EUROOPA
KOMISJON

Brüssel, 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV

meetmete kohta, millega tagada võrgu- ja infoturbe ühtlaselt kõrge tase kogu Euroopa Liidus

{SWD(2013) 31 final}
{SWD(2013) 32 final}

SELETUSKIRI

Käesolevas ettepanekus käsitletava direktiivi eesmärk on tagada võrgu- ja infoturbe ühtlaselt kõrge tase. See tähendab interneti ning ühiskonna ja majanduse toimimist toetavate privaatsete võrkude ja infosüsteemide turvalisuse parandamist. Selle eesmärgi saavutamiseks nõutakse liikmesriikidelt suuremat valmisolekut ja paremat omavahelist koostööd ning kohustatakse kriitiliste infrastruktuuride, näiteks energeetika- ja transpordisektori operaatoreid, peamisi infoühiskonnateenuste (e-kaubanduse platvormide, sotsiaalvõrgustike jms) pakkujaid ja haldusasutusi astuma vajalikke samme, et hallata turvariske ja teatada tõsistest intsidentidest riigi pädevatele asutustele.

Käesolev ettepanek esitatakse koos komisjoni ning liidu välisasjade ja julgeolekupoliitika kõrge esindaja ühisteatisega Euroopa küberjulgeoleku strateegia kohta. Strateegia eesmärk on tagada digitaalse keskkonna turvalisus ja usaldusväärsus ning edendada ja kaitsta samas põhiõigusi ja muid ELi põhiväärtusi. Käesolev ettepanek on strateegia peamine meede. Strateegia muud meetmed keskenduvad selles valdkonnas teadlikkuse suurendamisele, küberturbetoodete ja -teenuste siseturu väljakujundamisele ning teadus- ja arendustegevuse investeeringute soodustamisele. Neid meetmeid täiendavad muud meetmed, mille eesmärk on tõhustada võitlust küberkuritegevusega ja luua ELi rahvusvaheline küberturbe poliitika.

1.1. Ettepaneku põhjused ja eesmärgid

Võrgu- ja infoturbe olulisus meie majanduse ja ühiskonna jaoks kasvab ning lisaks on see hädavajalik eeltingimus, et luua ülemaailmse teenuskaubanduse jaoks usaldusväärne keskkond. Infosüsteeme võivad aga kahjustada turvaintsidendid, olgu nende põhjuseks siis inimlik eksimus, looduslik protsess, tehniline rike või pahatahtlik rünne. Intsidentide ulatus kasvab, neid esineb üha sagedamini ja need muutuvad üha keerukamaks. ELi võrgu- ja infoturbe parandamise üle peetud komisjoni avaliku konsultatsiooni[1] käigus selgus, et 57 % vastanuist oli eelnenud aasta jooksul kogenud võrgu- ja infoturbe intsidenti, mis mõjutas oluliselt nende tegevust. Puudulik võrgu- ja infoturve võib seada ohtu võrgu ja infosüsteemide terviklusest sõltuvad elutähtsad teenused. Selle tagajärjel võib katkeda ettevõtete töö, tekkida ELi majandusele suur finantskahju ja saada kahjustatud ühiskondlik heaolu.

Digitaalsed infosüsteemid, eelkõige internet, on riigipiiridest sõltumatud sidevahendid, mis on omavahel ühendatud üle liikmesriikide ning seega on nende roll kaupade, teenuste ja inimeste piiriülese liikumise hõlbustajana ülioluline. Kui ühes liikmesriigis on selliste süsteemide töös oluline katkestus, võib see mõjutada teisi liikmesriike ja ELi tervikuna. Seega on võrgu ja infosüsteemide vastupidavus ja stabiilsus digitaalse ühtse turu lõplikuks väljakujundamiseks ja siseturu tõrgeteta toimimiseks eluliselt olulised. Intsidentide esinemise tõenäosus ja sagedus ning suutmatus tagada tõhusat kaitset õõnestavad üldsuse usaldust võrgu- ja infoteenuste vastu. Näiteks ilmnes küberturvalisust käsitlenud 2012. aasta Eurobaromeetri uuringust, et ELis on 38 % internetikasutajaid mures internetimaksete turvalisuse pärast ning turvakaalutlustest johtuvalt on nad muutnud oma käitumist: 18 % vastanuist väitis, et on vähem tõenäoline, et nad ostavad oma kauba internetis, ning 15 % on väiksema tõenäosusega valmis kasutama internetipanka[2].

Praegune olukord ELis peegeldab senist rangelt vabatahtlikku lähenemist ega paku ELis piisavat kaitset võrgu ja info turvalisusega seotud intsidentide ja riskide eest. Võrgu- ja

[1] ELi võrgu- ja infoturbe parandamise üle peetud avalik konsultatsioon kestis 23. juulist kuni 15. oktoobrini 2012.

[2] Eurobaromeetri uuring 390/2012.

infoturbe praegune suutlikkus ja kasutatavad mehhanismid ei ole piisavad, et kiirelt muutuvatele ohtudele vastu panna ja tagada kõigis liikmesriikides kaitse ühtlaselt kõrge tase.

Vaatamata senistele algatustele on suutlikkuse ja valmisoleku tase liikmesriigiti väga erinev ning see põhjustab ELi lõikes lähenemisviiside killustatust. Arvestades, et võrgud ja süsteemid on omavahel seotud, nõrgestavad ebapiisava kaitsetasemega liikmesriigid kogu ELi võrgu- ja infoturbe üldist taset. Lisaks takistab selline olukord vastastikuse usalduse tekkimist, mis on aga koostöö ja teabe jagamise üks eeldusi. Tulemuseks on olukord, kus koostööd teeb vaid väike arv hea suutlikkusega liikmesriike.

Seega puudub ELi tasandil praegu tõhus mehhanism, mis võimaldaks liikmesriikidel koostööd teha ning võrgu ja info turvalisusega seotud intsidentide ja riskide kohta usaldusväärset teavet jagada. See võib tuua kaasa koordineerimatu regulatiivse sekkumise, omavahel vastuolus olevad strateegiad ja erinevad standardid, mis omakorda tähendab, et võrgu- ja infoturve kogu ELis on ebapiisav. Siseturul võivad tekkida tõrked, mis põhjustavad õigusaktide täitmisega seotud kulusid nende ettevõtjate jaoks, kes tegutsevad mitmes liikmesriigis.

Lisaks eelöeldule ei ole elutähtsate infrastruktuuride haldajatel ja ühiskonna toimimiseks hädavajalike teenuste pakkujatel asjakohast kohustust võtta riskihaldusmeetmeid ja vahetada teavet asjaomaste asutustega. Ühest küljest ei ole ettevõtjatel seega mõjusaid stiimuleid tegeleda tõsise riskihaldusega, mis hõlmaks riskide hindamist ning võrgu- ja infoturbe tagamiseks vajalike sammude astumist. Teisest küljest aga ei jõua suur osa intsidentidest pädevate asutusteni ja neid ei märgata. Samas on intsidente käsitlev teave ülioluline, et riigiasutused saaksid reageerida, võtta asjakohaseid leevendavaid meetmeid ja panna paika võrgu- ja infoturbe piisavad strateegilised prioriteedid.

Praeguse regulatiivse raamistiku kohaselt on vaid telekommunikatsiooniettevõtted kohustatud võtma riskihaldusmeetmeid ning teatama rasketest võrgu ja info turvalisusega seotud intsidentidest. Samas sõltuvad paljud teised sektorid oma töös IKTst ning seega peaksid ka nemad võrgu- ja infoturbe pärast muret tundma. Paljud spetsiifiliste taritute ja teenuste pakkujad on eriti haavatavad, sest nad on korralikult toimivast võrgust ja infosüsteemidest väga suures sõltuvuses. Sellistel sektoritel on oluline ülesanne pakkuda majanduse ja ühiskonna jaoks olulisi tugiteenuseid ning nende süsteemide turvalisus on siseturu toimimiseks eriti tähtis. Sellised sektorid on pangandus, väärtpaberibörsid, energia tootmine, ülekandmine ja jaotamine, transport (õhu-, raudtee- ja meretransport), tervishoid, internetiteenused ja avalik haldus.

Seepärast tuleb lähenemist võrgu- ja infoturbele ELis radikaalselt muuta. Võrdsete tingimuste loomiseks ja praeguste õigustühimike kaotamiseks on vaja õigusnormidega sätestatud kohustusi. Nende probleemide lahendamiseks ning võrgu- ja infoturbe taseme tõstmiseks Euroopa Liidus on kavandataval direktiivil allpool kirjeldatud eesmärgid.

Esiteks on ettepanekus sätestatud kohustus, et kõik liikmesriigid peavad tagama riikliku suutlikkuse miinimumtaseme ning asutavad selleks võrgu- ja infoturbe valdkonna pädevad asutused, loovad infoturbeintsidentidega tegelevad meeskonnad (Computer Emergency Response Team ehk CERT) ning võtavad vastu riiklikud võrgu- ja infoturbe strateegiad ja riiklikud võrgu- ja infoturbe koostöökavad.

Teiseks peaksid riikide pädevad asutused tegema koostööd sellise võrgustiku raames, mis võimaldaks tegevust turvaliselt ja tulemuslikult koordineerida, sh koordineeritult teavet vahetada, ning tegeleda intsidentide avastamise ja neile reageerimisega ELi tasandil. Selle võrgu kaudu peaksid liikmesriigid vahetama teavet ja tegema koostööd, et reageerida võrgu ja

info turvalisusega seotud ohtudele ja intsidentidele vastavalt Euroopa võrgu- ja infoturbe koostöökavale.

Kolmandaks on ettepaneku eesmärk tagada elektroonilise side raamdirektiivist lähtudes, et riskihalduskultuur areneb ning avalik ja erasektor jagavad omavahel teavet. Eespool kirjeldatud spetsiifilistes elutähtsates sektorites tegutsevatele ettevõtjatele ja haldusasutustele pannakse kohustus hinnata nende ees olevaid riske ning võtta võrgu ja infoturbe tagamiseks asjakohaseid ja proportsionaalseid meetmeid. Samuti pannakse neile kohustus teatada pädevatele asutustele kõigist intsidentidest, mis kahjustavad oluliselt nende võrke ja infosüsteeme ning mõjutavad elutähtsate teenuste ja kaupade pakkumise pidevust.

1.2. Üldine taust

Komisjon kirjeldas juba 2001. aasta teatises „Võrgu- ja infoturve: Euroopa lähenemisviisi ettepanek”[3] võrgu- ja infoturbe kasvavat olulisust. Sellele järgnes 2006. aastal turvalise infoühiskonna strateegia[4] vastuvõtmine, et arendada Euroopas võrgu- ja infoturbe kultuuri. Strateegia peamisi elemente kinnitas ka nõukogu oma resolutsiooniga[5].

30. märtsil 2009 võttis komisjon vastu teatise elutähtsa sideinfrastruktuuri kaitse kohta,[6] milles keskenduti sellele, kuidas turvalisuse parandamisega kaitsta Euroopat küberhäirete eest. Teatisega algatati tegevuskava, et toetada liikmesriikide tegevust tõrje ja reageerimise tagamisel. Tegevuskava kiideti heaks eesistujariigi järeldustes 2009. aastal Tallinnas toimunud elutähtsa sideinfrastruktuuri kaitse alase ministrite konverentsi kohta. 18. detsembril 2009 võttis nõukogu vastu resolutsiooni Euroopa ühise lähenemisviisi kohta võrgu- ja infoturbele[7].

2010. aasta mais vastuvõetud Euroopa digitaalarengu tegevuskavas[8] ja nõukogu järeldustes selle kohta[9] rõhutati ühist arusaama, et usaldus ja turvalisus on IKT laialdase kasutuse ja seeläbi ka strateegia „Euroopa 2020”[10] arukat majanduskasvu käsitlevate eesmärkide saavutamise peamised eeltingimused. Digitaalarengu tegevuskava usaldust ja turvalisust käsitlevas peatükis rõhutati, kui oluline on, et kõik sidusrühmad ühendaksid jõud, et tagada koos tõrjele, valmisolekule ja teadlikkusele keskendudes IKT taristu turvalisus ja vastupidavus ning töötada välja tulemuslikud ja koordineeritud turbemehhanismid. Euroopa digitaalarengu tegevuskava 6. põhimeetme kohaselt tuleb võtta meetmeid, mille eesmärk on tõhusam ja kõrgetasemeline võrgu- ja infoturbepoliitika.

2011. aasta märtsi teatises elutähtsate infoinfrastruktuuride kaitse kohta „Saavutused ja edasised sammud: üleilmse küberjulgeoleku suunas”[11] andis komisjon ülevaate sellest, mis oli saavutatud pärast seda, kui elutähtsa sideinfrastruktuuri kaitse tegevuskava 2009. aastal vastu võeti. Komisjoni tõdemuse kohaselt on tegevuskava rakendamisest näha, et puhtalt riigipõhine lähenemine turbe ja vastupidavuse alaste probleemide lahendamisele ei ole piisav ning Euroopa peaks edaspidigi püüdlema kogu ELi hõlmava ühtse ja koostööl põhineva

---

3 KOM(2001) 298.

4 KOM(2006) 251 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:ET:PDF

5 2007/068/01.

6 KOM(2009) 149.

7 2009/C 321/01.

8 KOM(2010) 245.

9 Nõukogu 31. mai 2010. aasta järeldused Euroopa digitaalse tegevuskava kohta (10130/10).

10 KOM(2010) 2020 ja Euroopa Ülemkogu 25./26. märtsi 2010. aasta järeldused (EUCO 7/10).

11 KOM(2011) 163.

lähenemise poole. Samas teatises kuulutati välja hulk meetmeid ning komisjon esitas liikmesriikidele üleskutse panna alus võrgu- ja infoturbealasele suutlikkusele ja piiriülesele koostööle. Enamik neist meetmetest oleks tulnud aastaks 2012 ellu viia, kuid neid ei ole veel rakendatud.

27. mai 2011. aasta järeldustes elutähtsate infoinfrastruktuuride kaitse kohta rõhutas Euroopa Liidu Nõukogu, et kiiremas korras tuleb muuta IKT süsteemid ja võrgud turvaliseks ja vastupidavaks kõikvõimalikele juhuslikele või tahtlikele häiretele, arendada valmisoleku, turvalisuse ja vastupidavuse alase suutlikkuse kõrget taset kogu ELis, parandada tehnilist pädevust, et Euroopa suudaks toime tulla võrgu- ja infotaristu kaitsmisega, ning soodustada liikmesriikidevahelist koostööd, luues nendevahelise intsidentidealase koostöö mehhanismid.

1.3. Kõnealuses valdkonnas kehtivad Euroopa Liidu ja rahvusvahelised sätted

Euroopa Ühendus lõi 2004. aastal määrusega (EÜ) nr 460/2004 Euroopa Võrgu- ja Infoturbeameti ehk ENISA,[12] et aidata tagada võrgu- ja infoturbe kõrge tase ja arendada võrgu- ja infoturbe kultuuri ELis. 2010. aasta 30. septembril võeti vastu ENISA volituste ajakohastamist käsitlev ettepanek,[13] mille üle arutlevad praegu nõukogu ja Euroopa Parlament. Alates 2009. aasta novembrist kehtiva elektroonilise side läbivaadatud õigusraamistikuga[14] nähti elektroonilisi sidevõrke pakkuvatele ettevõtjatele ette turbekohustus[15]. Need kohustused tuli riiklike õigusaktidega sätestada 2011. aasta maiks.

