Euroopa Parlament
2019-2024

Väliskomisjon

2023/0109(COD)

27.10.2023

ARVAMUS

Esitaja: väliskomisjon

Saaja: tööstuse, teadusuuringute ja energeetikakomisjon

ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus, millega nähakse ette meetmed, et tugevdada liidus solidaarsust ja suurendada suutlikkust küberohtude ja -intsidentide avastamiseks, nendeks valmistumiseks ja neile reageerimiseks
(COM(2023)0209) – C9-0136/2023 – 2023/0109(COD))

Arvamuse koostaja: Dragoş Tudorache

PA_Legam

Muudatusettepanek 1

Ettepanek võtta vastu määrus
Põhjendus 1

Komisjoni ettepanek	*Muudatusettepanek*
(1) Info- ja kommunikatsioonitehnoloogia kasutamine ja sõltuvus sellest tehnoloogiast on muutunud oluliseks küsimuseks kõigis ***majandussektorites***, kuna haldusasutused, ettevõtjad ja kodanikud on kõigis sektorites ja piiriüleselt omavahel seotud ja üksteisest sõltuvad rohkem kui kunagi varem.	(1) Info- ja kommunikatsioonitehnoloogia kasutamine ja sõltuvus sellest tehnoloogiast on muutunud oluliseks küsimuseks kõigis ***majandus- ja sõjalise tegevuse sektorites***, kuna haldusasutused, ettevõtjad ja kodanikud ***ning sõjalised ja kaitsevaldkonna osalejad*** on kõigis sektorites ja piiriüleselt omavahel seotud ja üksteisest sõltuvad rohkem kui kunagi varem.

Muudatusettepanek 2

Ettepanek võtta vastu määrus
Põhjendus 2

Komisjoni ettepanek	*Muudatusettepanek*
(2) Küberintsidentide ulatus, sagedus ja mõju üha suurenevad. Muu hulgas on sagenenud tarneahela ründed, mille eesmärk on küberspionaaž, lunaraha nõudmine või häirete põhjustamine. Need kujutavad endast suurt ohtu võrgu- ja infosüsteemide toimimisele. Võttes arvesse küberohtude vallas toimuvat kiiret arengut, nõuab oht, et aset võib leida ulatuslik intsident, mis põhjustab suuri häireid või olulist kahju elutähtsale taristule, kõrgendatud valmisolekut kõigil liidu küberturvalisuse raamistiku tasanditel. ***See oht, mis*** ei ole seotud üksnes Venemaa sõjalise agressiooniga Ukraina vastu***, jääb*** tõenäoliselt püsima, võttes arvesse praegustesse geopoliitilistesse pingetesse kaasatud valitsusega seotud osalejate, kurjategijate ja häktivistide arvukust. Küberintsidendid võivad takistada avalike teenuste osutamist ja majandustegevust, sealhulgas kriitilise või ülikriitilise	(2) Küberintsidentide ulatus, sagedus ja mõju üha suurenevad. Muu hulgas on sagenenud tarneahela ründed, mille eesmärk on küberspionaaž, lunaraha nõudmine või häirete põhjustamine. Need kujutavad endast suurt ohtu võrgu- ja infosüsteemide toimimisele. Võttes arvesse küberohtude vallas toimuvat kiiret arengut, nõuab oht, et aset võib leida ulatuslik intsident, mis põhjustab suuri häireid või olulist kahju elutähtsale taristule, kõrgendatud valmisolekut kõigil liidu küberturvalisuse raamistiku tasanditel. ***Nende ohtude tõsidust arvestades tõusis see teema päevakorras veelgi kõrgemale kohale sõja naasmise tõttu meie maailmajakku. Need ohud*** ei ole seotud üksnes Venemaa sõjalise agressiooniga Ukraina vastu ***ja jäävad*** tõenäoliselt püsima, võttes arvesse praegustesse geopoliitilistesse pingetesse kaasatud valitsusega seotud osalejate, kurjategijate

tähtsusega sektorites, tekitada märkimisväärset rahalist kahju, vähendada kasutajate kindlustunnet, põhjustada suurt kahju liidu majandusele ning isegi tuua tervist kahjustavaid või eluohtlikke tagajärgi. Peale selle on küberintsidendid prognoosimatud, kuna need tekivad ja arenevad sageli väga lühikese aja jooksul, ei piirdu ühe konkreetse geograafilise piirkonnaga ning hõlmavad mitut liikmesriiki või levivad kohe mitmesse liikmesriiki.	ja häktivistide arvukust. Küberintsidendid võivad takistada avalike teenuste osutamist ja majandustegevust, sealhulgas kriitilise või ülikriitilise tähtsusega sektorites, tekitada märkimisväärset rahalist kahju, vähendada kasutajate kindlustunnet, põhjustada suurt kahju liidu majandusele ***ja julgeolekule*** ning isegi tuua tervist kahjustavaid või eluohtlikke tagajärgi***, sest need võivad kahjustada kohaliku või riikliku julgeolekuga seotud rajatisi***. Peale selle on küberintsidendid prognoosimatud, kuna need tekivad ja arenevad sageli väga lühikese aja jooksul, ei piirdu ühe konkreetse geograafilise piirkonnaga ning hõlmavad mitut liikmesriiki või levivad kohe mitmesse liikmesriiki. ***Küberturvalisus on oluline, et kaitsta Euroopa väärtusi, ja see tagab meie demokraatia toimimise, kaitstes valimisteks vajalikku taristut ja demokraatlikke menetlusi igasuguse välissekkumise eest.***

Muudatusettepanek 3

Ettepanek võtta vastu määrus
Põhjendus 2 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(2a) Küberturvalisus on äärmiselt oluline, et tagada liidu turvalisus ning vältida olukorda, kus nii riiklikud kui ka valitsusvälised kuritahtlikud osalejad õõnestavad meie demokraatiat, majandust ja julgeolekut. On tähtis vältida killustumist, kuna see ei võimaldaks asjakohaselt reageerida, eriti mitme liikmesriigi või riikidevahelise elutähtsa taristu vastu suunatud ulatusliku küberrünnaku korral. Seetõttu on vaja liidu asutust, mis toimiks kõigi olemasolevate ja tulevaste küberjulgeoleku vahendite, rahastamisvahendite ja mehhanismide koordineerimise platvormina.

Muudatusettepanek 4

Ettepanek võtta vastu määrus
Põhjendus 3

Komisjoni ettepanek	*Muudatusettepanek*
(3) Vaja on suurendada liidu tööstus- ja teenustesektori konkurentsivõimet kogu digimajanduses ning toetada nende digiüleminekut, tõstes digitaalsel ühtsel turul küberturvalisuse taset. Nagu on soovitatud Euroopa tuleviku konverentsi kolmes ettepanekus,[16] tuleb suurendada kodanike, ettevõtjate ja elutähtsas taristus tegutsevate üksuste võimet pidada vastu üha suurenevatele küberohtudele, millel võib olla laastav mõju ühiskonnale ja majandusele. Seepärast on vaja suurendada investeeringuid taristutesse ja teenustesse, mis toetavad küberohtude ja -intsidentide kiiremat avastamist ja kiiremat reageerimist, ning liikmesriigid vajavad abi, et paremini valmistuda olulisteks ja ulatuslikeks küberintsidentideks ja neile paremini reageerida. Ka liit peaks suurendama neis valdkondades oma suutlikkust, eriti mis puudutab küberohte ja -intsidente käsitlevate andmete kogumist ja analüüsimist.	(3) Vaja on suurendada liidu tööstus- ja teenustesektori konkurentsivõimet kogu digimajanduses ning toetada nende digiüleminekut, tõstes digitaalsel ühtsel turul küberturvalisuse taset. Nagu on soovitatud Euroopa tuleviku konverentsi kolmes ettepanekus,[16] tuleb suurendada kodanike, ettevõtjate ja elutähtsas taristus tegutsevate üksuste võimet pidada vastu üha suurenevatele küberohtudele, millel võib olla laastav mõju ühiskonnale ja majandusele. Seepärast on vaja suurendada investeeringuid taristutesse ja teenustesse, mis toetavad küberohtude ja -intsidentide kiiremat avastamist ja kiiremat reageerimist, ning liikmesriigid vajavad abi, et paremini valmistuda olulisteks ja ulatuslikeks küberintsidentideks ja neile paremini reageerida. Ka liit peaks suurendama neis valdkondades oma suutlikkust, eriti mis puudutab küberohte ja -intsidente käsitlevate andmete kogumist ja analüüsimist ***ning suutlikkust tegutseda ennetavalt ja küberohtudele ja -intsidentidele otsustavalt reageerida***.
[16] https://futureu.europa.eu/et/.	[16] https://futureu.europa.eu/et/.

Muudatusettepanek 5

Ettepanek võtta vastu määrus
Põhjendus 4

Komisjoni ettepanek	*Muudatusettepanek*
(4) Liit on juba rakendanud mitut meedet, et vähendada nõrkusi ning suurendada elutähtsate taristute ja kriitilise	(4) Liit on juba rakendanud mitut meedet, et vähendada nõrkusi ning suurendada elutähtsate taristute ja kriitilise

tähtsusega üksuste vastupidavusvõimet küberriskide suhtes, eeskätt Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555,[17] komisjoni soovitust (EL) 2017/1584,[18] Euroopa Parlamendi ja nõukogu direktiivi 2013/40/EL[19] ning Euroopa Parlamendi ja nõukogu määrust (EL) 2019/881[20]. Peale selle kutsutakse nõukogu soovituses, mis käsitleb kogu liitu hõlmavat koordineeritud lähenemisviisi elutähtsa taristu toimepidevuse tugevdamiseks, liikmesriike üles võtma kiiresti tulemuslikke meetmeid ning tegema üksteise, komisjoni ja teiste asjaomaste avaliku sektori asutustega ning samuti asjaomaste üksustega lojaalselt, tulemuslikult, solidaarselt ja koordineeritult koostööd, et parandada siseturul oluliste teenuste osutamisel kasutatava elutähtsa taristu toimepidevust.

tähtsusega üksuste vastupidavusvõimet küberriskide suhtes, eeskätt Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555,[17] komisjoni soovitust (EL) 2017/1584,[18] Euroopa Parlamendi ja nõukogu direktiivi 2013/40/EL[19] ning Euroopa Parlamendi ja nõukogu määrust (EL) 2019/881[20]. Peale selle kutsutakse nõukogu soovituses, mis käsitleb kogu liitu hõlmavat koordineeritud lähenemisviisi elutähtsa taristu toimepidevuse tugevdamiseks, liikmesriike üles võtma kiiresti tulemuslikke meetmeid ning tegema üksteise, komisjoni ja teiste asjaomaste avaliku sektori asutustega ning samuti asjaomaste üksustega lojaalselt, tulemuslikult, ***ennetavalt,*** solidaarselt ja koordineeritult koostööd, et parandada siseturul oluliste teenuste osutamisel kasutatava elutähtsa taristu toimepidevust. ***Lisaks kiitis liit 2022. aasta märtsis heaks ja käivitas oma julgeoleku- ja kaitsevaldkonna strateegilise kompassi, milles keskendutakse muu hulgas küberjulgeoleku tugevdamisele ja rahvusvahelise koostöö tõhustamisele eelkõige selles küsimuses sarnaselt meelestatud liitlaste ja demokraatlike partneritega. Küberjulgeolekule keskenduti ka hiljutises ELi ja NATO koostööd käsitlevas kolmandas ühisdeklaratsioonis, mis võeti vastu 2023. aasta jaanuaris. Täpsemalt soovitati ELi ja NATO rakkerühma lõplikus hindamisaruandes täielikult ära kasutada ELi ja NATO vahelist koostoimet[1], sealhulgas vahetada tsiviil- ja sõjaliste osalejate vahel parimaid tavasid asjakohaste kübervaldkonna poliitikameetmete ja õigusaktide rakendamise kohta.***

[1] https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en

[17] Euroopa Parlamendi ja nõukogu

[17] Euroopa Parlamendi ja nõukogu

14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (ELT L 333, 27.12.2022).

