730-EESC-2020.
6 5573/21.
7 Arvamus 5/2021, mis käsitleb küberturvalisuse strateegiat ja küberturvalisuse 2. direktiivi (NIS 2.0).
8 https://www.consilium.europa.eu/en/press/press-releases/2021/02/26/statement-of-the-members-of-the-european-council-25-26-february-2021/

8. Oma 22. märtsi 2021. aasta järeldustes,[9] milles käsitletakse Euroopa Liidu küberturvalisuse strateegiat digikümnendi jaoks, tunnistab nõukogu, kui oluline on liidus küberturvalisuse puhul järgida terviklikku ja horisontaalset lähenemisviisi, austades samal ajal täielikult liikmesriikide pädevusi ja vajadusi, ning kui oluline on jätkuvalt toetada tehnilist abi ja koostööd liikmesriikide suutlikkuse arendamiseks. Nõukogu võttis küberohtude arengut arvesse võttes teadmiseks küberturvalisuse direktiivile tugineva uue direktiivi ettepaneku, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ning kordas oma toetust riiklike küberturvalisuse raamistike tugevdamisele ja ühtlustamisele ning liikmesriikidevahelisele püsivale koostööle. Lisaks rõhutas nõukogu sellele vajadust kõnealuse valdkonna õigusaktide vastavusse viimise ja sidususe järele.

II. TÖÖ NÕUKOGU ETTEVALMISTAVATES ORGANITES

9. Nõukogus toimub ettepaneku läbivaatamine horisontaalses küberküsimuste töörühmas (edaspidi „HWPCI“). Komisjon tutvustas uut küberturvalisuse strateegiat ja küberturvalisuse direktiivi läbivaatamise ettepanekut HWPCI mitteametlikul videokonverentsil 17. detsembril 2020. Seejärel esitas komisjon ettepaneku kohta põhjalikuma ülevaate 12. jaanuaril 2021.

10. HWPCI 19. jaanuari 2021. aasta mitteametlikul videokonverentsil tutvustas eesistujariik Portugal oma töömetoodikat seoses küberturvalisuse 2. direktiivi üle peetavate aruteludega. Võttes arvesse muudetud direktiivis sisalduvaid olulisi uuendusi, oli eesistujariik kavandanud ettepaneku põhjaliku läbivaatamise, võimaldades delegatsioonidel esitada märkusi ja küsimusi kirjalikult, millele järgneksid komisjoni selgitused.

[9] 6722/21.

11. Lisaks arutas HWPCI muudetud küberturvalisuse direktiivi koostoimet valdkondlike õigusaktidega, eelkõige direktiiviga kriitilise tähtsusega üksuste vastupidavusvõime kohta ja määrusega finantssektori digitaalse tegevuskerksuse kohta. Komisjon (DG HOME) tutvustas kriitilise tähtsusega üksuste vastupidavusvõime direktiivi uut ettepanekut, rõhutades peamisi koostoimeelemente küberturvalisuse 2. direktiiviga. HWPCI koosolekutel käsitleti ka seoseid kavandatava finantssektori digitaalse tegevuskerksuse määrusega, võttes aluseks (finantssektori digitaalse tegevuskerksuse määruse eest vastutava) finantsteenuste töörühmas eesistujariigi koostatud aruteludokumendi ning samuti kolme liikmesriigi poolt finantsteenuste töörühma raames esitatud mitteametliku dokumendi, milles käsitleti „võrgu- ja infoturbeasutuste ja riiklike pädevate asutuste vahelist seost finantssektori digitaalse tegevuskerksuse määruse raames“. HWPCI eesistuja osales ka elanikkonnakaitse töörühma koosolekul, et anda ülevaade küberturvalisuse 2. direktiivi üle peetavate arutelude seisust. Eesistujariik andis HWPCI-le korrapäraselt teavet elanikkonnakaitse töörühmas ja finantsteenuste töörühmas nende vastavate toimikute üle toimuvate asjakohaste arutelude arengust, korrates vajadust nende eelnõudega seotud erinevate vastutavate ministeeriumide vahelise tiheda koordineerimise järele riiklikul tasandil.