Andmekaitsealase õigusraamistiku[16] kohaselt on vastutavatel töötlejatel (näiteks pangad või haiglad) kohustus võtta isikuandmete kaitsmiseks kasutusele turbemeetmed. Lisaks peavad vastutavad töötlejad komisjoni 2012. aasta isikuandmete üldmääruse ettepaneku[17] kohaselt teatama isikuandmetega seotud rikkumistest riigi järelevalveasutusele. See tähendab, et näiteks võrgu- ja infoturbega seotud rikkumisest, mis kahjustab teenuse pakkumist, aga mitte isikuandmeid (nt IKT katkestus energiaettevõttes, mis põhjustab voolukatkestuse), polnuks vaja teatada.

Direktiivi 2008/114 (Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta) reguleerimisalas esitati Euroopa esmatähtsate infrastruktuuride kaitse programmiga (EPCIP)[18] üldine lähenemine kriitiliste infrastruktuuride kaitsele ELis. EPCIPi eesmärgid on täielikult kooskõlas käesoleva ettepanekuga ning direktiivi tuleks kohaldada ilma, et see piiraks direktiivi 2008/114 kohaldamist. EPCIPiga ei pandud operaatoritele kohustust teatada olulistest turvalisuse rikkumistest ega loodud mehhanisme, mis võimaldaksid liikmesriikidel koostööd teha ja intsidentidele reageerida.

Kaasseadusandjad arutlevad praegu komisjoni ettepaneku üle, milles käsitletakse direktiivi infosüsteemide vastu suunatud rünnete kohta[19] ja mille eesmärk on ühtlustada teatavat liiki käitumise kuritegelikuks tunnistamine. Ettepanekus käsitletakse vaid teatavat liiki käitumist ega pöörata tähelepanu võrgu ja info turvalisusega seotud intsidentide ja riskide vältimisele,

---

12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=DD:01:05:32004R0460:ET:PDF.

13 KOM(2010) 521.

14 Vt http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

15 Raamdirektiivi artiklid 13a ja 13b.

16 Direktiiv 2002/58/EÜ, 12. juuli 2002.

17 COM(2012) 11.

18 KOM(2006) 786 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:ET:PDF.

19 KOM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:ET:PDF

sellistele intsidentidele reageerimisele ja nende mõju leevendamisele. Käesolevat direktiivi tuleks kohaldada ilma, et see piiraks infosüsteemide vastu suunatud ründeid käsitleva direktiivi kohaldamist.

28. märtsil 2012 võttis komisjon vastu teatise küberkuritegevuse vastase võitluse Euroopa keskuse (EC3) loomise kohta[20]. Keskus loodi 11. jaanuaril 2013 Euroopa Politseiameti (Europol) osana ning sinna koondub küberkuritegevusega võitlemine ELis. EC3 peaks enda alla koondama Euroopa küberkuritegevusega võitlemise alased teadmised, et toetada liikmesriike suutlikkuse suurendamisel ja küberkuritegude uurimisel, ning tihedas koostöös Euroopa Õigusalase Koostöö Üksusega (Eurojust) peaks temast saama Euroopa küberkuritegevuse uurijate esindaja õiguskaitseasutustes ja kohtusüsteemis.

Euroopa institutsioonid, asutused ja organid on loonud oma infoturbeintsidentidega tegeleva rühma CERT-EU.

Rahvusvahelisel tasandil tegeleb EL küberturbega nii kahepoolsel kui ka mitmepoolsel tasandil. 2010. aastal toimunud ELi ja USA tippkohtumisel[21] loodi ELi ja USA ühine küberturbe ja küberkuritegevuse töörühm. EL tegutseb aktiivselt ka muudel asjaomastel mitmepoolsetel foorumitel, mille hulka kuuluvad näiteks Majanduskoostöö ja Arengu Organisatsioon (OECD), ÜRO Peaassamblee, Rahvusvaheline Telekommunikatsiooni Liit (ITU), Euroopa Julgeoleku- ja Koostööorganisatsioon (OSCE), infoühiskonna alane maailma tippkohtumine ja Interneti Haldamise Foorum.

2. HUVITATUD ISIKUTEGA KONSULTEERIMISE JA MÕJU HINDAMISE TULEMUSED

2.1. Konsulteerimine huvitatud isikutega ja eksperdiarvamuste kasutamine

23. juulist kuni 15. oktoobrini 2012 toimus avalik internetikonsultatsioon „Võrgu- ja infoturbe parandamine ELis”. Komisjon sai internetiküsimustikule kokku 160 vastust.
Peamine tulemus oli, et sidusrühmad suhtusid positiivselt vajadusse parandada võrgu- ja infoturvet kogu ELis. Olgu nimetatud, et 82,2 % vastanuist olid seisukohal, et ELi valitsused peaksid võrgu- ja infoturbe kõrge taseme tagamiseks tegema enam; 82,8 % leidsid, et info ja süsteemide kasutajad ei ole teadlikud võrgu ja info turvalisusega seotud ohtudest ja intsidentidest; 66,3 % oleksid põhimõtteliselt selle poolt, et võrgu ja info turvalisusega seotud riskide haldamiseks kehtestataks regulatiivsed nõuded, ning 84,8 % arvasid, et sellised nõuded tuleks kehtestada ELi tasandil. Suure osa vastajate arvates oleks oluline võtta võrgu- ja infoturbe nõuded vastu eelkõige järgmistes sektorites: pangandus ja finantssektor (91,1 %), energeetika (89,4 %), transport (81,7 %), tervishoid (89,4 %), internetiteenused (89,1 %) ja avalik haldus (87,5 %). Veel leidsid vastanud, et kui peaks kehtestatama nõue teatada võrgu ja info turvalisuse rikkumisest riigi pädevale asutusele, tuleks see kehtestada ELi tasandil (65,1 %), ning nad kinnitasid, et sama nõue peaks kehtima ka haldusasutuste jaoks (93,5 %). Peale selle kinnitasid vastanud, et nõue hallata võrgu ja info turvalisusega seotud riske parimate võimalike tehniliste vahenditega ei tooks nende jaoks kaasa märkimisväärseid lisakulusid (63,4 %) ning turvalisuse rikkumisest teatamise nõue ei põhjustaks märkimisväärseid lisakulusid (72,3 %).

[20] COM(2012) 140, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:ET:PDF.

[21] http://europa.eu/rapid/press-release_MEMO-10-597_en.htm.

Liikmesriikidega konsulteeriti nõukogu asjakohastes koosseisudes, liikmesriikide Euroopa foorumi raames, komisjoni ja Euroopa välisteenistuse korraldatud küberturbe konverentsil 6. juulil 2012 ning üksikute liikmesriikide taotlusel toimunud spetsiaalsetel kahepoolsetel kohtumistel.

Vastupidavust käsitleva Euroopa avaliku ja erasektori partnerluse[22] ja kahepoolsete kohtumiste käigus toimusid arutelud ka erasektoriga. Avaliku sektori esindajatest toimusid komisjonil arutelud ENISA ja ELi institutsioonide CERTiga.

2.2. Mõju hindamine

Komisjon hindas kolme poliitilise valiku mõju:

Variant 1: tavapärane tegevus (lähtestsenaarium): säilitatakse praegune lähenemisviis.

Variant 2: regulatiivne lähenemisviis, mis seisneb õigusakti ettepanekus ELi võrgu- ja infoturbe ühise raamistiku loomise kohta seoses liikmesriikide suutlikkusega, ELi tasandi koostöömehhanismidega ja nõuetega olulistele eraettevõtjatele ja haldusasutustele.

Variant 3: kombineeritud lähenemine, mis ühendab liikmesriikide võrgu- ja infoturbe alase suutlikkuse ja ELi tasandi koostöö mehhanismide vabatahtlikud algatused regulatiivsete nõuetega olulistele eraettevõtjatele ja haldusasutustele.

Komisjon jõudis järeldusele, et kõige suurem positiivsem mõju oleks 2. variandil, sest parandaks märkimisväärselt ELi tarbijate, ettevõtete ja valitsuste kaitstust võrgu ja info turvalisusega seotud intsidentide eest. Eelkõige tagaksid liikmesriikidele pandud kohustused riikide tasandil piisava valmisoleku ning aitaksid kaasa vastastikuse usalduse tekkimisele, mis on ELi tasandi tõhusa koostöö eeltingimus. Võrgustiku kaudu toimuva ELi tasandi koostöö mehhanismide loomine võimaldaks piiriüleseid võrgu ja info turvalisusega seotud riske ühtselt ja koordineeritult vältida või neile reageerida. Võrgu ja info turvalisusega seotud riskide haldamise nõuete kehtestamine haldusasutustele ja olulistele eraettevõtetele motiveeriks turvalisusega seotud riske tulemuslikult haldama. Võrgu ja info turvalisusega seotud olulise mõjuga intsidentidest teatamise kohustus parandaks intsidentidele reageerimise võimet ja soodustaks läbipaistvust. Pärast oma koduste asjade kordaseadmist saaks EL laiendada tegevusulatust rahvusvahelises plaanis ning olla veelgi usaldusväärsem koostööpartner kahe- ja mitmepoolsetes suhetes. Selle tulemusena paraneks ELi positsioon ning ta saaks põhiõigusi ja ELi põhiväärtusi mujal maailmas paremini propageerida.

Kvantitatiivne hindamine näitas, et 2. variant ei põhjustaks liikmesriikidele ebaproportsionaalseid kulutusi. Ka erasektori jaoks oleksid kulud piiratud, sest paljud asjaomased asutused peaksid juba praegu täitma kehtivaid turvanõudeid (näiteks vastutavate töötlejate kohustus võtta isikuandmete turvalisuse tagamiseks tehnilisi ja korralduslikke meetmeid, sealhulgas võrgu- ja infoturbemeetmeid). Arvesse on võetud ka erasektori praeguseid kulutusi turbele.

Ettepanekus järgitakse Euroopa Liidu põhiõiguste harta põhimõtteid, eelkõige õigust eraelu ja edastatavate sõnumite puutumatusele, isikuandmete kaitset, ettevõtlusvabadust, õigust omandile, õigust tõhusale õiguskaitsevahendile kohtus ja õiglasele kohtulikule arutamisele. Käesolevat direktiivi tuleb rakendada kooskõlas nimetatud õiguste ja põhimõtetega.

[22] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

3. ETTEPANEKU ÕIGUSLIK KÜLG

3.1. Õiguslik alus

Euroopa Liit on volitatud võtma meetmeid siseturu rajamiseks või selle toimimise tagamiseks vastavalt aluslepingute asjakohastele sätetele (Euroopa Liidu toimimise lepingu artikkel 26). Vastavalt ELi toimimise lepingu artiklile 114 võib EL võtta nii õigus- kui ka haldusnormide ühtlustamiseks meetmeid, mille eesmärk on siseturu rajamine ja selle toimimine.

Nagu eespool öeldud, on võrgul ja infosüsteemidel oluline roll kaupade, teenuste ja inimeste piiriülese liikumise hõlbustamisel. Need on sageli omavahel ühendatud ning internet on oma olemuselt ülemaailmne. Sellisest riikidevahelisest mõõtmest tulenevalt võib ühes liikmesriigis tekkinud katkestus mõjutada ka teisi liikmesriike ja ELi tervikuna. Seepärast on võrgu ja infosüsteemide vastupidavus ja stabiilsus siseturu sujuvaks toimimiseks hädavajalikud.

ELi seadusandja on juba tunnistanud vajadust ühtlustada siseturu arengu tagamiseks võrgu- ja infoturbe eeskirjad. See puudutas näiteks ELi toimimise lepingu artiklil 114 põhinevat määrust (EÜ) 460/2004, millega loodi ENISA[23].

Riikide võrgu- ja infoturbealase suutlikkuse, poliitilise lähenemise ja liikmesriikide kaitse taseme ebaühtluse põhjustatud lahknevused tekitavad tõrkeid siseturul ning seega on õigustatud tegutsemine ELi tasandil.

3.2. Subsidiaarsus

Euroopa sekkumine võrgu- ja infoturbe vallas on õigustatud subsidiaarsuse põhimõttega.

Esiteks on võrgu- ja infoturve oma olemuselt piiriülene ning seega tooks ELi tasandil sekkumata jätmine kaasa olukorra, kus iga liikmesriik tegutseb omaette, jättes tähelepanuta võrgu ja infosüsteemide omavahelise sõltuvuse ELis. Piisav liikmesriikidevaheline koostöö tagaks, et võrgu ja info turvalisusega seotud riske saaks hästi hallata ka siis, kui need on piiriülesed. Võrgu- ja infoturbe alaste õigusaktide erinevused on takistuseks ettevõtjatele, kes soovivad tegutseda mitmes riigis, ega lase saada kasu mastaabisäästust.

Teiseks on ELi tasandi regulatiivseid kohustusi vaja selleks, et luua võrdsed tingimused ja kaotada õigustühimikud. Puhtakujuliselt vabatahtliku lähenemisviisi tulemuseks on olukord, kus koostööd teeb vaid väike arv hea suutlikkusega liikmesriike. Kõigi liikmesriikide kaasamiseks tuleb tagada, et neil kõigil oleks suutlikkuse nõutav miinimumtase. Meetmed, mida valitsused võrgu- ja infoturbe vallas võtavad, peavad olema omavahel kooskõlas ja koordineeritud, et need võimaldaksid võrgu ja info turvalisusega seotud intsidente ohjeldada ja nende mõju minimeerida. Pädevad asutused ja komisjon kasutavad koostöövõrku, et parimate tavade vahetamise ja ENISA pideva kaasamise kaudu aidata kaasa direktiivi ühtsele kohaldamisele kogu ELis. Lisaks võivad kooskõlastatud võrgu- ja infoturbepoliitika meetmed avaldada tugevat positiivset mõju tõhusale põhiõiguste kaitsele, ja eriti isikuandmete ja eraelu puutumatuse õiguse kaitsele. Seega muudaks ELi tasandil tegutsemine riikide praegused tegutsemispõhimõtted tõhusamaks ja soodustaks nende arengut.

Kavandatavad meetmed on õigustatud ka proportsionaalsuse põhimõttega. Liikmesriikidele kehtestataks miinimumnõuded, mis võimaldaksid saavutada piisava valmisoleku ja

[23] Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 460/2004, 10. märts 2004, millega luuakse Euroopa Võrgu- ja Infoturbeamet (ELT L 77, 13.3.2004, lk 1).

võimaldada usaldusele rajatud koostööd. Ühtlasi võimaldab see liikmesriikidel võtta piisavalt arvesse riigi eripära ja tagada, et ELi ühiseid põhimõtteid kohaldatakse proportsionaalselt. Tänu kohaldamisala ulatuslikkusele saavad liikmesriigid direktiivi rakendamisel lähtuda tegelikult riiki ähvardavatest riskidest, nagu on riigi võrgu- ja infoturbe strateegias kindlaks määratud. Riskide haldamise nõue oleks suunatud ainult elutähtsatele üksustele ning kaasnevad meetmed on proportsionaalsed riskidega. Avaliku konsultatsiooni käigus rõhutati, kui oluline on tagada nende elutähtsate üksuste turvalisus. Intsidentidest teatamise nõuded puudutaksid vaid olulise mõjuga intsidente. Nagu eespool öeldud, ei põhjustaks meetmed ebaproportsionaalseid kulusid, sest paljud asjaomased üksused on vastutavad andmetöötlejad ning nad on juba praeguste andmekaitse eeskirjade kohaselt kohustatud kindlustama isikuandmete kaitse.