[18] Komisjoni 13. septembri 2017. aasta soovitus (EL) 2017/1584 koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral (ELT L 239, 19.9.2017, lk 36).

[19] Euroopa Parlamendi ja nõukogu 12. augusti 2013. aasta direktiiv 2013/40/EL, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega asendatakse nõukogu raamotsus 2005/222/JSK (ELT L 218, 14.8.2013, lk 8).

[20] Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 15).

14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (ELT L 333, 27.12.2022).

[18] Komisjoni 13. septembri 2017. aasta soovitus (EL) 2017/1584 koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral (ELT L 239, 19.9.2017, lk 36).

[19] Euroopa Parlamendi ja nõukogu 12. augusti 2013. aasta direktiiv 2013/40/EL, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega asendatakse nõukogu raamotsus 2005/222/JSK (ELT L 218, 14.8.2013, lk 8).

[20] Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 15).

Muudatusettepanek 6

Ettepanek võtta vastu määrus
Põhjendus 6

Komisjoni ettepanek	*Muudatusettepanek*
(6) Ühisteatises ELi küberkaitsepoliitika kohta,[22] mis võeti vastu 10. novembril 2022, teatati ELi kübersolidaarsuse algatusest, mille eesmärgid on parandada ELi ühist avastamis- ja reageerimissuutlikkust ning olukorrateadlikkust, edendades ELi infoturbekeskuste taristu kasutusele võtmist, ning toetada usaldusväärsete	(6) Ühisteatises ELi küberkaitsepoliitika kohta,[22] mis võeti vastu 10. novembril 2022, teatati ELi kübersolidaarsuse algatusest, mille eesmärgid on parandada ELi ühist avastamis- ja reageerimissuutlikkust ning olukorrateadlikkust, edendades ELi infoturbekeskuste taristu kasutusele võtmist, ning toetada usaldusväärsete

eraõiguslike teenuseosutajate teenuseid hõlmava ELi küberreservi järkjärgulist loomist ja kriitilise tähtsusega üksuste ELi riskihindamise alusel testimist võimalike nõrkuste avastamiseks.	eraõiguslike teenuseosutajate teenuseid hõlmava ELi küberreservi järkjärgulist loomist ja kriitilise tähtsusega üksuste ELi riskihindamise alusel testimist võimalike nõrkuste avastamiseks. ***Lisaks näitavad kiiresti arenev küberohtude keskkond ja tehnoloogia arengu kiire tempo vajadust tsiviil-sõjalise koordineerimise ja koostöö tõhustamise järele, nagu rõhutas nõukogu oma järeldustes ELi küberkaitsepoliitika kohta[1].*** ***[1] Nõukogu järeldused ELi küberkaitsepoliitika kohta, mille nõukogu kiitis heaks oma 22. mai 2023. aasta istungil (9618/23).***
[22] Ühisteatis Euroopa Parlamendile ja nõukogule „ELi küberkaitsepoliitika“, JOIN(2022) 49 final.	[22] Ühisteatis Euroopa Parlamendile ja nõukogule „ELi küberkaitsepoliitika“, JOIN(2022) 49 final.

Muudatusettepanek 7

Ettepanek võtta vastu määrus
Põhjendus 6 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(6a) Arvestades tsiviil- ja sõjaliste küsimuste vaheliste piiride hägustumist ning kübervahendite ja -tehnoloogia kahesugust kasutust, vajab digivaldkond kõikehõlmavat ja terviklikku lähenemisviisi. Rohkem kui ühte liikmesriiki hõlmava ulatusliku küberintsidendi ja kriisi korral tuleks kehtestada asjakohane kriisiohje ja -juhtimine. Sellised struktuurid peaksid korraldama teabevahetust, koordineerimist ja koostööd liidu välisjulgeoleku ja sõjalise kriisiohje struktuuridega ning liikmesriikide julgeoleku ja kaitse eest vastutavate organitega (küberkaitsekogukond). See peaks kehtima ka ühise julgeoleku- ja kaitsepoliitika operatsioonide ja missioonide kohta, mida viib liit ellu

selleks, et tagada rahu ja stabiilsus oma naabruses ja kaugemal.

Muudatusettepanek 8

Ettepanek võtta vastu määrus
Põhjendus 7

Komisjoni ettepanek	*Muudatusettepanek*
(7) Vaja on parandada küberohtude ja -intsidentide avastamist ja olukorrateadlikkust kogu liidus ning tugevdada solidaarsust, suurendades liikmesriikide ja liidu valmisolekut olulisteks ja ulatuslikeks küberintsidentideks ning suutlikkust neile reageerida. Seepärast tuleks välja arendada üleeuroopaline infoturbekeskuste taristu (Euroopa küberkilp), et tagada ja parandada ühist avastamissuutlikkust ja olukorrateadlikkust, luua küberhädaolukorra mehhanism, et toetada liikmesriike valmistumisel olulisteks ja ulatuslikeks küberintsidentideks, neile reageerimisel ja neist vahetul taastumisel, ning luua küberintsidentide läbivaatamise mehhanism, et vaadata läbi ja hinnata konkreetseid olulisi või ulatuslikke intsidente. Need meetmed ei piira Euroopa Liidu toimimise lepingu (edaspidi „ELi toimimise leping“) artiklite 107 ja 108 kohaldamist.	(7) Vaja on parandada küberohtude ja -intsidentide avastamist ja olukorrateadlikkust kogu liidus ning tugevdada solidaarsust, suurendades liikmesriikide ja liidu valmisolekut olulisteks ja ulatuslikeks küberintsidentideks ning suutlikkust neile reageerida. Seepärast tuleks välja arendada üleeuroopaline infoturbekeskuste taristu (Euroopa küberkilp), et tagada ja parandada ühist avastamissuutlikkust ja olukorrateadlikkust, luua küberhädaolukorra mehhanism, et toetada liikmesriike valmistumisel olulisteks ja ulatuslikeks küberintsidentideks, ***sealhulgas rohkem kui üht liikmesriiki hõlmavateks intsidentideks,*** neile reageerimisel ja neist vahetul taastumisel***.*** ***Kui see on teostatav ja vajalik***, ***peaks küberhädaolukorra mehhanism korraldama teabe jagamist ja koostööd liikmesriikide kaitseasutustega*** ning ***seda peaksid toetama ELi institutsioonid, organid ja asutused (ELi küberkaitsekogukond). Tuleks*** luua küberintsidentide läbivaatamise mehhanism, et vaadata läbi ja hinnata konkreetseid olulisi või ulatuslikke intsidente***. Sellised uued struktuurid peaksid toetama ka ELi ÜJKP operatsioone ja missioone***. Need meetmed ei piira Euroopa Liidu toimimise lepingu (edaspidi „ELi toimimise leping“) artiklite 107 ja 108 kohaldamist.

Muudatusettepanek 9

Ettepanek võtta vastu määrus
Põhjendus 11

Komisjoni ettepanek	*Muudatusettepanek*
(11) Usaldusväärse finantsjuhtimise tagamiseks tuleks sätestada kasutamata kulukohustuste ja maksete assigneeringute ülekandmise eeskirjad. Toetades küll põhimõtet, et liidu eelarve kinnitatakse igal aastal, tuleks küberturvalisuse keskkonna prognoosimatust, erandlikkust ja eripära arvesse võttes näha käesoleva määrusega lisaks finantsmääruses sätestatud võimalustele ette võimalus kasutamata vahendid üle kanda, millega maksimeeritakse küberhädaolukorra mehhanismi suutlikkust toetada liikmesriike tulemuslikus võitluses küberohtude vastu.	(11) Usaldusväärse finantsjuhtimise tagamiseks tuleks sätestada kasutamata kulukohustuste ja maksete assigneeringute ülekandmise eeskirjad. Toetades küll põhimõtet, et liidu eelarve kinnitatakse igal aastal, tuleks küberturvalisuse keskkonna prognoosimatust, erandlikkust ja eripära arvesse võttes näha käesoleva määrusega lisaks finantsmääruses sätestatud võimalustele ette võimalus kasutamata vahendid üle kanda, millega maksimeeritakse küberhädaolukorra mehhanismi suutlikkust toetada liikmesriike tulemuslikus võitluses küberohtude vastu. ***Need erireeglid võimaldaksid ka pikemaajalist rahalist toetust järgmise põlvkonna üliturvaliste vahendite ja taristu ühishangeteks, et parandada kollektiivset tuvastamissuutlikkust, kasutades uusimat tehisintellekti (TI) ja andmeanalüüsi.***

Muudatusettepanek 10

Ettepanek võtta vastu määrus
Põhjendus 13

Komisjoni ettepanek	*Muudatusettepanek*
(13) Iga liikmesriik peaks määrama liikmesriigi tasandi avaliku sektori asutuse, kelle ülesanne on koorineerida riigis küberohtude avastamise alast tegevust. See riiklik infoturbekeskus peaks olema liikmesriigi tasandi kontaktpunkt osalemiseks Euroopa küberkilbis ning see peaks tagama, et avaliku ja erasektori üksuste teavet küberohtude kohta kogutakse ja jagatakse liikmesriigi tasandil tõhusalt ja ühtlustatud viisil.	(13) Iga liikmesriik peaks määrama liikmesriigi tasandi avaliku sektori asutuse, kelle ülesanne on koorineerida riigis küberohtude avastamise alast tegevust. See riiklik infoturbekeskus peaks olema liikmesriigi tasandi kontaktpunkt osalemiseks Euroopa küberkilbis ning see peaks tagama, et avaliku ja erasektori üksuste teavet küberohtude kohta kogutakse ja jagatakse liikmesriigi tasandil tõhusalt ja ühtlustatud viisil. ***Kui see on teostatav ja vajalik, peaksid***

infoturbekeskused võimaldama ka kaitse valdkonna üksuste osalemist, luues juhtimise ja jagatud teabe liigi osas kaitsesamba, nagu on sätestatud ühisteatises ELi küberkaitsepoliitika kohta[1] ja mida toetab kõrge esindaja.

[1] Ühisteatis Euroopa Parlamendile ja nõukogule „ELi küberkaitsepoliitika“, JOIN(2022) 49 final.