12. 2. ja 9. veebruaril 2021 toimunud mitteametlikel videokonverentsidel alustas HWPCI ettepaneku kahe esimese artikli („Reguleerimisese“ ja „Kohaldamisala“) ning I ja II lisa läbivaatamist. 2. veebruaril toimunud koosolekul tegid komisjon ning võrgu- ja infoturbe koostöörühma esimees HWPCI-le ülevaate võrgu- ja infoturbe koostöörühmas tehtud töö seisu, sealhulgas koostöörühma rollist küberturvalisuse direktiivi rakendamise hõlbustamisel. Eespool nimetatud koosolekul tutvustas ENISA tegevdirektor ka ameti tööprogrammi, andes ühtlasi teavet ENISA võrgu- ja infoturbe investeeringute uuringu kohta ning ENISA rolli kohta liikmesriikide ja ELi institutsioonide toetamisel küberturvalisuse direktiiviga seotud poliitika ja nõuannete rakendamisel. Nimetatud koosolekutel peeti sisulisi arutelusid kohaldamisala üle ja tõstatati küsimusi proportsionaalsuse kohta.

13. HWPCI 22. veebruari 2021. aasta koosolekul tutvustas komisjon küberturvalisuse direktiivi läbivaatamise mõjuhinnangut ning jätkati ettepanekut käsitlevaid arutelusid artiklite 3 ja 4 („Minimaalne ühtlustamine“ ja „Mõisted“) üle.

14. 2. märtsil 2021 jätkati HWPCI koosolekul ettepaneku esialgset hindamist, pidades põhjalikke arutelusid artiklite 5 ja 6 („Riiklik küberturvalisuse strateegia“ ja „Nõrkuste koordineeritud avalikustamine ja Euroopa nõrkuste register“) üle, kus komisjon tutvustas põhjalikult nõrkuste koordineeritud avalikustamist ja ELi nõrkuste registrit.

15. HWPCI 9. märtsi 2021. aasta koosolekul jätkusid arutelud artiklite 7–11 üle, mis käsitlevad küberturvalisuse alaseid kriisiohjeraamistikke, riiklikke pädevaid asutusi ja ühtseid kontaktpunkte muudetud küberturvalisuse direktiivi alusel ning küberturbe intsidentide lahendamise üksusi (CSIRTid), sealhulgas neile esitatavaid nõudeid, nende ülesandeid ja koostööd riiklikul tasandil.

16. Oma erakorralisel koosolekul 17. märtsil 2021 arutas HWPCI artikleid 12–16 (III peatükk „Koostöö“), mis käsitlevad võrgu- ja infoturbe koostöörühma, CSIRTide võrgustikku, Euroopa küberkriisiga tegelevate kontaktasutuste võrgustikku (EU-CyCLONe), aruannet küberturvalisuse olukorra kohta liidus ning vastastikuste hindamiste küsimust. Eelkõige tõstatati mitmeid küsimusi ja paluti selgitusi nende artiklite kohta. Lisaks Europoli küberkuritegevuse vastase võitluse Euroopa keskuse (EC3) ennetamise ja teavitamise rühma juhi ettekandele, mis käsitles õiguskaitseasutuste arvamust muudetud küberturvalisuse direktiivi kohta, käsitleti sel koosolekul ka artiklit 17 „Juhtimine“.

17. Oma 24. märtsi 2021. aasta koosolekul analüüsis HWPCI IV peatükki „Küberturvalisusega seotud riskijuhtimis- ja teatamiskohustused“, nimelt artikleid 18 („Küberturvalisusega seotud riskijuhtimismeetmed“), 19 („Kriitilise tähtsusega tarneahelate ELi koordineeritud riskihindamised“) ja 20 („Teatamiskohustus“), kusjuures viimast peetakse üheks küberturvalisuse 2. direktiivi põhisätteks.