Selleks et vältida ebaproportsionaalset koormust väikestele operaatoritele, eelkõige VKEdele, on nõuded proportsionaalsed asjaomase võrgu või infosüsteemi puhul esineva riskiga ning neid ei kohaldata mikroettevõtjate suhtes. Esmajoones peavad riskid kindlaks määrama isikud, kelle suhtes neid kohustusi kohaldatakse ja kes peavad otsustama, milliseid meetmeid selliste riskide leevendamiseks võtta.

Arvestades võrgu ja info turvalisusega seotud intsidentide ja riskide piiriülesust, on nimetatud eesmärke parem saavutada ELi tasemel kui siis, kui liikmesriigid tegutseksid üksi. Euroopa Liit võib seega võtta meetmeid kooskõlas Euroopa Liidu lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Proportsionaalsuse põhimõtte kohaselt ei lähe kavandatav direktiiv kaugemale sellest, mis on nimetatud eesmärkide saavutamiseks vajalik.

Nende eesmärkide saavutamiseks tuleks komisjonile anda volitused võtta Euroopa Liidu toimimise lepingu artikli 290 alusel vastu delegeeritud õigusakte, et täiendada või muuta teatavaid alusõigusakti väheolulisi elemente. Komisjoni ettepanekus püütakse ühtlasi toetada eraõiguslikele ja avalik-õiguslikele operaatoritele pandud kohustuste proportsionaalset rakendamist.

Et tagada põhiõigusakti rakendamiseks ühetaolised tingimused, tuleks komisjonile anda volitused võtta Euroopa Liidu toimimise lepingu artikli 291 alusel vastu delegeeritud õigusakte.

Arvestades eelkõige kavandatava direktiivi reguleerimisala ulatuslikkust, asjaolu, et ta puudutab väga põhjalikult reguleeritud valdkondi, ning IV peatükist tulenevaid õiguslikke kohustusi, tuleks ülevõtmismeetmetest teatades esitada ka selgitavad dokumendid. Kooskõlas liikmesriikide ja komisjoni 28. septembri 2011. aasta ühise poliitilise deklaratsiooniga selgitavate dokumentide kohta kohustuvad liikmesriigid lisama põhjendatud juhtudel ülevõtmismeetmeid käsitlevale teatele ühe või mitu dokumenti, milles selgitatakse seost direktiivi komponentide ja ülevõtvate siseriiklike õigusaktide vastavate osade vahel. Käesoleva direktiivi puhul leiab seadusandja, et kõnealuste dokumentide edastamine on põhjendatud.

4. MÕJU EELARVELE

Liikmesriikidevahelisel koostööl ja teabevahetusel peaks toeks olema turvaline taristu. Ettepanek mõjutab ELi eelarvet ainult siis, kui liikmesriigid otsustavad kohandada olemasolevat taristut (nt sTESTA) ja paluvad komisjonil selle rakendada vastavalt 2014.–2020. aasta mitmeaastasele finantsraamistikule. Prognooside kohaselt on ühekordne kulu 1 250 000 eurot, mis kaetaks ELi eelarvest eelarverealt 09.03.02 (edendada avalike

elektrooniliste teenuste omavahelist ühendamist ja koostalitlust ning juurdepääsu sellistele võrkudele; peatükk 09.03, Euroopa ühendamise rahastu – telekommunikatsioonivõrgud), eeldusel et Euroopa ühendamise rahastus on piisavalt vahendeid. Alternatiivina võivad liikmesriigid kas omavahel jagada olemasoleva taristu kohandamise ühekordsed kulud või otsustada luua uue taristu ja kanda sellega seotud kulud, mis oleksid prognooside kohaselt ligikaudu 10 miljonit eurot aastas.

2013/0027 (COD)

Ettepanek:

EUROOPA PARLAMENDI JA NÕUKOGU DIREKTIIV

meetmete kohta, millega tagada võrgu- ja infoturbe ühtlaselt kõrge tase kogu Euroopa Liidus

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 114,

võttes arvesse Euroopa Komisjoni ettepanekut,

olles edastanud seadusandliku akti eelnõu riikide parlamentidele,

võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust[1],

olles konsulteerinud Euroopa andmekaitseinspektoriga,

toimides seadusandliku tavamenetluse kohaselt

ning arvestades järgmist:

(1) Võrgul ja infosüsteemidel ning -teenustel on ühiskonnas eluliselt tähtis koht. Nende usaldusväärsus ja turvalisus on majandustegevuse ja sotsiaalse heaolu ning ennekõike siseturu toimimise jaoks hädavajalik.

(2) Tahtlike ja juhuslike turvaintsidentide ulatus ja sagedus suurenevad ning see kujutab endast suurt ohtu võrkude ja infosüsteemide toimimisele. Sellised intsidendid võivad takistada majandustegevust, põhjustada olulist finantskahju, vähendada kasutajate usaldust ja tekitada ELi majandusele suurt kahju.

(3) Piire ületava sidevahendina on digitaalsetel infosüsteemidel ja eriti internetil oluline roll kaupade, teenuste ja inimeste piiriülese liikumise hõlbustamisel. Sellisest riikidevahelisusest tulenevalt võib nende süsteemide töö katkestus ühes liikmesriigis mõjutada ka teisi liikmesriike ja ELi tervikuna. Seepärast on võrgu ja infosüsteemide vastupidavus ja stabiilsus siseturu sujuvaks toimimiseks hädavajalikud.

(4) ELi tasandil tuleks luua koostöömehhanism, mis võimaldaks vahetada võrgu- ja infoturbe alast teavet ning tegeleda selles vallas koordineeritud avastamise ja reageerimisega. Et selline mehhanism oleks tõhus ja kaasav, on oluline, et kõigil liikmesriikidel oleks miinimumsuutlikkus ja strateegia võrgu- ja infoturbe kõrge taseme tagamiseks oma territooriumil. Minimaalseid turvanõudeid tuleks kohaldada ka haldusasutuste ja elutähtsa infotaristu operaatorite suhtes, et edendada riskihalduse kultuuri ja tagada, et kõige raskematest intsidentidest teatatakse.

(5) Et hõlmatud oleks kõik asjakohased intsidendid ja riskid, tuleks käesolevat direktiivi kohaldada kõigi võrgu- ja infosüsteemide suhtes. Haldusasutuste ja operaatorite suhtes kehtestatud kohustusi ei tuleks siiski kohaldada ettevõtjate suhtes, kes pakuvad üldkasutatavaid sidevõrke või üldkasutatavaid elektroonilisi sideteenuseid Euroopa

[1] ELT C […], […], lk […].

Parlamendi ja nõukogu 7. märtsi 2002. aasta direktiivi 2002/21/EÜ (elektrooniliste sidevõrkude ja -teenuste ühise reguleeriva raamistiku kohta(raamdirektiiv)) [2] tähenduses ja kelle suhtes kehtivad konkreetsed turva- ja terviklusnõuded, mis on sätestatud nimetatud direktiivi artiklis 13a, ning neid ei tuleks kohaldada ka usaldusteenuse pakkujate suhtes.

(6) Praegune suutlikkus ei ole ELis võrgu ja infoturbe kõrge taseme tagamiseks piisav. Liikmesriikide valmisoleku tase on väga erinev ning see põhjustab ELi lõikes lähenemisviiside killustatuse. See omakorda toob kaasa tarbijate ja ettevõtjate kaitstuse ebaühtluse ja vähendab võrgu- ja infoturbe üldist taset ELis. Kui haldusasutuste ja operaatorite suhtes ei kohaldata ühised miinimumnõuded, ei ole ELi tasemel võimalik luua üldist tõhusat koostöömehhanismi.

(7) Tulemuslik reageerimine võrgu ja infosüsteemide turvalisusega seotud probleemidele eeldab seega ELi tasandil üldist lähenemist, mis hõlmaks ühise miinimumsuutlikkuse loomist ja kavandamisnõudeid, teabevahetust ja tegevuse koordineerimist ning turvalisuse ühiseid miinimumnõudeid kõigile asjaomastele operaatoritele ja haldusasutustele.

(8) Käesoleva direktiivi sätted ei tohiks piidata liikmesriikide võimalust võtta vajalikke meetmeid, et tagada oma oluliste turvalisusega seotud huvide kaitse, tagada avalik kord ja julgeolek ning võimaldada kriminaalkuritegude uurimist, avastamist ja nende eest vastutuselevõtmist. Vastavalt ELi toimimise lepingu artiklile 346 ei tohi ühtki liikmesriiki kohustada andma teavet, mille avalikustamist ta peab oma oluliste julgeolekuhuvide vastaseks.

(9) Et saavutada võrgu ja infosüsteemide turvalisuse kõrge tase ja see säilitada, peaks igal liikmesriigil olema riiklik võrgu- ja infoturbe strateegia, milles oleks määratletud strateegilised eesmärgid ja konkreetsed poliitilised meetmed, mida rakendada. Riikide tasemel tuleb välja töötada olulistele nõuetele vastavad võrgu- ja infoturbe koostöökavad, et saavutada selline reageerimissuutlikkuse tase, mis võimaldaks teha intsidentide korral tulemuslikku ja tõhusat koostööd nii riikide kui ka ELi tasemel.

(10) Käesoleva direktiivi kohaselt vastuvõetud sätete tõhusa rakendamise huvides tuleks igas liikmesriigis luua või nimetada organ, kes vastutab võrgu- ja infoturbe alaste küsimuste koordineerimise eest ning tegutseb ELi taseme piiriülese koostöö keskusena. Sellistele organitele tuleks anda piisavad tehnilised, rahalised ja inimressursid, mis võimaldaksid neil oma ülesandeid tulemuslikult ja tõhusalt täita ning seeläbi saavutada käesoleva direktiivi eesmärgid.

(11) Kõik liikmesriigid peaksid olema nii tehniliselt kui ka töökorralduse mõttes piisavalt varustatud, et vältida ja avastada võrgu ja infosüsteemidega seotud intsidente ja riske ning neile reageerida ja nende mõju leevendada. Seepärast tuleks kõigis liikmesriikides luua hästi toimivad ja olulistele nõuetele vastavad infoturbeintsidentidega tegelevad meeskonnad, et kindlustada tulemuslik ja ühilduv suutlikkus tulla toime intsidentide ja riskidega ning tagada ELi tasandil tõhus koostöö.

(12) Arvestades liikmesriikide Euroopa foorumi (EFMS) märkimisväärset edu heade poliitiliste tavade üle peetud arutelude ja teabevahetuse soodustamisel, kaasa arvatud küberkriisialase Euroopa koostöö põhimõtete väljatöötamist, peaksid liikmesriigid ja

[2] EÜT L 108, 24.4.2002, lk 33.

komisjon looma võrgu, mis võimaldaks neil pidevalt suhelda ja toetaks nende koostööd. Turvaline ja tulemuslik koostöömehhanism peaks võimaldama struktureeritud ja koordineeritud teabevahetust ning probleemide avastamist ja neile reageerimist ELi tasandil.

(13) Euroopa Võrgu- ja Infoturbeamet (ENISA) peaks liikmesriike ja komisjoni abistama, pakkudes neile oma teadmisi ja andes nõu ning toetades parimate tavade vahetamist. Eriti peaks komisjon ENISAga konsulteerima käesoleva direktiivi kohaldamise üle. Et tagada liikmesriikide ja komisjoni tulemuslik ja õigeaegne teavitamine, tuleks varajased hoiatused intsidentide ja riskide kohta edastada koostöövõrgus. Liikmesriikide suutlikkuse ja teadmiste parandamise huvides peaks koostöövõrk pakkuma võimalusi ka parimate tavade vahetamiseks ning abistama oma liikmeid suutlikkuse suurendamisel ja juhtima vastastikuste eksperdihindamiste ja võrgu- ja infoturbe õppuste korraldamist.

(14) Luua tuleks turvaline teabejagamistaristu, mis võimaldaks vahetada koostöövõrgus tundlikku ja konfidentsiaalset teavet. Ilma et see piiraks liikmesriikide kohustust teatada koostöövõrgule ELi jaoks olulistest intsidentidest ja riskidest, peaksid liikmesriigid saama juurdepääsu teiste riikide konfidentsiaalsele teabele alles pärast seda, kui nad on tõendanud, et nende tehnilised, finants- ja inimressursid, protsessid ja sidetaristu tagavad nende tulemusliku, tõhusa ja turvalise osalemise võrgu töös.

(15) Enamiku võrkude ja infosüsteemide operaatorid on eraettevõtjad ning seepärast on avaliku ja erasektori koostöö hädavajalik. Soodustada tuleks operaatorite endi mitteametlikke koostöömehhanisme võrgu- ja infoturbe tagamiseks. Nad peaksid koostööd tegema ka avaliku sektoriga ning jagama teavet ja parimaid tavasid, et saada intsidentide korral pakutavat tegevustoetust.

(16) Et tagada läbipaistvus ja teavitada ELi kodanikke ja operaatoreid nõuetekohaselt, peaksid pädevad asutused looma ühise veebisaidi, millel avaldada mittekonfidentsiaalset teavet intsidentide ja riskide kohta.

(17) Kui teavet peetakse konfidentsiaalseks vastavalt ELi ja riikide ärisaladust käsitlevatele eeskirjadele, tuleb käesolevas direktiivis sätestatud toimingute teostamisel ja direktiivi eesmärkide täitmisel selline konfidentsiaalsus tagada.

(18) Lähtudes eelkõige riikide kriisihalduse alastest kogemustest, peaksid komisjon ja liikmesriigid koostöös ENISAga töötama välja ELi võrgu- ja infoturbe koostöökava, milles määratletakse koostöömehhanismid, et tulla toime riskide ja intsidentidega. Koostöövõrgus edastatavate varajaste hoiatuste puhul tuleks seda kava nõuetekohaselt arvesse võtta.

(19) Varajastest hoiatustest tuleks võrgus teatada vaid siis, kui asjaomase intsidendi või riski ulatus või raskusaste on nii olulised või võivad muutuda nii oluliseks, et vajalik on teavitamine või reageerimise koordineerimine ELi tasandil. Seega tuleks varajast hoiatamist kasutada vaid tegelike või võimalike intsidentide või riskide puhul, mille ulatus kasvab kiiresti, mis ületavad riigi reageerimissuutlikkuse või mis mõjutavad mitut liikmesriiki. Nõuetekohase hindamise tarvis tuleks edastada kogu riski või intsidendi hindamiseks vajalik teave koostöövõrgule.

(20) Kui pädevad asutused on saanud varajase hoiatuse ja seda hinnanud, peaksid nad kokku leppima koordineeritud reageerimises vastavalt ELi võrgu- ja infoturbe

koostöökavale. Pädevatele asutustele ja komisjonile tuleks teatada koordineeritud reageerimise tulemusena riigi tasandil võetud meetmetest.

(21) Arvestades võrgu ja info turvalisusega seotud probleemide globaalsust, on vaja teha tihedamat rahvusvahelist koostööd, et parandada turbestandardeid ja teabevahetust ning edendada ühtset üleilmselt lähenemist võrgu- ja infoturbe küsimustele.