Muudatusettepanek 11

Ettepanek võtta vastu määrus
Põhjendus 14

Komisjoni ettepanek	*Muudatusettepanek*
(14) Euroopa küberkilbi raames tuleks luua mitu piiriülest infoturbekeskust. Piiriülene infoturbekeskus peaks hõlmama vähemalt kolme liikmesriigi riiklikku infoturbekeskust, et oleks võimalik täielikult ära kasutada piiriülese ohtude avastamise ning teabe jagamise ja haldamise eeliseid. Piiriüleste infoturbekeskuste üldeesmärk peaks olema suurendada suutlikkust analüüsida, ennetada ja avastada küberohte ning toetada neid ohte käsitleva kvaliteetse luureteabe kogumist, eelkõige jagades eri allikatest (avalikust ja erasektorist) pärit andmeid, jagades ja ühiselt kasutades tipptasemel vahendeid ning arendades usaldusväärses keskkonnas ühiselt avastamis-, analüüsi- ja ennetamissuutlikkust. Need infoturbekeskused peaksid suurendama suutlikkust, toetades ja täiendades olemasolevaid infoturbekeskusi ja küberturbe intsidentide lahendamise üksusi (edaspidi „CSIRTid“) ning muid asjaomaseid osalejaid.	(14) Euroopa küberkilbi raames tuleks luua mitu piiriülest infoturbekeskust. Piiriülene infoturbekeskus peaks hõlmama vähemalt kolme liikmesriigi riiklikku infoturbekeskust, ***sh kaitsesammast,*** et oleks võimalik täielikult ära kasutada piiriülese ohtude avastamise ning teabe jagamise ja haldamise eeliseid. Piiriüleste infoturbekeskuste üldeesmärk peaks olema suurendada suutlikkust analüüsida, ennetada ja avastada küberohte ning toetada neid ohte käsitleva kvaliteetse luureteabe kogumist, eelkõige jagades eri allikatest (avalikust ja erasektorist) pärit andmeid ***ning – kui see on vajalik ja teabe jagamiseks piisavalt juhiseid andes teostatav – sõjalisi andmeid***, jagades ja ühiselt kasutades tipptasemel vahendeid ning arendades usaldusväärses keskkonnas ühiselt avastamis-, analüüsi- ja ennetamissuutlikkust. Need infoturbekeskused peaksid suurendama suutlikkust, toetades ja täiendades olemasolevaid infoturbekeskusi ja küberturbe intsidentide lahendamise üksusi (edaspidi „CSIRTid“) ning muid asjaomaseid osalejaid.

Muudatusettepanek 12

Ettepanek võtta vastu määrus
Põhjendus 15

Komisjoni ettepanek	*Muudatusettepanek*
(15) Liikmesriigi tasandil tagavad avaliku ja erasektori üksustele küberohtude seire, avastamise ja analüüsi tavaliselt infoturbekeskused koos CSIRTidega. Peale selle vahetavad CSIRTid teavet CSIRTide võrgustikus kooskõlas direktiiviga (EL) 2022/2555. Piiriülesed infoturbekeskused peaksid kujutama endast uut, CSIRTide võrgustikku täiendavat võimeüksust, kus kogutakse ja jagatakse avaliku ja erasektori üksuste andmeid küberohtude kohta, tõstetakse eksperdianalüüsi ning ühiselt soetatud taristute ja tipptasemel vahendite abil selliste andmete väärtust ning aidatakse arendada liidu võimekust ja ***tehnoloogilist suveräänsust***.	(15) Liikmesriigi tasandil tagavad avaliku ja erasektori üksustele küberohtude seire, avastamise ja analüüsi tavaliselt infoturbekeskused koos CSIRTidega. Peale selle vahetavad CSIRTid teavet CSIRTide võrgustikus kooskõlas direktiiviga (EL) 2022/2555. Piiriülesed infoturbekeskused peaksid kujutama endast uut, CSIRTide võrgustikku täiendavat võimeüksust, kus kogutakse ja jagatakse avaliku ja erasektori üksuste andmeid küberohtude kohta, tõstetakse eksperdianalüüsi ning ühiselt soetatud taristute ja tipptasemel vahendite abil selliste andmete väärtust ning aidatakse arendada liidu võimekust ja ***vastupidavusvõimet***.

Muudatusettepanek 13

Ettepanek võtta vastu määrus
Põhjendus 16

Komisjoni ettepanek	*Muudatusettepanek*
(16) Piiriülesed infoturbekeskused peaksid olema keskne kontaktpunkt, et koguda laialdaselt asjakohaseid andmeid ja küberohte käsitlevat luureteavet ning levitada ohuteavet arvukate ja mitmesuguste osalejate seas (nagu infoturbeintsidentidega tegelevad rühmad (CERTid), CSIRTid, teabe jagamise ja analüüsimise keskused ***ning*** elutähtsate taristute haldajad). Piiriülese infoturbekeskuse kaudu osalejate seas vahetatav teave võib hõlmata võrkude ja andurite andmeid, küberohtude alast luureteavet, rikkeindikaatoreid ning kontekstiteavet intsidentide, ohtude ja nõrkuste kohta. Peale selle peaksid	(16) Piiriülesed infoturbekeskused peaksid olema keskne kontaktpunkt, et koguda laialdaselt asjakohaseid andmeid ja küberohte käsitlevat luureteavet ning levitada ohuteavet arvukate ja mitmesuguste osalejate seas (nagu infoturbeintsidentidega tegelevad rühmad (CERTid), CSIRTid, teabe jagamise ja analüüsimise keskused***,*** elutähtsate taristute haldajad ***ja küberkaitsekogukond***). Piiriülese infoturbekeskuse kaudu osalejate seas vahetatav teave võib hõlmata võrkude ja andurite andmeid, küberohtude alast luureteavet, rikkeindikaatoreid ning kontekstiteavet intsidentide, ohtude ja nõrkuste kohta. Peale selle peaksid

piiriülesed infoturbekeskused sõlmima koostöölepingud teiste piiriüleste infoturbekeskustega.	piiriülesed infoturbekeskused sõlmima koostöölepingud teiste piiriüleste infoturbekeskustega ***ja sõjaliste infoturbeintsidentidega tegelevate rühmade (milCERTid) operatiivvõrgustikuga (MICNET) siis, kui see on moodustatud***.

Muudatusettepanek 14

Ettepanek võtta vastu määrus
Põhjendus 17

Komisjoni ettepanek	*Muudatusettepanek*
(17) Oluliste ja ulatuslike küberintsidentidega seotud valmisoleku ja koordineerimise tagamiseks kogu liidus on vältimatu eeltingimus asjaomaste ametiasutuste ühine olukorrateadlikkus. Direktiiviga (EL) 2022/2555 on ette nähtud EU-CyCLONe loomine, et toetada ulatuslike küberintsidentide ja -kriiside koordineeritud ohjamist operatiivtasandil ning tagada korrapärane asjakohase teabe vahetamine liikmesriikide ning liidu institutsioonide, organite ja asutuste vahel. Soovituses (EL) 2017/1584 koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral on käsitletud asjaomaste osalejate rolli. Direktiivis (EL) 2022/2555 tuletatakse ka meelde komisjoni vastutust Euroopa Parlamendi ja nõukogu otsusega nr 1313/2013/EL loodud liidu elanikkonnakaitse mehhanismi raames ning vastutust rakendusotsuse (EL) 2018/1993 kohase kriisidele poliitilist reageerimist käsitleva ELi integreeritud korra (IPCR) analüüsiaruannete esitamise eest. Seepärast peaks piiriülene infoturbekeskus, kui ta saab teavet võimaliku või käimasoleva ulatusliku küberintsidendi kohta, esitama asjaomase teabe EU-CyCLONe-le, CSIRTide võrgustikule ja komisjonile. Sõltuvalt olukorrast võib jagatav teave olla tehniline teave, teave ründe toimepanija või potentsiaalse toimepanija ja tema	(17) Oluliste ja ulatuslike küberintsidentidega seotud valmisoleku ja koordineerimise tagamiseks kogu liidus on vältimatu eeltingimus asjaomaste ametiasutuste ühine olukorrateadlikkus. Direktiiviga (EL) 2022/2555 on ette nähtud EU-CyCLONe loomine, et toetada ulatuslike küberintsidentide ja -kriiside koordineeritud ohjamist operatiivtasandil ning tagada korrapärane asjakohase teabe vahetamine liikmesriikide ning liidu institutsioonide, organite ja asutuste vahel. Soovituses (EL) 2017/1584 koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral on käsitletud asjaomaste osalejate rolli. Direktiivis (EL) 2022/2555 tuletatakse ka meelde komisjoni vastutust Euroopa Parlamendi ja nõukogu otsusega nr 1313/2013/EL loodud liidu elanikkonnakaitse mehhanismi raames ning vastutust rakendusotsuse (EL) 2018/1993 kohase kriisidele poliitilist reageerimist käsitleva ELi integreeritud korra (IPCR) analüüsiaruannete esitamise eest. Seepärast peaks piiriülene infoturbekeskus, kui ta saab teavet võimaliku või käimasoleva ulatusliku küberintsidendi kohta, esitama asjaomase teabe EU-CyCLONe-le, CSIRTide võrgustikule***,*** ***küberkaitsekogukonnale*** ja komisjonile. Sõltuvalt olukorrast võib jagatav teave olla tehniline teave, teave ründe toimepanija

motiivide kohta või kõrgetasemeline mittetehniline teave võimaliku või käimasoleva ulatusliku küberintsidendi kohta. Teabe jagamisel tuleks nõuetekohaselt arvesse võtta teadmisvajaduse põhimõtet ja jagatava teabe võimalikku tundlikkust.	või potentsiaalse toimepanija ja tema motiivide kohta või kõrgetasemeline mittetehniline teave võimaliku või käimasoleva ulatusliku küberintsidendi kohta. Teabe jagamisel tuleks nõuetekohaselt arvesse võtta teadmisvajaduse põhimõtet ja jagatava teabe võimalikku tundlikkust.

Muudatusettepanek 15

Ettepanek võtta vastu määrus
Põhjendus 19

Komisjoni ettepanek	*Muudatusettepanek*
(19) Selleks et eri allikatest pärit andmeid küberohtude kohta oleks võimalik vahetada ulatuslikult ja usaldusväärses keskkonnas, peaksid Euroopa küberkilbis osalevatel üksustel olema väga turvalised tipptasemel vahendid, seadmed ja taristud. Need – eelkõige uusim tehisintellekti- ja andmeanalüüsitehnoloogia – peaksid võimaldama parandada ühist avastamissuutlikkust ning ametiasutuste ja asjaomaste üksuste õigeaegset hoiatamist.	(19) Selleks et eri allikatest pärit andmeid küberohtude kohta oleks võimalik vahetada ulatuslikult ja usaldusväärses keskkonnas, peaksid Euroopa küberkilbis osalevatel üksustel olema väga turvalised tipptasemel vahendid, seadmed ja taristud***, välistades digielemente sisaldavate kriitilise tähtsusega toodete puhul suure riskiga tarnijad***. Need – eelkõige uusim tehisintellekti- ja andmeanalüüsitehnoloogia – peaksid võimaldama parandada ühist avastamissuutlikkust ning ametiasutuste ja asjaomaste üksuste õigeaegset hoiatamist. ***TI kasutamisel tuleks tagada inimjärelevalve ning piisav TI-pädevus, vajalik tugi ja volitused selle funktsiooni täitmiseks.***

Muudatusettepanek 16

Ettepanek võtta vastu määrus
Põhjendus 19 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	(19a) Kooskõlas määrusega [XX/XXXX (küberkerksuse määrus)] peaksid Euroopa küberkilbis osalevad üksused järgima ka käesolevas määruses sätestatud nõudeid kõigile digielemente

	sisaldavatele toodetele. Kuna majanduslik sõltuvus tekitab üha enam riske, tuleb ELi majandusjulgeoleku ühise strateegilise raamistiku abil vähendada ohte, mida võivad põhjustada kriitilise tähtsusega toodete suure riskiga tarnijad. Sõltuvus digielemente sisaldavate kriitilise tähtsusega toodete suure riskiga tarnijatest on strateegiline risk, mida tuleks maandada liidu tasandil, uurides eelkõige seda, kas riik tegeleb tööstusspionaaži või majandusliku survestamisega ja kas riigi õigusaktid kohustavad lubama meelevaldset juurdepääsu mis tahes liiki ettevõtte tegevusele või andmetele, eriti kui kriitilise tähtsusega tooted on ette nähtud kasutamiseks direktiivis (EL) 2022/2555 osutatud elutähtsatele üksustele.