18. Oma 14. aprilli koosolekul käsitles HWPCI artikleid 21 („Euroopa küberturvalisuse sertifitseerimise kavade kasutamine“), 22 („Standardimine“) ja 23 („Domeeninimede ja registreerimisandmete andmebaasid“) samuti neile järgnevaid artikleid 24 ja 25 („Jurisdiktsioon ja registreerimine“). Koosolekul arutati ka V ja VI peatükki (vastavalt teabevahetuse ning järelevalve ja täitmise tagamise kohta). Nende ulatuse ja üksikasjalikkuse tõttu esitasid liikmesriigid arvukalt märkusi ja küsimusi artiklite 29 ja 30 kohta, milles käsitletakse järelevalve ja täitmise tagamist vastavalt elutähtsate üksuste ja oluliste üksuste puhul. Samuti esitati sisulisi märkusi ja küsimusi seoses artiklitega 31, 32 ja 33, mis käsitlevad haldustrahve, isikuandmete väärkasutamisega seotud rikkumisi ning karistusi. Liikmesriigid palusid ka täiendavaid selgitusi vastastikust abi käsitleva artikli 34 kohta.

19. HWPCI käsitles VII peatükki ülemineku- ja lõppsätete kohta (artiklid 35–43) oma 19. aprilli koosolekul, lõpetades seega artiklite läbivaatamise.

20. Oma 28. aprilli 2021. aasta koosolekul käsitles HWPCI põhjendusi, viies sellega ettepaneku läbivaatamise lõpule. Tegemist oli Portugali eesistumise ajal toimunud esimese HWPCI füüsilise koosolekuga küberturvalisuse 2. direktiivi teemal. Komisjon oli põhjenduste ja teksti asjakohaste artiklite vastavustabeli esitanud juba 15. veebruaril 2021.

21. Oma 5. mai 2021. aasta koosolekul pidas HWPCI esimese arvamuste vahetuse, pidades silmas töö alustamist eelnõu tekstiga. Eelnõu menetlemisel edusammude saavutamiseks otsustas eesistujariik alustada tööd tekstiga selles osas, mis puudutab muudetud küberturvalisuse direktiivi ja asjakohaste valdkondlike õigusaktide koostoimet. See otsus tehti dokumendi läbivaatamise käigus HWPCI-s peetud arutelude põhjal, samuti asjaolu põhjal, et liikmesriigid olid selle küsimuse juba oluliseks tunnistanud, võttes arvesse konkreetset viidet nõukogu 22. märtsi järeldustes, milles käsitletakse Euroopa Liidu küberturvalisuse strateegiat digikümnendi jaoks. Liikmesriikidelt oodatakse selles küsimuses konkreetseid tekstiettepanekuid kuni 14. maini 2021.

22. Seni on HWPCI Portugali eesistumise ajal pühendanud ettepaneku tutvustamisele ja läbivaatamisele 17 koosolekut. Nende arutelude käigus on mõned liikmesriigid esitanud analüüsi reservatsiooni kogu ettepaneku või selle teatavate osade suhtes.

23. Eesistujariik on veendunud, et küberturvalisuse 2. direktiivi hoolikas läbivaatamine on võimaldanud liikmesriikidel saada komisjonilt üksikasjalikke selgitusi muudetud direktiivi põhjalike muudatuste kohta ning samal ajal tuua välja oma peamised ettepanekuga seotud mured, hõlbustades seeläbi edasist tööd ja muutes eelnõu sujuvamaks, et leppida õigeaegselt kokku üldises lähenemisviisis.

III. SISU

24. HWPCI-s peetud arutelude käigus liikmesriigid küll üldjoontes tervitasid muudetud võrgu- ja infoturbe direktiivi, kuid tõstatasid mitu olulist teemat ja mureküsimust, mida tuleks ettepaneku üle peetavatel läbirääkimistel kaaluda.

25. Üks arutelude käigus korduvalt tõstatatud küsimustest puudutas muudetud küberturvalisuse direktiivi ja valdkondlike õigusaktide koostoimet. Seni peetud arutelude käigus on valdav enamik liikmesriike märkinud, et muudetud küberturvalisuse direktiivi ettepanekut tuleb pidada ELi küberturvalisuse horisontaalseks raamistikuks ning et see peaks olema kõigi selle valdkonna asjaomaste valdkondlike õigusaktide minimaalse ühtlustamise alusstandard.