(22) Vastutus võrgu ja info turvalisuse tagamise eest lasub suuresti haldusasutustel ja operaatoritel. Asjakohaste regulatiivsete nõuete ja tööstuse vabatahtlike tegutsemisviiside kaudu tuleks levitada ja arendada riskihalduskultuuri, mis hõlmaks riskihindamist ja riskist lähtuvalt asjakohaste turvameetmete rakendamist. Samuti on oluline kehtestada võrdsed tingimused, et koostöövõrk saaks tegelikult toimida ja et tagatud oleks kõigi liikmesriikide tulemuslik koostöö.

(23) Direktiiviga 2002/21/EÜ on kehtestatud nõue, et üldkasutatavaid elektroonilisi sidevõrke või üldkasutatavaid elektroonilisi sideteenuseid pakkuvad ettevõtjad peavad võtma asjakohased meetmed, et kindlustada nende terviklus ja turvalisus, ning nõuded teatada turvalisuse rikkumisest ja tervikluskaost. Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiivis 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv),[3] on sätestatud nõue, et üldkasutatava elektroonilise sideteenuse pakkuja peab võtma oma teenuste turvalisuse tagamiseks asjakohased tehnilised ja korralduslikud meetmed.

(24) Neid kohustusi tuleks peale elektroonilise side sektori kohaldada ka infoühiskonnateenuste peamiste pakkujate suhtes, kes on määratletud Euroopa Parlamendi ja nõukogu 22. juuni 1998. aasta direktiivis 98/34/EÜ, millega nähakse ette tehnilistest standarditest ja eeskirjadest ning infoühiskonna teenuste eeskirjadest teatamise kord,[4] ning kelle teenustele toetuvad infoühiskonna järgmise tasandi teenused ja tegevus internetis, näiteks e-kaubanduse platvormid, internetimaksete lüüsid, sotsiaalvõrgustikud, otsingumootorid, pilvandmetöötluse teenused, tarkvarapoed. Katkestused sellistes infoühiskonna üldteenustes takistavad ka muude infoühiskonna teenuste pakkumist, mille olulised sisendid sõltuvad just sellistest üldteenustest. Tarkvaraarendajad ja riistvaratootjad ei ole infoühiskonna teenuste pakkujad ja seega jäetakse nemad välja. Need kohustused peaksid laienema ka haldusasutustele ja elutähtsate infrastruktuuride operaatoritele, kes sõltuvad suurel määral info- ja kommunikatsioonitehnoloogiast ning kelle tegevus on äärmiselt oluline, et säilitada majanduse ja ühiskonna jaoks hädavajalikud funktsioonid; nende hulka kuuluvad näiteks elektri-, gaasi-, transpordi- ja krediidiettevõtted, väärtpaberibörsid ja tervishoiuasutused. Selliste võrkude ja infosüsteemide töö katkestused mõjutaksid siseturgu.

(25) Haldusasutuste ja operaatorite suhtes kehtestatud tehnilised ja korralduslikud meetmed ei tohiks tähendada, et konkreetset turustatavat info- ja kommunikatsioonitehnoloogilist toodet tuleks projekteerida, arendada või toota konkreetsel viisil.

(26) Haldusasutused ja operaatorid peaksid tagama nende kontrolli all olevate võrkude ja süsteemide turvalisuse. Eelkõige on tegemist privaatvõrkude ja -süsteemidega, mida

[3] EÜT L 201, 31.7.2002, lk 37.
[4] EÜT L 204, 21.7.1998, lk 37.

haldavad kas asutuse enda IT-töötajad või mille turbega seotud teenused ostetakse sisse. Turbe- ja teatamiskohustust tuleks asjaomaste operaatorite ja haldusasutuste suhtes kohaldada olenemata sellest, kas nad haldavad oma võrke ja infosüsteeme ise või ostavad selle teenuse sisse.

(27) Vältimaks väikese suurusega operaatorite ja kasutajate ebaproportsionaalset finants- ja halduskoormust, peaksid nõuded olema proportsionaalsed asjaomase võrgu või infosüsteemi puhul esineva riskiga, võttes sealjuures arvesse selliste meetmete kõrget tehnilist taset. Kõnealuseid nõudeid ei tuleks kohaldada mikroettevõtjate suhtes.

(28) Pädevad asutused peaksid pöörama piisavat tähelepanu mitteametlike ja usaldusväärsete teabejagamiskanalite säilitamisele operaatorite ning avaliku ja erasektori vahel. Pädevatele asutustele teatatud intsidentide avalikustamisel tuleks seada tasakaalu üldsuse huvi saada ohtudest teada ning kahju, mida selline olukord võib põhjustada intsidendist teatanud haldusasutuse või operaatori mainele ja kaubandustegevusele. Teatamiskohustuse rakendamisel peaksid pädevad asutused pöörama erilist tähelepanu sellele, et teave toote nõrkuste kohta jääks rangelt konfidentsiaalseks kuni asjakohase turvapaiga avaldamiseni.

(29) Pädevatel asutustel peaksid olema oma ülesannete täitmiseks vajalikud vahendid, kaasa arvatud volitused saada operaatoritelt ja haldusasutustelt võrgu või infosüsteemi turvalisuse taseme hindamiseks piisavat teavet ning usaldusväärseid ja põhjalikke andmeid reaalsete intsidentide kohta, mis on mõjutanud võrgu või infosüsteemi tööd.

(30) Sageli on intsidendi põhjuseks kuritegelik käitumine. Intsidendi seotust kuriteoga võib kahtlustada ka siis, kui alguses ei ole nende kahtluste kinnitamiseks piisavalt selgeid tõendeid. Sellises olukorras peaks pädevate asutuste ja õiguskaitseasutuste asjakohane koostöö olema osa tulemuslikust ja igakülgsest reageerimisest turvaintsidentide ohule. Ohutu, turvalise ja vastupidavama keskkonna edendamine eeldab, et intsidentidest, mille puhul kahtlustatakse seotust raske kuriteoga, teatatakse süstemaatiliselt õiguskaitseasutustele. Intsidendi seotust raske kuriteoga tuleks hinnata lähtuvalt ELi õigusaktidest küberkuritegevuse kohta.

(31) Sageli on intsidendi tagajärjeks isikuandmete kaitstuse rikkumine. Sellises olukorras peaksid pädevad asutused ja andmekaitseasutused omavahel koostööd tegema ja vahetama teavet kõigis asjassepuutuvates küsimustes, et tulla toime intsidendi tagajärjel toimunud isikuandmetega seotud rikkumisega. Liikmesriigid rakendavad turvaintsidentidest teatamise kohustust selliselt, et kui turvaintsidendiga kaasneb isikuandmetega seotud rikkumine üksikisikute kaitset isikuandmete töötlemisel ja selliste andmete vaba liikumist käsitleva Euroopa Parlamendi ja nõukogu määruse[5] tähenduses, oleks halduskoormus võimalikult väike ENISA peab sidet pädevate asutuste ja andmekaitseasutustega ning seega võiks ta aidata luua teabevahetusmehhanismid ja -vormid, et vältida olukorda, kus tuleb kasutada kaht teatamisvormi. Ühtne teatamisvorm hõlbustaks isikuandmete rikkumisega seotud intsidentidest teatamist ja vähendaks seega ettevõtjate ja haldusasutuste halduskoormust.

(32) Turvanõuete standardimine on turumajanduslik protsess. Et tagada turvastandardite ühtne kohaldamine, peaksid liikmesriigid julgustama konkreetsete standardite

[5] SEC(2012)72 (final).

järgimist ja vastavust neile, et tagada ELi tasandil turvalisuse kõrge tase. Selleks võib osutuda vajalikuks harmoneeritud standardite koostamine, mida tuleks teha kooskõlas Euroopa Parlamendi ja nõukogu 25. oktoobri 2012. aasta määrusega (EL) nr 1025/2012, mis käsitleb Euroopa standardimist ning millega muudetakse nõukogu direktiive 89/686/EMÜ ja 93/15/EMÜ ning Euroopa Parlamendi ja nõukogu direktiive 94/9/EÜ, 94/25/EÜ, 95/16/EÜ, 97/23/EÜ, 98/34/EÜ, 2004/22/EÜ, 2007/23/EÜ, 2009/23/EÜ ja 2009/105/EÜ ning millega tunnistatakse kehtetuks nõukogu otsus 87/95/EMÜ ning Euroopa Parlamendi ja nõukogu otsus nr 1673/2006/EÜ[6].

(33) Komisjon peaks käesoleva direktiivi sätted regulaarselt läbi vaatama eelkõige selleks, et teha kindlaks, kas neid on vaja muuta seoses tehnoloogia ja turutingimuste muutumisega.

(34) Et koostöövõrk saaks nõuetekohaselt toimida, tuleks komisjonile anda volitused võtta kooskõlas Euroopa Liidu toimimise lepingu artikliga 290 vastu õigusakte, et määratleda kriteeriumid, millele liikmesriik peab vastama, et tal lubataks osaleda turvalises teabevahetussüsteemis, panna paika selliste sündmuste täpsemad kirjeldused, mille puhul tuleks kasuta varajast hoiatust, ja määratleda asjaolud, mille korral operaatorid ja haldusasutused peavad intsidendist teatama.

(35) On eriti tähtis, et komisjon viiks oma ettevalmistava töö käigus läbi asjakohaseid konsultatsioone, sealhulgas ekspertide tasandil. Komisjon peaks delegeeritud õigusaktide ettevalmistamise ja koostamise ajal tagama asjaomaste dokumentide sama- ja õigeaegse ning nõuetekohase edastamise Euroopa Parlamendile ja nõukogule.

(36) Et tagada käesoleva direktiivi rakendamiseks ühetaolised tingimused, tuleks komisjonile anda rakendusvolitused seoses järgmisega: koostöövõrgu raames toimuv pädevate asutuste ja komisjoni koostöö, juurdepääs turvalisele teabevahetustaristule, ELi võrgu- ja infoturbe koostöökava, intsidentidest üldsusele teatamise vorm ja kord ning võrgu- ja infoturbe jaoks olulised standardid ja/või tehnilised kirjeldused. Neid volitusi tuleks teostada vastavalt Euroopa Parlamendi ja nõukogu 16. veebruari 2011. aasta määrusele (EL) nr 182/2011, millega kehtestatakse eeskirjad ja üldpõhimõtted, mis käsitlevad liikmesriikide läbiviidava kontrolli mehhanisme, mida kohaldatakse komisjoni rakendamisvolituste teostamise suhtes[7].

(37) Käesoleva direktiivi kohaldamisel peaks komisjon pidama vastavalt vajadusele sidet asjaomaste valdkondlike komiteede ja asjaomaste organitega, mis on loodud ELi tasandil eelkõige energeetika, transpordi ja tervishoiu valdkonnas.

(38) Teavet, mida pädev asutus peab konfidentsiaalseks vastavalt ärisaladusi käsitlevatele ELi ja siseriiklikele eeskirjadele, tuleks komisjoni ja teiste pädevate asutustega vahetada ainult siis, kui selline teabevahetus on hädavajalik käesoleva direktiivi kohaldamiseks. Vahetada võib ainult teavet, mis on sellise teabevahetuse eesmärgi seisukohast oluline ja proportsionaalne.

(39) Koostöövõrgus riskide ja intsidentide kohta teabe jagamine ning intsidentidest riigi pädevatele asutustele teatamise nõude järgimine võib eeldada isikuandmete töötlemist. Selline isikuandmete töötlemine on vajalik käesoleva direktiivi eesmärgiks oleva üldiste huvide järgimise jaoks ja on seega õiguspärane vastavalt direktiivi 95/46/EÜ

[6] ELT L 316, 14.11.2012, lk 12.
[7] ELT L 55, 28.2.2011, lk 13.

artiklile 7. Nimetatud õiguspärast eesmärki arvestades ei ole tegemist ebaproportsionaalse ega talumatu sekkumisega, mis kahjustaks olemuslikult põhiõiguste harta artikliga 8 tagatud õigust isikuandmete kaitsele. Käesoleva direktiivi kohaldamisel tuleks vajaduse korral kohaldada Euroopa Parlamendi ja nõukogu 30. mai 2001. aasta määrust (EÜ) nr 1049/2001 üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele[8]. Kui ELi institutsioonid ja organid töötlevad käesoleva direktiivi kohaldamisel andmeid, peaks see toimuma kooskõlas Euroopa Parlamendi ja nõukogu 18. detsembri 2000. aasta määrusega (EÜ) nr 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta.

(40) Kuna liikmesriigid üksi ei suuda piisavalt saavutada käesoleva direktiivi eesmärke, st võrgu- ja infoturbe kõrge taseme tagamist ELis, ning tegevuse mõju tõttu on seda parem teha liidu tasandil, võib liit võtta meetmeid kooskõlas Euroopa Liidu lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Kooskõlas nimetatud artiklis sätestatud proportsionaalsuse põhimõttega ei lähe käesolev direktiiv nimetatud eesmärkide saavutamiseks vajalikust kaugemale.

(41) Käesolevas direktiivis järgitakse Euroopa Liidu põhiõiguste harta põhiõigusi ja põhimõtteid, eelkõige õigust eraelu ja edastatavate sõnumite puutumatusele, isikuandmete kaitset, ettevõtlusvabadust ning õigust tõhusale õiguskaitsevahendile kohtus ja õiglasele kohtulikule arutamisele. Käesolevat direktiivi tuleb rakendada nende õiguste ja põhimõtete alusel,

ON VASTU VÕTNUD KÄESOLEVA DIREKTIIVI:

I PEATÜKK

ÜLDSÄTTED

Artikkel 1

Reguleerimisese ja reguleerimisala

1. Käesoleva direktiiviga nähakse ette meetmed võrgu- ja infoturbe ühtlaselt kõrge taseme tagamiseks.

2. Selle eesmärgi saavutamiseks tehakse käesoleva direktiiviga järgmist:

(a) sätestatakse kõigile liikmesriikidele kohustused seoses võrke ja infosüsteeme mõjutavate riskide ja intsidentide vältimise ja käsitlemise ning neile reageerimisega;

(b) luuakse liikmesriikidevahelise koostöö mehhanism, et tagada käesoleva direktiivi ühetaoline kohaldamine ELis ning vajaduse korral võrke ja infosüsteeme mõjutavate riskide ja intsidentide koordineeritud ja tõhus käsitlemine ja neile reageerimine;

(c) kehtestatakse operaatoritele ja haldusasutustele turvanõuded.

3. Artiklis 14 sätestatud turvanõudeid ei kohaldata direktiivis 2002/21/EÜ osutatud üldkasutatavaid sidevõrke või üldkasutatavaid elektroonilisi sideteenuseid pakkuvate

[8] EÜT L 145, 31.5.2001, lk 43.

ettevõtjate suhtes, kes peavad täitma konkreetseid turva- ja terviklusnõudeid, mis on sätestatud nimetatud direktiivi artiklites 13a ja 13b, ega usaldusteenuse pakkujate suhtes.

4. Käesolev direktiivi ei piira küberkuritegevust käsitlevate ELi õigusaktide ega nõukogu 8. detsembri 2008. aasta direktiivi 2008/114/EÜ (Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta)[9] kohaldamist.

5. Samuti ei piira käesolev direktiiv järgmiste õigusaktide kohaldamist: Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta,[10] Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris, ning Euroopa Parlamendi ja nõukogu määrus üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta[11].