Muudatusettepanek 17

Ettepanek võtta vastu määrus
Põhjendus 20

Komisjoni ettepanek	*Muudatusettepanek*
(20) Euroopa küberkilp peaks andmete kogumise, jagamise ja vahetamise kaudu aitama suurendada liidu tehnoloogilist suveräänsust. Kvaliteetsete kureeritud andmete kogumine peaks aitama ka arendada tipptasemel tehisintellekti- ja andmeanalüüsitehnoloogiat. Seda tuleks hõlbustada, sidudes Euroopa küberkilbi üleeuroopalise kõrgjõudlusega andmetöötluse taristuga, mis on loodud nõukogu määrusega (EL) 2021/1173 [25].	(20) Euroopa küberkilp peaks andmete kogumise, jagamise ja vahetamise kaudu aitama suurendada liidu tehnoloogilist suveräänsust***, strateegilist sõltumatust, konkurentsivõimet ja vastupidavusvõimet***. Kvaliteetsete kureeritud andmete kogumine peaks aitama ka arendada tipptasemel tehisintellekti- ja andmeanalüüsitehnoloogiat. Seda tuleks hõlbustada, sidudes Euroopa küberkilbi üleeuroopalise kõrgjõudlusega andmetöötluse taristuga, mis on loodud nõukogu määrusega (EL) 2021/1173 [25].
[25] Nõukogu 13. juuli 2021. aasta määrus (EL) 2021/1173, millega asutatakse Euroopa kõrgjõudlusega andmetöötluse ühisettevõte ning tunnistatakse kehtetuks määrus (EL) 2018/1488 (ELT L 256,	[25] Nõukogu 13. juuli 2021. aasta määrus (EL) 2021/1173, millega asutatakse Euroopa kõrgjõudlusega andmetöötluse ühisettevõte ning tunnistatakse kehtetuks määrus (EL) 2018/1488 (ELT L 256,

19.7.2021, lk 3).

19.7.2021, lk 3).

Muudatusettepanek 18

Ettepanek võtta vastu määrus
Põhjendus 25

Komisjoni ettepanek	*Muudatusettepanek*
(25) Küberhädaolukorra mehhanismi kaudu tuleks anda liikmesriikidele toetust, mis täiendab nende endi meetmeid ja vahendeid, ning pakkuda muud toetust olulistele ja ulatuslikele küberintsidentidele reageerimisel ja neist vahetul taastumisel, nagu teenused, mida osutab oma volitustest lähtuvalt Euroopa Liidu Küberturvalisuse Amet (ENISA), CSIRTide võrgustiku pakutav koordineeritud reageerimine ja abi, EU-CyCLONe toetus olukorra leevendamiseks ning liikmesriikide vastastikune abi, sealhulgas ELi lepingu artikli 42 lõike 7 raames ning alalise struktureeritud koostöö (PESCO) küberturbe ***kiirreageerimisrühmade26*** ja hübriidohtudega tegelevate kiirreageerimisrühmade kaudu. Selle mehhanismiga tuleks tagada, et olemas on erivahendid, millega toetada valmisolekut küberintsidentideks ja neile reageerimist kogu liidus ja kolmandates riikides.	(25) Küberhädaolukorra mehhanismi kaudu tuleks anda liikmesriikidele toetust, mis täiendab nende endi meetmeid ja vahendeid, ning pakkuda muud toetust olulistele ja ulatuslikele küberintsidentidele reageerimisel ja neist vahetul taastumisel, nagu teenused, mida osutab oma volitustest lähtuvalt Euroopa Liidu Küberturvalisuse Amet (ENISA), CSIRTide võrgustiku pakutav koordineeritud reageerimine ja abi, EU-CyCLONe toetus olukorra leevendamiseks ning liikmesriikide vastastikune abi, sealhulgas ELi lepingu artikli 42 lõike 7 raames ning alalise struktureeritud koostöö (PESCO) küberturbe ***kiirreageerimisrühmade[1], uue PESCO projekti, küber-*** ja ***teabevaldkonna koordinatsioonikeskuse (CIDCC) ja selle kavandatava järeltulija ELi küberkaitse koordineerimiskeskuse (EUCDCC) ning*** hübriidohtudega tegelevate kiirreageerimisrühmade kaudu. Selle mehhanismiga tuleks tagada, et olemas on erivahendid, millega toetada valmisolekut küberintsidentideks ja neile reageerimist kogu liidus ja kolmandates riikides***, eelkõige ELi ühist välis- ja julgeolekupoliitikat ning ühist julgeoleku- ja kaitsepoliitikat järgivates ELi kandidaatriikides, aidates neil suurendada oma kübervõimekust ning tõhustada nende kandidaatriikide vahelist piiriülest ja piirkondlikku koostööd kübervaldkonnas***. ***[1] Nõukogu 11. detsembri 2017. aasta otsus (ÜVJP) 2017/2315, millega luuakse alaline struktureeritud koostöö ning määratakse kindlaks selles osalevate***

liikmesriikide nimekiri.

[26] Nõukogu 11. detsembri 2017. aasta otsus (ÜVJP) 2017/2315, millega luuakse alaline struktureeritud koostöö ning määratakse kindlaks selles osalevate liikmesriikide nimekiri.

[26] Nõukogu 11. detsembri 2017. aasta otsus (ÜVJP) 2017/2315, millega luuakse alaline struktureeritud koostöö ning määratakse kindlaks selles osalevate liikmesriikide nimekiri.

Muudatusettepanek 19

Ettepanek võtta vastu määrus
Põhjendus 26

Komisjoni ettepanek	*Muudatusettepanek*
(26) Küberhädaolukorra mehhanism ei piira selliste menetluste ja raamistike kohaldamist, millega koordineeritakse kriisile reageerimist liidu tasandil, milleks on eelkõige liidu elanikkonnakaitse mehhanism,[27] IPCR[28], ja direktiiv (EL) 2022/2555. Mehhanism võib toetada või täiendada meetmeid, mida rakendatakse ELi lepingu artikli 42 lõike 7 raames või ELi toimimise lepingu artiklis 222 määratletud olukordades. Mehhanismi kasutamist tuleks ***asjakohasel juhul*** kooskõlastada ka küberdiplomaatia meetmete rakendamisega.	(26) Küberhädaolukorra mehhanism ei piira selliste menetluste ja raamistike kohaldamist, millega koordineeritakse kriisile reageerimist liidu tasandil, milleks on eelkõige liidu elanikkonnakaitse mehhanism,[27] IPCR[28], ja direktiiv (EL) 2022/2555. Mehhanism võib toetada või täiendada meetmeid, mida rakendatakse ELi lepingu artikli 42 lõike 7 raames või ELi toimimise lepingu artiklis 222 määratletud olukordades. Mehhanismi kasutamist tuleks kooskõlastada ka küberdiplomaatia meetmete rakendamisega***, tõhustades küberkaitse- ja muude küberkogukondade vahelist strateegilist, operatiiv- ja tehnilist koostööd eelkõige selleks, et tugevdada suutlikkust võidelda väljastpoolt liitu lähtuvate küberohtude vastu, sealhulgas piiravate meetmete abil, mida saab kasutada pahatahtliku kübertegevuse ennetamiseks ja sellele reageerimiseks***.

[27] Euroopa Parlamendi ja nõukogu 17. detsembri 2013. aasta otsus nr 1313/2013/EL liidu elanikkonnakaitse mehhanismi kohta (ELT L 347, 20.12.2013, lk 924).

[27] Euroopa Parlamendi ja nõukogu 17. detsembri 2013. aasta otsus nr 1313/2013/EL liidu elanikkonnakaitse mehhanismi kohta (ELT L 347, 20.12.2013, lk 924).

[27] Kriisidele poliitilist reageerimist käsitlev ELi integreeritud kord ja komisjoni

[27] Kriisidele poliitilist reageerimist käsitlev ELi integreeritud kord ja komisjoni

13. septembri 2017. aasta soovitus (EL) 2017/1584 koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral.	13. septembri 2017. aasta soovitus (EL) 2017/1584 koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral.

Muudatusettepanek 20

Ettepanek võtta vastu määrus
Põhjendus 28

Komisjoni ettepanek	*Muudatusettepanek*
(28) Direktiivi (EL) 2022/2555 kohaselt peavad liikmesriigid määrama või looma ühe või mitu küberkriisiohje asutust ning tagama, et neil on piisavad vahendid, et täita oma ülesandeid tulemuslikult ja tõhusalt. Direktiivis nõutakse ka, et liikmesriigid määraksid kindlaks oma võimekuse, vahendid ja menetlused, mida saab rakendada kriisiolukorras, ning võtaksid vastu riikliku ulatuslike küberintsidentide ja -kriiside lahendamise kava, milles on kirjeldatud ulatuslike küberintsidentide ja -kriiside ohjamise eesmärke ja korda. Samuti peavad liikmesriigid looma ühe või mitu CSIRTi, mis hõlmavad vähemalt selle direktiivi kohaldamisalasse kuuluvaid sektoreid, allsektoreid ja üksuseid ning mille ülesanne on käsitleda kindlat menetlust järgides intsidente, ning kandma hoolt selle eest, et neil on oma ülesannete tulemuslikuks täitmiseks piisavad vahendid. Käesolev määrus ei piira komisjoni rolli selle tagamisel, et liikmesriigid täidavad oma direktiivis (EL) 2022/2555 sätestatud kohustusi. Küberhädaolukorra mehhanismi kaudu tuleks pakkuda abi meetmete jaoks, mille eesmärk on parandada valmisolekut, ning intsidentidele reageerimise meetmete jaoks, et leevendada oluliste ja ulatuslike küberintsidentide mõju, toetada vahetut taastumist ja/või taastada oluliste teenuste toimimine.	(28) Direktiivi (EL) 2022/2555 kohaselt peavad liikmesriigid määrama või looma ühe või mitu küberkriisiohje asutust ning tagama, et neil on piisavad vahendid, et täita oma ülesandeid tulemuslikult ja tõhusalt. Direktiivis nõutakse ka, et liikmesriigid määraksid kindlaks oma võimekuse, vahendid ja menetlused, mida saab rakendada kriisiolukorras, ning võtaksid vastu riikliku ulatuslike küberintsidentide ja -kriiside lahendamise kava, milles on kirjeldatud ulatuslike küberintsidentide ja -kriiside ohjamise eesmärke ja korda. Samuti peavad liikmesriigid looma ühe või mitu CSIRTi, mis hõlmavad vähemalt selle direktiivi kohaldamisalasse kuuluvaid sektoreid, allsektoreid ja üksuseid ning mille ülesanne on käsitleda kindlat menetlust järgides intsidente, ning kandma hoolt selle eest, et neil on oma ülesannete tulemuslikuks täitmiseks piisavad vahendid. Käesolev määrus ei piira komisjoni rolli selle tagamisel, et liikmesriigid täidavad oma direktiivis (EL) 2022/2555 sätestatud kohustusi. Küberhädaolukorra mehhanismi kaudu tuleks pakkuda abi meetmete jaoks, mille eesmärk on parandada valmisolekut, ning intsidentidele reageerimise meetmete jaoks, et leevendada oluliste ja ulatuslike küberintsidentide mõju, toetada vahetut taastumist ja/või taastada oluliste teenuste toimimine***, kasutades sobival viisil ära kõiki tsiviil- ja sõjalistele kogukondadele***

kättesaadavaid kaitsevõimalusi.