26. Teiseks väljendati mitu korda muret seoses muudetud küberturvalisuse direktiivi kohaldamisala märkimisväärse laiendamisega: direktiivi kohaldamisalasse kuuluvate elutähtsate ja oluliste üksuste määr; liikmesriikide kohustused elutähtsate ja oluliste üksuste kindlaksmääramisel; mõju riiklike pädevate asutuste suutlikkusele neid üksuste loetelusid jälgida; lisade üksikasjad, milles on täpselt välja toodud kohaldamisalasse kuuluvad elutähtsad ja olulised üksused, nt toidu- ja transpordisektori ulatuslik kaasamine, olenemata nende tähtsusest asjaomase sektori jaoks; suuruse ülempiiri kehtestamise piirangud, eriti kui tegemist on üksustega, kes osutavad rohkem kui üht teenust, või väikeste ja mikroettevõtjatega, kes on tugevas vastastikuses sõltuvussuhtes teiste teenustega, millega kaasneb doominoefekt.

27. Kolmandaks tõstatasid mõned liikmesriigid ka suuruse ülempiiri kriteeriumide küsimuse, mis on ainus element direktiivi kohaldamisalasse kuuluvate elutähtsate ja oluliste üksuste identifitseerimisel. Need liikmesriigid eelistaksid kumulatiivset, riskipõhist lähenemisviisi või täiendavaid riiklikul tasandil kehtestatud kvalitatiivseid kriteeriume. Komisjon on selgelt väljendanud, et kuigi suuruse ülempiiri kriteeriumid ei pruugi olla ideaalsed, on need siiski kõige optimaalsemad praegusest küberturvalisuse direktiivist tuleneva ebatõhusa identifitseerimisprotsessi käsitlemiseks, vältides seeläbi killustumist tulevase vahendi kohaldamisel.

28. Mõned liikmesriigid on seadnud kahtluse alla, kas ühtse turu õiguslik alus (ELi toimimise lepingu artikkel 114) võimaldab lisada muudetud direktiivi kohaldamisalasse ka avaliku halduse. Kolm liikmesriiki väljendasid huvi saada nõukogu õigustalituse käest kirjalik arvamus kõnealuses küsimuses. Lisaks seati kahtluse alla avaliku halduse üksuste identifitseerimise kriteeriumid (ühine statistiliste territoriaalüksuste liigitus – NUTS).

29. Viies küsimus, millele mitu liikmesriiki arutelude käigus tähelepanu juhtis, on seotud riiklike julgeolekuprobleemidega ning avaliku julgeoleku, riigikaitse ja riigi julgeoleku tagamisega tegelevate avaliku sektori asutuste väljajätmisega muudetud direktiivi kohaldamisalast.

30. Muud liikmesriikide tõstatatud huviküsimused olid seotud ELi tasandi küberturvalisuse valdkonna erinevate struktuuride, võrgustike ja mehhanismide vaheliste seoste ja võimaliku dubleerimisega, eelkõige seoses EU CyCLONe kasutuselevõtuga, kuid mõeldi ka sellistele tulevastele ettepanekutele ja/või algatustele nagu turbekeskuste võrgustiku loomine või ühise küberüksuse ettepanek.

31. Seoses vastastikuste hindamiste kasutuselevõtmisega on mõned liikmesriigid seadnud kahtluse alla kõnealuse hindamise kohustuslikkuse ja vastava metoodika kehtestamise mehhanismi, tõstatanud küsimusi vahetatava teabe konfidentsiaalsuse ja kättesaadavuse kohta ning rõhutanud selliste hindamiste läbiviimiseks kättesaadavate ressursside nappust, eelkõige väiksemates liikmesriikides.

32. Seoses tarneahela turvalisusega, täpsemalt artiklis 18 kindlaks määratud küberturvalisuse riskijuhtimismeetmetega, ja muudetud direktiivi ettepaneku artiklis 19 käsitletud kriitilise tähtsusega tarneahelate ELi koordineeritud riskihindamistega on komisjon märkinud, et kaalub praegu terviklikku lähenemisviisi, sealhulgas võimalikke uusi horisontaalseid reegleid, et parandada kõigi siseturul pakutavate ühendatud toodete ja nendega seotud teenuste küberturvalisust.

33. Nagu eespool mainitud, tõstatasid liikmesriigid mitu küsimust seoses nõrkuste koordineeritud avalikustamise ja Euroopa nõrkuste registri loomisega ENISA poolt. Komisjon tegi nende kahe küsimuse kohta üksikasjaliku ettekande, märkides, et nende väljatöötamisel lähtutakse selles valdkonnas olemasolevatest riiklikest ja rahvusvahelistest parimatest tavadest ja menetlustest.