6. Info jagamisega koostöövõrgu raames vastavalt III peatükile ning võrgu- ja infoturbe intsidentidest teatamisega vastavalt artiklile 14 võib kaasneda vajadus töödelda isikuandmeid. Käesoleva direktiiviga taotletavate avaliku huvi eesmärkide saavutamise jaoks vajalikuks töötlemiseks peab olema liikmesriigi luba vastavalt direktiivi 95/46/EÜ artiklile 7 ja direktiivile 2002/58/EÜ selliselt, nagu neid siseriikliku õigusega kohaldatakse.

Artikkel 2

Minimaalne ühtlustamine

Miski ei takista liikmesriike võtmast vastu ja säilitamast sätteid, millega tagatakse turvalisuse kõrgem tase, ilma et see piiraks nende ELi õigusest tulenevaid kohustusi.

Artikkel 3

Mõisted

Käesolevas direktiivis kasutatakse järgmisi mõisteid:

(1) „võrk ja infosüsteem” –

(a) elektrooniline sidevõrk direktiivis 2002/21/EÜ sätestatud tähenduses ja

(b) seade või omavahel ühendatud või seotud seadmete rühm, millest vähemalt ühes toimub mõne programmi kohaselt arvutiandmete automaatne töötlemine, ning

(c) arvutiandmed, mida salvestatakse, töödeldakse, võetakse välja või edastatakse punktides a ja b kirjeldatud komponentide töö, kasutamise, kaitsmise või hooldamise jaoks;

[9] ELT L 345, 23.12.2008, lk 75.
[10] EÜT L 281, 23.11.1995, lk 31.
[11] SEC(2012) 72 (final).

(2) „turvalisus” – võrgu ja infosüsteemi võime panna teatava kindlusega vastu õnnetusele või pahatahtlikule tegevusele, mis seab ohtu salvestatud või edastatud andmete või selle võrgu ja infosüsteemi kaudu pakutavate või nende kaudu juurdepääsetavate teenuste käideldavuse, autentsuse, tervikluse ja konfidentsiaalsuse;

(3) „risk” – asjaolu või sündmus, mis võib kahjustada turvalisust;

(4) „intsident” – asjaolu või sündmus, mis tegelikult kahjustab turvalisust;

(5) „infoühiskonna teenus” – teenus direktiivi 98/34/EÜ artikli 1 punkti 2 tähenduses;

(6) „võrgu- ja infoturbe koostöökava” – kava, millega luuakse organisatsiooniliste ülesannete, vastutuse ja protseduuride raamistik, et säilitada või taastada võrkude ja infosüsteemide töö neid mõjutava ohu või intsidendi korral;

(7) „intsidentide käsitlemine” – intsidendi analüüsimist ja ohjeldamist ning intsidendile reageerimist toetavad protseduurid;

(8) „operaator” –

(a) muude infoühiskonna teenuste pakkumist võimaldavate infoühiskonna teenuste pakkuja; infoühiskonna teenuste mittetäielik loetelu on esitatud II lisas;

(b) energeetika, transpordi, panganduse, väärtpaberitega kauplemise ja tervishoiu valdkonnas esmatähtsa majandusliku ja ühiskondliku tegevuse säilitamiseks vajaliku elutähtsa infrastruktuuri operaator; operaatorite mittetäielik loetelu on esitatud II lisas;

(9) „standard” – määruses (EL) nr 1025/2012 osutatud standard;

(10) „spetsifikatsioon” – määruses (EL) nr 1025/2012 osutatud spetsifikatsioon;

(11) „usaldusteenuse pakkuja” – füüsiline või juriidiline isik, kes pakub elektroonilist teenust, mis seisneb e-allkirjade, e-templite, e-ajatemplite, e-dokumentide, e-andmevahetusteenuste, veebisaitide autentimise ja e-tõendite, sealhulgas e-allkirja ja e-templi jaoks vajalike sertifikaatide loomises, kontrollimises, valideerimises, käsitlemises ja säilitamises.

II PEATÜKK

VÕRGU- JA INFOTURBE RIIKLIKUD RAAMISTIKUD

Artikkel 4

Põhimõte

Liikmesriigid tagavad oma territooriumil võrgu ja infosüsteemide turvalisuse kõrge taseme kooskõlas käesoleva direktiiviga.

Artikkel 5

Riiklik võrgu ja infoturbe strateegia ning riiklik võrgu ja infoturbe koostöökava

1. Iga liikmesriik võtab vastu riikliku võrgu- ja infoturbe strateegia, milles määratletakse strateegilised eesmärgid ning konkreetsed poliitilised ja regulatiivsed meetmed, mille abil saavutada võrgu ja info turvalisuse kõrge tase ja seda säilitada. Eelkõige käsitletakse riiklikus võrgu- ja infoturbe strateegias järgmisi küsimusi:

(a) strateegia eesmärkide ja prioriteetide määratlus, lähtudes ajakohasest riski- ja intsidendianalüüsist;

(b) juhtimisraamistik, mille toel strateegia eesmärgid ja prioriteedid ellu viia; see hõlmab valitsusasutuste ja muude asjaosaliste ülesannete ja vastutuse selget määratlust;

(c) valmisoleku, reageerimise ja taaste üldmeetmete, kaasa arvatud avaliku ja erasektori koostöö mehhanismide kindlaksmääramine;

(d) teadlikkuse suurendamise ning haridus- ja koolitusprogrammide kirjeldus;

(e) teadus- ja arendustegevuse kavad ja kirjeldus selle kohta, kuidas neis kavades kajastuvad määratletud prioriteedid.

2. Riiklik võrgu- ja infoturbe strateegia sisaldab riiklikku võrgu- ja infoturbe koostöökava, mis vastab vähemalt järgmistele nõuetele:

(a) riski hindamise kava, et teha kindlaks riskid ja hinnata võimalike intsidentide mõju;

(b) kava rakendamises osalevate isikute ülesannete ja vastutuse määratlus;

(c) vältimise, avastamise, reageerimise, parandamise ja taaste tagamiseks vajalike ja vastavalt hoiatustasemetele kohandatud koostöö- ja teavitusprotsesside määratlus;

(d) võrgu- ja infoturbe õppuste ja koolituste plaan, mille põhjal kava kinnistada, valideerida ja katsetada. Omandatud kogemused tuleb dokumenteerida ja kava ajakohastamisel neid arvesse võtta.

3. Riiklik võrgu- ja infoturbe strateegia ning riiklik võrgu- ja infoturbe koostöökava edastatakse komisjonile ühe kuu jooksul pärast seda, kui need on vastu võetud.

Artikkel 6

Riigi pädev asutus võrgu ja infosüsteemide turbe vallas

1. Iga liikmesriik nimetab võrgu ja infosüsteemide turbe vallas oma riigi pädeva asutuse (edaspidi „pädev asutus”).

2. Pädevad asutused jälgivad käesoleva direktiivi rakendamist riigi tasandil ning aitavad kaasa selle ühetaolisele kohaldamisele kogu ELis.

3. Liikmesriigid tagavad, et pädevatel asutustel oleksid piisavad tehnilised, rahalised ja inimressursid, mis võimaldaksid neil oma ülesandeid tulemuslikult ja tõhusalt täita ning seeläbi saavutada käesoleva direktiivi eesmärgid. Liikmesriigid tagavad pädevate asutuste tõhusa, tulemusliku ja turvalise koostöö artiklis 8 osutatud koostöövõrgu kaudu.

4. Liikmesriigid tagavad, et pädevad asutused saavad kätte haldusasutuste ja operaatorite teated intsidentide kohta vastavalt artikli 14 lõikele 2 ning et neile antakse artiklis 15 osutatud rakendamis- ja jõustamispädevus.

5. Vajaduse korral konsulteerivad pädevad asutused riigi asjaomaste õiguskaitseasutuste ja andmekaitseasutustega, ning teevad nendega koostööd.

6. Iga liikmesriik teatab komisjonile viivitamata pädeva asutuse määramisest, tema ülesannetest ja nende hilisemast muutmisest. Iga liikmesriik avalikustab määratud pädeva asutuse.

Artikkel 7

Infoturbeintsidentidega tegelev meeskond

1. Iga liikmesriik loob infoturbeintsidentidega tegeleva rühma (edaspidi „CERT”), kes vastutab intsidentide ja riskide käsitlemise eest põhjalikult määratletud protseduuri kohaselt ning vastab I lisa punktis 1 osutatud nõuetele. CERTi võib luua pädeva asutuse osana.

2. Liikmesriigid tagavad, et CERTil on I lisa punktis 2 osutatud ülesannete tulemuslikuks täitmiseks piisavad tehnilised, rahalised ja inimressursid.

3. Liikmesriigid tagavad, et riigi tasandil on CERTi kasutada turvaline ja vastupidav side- ja infotaristu, mis on koosolu- ja koostalitlusvõimeline artiklis 9 osutatud turvalise infojagamissüsteemiga.

4. Liikmesriigid teatavad komisjonile, millised on CERTi ressursid, volitused ja intsidentide käsitlemise protsess.

5. CERT tegutseb pädeva asutuse järelevalve all ning pädev asutus kontrollib regulaarselt, kas CERTi ressursid, volitused ja intsidentide käsitlemise protsessi tulemuslikkus on piisavad.

III PEATÜKK

PÄDEVATE ASUTUSTE KOOSTÖÖ

Artikkel 8

Koostöövõrk

1. Pädevad asutused ja komisjon moodustavad võrgu („koostöövõrk”), et teha võrku ja infosüsteeme mõjutavate riskide ja intsidentidega võitlemiseks koostööd.

2. Koostöövõrk võimaldab pidevat teabevahetust komisjoni ja pädevate asutuste vahel. Taotluse korral abistab Euroopa Võrgu- ja Infoturbeamet („ENISA”) koostöövõrku oma teadmiste ja nõuannetega.

3. Pädevad asutused teevad koostöövõrgus järgmist:

(a) levitavad varajasi hoiatusi riskide ja intsidentide kohta vastavalt artiklile 10;

(b) tagavad koordineeritud reageerimise vastavalt artiklile 11;

(c) avaldavad ühisel veebisaidil korrapäraselt mittekonfidentsiaalset teavet töös olevate varajaste hoiatuste ja koordineeritud reageerimise kohta;

(d) arutavad ja hindavad ühe liikmesriigi või komisjoni taotlusel ühiselt üht või mitut artiklis 5 osutatud riiklikku võrgu- ja infoturbe strateegiat või riiklikku võrgu- ja infoturbe koostöökava käesoleva direktiivi reguleerimisala piires;

(e) arutavad ja hindavad liikmesriigi või komisjoni taotlusel ühiselt CERTide töö tulemuslikkust, eelkõige juhul, kui ELi tasandil toimuvad võrgu- ja infoturbe õppused;

(f) teevad koostööd ja vahetavad infot Europoli juures tegutseva küberkuritegevuse vastase võitluse Euroopa keskuse ja muude asjaomaste Euroopa asutustega kõigil asjakohastel teemadel, eelkõige andmekaitse, energeetika, transpordi, panganduse, väärtpaberitega kauplemise ja tervishoiu vallas;

(g) vahetavad omavahel ja komisjoniga infot ja parimaid tavasid ning aitavad üksteist võrgu- ja infoturbe alase suutlikkuse loomisel;

(h) korraldavad vastastikku suutlikkuse ja valmisoleku eksperdihindamisi;

(i) korraldavad ELi tasandil võrgu- ja infoturbe õppusi ja osalevad vastavalt vajadusele rahvusvahelistel võrgu- ja infoturbe õppustel.

4. Komisjon kehtestab rakendusaktidega korra, mis hõlbustaks lõigetes 2 ja 3 osutatud koostööd pädevate asutuste ja komisjoni vahel. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 19 lõikes 2 osutatud nõuandemenetlusega.

Artikkel 9

Turvaline infojagamissüsteem

1. Koostöövõrgus vahetatakse tundlikku ja konfidentsiaalset infot turvalise taristu kaudu.

2. Komisjonile antakse volitused võtta vastavalt artiklile 18 vastu delegeeritud õigusaktid, et määratleda kriteeriumid millele liikmesriik peab vastama, et tal lubataks osaleda turvalises infojagamissüsteemis; kriteeriumid puudutavad järgmist:

(a) turvalise ja vastupidava ning koostöövõrgu turvalise taristuga koosolu- ja koostalitlusvõimelise side- ja infotaristu käideldavus riigi tasandil vastavalt artikli 7 lõikele 3 ning

(b) piisavate tehniliste, rahaliste ja inimressursside ning protsesside olemasolu pädevas asutuses ja CERTis, mis võimaldaks tulemuslikku, tõhusat ja turvalist osalust turvalises infojagamissüsteemis vastavalt artikli 6 lõikele 3 ning artikli 7 lõigetele 2 ja 3.

3. Lähtudes lõigetes 2 ja 3 osutatud kriteeriumidest, võtab komisjon rakendusaktidega vastu otsused liikmesriikide juurdepääsu kohta sellele turvalisele taristule. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 19 lõikes 3 osutatud kontrollimenetlusega.

Artikkel 10
Varajased hoiatused

1. Pädevad asutused ja komisjon annavad koostöövõrgus varajasi hoiatusi riskide ja intsidentide kohta, mis vastavad vähemalt ühele järgmistest tingimustest:

   (a) nende ulatus kasvab või võib kasvada kiiresti;

   (b) need ületavad või võivad ületada riigi reageerimissuulikkuse;

   (c) need mõjutavad või võivad mõjutada rohkem kui üht liikmesriiki.

2. Varajases hoiatuses edastab pädev asutus või komisjon kogu talle teadaoleva asjakohase teabe, mis võib olla riski või intsidendi hindamiseks kasulik.

3. Komisjon võib mõne liikmesriigi taotlusel või omal algatusel paluda, et liikmesriik esitaks kogu asjakohase teabe konkreetse riski või intsidendi kohta.

4. Kui kahtlustatakse, et varajases hoiatuses käsitletav risk või intsident on seotud kuriteoga, teatab pädev asutus või komisjon sellest Europoli juures tegutsevale küberkuritegevuse vastase võitluse Euroopa keskusele.

5. Komisjonile antakse volitused võtta vastavalt artiklile 18 vastu delegeeritud õigusakte selliste riskide ja intsidentide täpsemate spetsifikatsioonide kohta, mille puhul tuleb esitada lõikes 1 osutatud varajane hoiatus.

Artikkel 11
Koordineeritud reageerimine

1. Pärast artiklis 10 osutatud varajast hoiatust lepivad pädevad asutused asjakohase info hindamise järel kokku koordineeritud reageerimises vastavalt artiklis 12 osutatud ELi võrgu- ja infoturbe koostöökavale.

2. Koordineeritud reageerimise tulemusena riigi tasandil võetud meetmetest teatatakse koostöövõrgule.

Artikkel 12

ELi võrgu- ja infoturbe koostöökava

1. Komisjonile antakse volitused võtta rakendusaktiga vastu ELi võrgu- ja infoturbe koostöökava. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 19 lõikes 3 osutatud kontrollimenetlusega.

2. ELi võrgu- ja infoturbe koostöökava sisaldab järgmist:

(a) artikli 10 kohaldamiseks:

– pädevate asutuste poolt riskide ja intsidentide kohta kogutava ja jagatava ühilduva ja võrreldava teabe vormingu ning kogumise ja jagamise korra määratlus;

– koostöövõrgus riskidele ja intsidentidele hinnangu andmise protseduuride ja kriteeriumide määratlus;

(b) artikli 11 kohase koordineeritud reageerimise protsessid, kaasa arvatud ülesannete, vastutuse ja koostööprotseduuride kindlaksmääramine;

(c) võrgu- ja infoturbe õppuste ja koolituste plaan, mille põhjal kava kinnistada, valideerida ja katsetada;

(d) liikmesriikide vahelise teadmussiirde programm suutlikkuse suurendamiseks ja vastastikuseks õppimiseks;

(e) liikmesriikidevaheline teadlikkuse suurendamise ja koolitusprogramm.