Muudatusettepanek 21

Ettepanek võtta vastu määrus
Põhjendus 29

Komisjoni ettepanek	*Muudatusettepanek*
(29) Selleks et edendada järjekindlat lähenemisviisi ning suurendada turvalisust kogu liidus ja liidu siseturul, tuleks valmisolekumeetmete raames anda toetust direktiivi (EL) 2022/2555 kohaselt kindlaks tehtud ülikriitilise tähtsusega sektorites tegutsevate üksuste küberturvalisuse koordineeritud testimiseks ja hindamiseks. Selleks peaks komisjon ENISA toel ja koostöös direktiiviga (EL) 2022/2555 loodud võrgu- ja infoturbe koostöörühmaga määrama korrapäraselt kindlaks sektorid või allsektorid, kus on võimalik saada rahalist toetust koordineeritud testimiseks liidu tasandil. ***Need sektorid*** ja ***allsektorid*** tuleks valida direktiivi (EL) 2022/2555 I lisast („Kriitilise tähtsusega sektorid“). Koordineeritud testimine peaks põhinema ühistel riskistsenaariumidel ja metoodikatel. Sektorite valimisel ja riskistsenaariumide koostamisel tuleks arvesse võtta asjakohaseid kogu liitu hõlmavaid riskihinnanguid ja riskistsenaariume (sh pidades silmas vajadust vältida topelttööd), nagu riskihinnang ja riskistsenaariumid, mille komisjon, kõrge esindaja ning võrgu- ja infoturbe koostöörühm koostavad koostöös asjaomaste tsiviil- ja sõjaväeorganite ja -ametite ning väljakujunenud võrgustike, sealhulgas EU-CyCLONega, järgides ELi kübervaldkonna positsiooni arendamist käsitlevates nõukogu järeldustes esitatud üleskutset; sidevõrkude ja taristute riskihindamine, mida nõutakse Neversi kohtumisel esitatud ministrite ühises üleskutses ning mille teeb võrgu- ja infoturbe koostöörühm komisjoni ja	(29) Selleks et edendada järjekindlat lähenemisviisi ning suurendada turvalisust kogu liidus ja liidu siseturul, tuleks valmisolekumeetmete raames anda toetust direktiivi (EL) 2022/2555 kohaselt kindlaks tehtud ülikriitilise tähtsusega sektorites tegutsevate üksuste küberturvalisuse koordineeritud testimiseks ja hindamiseks. Selleks peaks komisjon ENISA toel ja koostöös direktiiviga (EL) 2022/2555 loodud võrgu- ja infoturbe koostöörühmaga määrama korrapäraselt kindlaks sektorid või allsektorid, kus on võimalik saada rahalist toetust koordineeritud testimiseks liidu tasandil. ***Asjakohasel juhul tuleks Euroopa välisteenistus, eelkõige ELi luure-*** ja ***situatsioonikeskuse (INTCEN) ja selle hübriidohtude ühisüksuse kaudu, keda toetab Euroopa Liidu sõjalise staabi (EUMS) luuredirektoraat ühtse luureandmete analüüsivõime üksuse (SIAC) raames, samuti kaasata ajakohaste hindamiste tegemisse ja seega aidata kaasa selliste sektorite ja allsektorite kindlakstegemisele, mis*** tuleks valida direktiivi (EL) 2022/2555 I lisast („Kriitilise tähtsusega sektorid“). Koordineeritud testimine peaks põhinema ühistel riskistsenaariumidel ja metoodikatel***. Testimisel võib olla oluline roll ka tsiviil- ja sõjaliste struktuuride vahelise koostöö parandamisel. Õppuste korraldamisel peaksid komisjon, Euroopa välisteenistus ja ENISA seetõttu süstemaatiliselt kaaluma osalejate kaasamist teistest küberkogukondadest, näiteks Euroopa Kaitseagentuurist (EDA) ja muudest asjaomastest üksustest.***

ENISA toel koostöös elektroonilise side Euroopa reguleerivate asutuste ametiga (BEREC), ning koordineeritud riskihindamised direktiivi (EL) 2022/2555 artikli 22 alusel ja digitaalse tegevuskerksuse testimine, mis on ette nähtud Euroopa Parlamendi ja nõukogu määrusega (EL) 2022/***255429***. Samuti tuleks sektorite valimisel arvesse võtta nõukogu soovitust, mis käsitleb kogu liitu hõlmavat koordineeritud lähenemisviisi elutähtsa taristu toimepidevuse tugevdamiseks.

Sektorite valimisel ja riskistsenaariumide koostamisel tuleks arvesse võtta asjakohaseid kogu liitu hõlmavaid riskihinnanguid ja riskistsenaariume (sh pidades silmas vajadust vältida topelttööd), nagu riskihinnang ja riskistsenaariumid, mille komisjon, kõrge esindaja ning võrgu- ja infoturbe koostöörühm koostavad koostöös asjaomaste tsiviil- ja sõjaväeorganite ja -ametite ning väljakujunenud võrgustike, sealhulgas EU-CyCLONega, järgides ELi kübervaldkonna positsiooni arendamist käsitlevates nõukogu järeldustes esitatud üleskutset; sidevõrkude ja taristute riskihindamine, mida nõutakse Neversi kohtumisel esitatud ministrite ühises üleskutses ning mille teeb võrgu- ja infoturbe koostöörühm komisjoni ja ENISA toel koostöös elektroonilise side Euroopa reguleerivate asutuste ametiga (BEREC), ning koordineeritud riskihindamised direktiivi (EL) 2022/2555 artikli 22 alusel ja digitaalse tegevuskerksuse testimine, mis on ette nähtud Euroopa Parlamendi ja nõukogu määrusega (EL) 2022/2554 ***[1]***. Samuti tuleks sektorite valimisel arvesse võtta nõukogu soovitust, mis käsitleb kogu liitu hõlmavat koordineeritud lähenemisviisi elutähtsa taristu toimepidevuse tugevdamiseks.

[1] Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrus (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011.

---

[29] Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrus (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011.

[29] Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrus (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011.

Muudatusettepanek 22

Ettepanek võtta vastu määrus
Põhjendus 32

Komisjoni ettepanek	*Muudatusettepanek*
(32) Küberhädaolukorra mehhanismi abil tuleks toetada liikmesriike, sealhulgas direktiivi (EL) 2022/2555 artikli 15 kohast CSIRTide võrgustikku, abi andmisel liikmesriigile, kes on olulisest või ulatuslikust küberintsidendist mõjutatud. Abi andvatel liikmesriikidel peaks olema lubatud esitada taotlusi vastastikuse abistamise raames toimuva eksperdirühmade lähetamisega seotud kulude katmiseks. Rahastamiskõlblike kulude hulka võivad kuuluda küberturvalisuse ekspertide sõidu- ja majutuskulud ning päevarahad.	(32) Küberhädaolukorra mehhanismi abil tuleks toetada liikmesriike, sealhulgas direktiivi (EL) 2022/2555 artikli 15 kohast CSIRTide võrgustikku, abi andmisel liikmesriigile, kes on olulisest või ulatuslikust küberintsidendist mõjutatud. Abi andvatel liikmesriikidel peaks olema ***kolmandatele riikidele, eelkõige Ukrainale ja Moldovale abi andmisel*** lubatud esitada taotlusi vastastikuse abistamise raames toimuva eksperdirühmade lähetamisega seotud kulude katmiseks***, tagades tõhusa koordineerimise ELi asjaomaste programmide ja vahendite vahel, sealhulgas Euroopa rahutagamisrahastu, ÜVJP ning naabruspiirkonna, arengu- ja rahvusvahelise koostöö instrument „Globaalne Euroopa“***. Rahastamiskõlblike kulude hulka võivad kuuluda küberturvalisuse ekspertide sõidu- ja majutuskulud ning päevarahad.

Muudatusettepanek 23

Ettepanek võtta vastu määrus
Põhjendus 33

Komisjoni ettepanek	*Muudatusettepanek*
(33) Järk-järgult tuleks luua eraõiguslike turbetarnijate teenuseid hõlmav ELi küberreserv, et toetada reageerimist ja vahetut taastumist oluliste või ulatuslike küberintsidentide korral. Küberreserv peaks tagama teenuste kättesaadavuse ja kasutamisvalmiduse. Küberreservi teenustega tuleks toetada liikmesriikide ametiasutusi kriitilise või ülikriitilise	(33) Järk-järgult tuleks luua eraõiguslike turbetarnijate teenuseid hõlmav ELi küberreserv, et toetada reageerimist ja vahetut taastumist oluliste või ulatuslike küberintsidentide korral. Küberreserv peaks tagama teenuste kättesaadavuse ja kasutamisvalmiduse. Küberreservi teenustega tuleks toetada liikmesriikide ametiasutusi kriitilise või ülikriitilise

tähtsusega sektorites tegutsevatele mõjutatud üksustele abi andmisel, täiendades liikmesriigi tasandil võetavaid meetmeid. Küberreservist toetust taotledes peaks liikmesriik nimetama, mis liiki toetust antakse mõjutatud üksusele liikmesriigi tasandil, mida tuleks arvesse võtta liikmesriigi taotluse hindamisel. Küberreservi teenustega võidakse toetada samadel tingimustel ka liidu institutsioone, organeid ja asutusi.	tähtsusega sektorites tegutsevatele mõjutatud üksustele abi andmisel, täiendades liikmesriigi tasandil võetavaid meetmeid. Küberreservist toetust taotledes peaks liikmesriik nimetama, mis liiki toetust antakse mõjutatud üksusele liikmesriigi tasandil, mida tuleks arvesse võtta liikmesriigi taotluse hindamisel. Küberreservi teenustega võidakse toetada samadel tingimustel ka liidu institutsioone, organeid ja asutusi***, sh ÜJKP missioone***.

Muudatusettepanek 24

Ettepanek võtta vastu määrus
Põhjendus 34

Komisjoni ettepanek	*Muudatusettepanek*
(34) ELi küberreservi raames teenuseid osutama hakkavate erasektori teenuseosutajate väljavalimiseks on vaja kehtestada rida miinimumkriteeriumeid, mida tuleks rakendada teenuseosutajate väljavalimiseks korraldatavates pakkumismenetlustes, et vastata liikmesriikide ametiasutuste ja kriitilise või ülikriitilise tähtsusega sektorites tegutsevate üksuste vajadustele.	(34) ELi küberreservi raames teenuseid osutama hakkavate erasektori teenuseosutajate väljavalimiseks on vaja kehtestada rida miinimumkriteeriumeid, mida tuleks rakendada teenuseosutajate väljavalimiseks korraldatavates pakkumismenetlustes, et vastata liikmesriikide ametiasutuste ja kriitilise või ülikriitilise tähtsusega sektorites tegutsevate üksuste vajadustele***, võttes arvesse ka strateegilistest konkureerivatest riikidest pärit teenuseosutajate osalemisega seotud riske, mis võivad põhjustada majandusjulgeolekuriske ning mõjutada liidu strateegilist julgeolekut***.