34. Aruandlusega seonduvalt väljendasid liikmesriigid oma seisukohti halduskoormuse, sellest tuleneva vastutuse mõju, 24-tunnise teatamistähtaja ning aruandluse kohta seoses oluliste küberohtude ja ohuolukordadega.

35. Paljud liikmesriigid, kes on ka palunud Euroopa Komisjonilt nende punktide kohta täiendavaid selgitusi, on osutanud praktilistele ja õiguslikele kaalutlustele seoses viitega eIDASe määruse ja Euroopa elektroonilise side seadustiku asjakohaste sätete kehtetuks tunnistamise kohta.

36. Liikmesriigid on samuti seadnud kahtluse alla muudetud küberturvalisuse direktiivis komisjonile ette nähtud ulatuslikud volitused seoses delegeeritud õigusaktide ja rakendusaktide vastuvõtmisega. See hõlmas küsimusi selle kohta, millised seosed on sertifitseerimise osas küberturvalisuse määrusega.

IV. KOKKUVÕTE

37. Eesistujariik väljendab siirast tunnustust komisjoni pühendumusele põhjaliku läbivaatamisprotsessi käigus, püüdes anda vastuseid ja selgitusi liikmesriikide poolt arutelude käigus esitatud küsimustele ja märkustele.

38. Lisaks tunnustab eesistujariik liikmesriikide pühendumust sellele protsessile, mida tõendavad arutelude käigus esitatud arvukad üksikasjalikud märkused ja küsimused. Eesistujariik on täiesti teadlik olulistest jõupingutustest, mida liikmesriigid on teinud seoses eelnõu ministeeriumidevahelise koordineerimisega riiklikul tasandil.

39. Tuginedes eespool kirjeldatud HWPCI aruteludele, on eesistujariik veendunud, et küberturvalisuse direktiivi muudetud ettepaneku teatavaid olulisi elemente ei ole veel piisavalt arutatud, et teha liikmesriikidevaheliste läbirääkimiste käigus piisavaid edusamme nende sõnastamiseks. Seetõttu arvab eesistujariik, et muudetud küberturvalisuse direktiivi ja asjakohaste valdkondlike õigusaktide koostoime küsimuse lahendamine võimaldab ettepanekuga edasi liikuda ning aitab kaasa vajaliku selguse saavutamisele küberturvalisuse 2. direktiivi vastavate sätete ja muude praegu ja/või peatselt nõukogu ettevalmistavates organites arutatavate õigusaktide vahel (eelkõige, kuid mitte ainult finantssektori digitaalse tegevuskerksuse määrus ja kriitilise tähtsusega üksuste vastupidavusvõime direktiiv). Samuti tuleb meeles pidada, et iga sellisest koostoimest mõjutatud õigusakt on nõukogu pädevates ettevalmistavates organites toimuvate läbirääkimiste eri etappides. Asjaomaste valdkondlike õigusaktidega koostoime küsimuse käsitlemine alates küberturvalisuse 2. direktiivi koostamise protsessi algusest peaks võimaldama läbirääkimiste alustamist eri õigusaktide üle sujuvalt, sõltumatult ja kindlal alusel.

40. Eesistujariigi Portugali praeguse kava kohaselt peaks HWPCI kuni 2021. aasta juuni lõpuni pidama kokku 19 muudetud küberturvalisuse direktiivile pühendatud koosolekut. Eesistujariik leiab, et kuna nõukogu on viinud lõpule muudetud direktiivi põhjaliku ja meie arvates vajaliku läbivaatamise, ning on seejärel algatanud teksti koostamise protsessi, on ta täielikult vastanud Euroopa Ülemkogu 26. veebruari kohtumisel esitatud üleskutsele jätkata kiiresti tööd võrgu- ja infosüsteemide turvalisust käsitleva muudetud direktiiviga.

41. Eesistujariik Portugal on pühendunud tihedale koostööle järgmise eesistujariigi Sloveeniaga, et hõlbustada arutelude jätkamist HWPCI-s ja tagada dokumendi sujuv menetlemine nõukogus.

42. Eespool toodut arvesse võttes palutakse alaliste esindajate komiteel ja nõukogul võtta teadmiseks kavandatava direktiivi läbivaatamisel tehtud edusammud.