3. ELi võrgu- ja infoturbe koostöökava võetakse vastu hiljemalt üks aasta pärast käesoleva direktiivi jõustumist ning see vaadatakse regulaarselt läbi.

Artikkel 13

Rahvusvaheline koostöö

EL võib sõlmida rahvusvahelisi lepinguid kolmandate riikide või rahvusvaheliste organisatsioonidega, et võimaldada neil osaleda ja korraldada nende osalus mõningates koostöövõrgu tegevustes, ilma et see piiraks koostöövõrgu võimalusi teha mitteametlikku rahvusvahelist koostööd. Sellises lepingus arvestatakse vajadusega tagada koostöövõrgus ringlevate isikuandmete piisav kaitse.

IV PEATÜKK

HALDUSASUTUSTE JA OPERAATORITE VÕRKUDE JA INFOSÜSTEEMIDE TURVE

Artikkel 14

Turvanõuded ja intsidentidest teatamine

1. Liikmesriigid tagavad, et haldusasutused ja operaatorid võtavad vajalikud tehnilised ja korralduslikud meetmed, et hallata riske, mis ohustavad nende kontrollitavate ja nende töös kasutatavate võrkude ja infosüsteemide turvalisust. Tehnika taset arvesse võttes tagatakse nende meetmetega turvalisuse tase, mis on vastavuses konkreetse ohuga. Eelkõige võetakse meetmeid, et vältida ja minimeerida nende asutuste pakutavate põhiteenuste võrku ja infosüsteemi kahjustavate intsidentide mõju ning tagada seega neid võrke ja infosüsteeme kasutavate teenuste pidevus.

2. Liikmesriigid tagavad, et haldusasutused ja operaatorid teatavad pädevale asutusele intsidentidest, millel on oluline mõju nende pakutavate põhiteenuste turvalisusele.

3. Lõigetes 1 ja 2 sätestatud nõudeid kohaldatakse kõigi operaatorite suhtes, kes pakuvad Euroopa Liidus teenuseid.

4. Kui pädev asutus leiab, et intsidendi avalikustamine on üldsuse huvides, võib ta üldsust teavitada või nõuda, et seda teeks haldusasutus või operaator. Kord aastas esitab pädev asutus koostöövõrgule koondaruande käesoleva lõike kohaselt saadud teadete ja võetud meetmete kohta.

5. Komisjonile antakse volitused võtta vastavalt artiklile 18 vastu delegeeritud õigusakte nende asjaolude määratlemiseks, mille korral haldusasutused ja operaatorid peavad intsidentidest teatama.

6. Kui lõike 5 alusel vastuvõetud delegeeritud õigusaktides ei ole sätestatud teisiti, võivad pädevad asutused võtta vastu suuniseid ja vajaduse korral anda välja juhiseid asjaolude kohta, mille korral haldusasutused ja operaatorid peavad intsidentidest teatama.

7. Komisjonile antakse volitused määratleda rakendusaktidega lõike 2 kohaldamiseks vajalikud vormingud ja protseduurid. Nimetatud rakendusaktid võetakse vastu kooskõlas artikli 19 lõikes 3 osutatud kontrollimenetlusega.

8. Lõikeid 1 ja 2 ei kohaldata mikroettevõtjate suhtes, kes on määratletud komisjoni 6. mai 2003. aasta soovituses 2003/361/EÜ mikroettevõtjate, väikeste ja keskmise suurusega ettevõtjate määratluse kohta[12].

Artikkel 15

Rakendamine ja jõustamine

1. Liikmesriigid tagavad, et pädevatel asutustel on kõik volitused, mida nad vajavad, et uurida juhtumeid, mil haldusasutus või operaator ei täitnud artiklist 14 tulenevaid kohustusi, ja nende juhtumite mõju võrkude ja infosüsteemide turvalisusele.

2. Liikmesriigid tagavad, et pädevatel asutustel on volitused nõuda operaatoritelt ja haldusasutustelt, et nad:

   (a) esitaksid oma võrkude ja infosüsteemide turvalisuse hindamiseks vajalikud andmed, sealhulgas dokumenteeritud turvapõhimõtted;

   (b) laseksid kvalifitseeritud sõltumatul asutusel või riigiasutusel teha turvaauditi ja avaldaksid selle tulemused pädevale asutusele.

3. Liikmesriigid tagavad, et pädevatel asutustel on volitused anda operaatoritele ja haldusasutustele siduvaid juhiseid.

4. Kui kahtlustatakse, et intsident on seotud raske kuriteoga, teatavad pädevad asutused sellest õiguskaitseasutustele.

[12] ELT L 124, 20.5.2003, lk 36.

5. Kui intsident põhjustab isikuandmetega seotud rikkumise, teevad pädevad asutused selle lahendamisel tihedat koostööd isikuandmete kaitse asutustega.

6. Liikmesriigid tagavad, et kõik käesoleva peatükiga haldusasutustele ja operaatoritele pandud kohustused võib kohtus läbi vaadata.

Artikkel 16

Standardimine

1. Artikli 14 lõike 1 ühtse kohaldamise tagamiseks julgustavad liikmesriigid võrgu- ja infoturbe seisukohast asjakohaste standardite ja/või spetsifikatsioonide kasutamist.

2. Komisjon koostab rakendusaktidega lõikes 1 osutatud standardite nimekirja. Nimekiri avaldatakse *Euroopa Liidu Teatajas*.

V PEATÜKK

LÕPPSÄTTED

Artikkel 17

Sanktsioonid

1. Liikmesriigid kehtestavad eeskirjad sanktsioonide kohta, mida rakendatakse käesoleva direktiivi kohaselt vastuvõetud siseriiklike õigusnormide rikkumise korral, ning võtavad kõik vajalikud meetmed nende rakendamise tagamiseks. Ettenähtud sanktsioonid peavad olema tõhusad, proportsionaalsed ja hoiatavad. Liikmesriigid teatavad kõnealustest sätetest komisjonile hiljemalt käesoleva direktiivi ülevõtmise kuupäevaks, samuti teatavad nad viivitamata kõigist neid sätteid mõjutavatest hilisematest muudatustest.

2. Liikmesriigid tagavad, et kui turvaintsident puudutab isikuandmeid, on ettenähtud sanktsioonid kooskõlas sanktsioonidega, mis on sätestatud Euroopa Parlamendi ja nõukogu määruses üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta[13].

Artikkel 18

Delegeeritud volituste rakendamine

1. Komisjonile antakse õigus võtta vastu delegeeritud õigusakte käesolevas artiklis sätestatud tingimustel.

2. Komisjonile antakse õigus võtta vastu artikli 9 lõikes 2, artikli 10 lõikes 5 ja artikli 14 lõikes 5 osutatud delegeeritud õigusakte. Komisjon koostab delegeeritud volituste kasutamise kohta aruande hiljemalt üheksa kuud enne viieaastase tähtaja möödumist. Volituste delegeerimist uuendatakse automaatselt samaks ajavahemikuks, välja

[13] SEC(2012) 72 (final).

arvatud juhul, kui Euroopa Parlament või nõukogu esitab selle suhtes vastuväite hiljemalt kolm kuud enne iga ajavahemiku lõppemist.

3. Euroopa Parlament ja nõukogu võivad artikli 9 lõikes 2, artikli 10 lõikes 5 ja artikli 14 lõikes 5 osutatud volituste delegeerimise igal ajal tagasi võtta. Tagasivõtmise otsusega lõpetatakse otsuses nimetatud volituste delegeerimine. Otsus jõustub järgmisel päeval pärast selle avaldamist *Euroopa Liidu Teatajas* või otsuses kindlaksmääratud hilisemal kuupäeval. See ei mõjuta juba jõustunud delegeeritud õigusaktide kehtivust.

4. Niipea kui komisjon on delegeeritud õigusakti vastu võtnud, teeb ta selle üheaegselt teatavaks Euroopa Parlamendile ja nõukogule.

5. Artikli 9 lõike 2, artikli 10 lõike 5 ja artikli 14 lõike 5 alusel vastu võetud delegeeritud õigusakt jõustub üksnes juhul, kui Euroopa Parlament ega nõukogu ei ole kahe kuu jooksul pärast õigusakti teatavakstegemist Euroopa Parlamendile ja nõukogule esitanud selle suhtes vastuväiteid või kui Euroopa Parlament ja nõukogu on enne selle tähtaja möödumist komisjonile teatanud, et nad ei esita vastuväiteid. Kõnealust ajavahemikku võib Euroopa Parlamendi või nõukogu taotlusel kahe kuu võrra pikendada.

Artikkel 19

Komiteemenetlus

1. Komisjoni abistab komitee (võrgu- ja infoturbe komitee). Kõnealune komitee on komitee määruse (EL) nr 182/2011 tähenduses.

2. Käesolevale lõikele viitamisel kohaldatakse määruse (EL) nr 182/2011 artiklit 4.

3. Käesolevale lõikele viitamisel kohaldatakse määruse (EL) nr 182/2011 artiklit 5.

Artikkel 20

Läbivaatamine

Komisjon vaatab käesoleva direktiivi toimimise korrapäraselt läbi ning esitab aruande Euroopa Parlamendile ja nõukogule. Esimene aruanne esitatakse hiljemalt kolm aastat pärast artiklis 21 osutatud ülevõtmise kuupäeva. Selleks võib komisjon paluda, et liikmesriigid esitaksid teavet ilma põhjendamatult viivitamata.

Artikkel 21

Ülevõtmine

1. Liikmesriigid võtavad vastu ja avaldavad käesoleva direktiivi järgimiseks vajalikud õigusnormid hiljemalt [poolteist aastat pärast vastuvõtmist]. Nad edastavad kõnealuste sätete teksti viivitamata komisjonile.

Nad hakkavad neid meetmeid kohaldama alates [poolteist aastat pärast vastuvõtmist].

Kui liikmesriigid need meetmed vastu võtavad, lisavad nad nendesse meetmetesse või nende meetmete ametliku avaldamise korral nende juurde viite käesolevale direktiivile. Sellise viitamise viisi näevad ette liikmesriigid.

2. Liikmesriigid edastavad komisjonile käesoleva direktiiviga reguleeritavas valdkonnas nende poolt vastuvõetud põhiliste siseriiklike õigusnormide teksti.

Artikkel 22

Jõustumine

Käesolev direktiiv jõustub [kahekümnendal] päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Artikkel 23

Adressaadid

Käesolev direktiiv on adresseeritud liikmesriikidele.

Brüssel,

Euroopa Parlamendi nimel *president*	*Nõukogu nimel* *eesistuja*

I LISA

Infoturbeintsidentidega tegelevale meeskonnale (CERT) esitatavad nõuded ja meeskonna ülesanded

CERTile esitatavad nõuded ja tema ülesanded tuleb määratleda piisavalt ja selgelt ning riigi poliitika ja/või õigusnormid peavad neid toetama. Nõuded hõlmavad järgmist:

(1) CERTile esitatavad nõuded

(a) CERT peab tagama oma sideteenuste käideldavuse kõrge taseme, vältides nõrku lülisid, ning kasutama mitmesuguseid vahendeid, mis võimaldavad tal teistega ja teistel temaga ühendust võtta. Sidekanalid peavad olema selgelt nimetatud ning kasutajatele ja koostööpartneritele hästi teada.

(b) CERT peab rakendama ja haldama turvameetmeid, et tagada temani jõudva ja tema poolt käideldava teabe konfidentsiaalsus, terviklus, käideldavus ja autentsus.

(c) CERTi ametiruumide ja tema tööd toetavate infosüsteemide asukoht peab olema turvaline.

(d) Luua tuleb teenusehalduse kvaliteedisüsteem, et CERTi töö tulemuste põhjal järelmeetmeid võtta ja süsteemi pidevalt paremaks muuta. Süsteem peab põhinema selgelt määratletud parameetritel, mille hulka kuuluvad ka ametlikud teenusetasemed ja peamised tulemuslikkuse näitajad.

(e) Talitluspidevus:

– CERTil peab olema taotluste haldamiseks ja suunamiseks sobiv süsteem, et hõlbustada üleandmisi;

– CERTil peab olema piisavalt töötajaid, et tagada alaline kättesaadavus;

– CERTi kasutatava taristu pidevus peab olema tagatud. Selle eesmärgi nimel antakse CERTi kasutusse liiased süsteemid ja varutöökeskkond, et tagada alaline juurdepääs sidevahenditele.

(2) CERTi ülesanded

(a) CERTi ülesanded peavad sisaldama vähemalt järgmist:

– intsidentide seire riigis,

– riskide ja intsidentide kohta varajaste hoiatuste, hoiatuste ja teadaannete esitamine ning teabe levitamine sidusrühmadele,

– intsidentidele reageerimine,

– pidev riskide ja intsidentide analüüsimine ja teadlikkus olukorrast,

– üldsuse teadlikkuse suurendamine interneti kasutamisega seotud riskidest;

– võrgu- ja infoturbealaste kampaaniate korraldamine.

(b) CERT peab sisse seadma koostöö erasektoriga.

(c) Koostöö hõlbustamiseks peab CERT toetama ühiste või standardtoimingute vastuvõtmist ja kasutamist järgmistes valdkondades:

– intsidentide ja riskide käsitlemise protseduurid,

– intsidentide, riskide ja teabe liigitamise kavad,

– parameetrite süstematiseerimine,

– riskide ja intsidentide kohta vahetatava teabe ja süsteemis kasutatavate nimetuste vormingud.