Muudatusettepanek 25

Ettepanek võtta vastu määrus
Põhjendus 36

Komisjoni ettepanek	*Muudatusettepanek*
(36) Selleks et aidata saavutada käesoleva määruse eesmärke parandada ühist olukorrateadlikkust, suurendada liidu vastupidavusvõimet ning võimaldada tulemuslikult reageerida olulistele ja	(36) Selleks et aidata saavutada käesoleva määruse eesmärke parandada ühist olukorrateadlikkust, suurendada liidu vastupidavusvõimet ning võimaldada tulemuslikult reageerida olulistele ja

ulatuslikele küberintsidentidele, peaks EU-CyCLONe-l, CSIRTide võrgustikul või komisjonil olema võimalik paluda ENISA-l läbi vaadata ja hinnata konkreetse olulise või ulatusliku küberintsidendiga seotud ohte, nõrkusi ja leevendusmeetmeid. Pärast intsidendi läbivaatamist ja hindamist peaks ENISA koostama läbivaatamisaruande, tehes seda koostöös asjaomaste sidusrühmade, sealhulgas erasektori, liikmesriikide, komisjoni ning muude asjaomaste ELi institutsioonide, organite ja asutuste esindajatega. Mis puudutab erasektorit, siis töötab ENISA praegu välja kanaleid teabe vahetamiseks spetsialiseerunud teenuseosutajatega, sealhulgas hallatud turbelahenduste pakkujatega, et täita oma ülesannet saavutada küberturvalisuse ühtlaselt kõrge tase kogu liidus. Konkreetse intsidendi läbivaatamisel tuleks püüda hinnata aset leidnud intsidendi põhjuseid, mõju ja leevendamist, tehes koostööd sidusrühmadega, sealhulgas erasektoriga. Läbivaatamisaruandes tuleks pöörata erilist tähelepanu teabele ja kogemustele, mida on jaganud turbetarnijad, kes vastavad käesoleva määrusega ette nähtud suurima erialase kohusetunde, erapooletuse ja nõutava tehnilise pädevuse kriteeriumile. Aruanne tuleks esitada EU-CyCLONe-le, CSIRTide võrgustikule ja komisjonile kasutamiseks nende töös. Kui intsident on seotud kolmanda riigiga, jagab komisjon ***aurannet*** ka kõrge esindajaga.

ulatuslikele küberintsidentidele, peaks EU-CyCLONe-l, CSIRTide võrgustikul või komisjonil olema võimalik paluda ENISA-l läbi vaadata ja hinnata konkreetse olulise või ulatusliku küberintsidendiga seotud ohte, nõrkusi ja leevendusmeetmeid. ***Võttes arvesse turvalise ühenduvussüsteemi väljatöötamist, mis põhineb Euroopa kvantsidetaristul (EuroQCI) ja Euroopa Liidu valitsuste satelliitsidel (GOVSATCOM), eelkõige Galileo GNSSi rakendamist kaitsevaldkonna kasutajate jaoks, tuleks mis tahes võimalikus arendamises võtta arvesse „hüpersõja“ võimalust, mis ühendab kvantandmetöötluse kiiruse ja keerukuse üliautonoomsete sõjaliste süsteemidega.*** Pärast intsidendi läbivaatamist ja hindamist peaks ENISA koostama läbivaatamisaruande, tehes seda koostöös asjaomaste sidusrühmade, sealhulgas erasektori, liikmesriikide, komisjoni ning muude asjaomaste ELi institutsioonide, organite ja asutuste esindajatega. Mis puudutab erasektorit, siis töötab ENISA praegu välja kanaleid teabe vahetamiseks spetsialiseerunud teenuseosutajatega, sealhulgas hallatud turbelahenduste pakkujatega, et täita oma ülesannet saavutada küberturvalisuse ühtlaselt kõrge tase kogu liidus. Konkreetse intsidendi läbivaatamisel tuleks püüda hinnata aset leidnud intsidendi põhjuseid, mõju ja leevendamist, tehes koostööd sidusrühmadega, sealhulgas erasektoriga. Läbivaatamisaruandes tuleks pöörata erilist tähelepanu teabele ja kogemustele, mida on jaganud turbetarnijad, kes vastavad käesoleva määrusega ette nähtud suurima erialase kohusetunde, erapooletuse ja nõutava tehnilise pädevuse kriteeriumile. Aruanne tuleks esitada EU-CyCLONe-le, CSIRTide võrgustikule ja komisjonile kasutamiseks nende töös. Kui intsident on seotud kolmanda riigiga, jagab komisjon ***aruannet*** ka kõrge esindajaga***, Euroopa välisteenistusega ja intsidendist mõjutatud riigis tegutseva ÜJKP missiooniga nende***

peakorteri kaudu.

Muudatusettepanek 26

Ettepanek võtta vastu määrus
Põhjendus 37

Komisjoni ettepanek	*Muudatusettepanek*
(37) Võttes arvesse küberrünnete prognoosimatust ja asjaolu, et sageli ei piirdu rünne konkreetse geograafilise piirkonnaga ja sellega kaasneb suur mõju ülekandumise oht, on liidu kui terviku kaitse huvides kasulik suurendada naaberriikide vastupidavusvõimet ning suutlikkust reageerida tõhusalt olulistele ja ulatuslikele küberintsidentidele. Seepärast ***võib*** toetada ELi küberreservist programmiga „Digitaalne Euroopa“ assotsieerunud kolmandaid riike, ***kui see*** on ***ette nähtud programmiga seotud asjaomase assotsieerimislepinguga***. Liit peaks andma assotsieerunud kolmandatele riikidele rahalisi vahendeid asjaomaste partnerluste ja rahastamisvahendite raames. Toetus peaks hõlmama teenuseid sellistes valdkondades nagu reageerimine olulistele ja ulatuslikele küberintsidentidele ning neist vahetu taastumine. Programmiga „Digitaalne Euroopa“ assotsieerunud kolmandate riikide toetamisel tuleks kohaldada käesolevas määruses ELi küberreservi ja usaldusväärsete teenuseosutajate jaoks sätestatud tingimusi.	(37) Võttes arvesse küberrünnete prognoosimatust ja asjaolu, et sageli ei piirdu rünne konkreetse geograafilise piirkonnaga ja sellega kaasneb suur mõju ülekandumise oht, on liidu kui terviku kaitse huvides kasulik suurendada naaberriikide***, eelkõige Ukraina ja Moldova*** vastupidavusvõimet ning suutlikkust reageerida tõhusalt olulistele ja ulatuslikele küberintsidentidele. Seepärast ***tuleks*** toetada ELi küberreservist programmiga „Digitaalne Euroopa“ assotsieerunud kolmandaid riike***. Toetust tuleks anda ka neile kolmandatele riikidele***, ***kuhu lähetatakse ÜJKP missioon erivolitusega tugevdada vastupidavusvõimet hübriidohtudele, sealhulgas küberohtudele, või kus on vastu võetud Euroopa rahutagamisrahastu abimeede riigi kübervastupidavusvõime tugevdamiseks***. Liit peaks andma assotsieerunud kolmandatele riikidele rahalisi vahendeid asjaomaste partnerluste ja rahastamisvahendite raames. Toetus peaks hõlmama teenuseid sellistes valdkondades nagu reageerimine olulistele ja ulatuslikele küberintsidentidele ning neist vahetu taastumine. Programmiga „Digitaalne Euroopa“ assotsieerunud kolmandate riikide toetamisel tuleks kohaldada käesolevas määruses ELi küberreservi ja usaldusväärsete teenuseosutajate jaoks sätestatud tingimusi.

Muudatusettepanek 27

Ettepanek võtta vastu määrus
Artikkel 1 – lõige 1 – punkt c

Komisjoni ettepanek	*Muudatusettepanek*
c) luues Euroopa küberintsidentide läbivaatamise mehhanismi, et vaadata läbi ja hinnata olulisi või ulatuslikke intsidente.	c) luues Euroopa küberintsidentide läbivaatamise mehhanismi, et vaadata läbi ja hinnata olulisi või ulatuslikke intsidente ***või ohte***.

Muudatusettepanek 28

Ettepanek võtta vastu määrus
Artikkel 1 – lõige 2 – punkt a

Komisjoni ettepanek	*Muudatusettepanek*
a) parandada küberohtude ja -intsidentide ühist avastamist ja olukorrateadlikkust liidus, suurendades sellega liidu tööstus- ja teenustesektori konkurentsivõimet kogu digimajanduses ja liidu tehnoloogilist ***suveräänsust*** küberturvalisuse valdkonnas;	a) parandada küberohtude ja -intsidentide ühist avastamist ja olukorrateadlikkust liidus, suurendades sellega liidu tööstus- ja teenustesektori konkurentsivõimet kogu digimajanduses ja liidu tehnoloogilist ***vastupidavusvõimet*** küberturvalisuse valdkonnas;

Muudatusettepanek 29

Ettepanek võtta vastu määrus
Artikkel 1 – lõige 2 – punkt b

Komisjoni ettepanek	*Muudatusettepanek*
b) parandada kriitilise ja ülikriitilise tähtsusega sektorites tegutsevate üksuste valmisolekut kõikjal liidus ja tugevdada solidaarsust, suurendades suutlikkust reageerida ühiselt olulistele või ulatuslikele küberintsidentidele, sealhulgas tehes liidus küberintsidentidele reageerimiseks pakutava toetuse kättesaadavaks ka programmiga „Digitaalne Euroopa“ assotsieerunud kolmandatele riikidele;	b) parandada kriitilise ja ülikriitilise tähtsusega sektorites tegutsevate üksuste valmisolekut kõikjal liidus ja tugevdada solidaarsust, suurendades suutlikkust reageerida ühiselt olulistele või ulatuslikele küberintsidentidele, sealhulgas tehes liidus küberintsidentidele reageerimiseks pakutava toetuse kättesaadavaks ka programmiga „Digitaalne Euroopa“ assotsieerunud kolmandatele riikidele ***või neile kolmandatele riikidele, kes on kandidaatriigid ega ole vastuolus liidu ja selle liikmesriikide julgeoleku- ja***

kaitsehuvidega, nagu need on kindlaks määratud ÜVJP raames vastavalt ELi lepingu V jaotisele; Liikmesriigid peaksid kaaluma aktiivse küberkaitseprogrammi lisamist oma riiklikku küberjulgeolekustrateegiasse, mis hõlmab korrapäraseid ühiseid õppusi liikmesriikide vahel ja rahvusvahelistes organisatsioonides. Selline programm peaks tagama sünkroniseeritud ning reaalajas toimiva suutlikkuse ohte avastada, tuvastada, analüüsida ja leevendada;

Muudatusettepanek 30

Ettepanek võtta vastu määrus
Artikkel 1 – lõige 2 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	2a. vähendada süsteemseid küberriske, mis tulenevad sõltuvusest kriitilise tähtsusega seadmetest, mida tarnitaks riikidest, mis oleks vastuolus liidu ja selle liikmesriikide julgeoleku- ja kaitsehuvidega, nagu need on kindlaks määratud ÜVJP raames vastavalt ELi lepingu V jaotisele;

Muudatusettepanek 31

Ettepanek võtta vastu määrus
Artikkel 2 – lõik 2 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	„küberkaitsekogukond“ – liikmesriikide kaitseasutused, keda toetavad ELi institutsioonid, organid ja asutused, nagu on märgitud ühisteatises ELi küberkaitsepoliitika kohta[1];
	[1] Ühisteatis Euroopa Parlamendile ja nõukogule „ELi küberkaitsepoliitika“, JOIN(2022) 49 final.