II LISA

Operaatorite loetelu

Vastavalt artikli 3 lõike 8 punktile a:

1. e-kaubanduse platvormid

2. Internetimaksete lüüsid

3. Suhtlusvõrgud

4. Otsingumootorid

5. Pilvandmetöötluse teenused

6. Tarkvarapoed

Vastavalt artikli 3 lõike 8 punktile b:

1. Energeetika

- Elektri- ja gaasitarnijad
- Elektri- ja/või gaasitarnesüsteemide operaatorid ning elektri ja gaasi jaemüüjad lõpptarbijatele
- Maagaasi ülekandesüsteemi, gaasihoidlate ja veeldusjaamade haldurid
- Elektrienergia põhivõrguettevõtjad
- Naftajuhtmed ja naftahoidlad
- Elektri- ja gaasituru operaatorid
- Nafta ja maagaasi tootmise, rafineerimise ja töötlemisega tegelevad operaatorid

2. Transport

- Lennuettevõtjad (kauba ja reisijate õhuvedu)
- Meretransporditeenuste osutajad (ettevõtjad, kes tegelevad sõitjate ja kauba vedamisega merel ja rannavetes)
- Raudtee (taristu haldajad, integreeritud ettevõtjad ja raudteeveoettevõtted)
- Lennujaamad
- Sadamad
- Liikluskorraldusettevõtted
- Logistika abiteenused: a) ladustamine ja hoiustamine, b) veoste käitlemine ja c) muud transpordi tugiteenused

3. Pangandus: krediidiasutused vastavalt direktiivi 2006/48/EÜ artikli 4 lõikele 1.

4. Finantsturu taristu: väärtpaberibörsid ja keskse vastaspoolega kliiringukojad

5. Tervishoiusektor: tervishoiuasutused (kaasa arvatud haiglad ja erakliinikud) ning muud tervishoiuteenuste pakkumises osalevad üksused

ÕIGUSAKTILE LISATAV FINANTSSELGITUS

1. ETTEPANEKU/ALGATUSE RAAMISTIK

1.1. Ettepaneku/algatuse nimetus

1.2. Asjaomased poliitikavaldkonnad vastavalt tegevuspõhise juhtimise ja eelarvestamise (ABM/ABB) struktuurile

1.3. Ettepaneku/algatuse liik

1.4. Eesmärgid

1.5. Ettepaneku/algatuse põhjendus

1.6. Meetme kestus ja finantsmõju

1.7. Ettenähtud eelarve täitmise viisid

2. HALDUSMEETMED

2.1. Seoses ÜPP järelevalve ja hindamisega esitab komisjon Euroopa Parlamendile ja nõukogule iga nelja aasta järel aruande;

2.2. Haldus- ja kontrollisüsteemid

2.3. Pettuste ja muude rikkumiste ärahoidmine

3. ETTEPANEKU/ALGATUSE HINNANGULINE FINANTSMÕJU

3.1. Mitmeaastase finantsraamistiku rubriigid ja kulude eelarveread, millele mõju avaldub

3.2. Hinnanguline mõju kuludele

3.2.1. Üldine hinnanguline mõju kuludele

3.2.2. Hinnanguline mõju tegevusassigneeringutele

3.2.3. Hinnanguline mõju haldusassigneeringutele

3.2.4. Kooskõla kehtiva mitmeaastase finantsraamistikuga

3.2.5. Kolmandate isikute rahaline toetus

3.3. Hinnanguline mõju tuludele

ÕIGUSAKTILE LISATAV FINANTSSELGITUS

1. ETTEPANEKU/ALGATUSE RAAMISTIK

1.1. Ettepaneku/algatuse nimetus

Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv meetmete kohta, millega tagada võrgu- ja infoturbe ühtlaselt kõrge tase kogu Euroopa Liidus

1.2. Asjaomased poliitikavaldkonnad vastavalt tegevuspõhise juhtimise ja eelarvestamise struktuurile[37]

– 09 – Kommunikatsioonivõrgud, sisu ja tehnoloogia

1.3. Ettepaneku/algatuse liik

☒ Ettepanek/algatus käsitleb **uut meedet**

☐ Ettepanek/algatus käsitleb **uut meedet, mis tuleneb katseprojektist / ettevalmistavast meetmest**[38]

☐ Ettepanek/algatus käsitleb **olemasoleva meetme pikendamist**

☐ Ettepanek/algatus käsitleb **ümbersuunatud meedet**

1.4. Eesmärgid

1.4.1. Komisjoni mitmeaastased strateegilised eesmärgid, mida ettepaneku/algatuse kaudu täidetakse

Käesolevas ettepanekus käsitletava direktiivi eesmärk on tagada võrgu- ja infoturbe ühtlaselt kõrge tase kogu Euroopa Liidus.

1.4.2. Erieesmärgid ning asjaomased tegevusalad vastavalt tegevuspõhise juhtimise ja eelarvestamise süsteemile

Ettepanekuga nähakse ette meetmed, millega tagada võrgu ja infosüsteemide ühtlaselt kõrge tase kogu Euroopa Liidus

Erieesmärgid on järgmised:

1. Luua liikmesriikides võrgu- ja infoturbe miinimumtase ja ning parandada seeläbi valmisoleku ja reageerimissuutlikkuse üldist taset.

2. Parandada ELi tasandil võrgu- ja infoturbe alast koostööd, et tulla tõhusalt toiime piiriüleste intsidentide ja ohtudega. Luuakse turvaline teabejagamistaristu, mille kaudu saaksid pädevad asutused vahetada tundlikku ja konfidentsiaalset teavet.

3. Luua riskihalduskultuur ja parandada teabevahetust avaliku ja erasektori vahel.

---

[37] Tegevuspõhine juhtimine ehk ABM (Activity-Based Management) ja tegevuspõhine eelarvestamise struktuur ehk ABB (Activity-Based Budgeting).

[38] Vastavalt finantsmääruse artikli 49 lõike 6 punktile a või b.

Asjaomased tegevusalad vastavalt tegevuspõhise juhtimise ja eelarvestamise süsteemile

Direktiiv puudutab eri sektoritesse (energeetika, transport, krediidiasutused, väärtpaberitega kauplemine, tervishoid ja peamiste internetiteenuste võimaldajad) kuuluvaid üksusi (ettevõtted ja organisatsioonid, sh mõned VKEd), aga ka haldusasutusi. Selles käsitletakse seoseid õigus- ja andmekaitsega ning välissuhete võrgu- ja infoturbealaseid aspekte.

– 09 – Kommunikatsioonivõrgud, sisu ja tehnoloogia

– 02 – Ettevõtlus

– 32 – Energeetika

– 06 – Liikuvus ja transport

– 17: Tervise- ja tarbijakaitse

– 18 – Siseküsimused

– 19 – Välissuhted

– 33 – Õigusküsimused

– 12 – Siseturg

1.4.3. Oodatavad tulemused ja mõju

Täpsustage, milline peaks olema ettepaneku/algatuse oodatav mõju abisaajatele/sihtrühmadele

ELi tarbijate, ettevõtjate ja valitsuste kaitse võrgu ja info turvalisusega seotud ohtude ja riskide eest paraneks märgatavalt.

Täpsemad üksikasjad on esitatud käesolevale õigusakti ettepanekule lisatud komisjoni talituste töödokumendi „Mõjuhinnang” jaotises 8.2 (2. variandi ehk regulatiivse lähenemise mõju).

1.4.4. Tulemus- ja mõjunäitajad

Täpsustage, milliste näitajate alusel hinnatakse ettepaneku/algatuse elluviimist.

Seire ja hindamise näitajaid on kirjeldatud mõjuhindamise jaotises 10.

1.5. Ettepaneku/algatuse põhjendus

1.5.1. Lühi- või pikaajalises perspektiivis täidetavad vajadused

Igal liikmesriigil peaks olema:

– riiklik võrgu- ja infoturbe strateegia;

– võrgu- ja infoturbe koostöökava;

– pädev riiklik võrgu- ja infoturbeasutus ning

–infoturbeintsidentidega tegelev meeskond (CERT)

ELi tasandil peaksid liikmesriigid tegema koostööd koostöövõrgu kaudu.

Haldusasutused ja olulised eraettevõtted peaksid haldama võrgu ja info turvalisusega seotud riske ning teatama pädevatele asutustele võrgu ja info turvalisusega seotud olulise mõjuga intsidentidest.

1.5.2. Euroopa Liidu meetme lisandväärtus

Arvestades, et võrgu- ja infoturve on oma olemuselt piiriülene, ei lase asjaomaste õigusaktide ja põhimõtete erinevused ettevõtjatel vabalt tegutseda mitmes riigis ega saada kasu mastaabisäästust. Kui ELi tasandil ei sekkuta, tekib olukord, kus iga liikmesriik tegutseb üksi, jättes tähelepanuta võrgu ja infosüsteemide omavahelise sõltuvuse.

Seega on nimetatud eemärke parem saavutada ELi tasandi meetmetega kui siis, kui liikmesriigid tegutseksid üksi.

1.5.3. Samalaadsetest kogemustest saadud õppetunnid

Ettepanek toetub analüüsile, mille kohaselt on vaja õigusaktidega ettenähtud kohustusi, et luua võrdsed tingimused ja kaotada mõningad õigustühimikud. Puhtakujuliselt vabatahtliku lähenemisviisi tulemuseks on selles valdkonnas olukord, kus koostööd teeb vaid väike arv hea suutlikkusega liikmesriike.

1.5.4. Kooskõla ja võimalik koostoime muude asjaomaste meetmetega

Ettepanek on täielikult kooskõlas Euroopa digitaalarengu tegevuskavaga ja ühtlasi ka strateegiaga „Euroopa 2020”. Samuti on ettepanek kooskõlas ELi elektroonilise side regulatiivse raamistikuga, ELi direktiiviga Euroopa esmatähtsate infrastruktuuride kohta ja ELi andmekaitsedirektiiviga ning täiendab neid.

Käesolev ettepanek esitatakse koos komisjoni ja liidu välisasjade ja julgeolekupoliitika kõrge esindaja ühisteatisega Euroopa küberjulgeoleku strateegia kohta ning on selle oluline osa.

1.6. Meetme kestus ja finantsmõju

– ☐ Piiratud kestusega ettepanek/algatus

– ☐ Ettepanek/algatus hõlmab ajavahemikku [PP/KK]AAAA–[PP/KK]AAAA

– ☐ Finantsmõju avaldub ajavahemikul AAAA–AAAA

– ☒ Piiramatu kestusega ettepanek/algatus

– Ülevõtmisaeg algab kohe pärast vastuvõtmist (eeldatavasti aastal 2015) ja kestab 18 kuud. Direktiivi rakendamine algab siiski pärast vastuvõtmist ning hõlmab liikmesriikide koostööd toetava turvalise taristu loomist.

– millele järgneb täieulatuslik rakendamine.

1.7. Ettenähtud eelarve täitmise viisid[39]

– ☒ Otsene tsentraliseeritud eelarve täitmine komisjoni poolt

– ☒ Kaudne tsentraliseeritud eelarve täitmine, mille puhul eelarve täitmise ülesanded on delegeeritud:

– ☐rakendusametitele

– ☒ ühenduste asutatud asutustele[40]

– ☐ riigi avalik-õiguslikele asutustele või avalikke teenuseid osutavatele asutustele

– ☐ isikutele, kellele on delegeeritud konkreetsete meetmete rakendamine Euroopa Liidu lepingu V jaotise kohaselt ja kes on kindlaks määratud asjaomases alusaktis finantsmääruse artikli 49 tähenduses

– ☐ Eelarve täitmine koostöös liikmesriikidega

– ☐ Detsentraliseeritud eelarve täitmine koostöös kolmandate riikidega

– ☐ Eelarve täimine ühiselt rahvusvaheliste organisatsioonidega, sealhulgas Euroopa Kosmoseagentuuriga

Mitme eelarve täitmise viisi valimise korral esitage üksikasjad rubriigis „Märkused”.

Märkused:
ENISA on ühenduste loodud detsentraliseeritud amet, kes võib abistada liikmesriike ja komisjoni direktiivi rakendamisel lähtuvalt oma volitustest ja kasutades ameti jaoks 2014.–2020. aasta mitmeaastase finantsaamistikuga ettenähtud vahendeid.

[39] Eelarve täitmise viise selgitatakse koos viidetega finantsmäärusele veebisaidil BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.htmlhttp://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[40] Määratletud finantsmääruse artiklis 185.

2. HALDUSMEETMED

2.1. Järelevalve ja aruandluse eeskirjad

Täpsustage tingimused ja sagedus.

Komisjon vaatab käesoleva direktiivi toimimise korrapäraselt läbi ning esitab aruande Euroopa Parlamendile ja nõukogule.

Komisjon hindab ka direktiivi nõuetekohast ülevõtmist liikmesriikides.

Euroopa ühendamise rahastu ettepanekuga nähakse ette ka võimalus hinnata projektide elluviimise meetodeid ning nende rakendamise mõju, hindamaks kas eesmärgid, sealhulgas keskkonnakaitsealased eesmärgid, on saavutatud.

2.2. Haldus- ja kontrollisüsteemid

2.2.1. Tuvastatud ohud

– projekti rakendamisel võib esineda viivitusi seoses turvalise taristu rajamisega

2.2.2. Ettenähtud kontrollimeetodid

Euroopa ühendamise rahastu toimingute rakendamise lepingutega ja otsustega nähakse ette komisjoni või komisjoni volitatud esindaja teostatav järelevalve ja finantskontroll ning Euroopa Kontrollikoja auditid ja Euroopa Pettustevastase Ameti (OLAFi) poolt kohapeal tehtav kontrollimine.

2.2.3. Kontrollimisega seotud kulud ja tulud ning tõenäoline mittevastavuse tase

Riskipõhine eel- ja järelkontroll ja kohapeal auditeerimise võimalus tagavad, et kontrollimise kulud on mõistlikud.

2.3. Pettuste ja muude rikkumiste ärahoidmine

Täpsustage rakendatavad või kavandatud ennetus- ja kaitsemeetmed.

Komisjon astub vajalikke samme, tagamaks, et käesoleva direktiivi alusel rahastatavate meetmete rakendamisel kaitstakse liidu finantshuve pettuse, korruptsiooni ja muu ebaseadusliku tegevuse vastu ennetustegevusega, tõhusa kontrolliga ja alusetult väljamakstud summade sissenõudmisega ning vajaduse korral tõhusate, proportsionaalsete ja hoiatavate karistustega.

Komisjonil või tema esindajatel ja kontrollikojal on õigus auditeerida dokumentide põhjal ja kohapeal kõiki toetusesaajaid, töövõtjaid ja alltöövõtjaid, keda on käesoleva programmi alusel rahastatud liidu vahenditest.

Euroopa Pettustevastane Amet (OLAF) võib korraldada sellise rahastamisega otseselt või kaudselt seotud ettevõtjate tööruumides kohapealseid kontrolle, mis peavad toimuma määruses (Euratom, EÜ) nr 2185/96 sätestatud korras ning mille eesmärk on teha kindlaks, kas toetuslepingu, toetuse andmise otsuse või liidu

eelarvest rahastamise lepinguga seoses esineb pettust, korruptsiooni või mis tahes muud liidu finantshuve kahjustavat ebaseaduslikku tegevust.

Ilma et see piiraks eelmiste lõikude kohaldamist, antakse kolmandate riikide ja rahvusvaheliste organisatsioonidega sõlmitud lepingutega, toetuslepingutega ja toetuse määramise otsustega, samuti käesoleva direktiivi rakendamisest tulenevate lepingutega komisjonile, kontrollikojale ja OLAFile selgesõnaliselt õigus selliseks auditeerimiseks ja kohapealseks kontrolliks.

Euroopa ühendamise rahastu kohaselt põhinevad toetus- ja hankelepingud tavamallidel, millega nähakse ette üldiselt rakendatavad pettusevastased meetmed

3. ETTEPANEKU/ALGATUSE HINNANGULINE FINANTSMÕJU

3.1. Mitmeaastase finantsraamistiku rubriigid ja kulude eelarveread, millele mõju avaldub

- Olemasolevad eelarveread

Järjestage mitmeaastase finantsraamistiku rubriikide kaupa ja iga rubriigi sees eelarveridade kaupa.

Mitmeaastase finantsraamistiku rubriik	Eelarverida	Assigneeringute liik	Rahaline osalus			
	Nr [Nimetus……...…….]	Liigendatud/ liigendamata[41]	EFTA[42] riigid	Kandidaatriigid[43]	Kolmandad riigid	Rahaline osalus finantsmääruse artikli 18 lõike 1 punkti aa tähenduses
	09 03 02 Avalike elektrooniliste teenuste omavahelise ühendamise ja koostalitluse ning sellistele võrkudele juurdepääsu tagamine.	Liigendatud	EI	EI	EI	EI

- Uued eelarveread, mille loomist taotletakse (ei kohaldata)

Järjestage mitmeaastase finantsraamistiku rubriikide kaupa ja iga rubriigi sees eelarveridade kaupa.

Mitmeaastase finantsraamistiku rubriik	Eelarverida	Assigneeringute liik	Osalus			
	Number [Nimetus……..]	Liigendatud/liigendamata	EFTA riigid	Kandidaatriigid	Kolmandad riigid	Rahaline osalus finantsmääruse artikli 18 lõike 1 punkti aa tähenduses
	[XX.YY.YY.YY]		JAH/EI	JAH/EI	JAH/EI	JAH/EI

41 Liigendatud assigneeringud / liigendamata assigneeringud

42 EFTA: Euroopa Vabakaubanduse Assotsiatsioon.

43 Kandidaatriigid ja vajaduse korral Lääne-Balkani potentsiaalsed kandidaatriigid.

3.2. Hinnanguline mõju kuludele

3.2.1. Üldine hinnanguline mõju kuludele

miljonites eurodes (kolm kohta pärast koma)

Mitmeaastase finantsraamistiku rubriik:	1	Arukas ja kaasav majanduskasv

<….> peadirektoraat			2015* [44]	Aasta **2016**	Aasta **2017**	Aasta **2018**	Järgmised aastad (2019–2021) ja edaspidi			**KOKKU**
• Tegevusassigneeringud										
09 03 02	Kulukohustused	(1)	1,250**	0,00						**1,250**
	Maksed	(2)	0,750	0,250	0,250					**1,250**
Eriprogrammide vahenditest rahastatavad haldusassigneeringud[45]			**0,00**							**0,0**
Eelarverea number		(3)	**0,00**							**0,00**
<….> peadirektoraadi assigneeringud KOKKU	Kulukohustused	=1+1a +3	1,250	0,00						**1,250**
	Maksed	=2+2a +3	0,750	0,250	0,250					**1,250**

• Tegevusassigneeringud KOKKU	Kulukohustused	(4)	1,250	0,00						**1,250**
	Maksed	(5)	0,750	0,250	0,250					**1,250**

[44] Aasta N, mil alustatakse ettepaneku/algatuse rakendamist.

[45] Tehniline ja/või haldusabi ning ELi programmide ja/või meetmete rakendamiseks antava toetusega seotud kulud (endised B..A read), otsene teadustegevus, kaudne teadustegevus.

• Eriprogrammide vahenditest rahastatavad haldusassigneeringud KOKKU		(6)	**0,00**							
Mitmeaastase finantsraamistiku **RUBRIIGI 1 assigneeringud KOKKU**	Kulukohustused	=4+ 6	1,250	0,000						**1,250**
	Kulukohustused	=5+ 6	0,750	0,250	0,250					**1,250**

* Täpne ajastus oleneb sellest, millal seadusandja ettepaneku vastu võtab (st kui direktiiv võetakse vastu 2014. aastal, algab olemasoleva taristu kohandamine 2015. aastal, vastasel juhul aga aasta hiljem).

** Kui liikmesriigid otsustavad kasutada olemasolevat taristut ja katta ühekordsed kohandamiskulud ELi eelarvest, nagu selgitati jaotistes 1.4.3 ja 1.7, on direktiivi III peatüki kohast liikmesriikide koostööd (varajane hoiatamine, koordineeritud reageerimine jne) toetava võrgu kohandamise kulud hinnanguliselt 1 250 000 eurot. See summa on pisut suurem kui mõjuhinnangus nimetatud („ligikaudu 1 miljon eurot”), sest aluseks on võetud täpsem prognoos selle kohta, millistest komponentidest peaks selline taristu koosnema. Vajalike komponentide ja nendega seotud kulude puhul lähtuti Teadusuuringute Ühiskeskuse hinnangust, mis toetub muudes valdkondades (nt rahvatervis) samalaadsete süsteemide väljatöötamisel omandatud kogemustele. Komponendid hõlmaksid järgmist: võrgu- ja infoturbe kiirhoiatuste ja teatamise süsteem (275 000 eurot), teabevahetusplatvorm (400 000 eurot), varajase hoiatamise ja reageerimise süsteem (275 000 eurot), kriisikeskus (300 000 eurot) ehk kokku 1 250 000 eurot. Üksikasjalikum rakenduskava koostatakse tulevase teostatavusuuringu raames vastavalt erilepingule SMART 2012/0010 „'Feasibility study and preparatory activities for the implementation of a European early warning and response system against cyber-attacks and disruptions”.

Juhul kui ettepanek/algatus mõjutab mitut rubriiki:

• Tegevusassigneeringud KOKKU	Kulukohustused	(4)	0,000	0,000						
	Kulukohustused	(5)	0,000	0,000						
• Eriprogrammide vahenditest rahastatavad haldusassigneeringud KOKKU		(6)	**0,000**	**0,000**						
Mitmeaastase finantsraamistiku **RUBRIIKIDE 1–4 assigneeringud KOKKU** (võrdlussumma)	Kulukohustused	=4+ 6	1,250	0,000						1,250
	Maksed	=5+ 6	0,750	0,250	0,250					1,250

Mitmeaastase finantsraamistiku rubriik	**5**	„Halduskulud”

miljonites eurodes (kolm kohta pärast koma)

		Aasta **2015**	Aasta **2016**	Aasta **2017**	Aasta **2018**	Järgmised aastad (2019–2021) ja edaspidi			**KOKKU**
DG:CNECT									
• Personalikulud		0,572	0,572	0,572	0,572	0,572	0,572	**0,572**	**4,004**
• Muud halduskulud		0,318	0,118	0,318	0,118	0,318	0,118	**0,118**	**1,426**
Peadirektoraat CNECT **KOKKU**	Assigneeringud	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Mitmeaastase finantsraamistiku **RUBRIIGI 5 assigneeringud KOKKU**	(Kulukohustuste kogusumma = maksete kogusumma)	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

miljonites eurodes (kolm kohta pärast koma)

		Aasta **2015**[46]	Aasta **2016**	Aasta **2017**	Aasta **2018**	Järgmised aastad (2019–2021) ja edaspidi			**KOKKU**
Mitmeaastase finantsraamistiku **RUBRIIKIDE 1–5 assigneeringud KOKKU**	Kulukohustused	2,140	0,690	0,890	0,690	0,890	0,690	0,690	**6,680**
	Kulukohustused	1,640	0,940	1,140	0,690	0,890	0,690	0,690	**6,680**

[46] Aasta N, mil alustatakse ettepaneku/algatuse rakendamist.

3.2.2. Hinnanguline mõju tegevusassigneeringutele

– ☐ Ettepanek/algatus ei hõlma tegevusassigneeringute kasutamist

– ☑ Ettepanek/algatus hõlmab tegevusassigneeringute kasutamist, mis toimub järgmiselt:

– kulukohustuste assigneeringud miljonites eurodes (kolm kohta pärast koma)

Täpsustada eesmärgid ja väljundid ⇩			Aasta **2015***		Aasta **2016**		Aasta **2017**		Aasta **2018**		Järgmised aastad (2019–2021) ja edaspidi						**KOKKU**	
	VÄLJUNDID																	
	Väljundi liik[47]	Väljundi keskmine kulu	Väljundite arv	Kulu	Väljundite arv	Kulu	Väljundite arv	Kulu	Väljundite arv	Kulu	Väljundite arv	Kulu	Väljundite arv	Kulu	Väljundite arv	Kulu	Väljundite arv kokku	Kulud kokku
ERIEESMÄRK nr 2[48] Turvaline infovahetustaristu																		
–Väljund	Infrastruktuuri kohandamine																	
Erieesmärk nr 2 kokku			1	1,250**													1	1,250
KULUD KOKKU				1,250														1,250

47 Väljunditena käsitatakse tarnitavaid tooteid ja osutatavaid teenuseid (nt rahastatud üliõpilasvahetuste arv, ehitatud teede pikkus kilomeetrites jms).

48 Vastavalt punktis 1.4.2 nimetatud erieesmärkidele.

* Täpne ajastus oleneb sellest, millal seadusandja ettepaneku vastu võtab (st kui direktiiv võetakse vastu 2014. aastal, algab olemasoleva taristu kohandamine 2015. aastal, vastasel juhul aga aasta hiljem).

** Vt punkt 3.2.1.

3.2.3. Hinnanguline mõju haldusassigneeringutele

3.2.3.1. Ülevaade

– ☐ Ettepanek/algatus ei hõlma haldusassigneeringute kasutamist

– ☑ Ettepanek/algatus hõlmab haldusassigneeringute kasutamist, mis toimub järgmiselt:

miljonites eurodes (kolm kohta pärast koma)

	Aasta **2015**[49]	Aasta **2016**	Aasta **2017**	Aasta **2018**	Järgmised aastad (2019–2021) ja edaspidi			**KOKKU**
Mitmeaastase finantsraamistiku RUBRIIK 5								
Personalikulud	0,572	0,572	0,572	0,572	0,572	0,572	0,572	**4,004**
Muud halduskulud	0,318	0,118	0,318	0,118	0,318	0,118	0,118	**1,426**
Mitmeaastase finantsraamistiku RUBRIIK 5 kokku	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Mitmeaastase finantsraamistiku RUBRIIGIST 5[50] välja jäävad kulud								
Personalikulud	0,000	0,000						**0,000**
Muud halduskulud								
Mitmeaastase finantsraamistiku RUBRIIGIST 5 välja jäävad kulud kokku	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

KOKKU	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Vajalikud haldusassigneeringud kaetakse juba meetme haldamiseks määratud CNECT peadirektoraadi assigneeringutega ja/või peadirektoraadi sees ümbermääratud assigneeringute teel; vajaduse korral võidakse meedet haldavale peadirektoraadile eraldada iga-aastase

49 Aasta N, mil alustatakse ettepaneku/algatuse rakendamist.

50 Tehniline ja/või haldusabi ning ELi programmide ja/või meetmete rakendamiseks antava toetusega seotud kulud (endised B..A read), otsene teadustegevus, kaudne teadustegevus.

vahendite eraldamise menetluse käigus täiendavaid assigneeringuid, arvestades olemasolevate eelarvepiirangutega.

Euroopa Võrgu- ja Infoturbeamet (ENISA) võib abistada liikmesriike ja komisjoni direktiivi rakendamisel lähtuvalt oma volitustest ja kasutades ameti jaoks 2014.–2020. aasta mitmeaastase finantsaamistikuga ettenähtud vahendeid, st ilma et selleks nähtaks ette täiendavaid eelarvevahendeid või inimjõudu.

3.2.3.2. Hinnanguline personalivajadus

– ☐ Ettepanek/algatus ei hõlma personali kasutamist

– ☑ Ettepanek/algatus hõlmab personali kasutamist, mis toimub järgmiselt:

Põhimõtteliselt ei ole täiendavaid töötajaid vaja. Personalivajadused on väga väikesed ning kaetakse tegevust haldava peadirektoraadi töötajatega.

Hinnanguline väärtus täisarvuna (või maksimaalselt ühe kohaga pärast koma)

		Aasta **2015**	Aasta **2016**	Aasta **2017**	Aasta **2018**	Järgmised aastad (2019–2021) ja edaspidi		
• Ametikohtade loeteluga ette nähtud ametikohad (ametnikud ja ajutised töötajad)								
09 01 01 01 (komisjoni peakorteris ja esindustes)		4	4	4	4	4	4	4
XX 01 01 02 (delegatsioonid)								
XX 01 05 01 (kaudne teadustegevus)								
10 01 05 01 (otsene teadustegevus)								
• Koosseisuvälised töötajad (täistööajale taandatud töötajad)[51]								
09 01 02 01 (üldvahenditest rahastatavad CA, INT, SNE)		1	1	1	1	1	1	1
XX 01 02 02 (lepingulised töötajad, kohalikud töötajad, riikide lähetatud eksperdid, renditööjõud ja noored eksperdid delegatsioonides)								
XX 01 04 aa[52]	- peakorteris[53]							
	- delegatsioonides							
XX 01 05 02 ((lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud kaudse teadustegevuse valdkonnas)								
10 01 05 02 (lepingulised töötajad, riikide lähetatud eksperdid ja renditööjõud otsese teadustegevuse valdkonnas)								
Muud eelarveread (täpsustage)								
KOKKU		**5**	**5**	**5**	**5**	**5**	**5**	**5**

XX osutab asjaomasele poliitikavaldkonnale või eelarvejaotisele.

51 Lepingulised töötajad, renditööjõud, noored eksperdid delegatsioonides, kohalikud töötajad, riikide lähetatud eksperdid.

52 Tegevusassigneeringutest rahastatavate koosseisuväliste töötajate ülempiiri arvestades (endised B.A read).

53 Peamiselt struktuurifondid, Euroopa Maaelu Arengu Põllumajandusfond ja Euroopa Kalandusfond.

Personalivajadused kaetakse haldavale peadirektoraadile CNECT juba jaotatud ja/või peadirektoraadis ümberpaigutatud vahenditest, vajaduse korral koos lisaeraldistega, mis võidakse meedet juhtivale peadirektoraadile anda iga-aastase vahendite eraldamise protseduuri raames, võttes arvesse eelarvepiiranguid.

Euroopa Võrgu- ja Infoturbeamet (ENISA) võib abistada liikmesriike ja komisjoni direktiivi rakendamisel lähtuvalt oma praegustest volitustest ja kasutades ameti jaoks 2014.–2020. aasta mitmeaastase finantsaamistikuga ettenähtud vahendeid, st ilma et selleks nähtaks ette täiendavaid eelarvevahendeid või inimjõudu.

Ülesannete kirjeldus:

Ametnikud ja ajutised teenistujad	– Delegeeritud õigusaktide ettevalmistamine vastavalt artikli 14 lõikele 3 – Rakendusaktide ettevalmistamine vastavalt artiklile 8, artikli 9 lõikele 2, artiklile 12, artikli 14 lõikele 5 ja artiklile 16 – Võrgu kaudu toimuvale koostööle kaasaaitamine nii poliitilisel kui ka praktilise töö tasandil – Rahvusvaheliste läbirääkimiste pidamine ja võimalike rahvusvaheliste kokkulepete sõlmimine
Koosseisuvälised töötajad	Kõigi eelkirjeldatud ülesannete toetamine vastavalt vajadusele

3.2.4. Kooskõla kehtiva mitmeaastase finantsraamistikuga

– ☑ Ettepanek/algatus on kooskõlas kehtiva mitmeaastase finantsraamistikuga.

– ☐ Ettepanekuga/algatusega kaasneb mitmeaastase finantsraamistiku asjaomase rubriigi ümberplaneerimine.

Ettepaneku hinnanguline finantsmõju tegevuskuludele tekib siis, kui liikmesriigid otsustavad kohandada olemasolevat taristut ja annavad selle ülesande elluviimise komisjonile vastavalt 2014.–2020. aasta mitmeaastasele finantsraamistikule. Asjaomased ühekordsed kulud kaetaks Euroopa ühendamise rahastust piisavate vahendite olemasolu korral. Alternatiivina võivad liikmesriigid jagada omavahel taristu kohandamise või uue taristu loomise kulud.

– ☐ Ettepanekuga/algatusega seoses on vajalik paindlikkusinstrumendi kohaldamine või mitmeaastase finantsraamistiku läbivaatamine[54].

Ei kohaldata.

3.2.5. Kolmandate isikute rahaline toetus

– Ettepanek/algatus ei hõlma kolmandate isikute poolset kaasrahastamist.

3.3. Hinnanguline mõju tuludele

– ☑ Ettepanekul/algatusel puudub finantsmõju tuludele.

[54] Vt institutsioonidevahelise kokkuleppe punktid 19 ja 24.