Muudatusettepanek 32

Ettepanek võtta vastu määrus
Artikkel 3 – lõige 2 – lõik 1 – punkt b a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ba) aidata ajakohastada kogu küberkaitse süsteeme, parandada küberkaitsevõime kvaliteeti TI-süsteemide kasutuselevõtu kaudu ning kiirendada teabevahetust riiklike infoturbekeskuste ja piiriüleste infoturbekeskuste vahel;

Muudatusettepanek 33

Ettepanek võtta vastu määrus
Artikkel 3 – lõige 2 – lõik 1 – punkt d a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	da) vaatab läbi ja hindab kriitilise tähtsusega küberturvalisuse tehnoloogiaid ja seadmeid, mida kasutavad infoturbekeskused selleks, et reageerida küberintsidentidele, mis tulenevad süsteemsetest riskidest seoses sellega, et suure riskiga teenuseosutajate üle omavad kontrolli riigid, mis oleks vastuolus liidu ja selle liikmesriikide julgeoleku- ja kaitsehuvidega, nagu need on kindlaks määratud ÜVJP raames vastavalt ELi lepingu V jaotisele.

Muudatusettepanek 34

Ettepanek võtta vastu määrus
Artikkel 4 – lõige 1 – lõik 2

Komisjoni ettepanek	*Muudatusettepanek*
Riiklikul infoturbekeskusel peab olema suutlikkus tegutseda liikmesriigi tasandi kontaktpunktina teistele avaliku ja erasektori organisatsioonidele, et koguda ja analüüsida küberohte ja -intsidente käsitlevat teavet ning panustada piiriülese	Riiklikul infoturbekeskusel peab olema suutlikkus tegutseda liikmesriigi tasandi kontaktpunktina teistele avaliku ja erasektori organisatsioonidele ***ning vajadusel sõjalistele organitele***, et koguda ja analüüsida küberohte ja -intsidente

infoturbekeskuse tegevusse. Riiklik infoturbekeskus varustatakse tipptasemel tehnoloogiaga, mis võimaldab avastada, koondada ja analüüsida küberohtude ja -intsidentidega seotud andmeid.	käsitlevat teavet ning panustada piiriülese infoturbekeskuse tegevusse. Riiklik infoturbekeskus varustatakse tipptasemel tehnoloogiaga, mis võimaldab avastada, koondada ja analüüsida küberohtude ja -intsidentidega seotud andmeid.

Muudatusettepanek 35

Ettepanek võtta vastu määrus
Artikkel 4 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Euroopa küberturvalisuse pädevuskeskus valib osalemiskutse alusel riiklikud infoturbekeskused osalema endaga koos vahendite ja taristute ühishankes. Euroopa küberturvalisuse pädevuskeskus võib anda riiklikele infoturbekeskustele toetusi, et rahastada nende vahendite ja taristute käitamist. Liidu rahalise panusega kaetakse kuni 50 % vahendite ja taristute soetamise kuludest ning kuni 50 % käitamiskuludest; ülejäänud kulud katab liikmesriik. Enne vahendite ja taristute soetamise menetluse algatamist sõlmivad Euroopa küberturvalisuse pädevuskeskus ja riiklik infoturbekeskus majutus- ja kasutuslepingu, millega reguleeritakse vahendite ja taristute kasutamist.	2. Euroopa küberturvalisuse pädevuskeskus valib osalemiskutse alusel riiklikud infoturbekeskused osalema endaga koos vahendite ja taristute ühishankes. Euroopa küberturvalisuse pädevuskeskus võib anda riiklikele infoturbekeskustele toetusi, et rahastada nende vahendite ja taristute käitamist ***rangel tingimusel, et neid vahendeid ja taristuid pakuvad usaldusväärsed teenuseosutajad kooskõlas artikliga 16***. Liidu rahalise panusega kaetakse kuni 50 % vahendite ja taristute soetamise kuludest ning kuni 50 % käitamiskuludest; ülejäänud kulud katab liikmesriik. Enne vahendite ja taristute soetamise menetluse algatamist sõlmivad Euroopa küberturvalisuse pädevuskeskus ja riiklik infoturbekeskus majutus- ja kasutuslepingu, millega reguleeritakse vahendite ja taristute kasutamist.

Muudatusettepanek 36

Ettepanek võtta vastu määrus
Artikkel 5 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Euroopa küberturvalisuse pädevuskeskus valib osalemiskutse alusel majutuskonsortsiumi, kellega koos osaleda vahendite ja taristute ühishankes. Euroopa	2. Euroopa küberturvalisuse pädevuskeskus valib osalemiskutse alusel majutuskonsortsiumi, kellega koos osaleda vahendite ja taristute ühishankes. Euroopa

küberturvalisuse pädevuskeskus võib anda majutuskonsortsiumile ***toetuse***, et rahastada ***asjaomaste*** vahendite ja taristute käitamist. Liidu rahalise panusega kaetakse kuni 75 % vahendite ja taristute soetamise kuludest ning kuni 50 % käitamiskuludest; ülejäänud kulud katab majutuskonsortsium. Enne vahendite ja taristute soetamise menetluse algatamist sõlmivad Euroopa küberturvalisuse pädevuskeskus ja majutuskonsortsium majutus- ja kasutuslepingu, millega reguleeritakse vahendite ja taristute kasutamist.

küberturvalisuse pädevuskeskus võib anda majutuskonsortsiumile ***toetust***, et rahastada ***nende*** vahendite ja taristute käitamist ***rangel tingimusel, et neid vahendeid ja taristuid pakuvad usaldusväärsed teenuseosutajad kooskõlas artikliga 16***. Liidu rahalise panusega kaetakse kuni 75 % vahendite ja taristute soetamise kuludest ning kuni 50 % käitamiskuludest; ülejäänud kulud katab majutuskonsortsium. Enne vahendite ja taristute soetamise menetluse algatamist sõlmivad Euroopa küberturvalisuse pädevuskeskus ja majutuskonsortsium majutus- ja kasutuslepingu, millega reguleeritakse vahendite ja taristute kasutamist.

Muudatusettepanek 37

Ettepanek võtta vastu määrus
Artikkel 5 – lõige 2 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	2a. Suure riskiga kolmandast riigist pärit taristu ja teenuseosutajad jäetakse automaatselt kõrvale.

Muudatusettepanek 38

Ettepanek võtta vastu määrus
Artikkel 6 – lõige 1 – punkt b a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ba) toetab otseselt osalevate liikmete sõjalise ja kaitsevõime tugevdamist või hoiab ära otsese ja vahetu ohu nende julgeolekule. Kuna kaitsesektori nõrkuste ärakasutamine võib põhjustada märkimisväärseid häireid ja kahju, nõuab kaitsetööstuse küberturvalisus erimeetmeid, et tagada tarneahelate turvalisus, eelkõige tarneahelate madalama tasandi üksuste puhul, mis ei nõua juurdepääsu salastatud teabele, kuid mis võivad kujutada endast tõsist ohtu

	kogu sektorile. Erilist tähelepanu tuleks pöörata mõjule, mida mis tahes rikkumine võib avaldada, ja võrguandmete võimaliku manipuleerimise ohule, mis võib muuta elutähtsad kaitsevahendid kasutuks või isegi nende operatsioonisüsteemid üle võtta, muutes need kaaperdamise vastu kaitsetuks.

Muudatusettepanek 39

Ettepanek võtta vastu määrus
Artikkel 6 – lõige 1 – punkt b a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	bb) toetab osalevate liikmete kaitsevõime tugevdamist või hoiab ära otsese ja vahetu ohu nende julgeolekule, tagades tarneahelate turvalisuse, eelkõige tarneahelate madalama tasandi üksuste puhul, mis ei vaja juurdepääsu salastatud teabele, kuid mis võivad kujutada endast tõsist ohtu kogu sektorile.

Muudatusettepanek 40

Ettepanek võtta vastu määrus
Artikkel 7 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Kui piiriülene infoturbekeskus saab teavet võimaliku või käimasoleva ulatusliku küberintsidendi kohta, esitab ta asjaomase teabe tarbetu viivituseta EU-CyCLONe-le, CSIRTide võrgustikule ja komisjonile, pidades silmas nende direktiivi (EL) 2022/2555 kohast rolli kriiside ohjamisel.	1. Kui piiriülene infoturbekeskus saab teavet võimaliku või käimasoleva ulatusliku küberintsidendi kohta, esitab ta asjaomase teabe tarbetu viivituseta EU-CyCLONe-le, CSIRTide võrgustikule ja komisjonile, ***sh kõrgele esindajale ja Euroopa välisteenistusele, kui tegu on kolmanda riigiga,*** pidades silmas nende direktiivi (EL) 2022/2555 kohast rolli kriiside ohjamisel.

Muudatusettepanek 41

Ettepanek võtta vastu määrus
Artikkel 8 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Euroopa küberkilbis osalevad liikmesriigid tagavad kõrgetasemelise andmeturbe ja Euroopa küberkilbi taristu füüsilise turbe ning selle taristu nõuetekohase haldamise ja kontrollimise, et kaitsta taristut ohtude eest ning tagada taristu ja selle süsteemide, sealhulgas taristu kaudu vahetatavate andmete ***turvalisus***.	1. Euroopa küberkilbis osalevad liikmesriigid tagavad kõrgetasemelise andmeturbe ja Euroopa küberkilbi taristu füüsilise turbe ning selle taristu nõuetekohase haldamise ja kontrollimise, et kaitsta taristut ohtude eest ning tagada taristu ja selle süsteemide ***turvalisus, vähendades riske ja edendades ELi tehnoloogilist eelist kriitilise tähtsusega sektorites***, sealhulgas ***meetmed suure riskiga tarnijate kasutamise piiramiseks või välistamiseks, ning et kaitsta*** taristu kaudu vahetatavate andmete ***turvalisust***.

Muudatusettepanek 42

Ettepanek võtta vastu määrus
Artikkel 8 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Euroopa küberkilbis osalevad liikmesriigid tagavad, et Euroopa küberkilbi raames toimuv teabe jagamine üksustega, mis ei ole liikmesriikide avaliku sektori asutused, ei kahjusta liidu julgeolekuhuve.	2. Euroopa küberkilbis osalevad liikmesriigid tagavad, et Euroopa küberkilbi raames toimuv teabe jagamine üksustega, mis ei ole liikmesriikide avaliku sektori asutused, ei kahjusta liidu julgeolekuhuve ***ning et teabe jagamine suure riskiga teenuseosutajatega on piiratud ega kahjusta liidu julgeolekut ega strateegilisi huve***.

Muudatusettepanek 43

Ettepanek võtta vastu määrus
Artikkel 8 – lõige 3

Komisjoni ettepanek	*Muudatusettepanek*
3. Komisjon võib vastu võtta rakendusaktid, millega kehtestatakse	3. Komisjon võib vastu võtta rakendusaktid, millega kehtestatakse

tehnilised nõuded, et liikmesriigid saaksid täita oma lõigetes 1 ja 2 osutatud kohustusi. Need rakendusaktid võetakse vastu kooskõlas käesoleva määruse artikli 21 lõikes 2 osutatud kontrollimenetlusega. Seda tehes võtab komisjon, keda toetab kõrge esindaja, arvesse asjaomaseid kaitsetasandi turvastandardeid, et hõlbustada koostööd sõjaliste osalejatega.	tehnilised nõuded, et liikmesriigid saaksid täita oma lõigetes 1 ja 2 osutatud kohustusi. Need rakendusaktid võetakse vastu kooskõlas käesoleva määruse artikli 21 lõikes 2 osutatud kontrollimenetlusega. Seda tehes võtab komisjon, keda toetab kõrge esindaja, arvesse asjaomaseid kaitsetasandi turvastandardeid, et hõlbustada koostööd sõjaliste osalejatega***, kasutades sobival viisil ära kõiki tsiviil- ja sõjalistele kogukondadele kättesaadavaid kaitsevõimalusi ELi laiema julgeoleku ja kaitse jaoks, ning teavitab Euroopa Parlamenti***.

Muudatusettepanek 44

Ettepanek võtta vastu määrus
Artikkel 9 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Mehhanismi rakendamise meetmeid toetatakse rahaliselt programmist „Digitaalne Euroopa“ ja neid rakendatakse kooskõlas määrusega (EL) 2021/694, eriti selle erieesmärgiga nr 3.	2. Mehhanismi rakendamise meetmeid toetatakse rahaliselt programmist „Digitaalne Euroopa“ ja neid rakendatakse kooskõlas määrusega (EL) 2021/694, eriti selle erieesmärgiga nr 3***, ja kolmandatele riikidele, eelkõige Ukrainale ja Moldovale, abimeetmete pakkumise korral Euroopa rahutagamisrahastust***.

Muudatusettepanek 45

Ettepanek võtta vastu määrus
Artikkel 10 – lõige 1 – punkt a

Komisjoni ettepanek	*Muudatusettepanek*
a) valmisolekumeetmed, sealhulgas ülikriitilise tähtsusega sektorites tegutsevate üksuste valmisoleku koordineeritud testimine kõikjal liidus;	a) valmisolekumeetmed, sealhulgas ülikriitilise tähtsusega sektorites***, näiteks avalikus taristus, valimistaristus, transpordis, tervishoius, telekommunikatsioonis, toiduga varustamise valdkonnas ja julgeolekus*** tegutsevate üksuste valmisoleku

	koordineeritud testimine kõikjal liidus;

Muudatusettepanek 46

Ettepanek võtta vastu määrus
Artikkel 10 – lõige 1 – punkt c

Komisjoni ettepanek	*Muudatusettepanek*
c) vastastikuse abistamise meetmed, mille puhul ühe liikmesriigi ametiasutused abistavad teist liikmesriiki, eelkõige direktiivi (EL) 2022/2555 artikli 11 lõike 3 punktis f sätestatud meetmed.	c) vastastikuse abistamise meetmed, mille puhul ühe liikmesriigi ametiasutused abistavad teist liikmesriiki, eelkõige direktiivi (EL) 2022/2555 artikli 11 lõike 3 punktis f sätestatud meetmed ***ning võttes arvesse ELi lepingu artikli 42 lõiget 7 ja ELi toimimise lepingu artiklit 222;***

Muudatusettepanek 47

Ettepanek võtta vastu määrus
Artikkel 10 – lõige 1 – punkt c a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ca) vähendada süsteemseid küberriske, mis tulenevad sõltuvusest kriitilise tähtsusega seadmetest, mis tarnitakse riikidest, mis oleks vastuolus liidu ja selle liikmesriikide julgeoleku- ja kaitsehuvidega, nagu need on kindlaks määratud ÜVJP raames vastavalt ELi lepingu V jaotisele;

Muudatusettepanek 48

Ettepanek võtta vastu määrus
Artikkel 11 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. Võrgu- ja infoturbe koostöörühm koostöös komisjoni, ENISA ja ***kõrge esindajaga*** töötavad välja ühised riskistsenaariumid ja metoodikad koordineeritud testimise jaoks.	2. Võrgu- ja infoturbe koostöörühm koostöös komisjoni, ENISA***, kõrge esindaja, Euroopa välisteenistuse*** ja ***asjakohasel juhul EDAga*** töötavad välja ühised riskistsenaariumid ja metoodikad

koordineeritud testimise jaoks.

Muudatusettepanek 49

Ettepanek võtta vastu määrus
Artikkel 12 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. ELi küberreserv hõlmab intsidentidele reageerimise teenuseid, mida osutavad artiklis 16 sätestatud kriteeriumide alusel välja valitud usaldusväärsed teenuseosutajad. Küberreserv sisaldab eelnevalt kindlaks määratud teenuseid. Teenuseid saab kasutada kõigis liikmesriikides.	2. ELi küberreserv hõlmab intsidentidele reageerimise teenuseid, mida osutavad artiklis 16 sätestatud kriteeriumide alusel välja valitud usaldusväärsed teenuseosutajad. Küberreserv sisaldab eelnevalt kindlaks määratud teenuseid. Teenuseid saab kasutada kõigis liikmesriikides ***ja neis kolmandates riikides, mis vastavad käesoleva määruse alusel kohaldatavatele nõuetele***.

Muudatusettepanek 50

Ettepanek võtta vastu määrus
Artikkel 12 – lõige 3 – punkt b

Komisjoni ettepanek	*Muudatusettepanek*
b) liidu institutsioonid, organid ja asutused.	b) liidu institutsioonid, organid ja asutused***, sh ÜJKP missioonid***.

Muudatusettepanek 51

Ettepanek võtta vastu määrus
Artikkel 12 – lõige 4

Komisjoni ettepanek	*Muudatusettepanek*
4. Lõike 3 punktis a osutatud kasutajad kasutavad ELi küberreservi teenuseid ***selleks***, et reageerida olulistele või ulatuslikele intsidentidele, mis mõjutavad kriitilise või ***ülikriitilise tähtsusega*** sektorites ***tegutsevaid üksusi***, ***või toetada sellistele intsidentidele***	4. Lõike 3 punktis a osutatud kasutajad kasutavad ELi küberreservi teenuseid, et reageerida olulistele või ulatuslikele intsidentidele, mis mõjutavad ***üksusi, mis tegutsevad*** kriitilise ***tähtsusega*** või ***ülikriitilistes*** sektorites***, nagu avalik taristu***, ***valimistaristu, transport, tervishoid, finantssektor,***

reageerimist ja ***neist vahetut*** taastumist.	***telekommunikatsioon, toiduga kindlustatus*** ja ***julgeolek, või toetada nendest intsidentidest vahetut*** taastumist.

Muudatusettepanek 52

Ettepanek võtta vastu määrus
Artikkel 12 – lõige 5

Komisjoni ettepanek	*Muudatusettepanek*
5. Üldine vastutus ELi küberreservi rakendamise eest lasub komisjonil. Komisjon määrab kindlaks ELi küberreservi prioriteedid ja arengu, võttes arvesse lõikes 3 osutatud kasutajate vajadusi, ja teeb järelevalvet selle rakendamise üle ning tagab vastastikuse täiendavuse, järjepidevuse, koostoime ja seosed muude käesoleva määruse kohaste toetusmeetmetega ning muude liidu meetmete ja ***programmidega***.	5. Üldine vastutus ELi küberreservi rakendamise eest lasub komisjonil. Komisjon määrab kindlaks ELi küberreservi prioriteedid ja arengu, võttes arvesse lõikes 3 osutatud kasutajate vajadusi, ja teeb järelevalvet selle rakendamise üle ning tagab vastastikuse täiendavuse, järjepidevuse, koostoime ja seosed muude käesoleva määruse kohaste toetusmeetmetega ning muude liidu meetmete***, programmide*** ja ***eesmärkidega, eelkõige strateegilise eesmärgiga vähendada sõltuvust suure riskiga tarnijatest, kes oleks vastuolus liidu ja selle liikmesriikide julgeoleku- ja kaitsehuvidega, nagu need on kindlaks määratud ÜVJP raames vastavalt ELi lepingu V jaotisele***.

Muudatusettepanek 53

Ettepanek võtta vastu määrus
Artikkel 12 – lõige 7

Komisjoni ettepanek	*Muudatusettepanek*
7. Selleks et toetada komisjoni ELi küberreservi loomisel, koostab ENISA pärast konsulteerimist liikmesriikide ja komisjoniga ülevaate vajalikest teenustest. ENISA koostab pärast komisjoniga konsulteerimist sarnase ülevaate ka selle kohta, millised vajadused on kolmandatel riikidel, kellel on artikli 17 alusel õigus saada ELi küberreservist toetust. Vajaduse korral konsulteerib komisjon kõrge	7. Selleks et toetada komisjoni ELi küberreservi loomisel, koostab ENISA pärast konsulteerimist liikmesriikide ja komisjoniga ülevaate vajalikest teenustest. ENISA koostab pärast komisjoniga konsulteerimist ***Euroopa välisteenistuse abiga*** sarnase ülevaate ka selle kohta, millised vajadused on kolmandatel riikidel, kellel on artikli 17 alusel õigus saada ELi küberreservist toetust. Vajaduse korral

esindajaga.

konsulteerib komisjon kõrge esindajaga.

Muudatusettepanek 54

Ettepanek võtta vastu määrus
Artikkel 14 – lõige 2 – punkt a a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	aa) intsidendi mõju liidu julgeolekule ja kaitsele;

Muudatusettepanek 55

Ettepanek võtta vastu määrus
Artikkel 15 – lõige 3

Komisjoni ettepanek	*Muudatusettepanek*
3. Olles eelnevalt konsulteerinud kõrge esindajaga, võib küberhädaolukorra mehhanismi kaudu antava toetusega täiendada abi, mida antakse ühise välis- ja julgeolekupoliitika ning ühise julgeoleku- ja kaitsepoliitika raames, sealhulgas küberturbe kiirreageerimisrühmade kaudu. Samuti võib see toetus täiendada abi, mida üks liikmesriik annab teisele liikmesriigile ELi lepingu artikli 42 lõike 7 alusel.	3. Olles eelnevalt konsulteerinud kõrge esindajaga, võib küberhädaolukorra mehhanismi kaudu antava toetusega täiendada abi, mida antakse ühise välis- ja julgeolekupoliitika ning ühise julgeoleku- ja kaitsepoliitika raames, sealhulgas küberturbe kiirreageerimisrühmade kaudu***, et toetada paremini ELi liikmesriike, ÜJKP missioone ja operatsioone ning neid kolmandaid riike, kes on oma asjaomase poliitika viinud vastavusse ELi ühise välis- ja julgeolekupoliitikaga ning ühise julgeoleku- ja kaitsepoliitikaga, eelkõige Ukrainat ja Moldovat, et toetada pingutusi, mida nad küberkaitsesuutlikkuse suurendamisel teevad***. Samuti võib see toetus täiendada abi, mida üks liikmesriik annab teisele liikmesriigile ELi lepingu artikli 42 lõike 7 alusel.

Muudatusettepanek 56

Ettepanek võtta vastu määrus
Artikkel 16 – lõige 2 – punkt b a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	aa) teenuseosutaja tõendab, et tema otsustus- ja juhtimisstruktuurid on vabad riikide valitsuste lubamatust mõjust, mis oleks vastuolus liidu ja selle liikmesriikide julgeoleku- ja kaitsehuvidega, nagu need on kindlaks määratud ÜVJP raames vastavalt ELi lepingu V jaotisele;

Muudatusettepanek 57

Ettepanek võtta vastu määrus
Artikkel 16 – lõige 2 – punkt f

Komisjoni ettepanek	*Muudatusettepanek*
f) teenuseosutajal on nõutava teenuse jaoks vajalikud riist- ja tarkvaraseadmed;	f) teenuseosutajal on nõutava teenuse jaoks vajalikud riist- ja tarkvaraseadmed ***ning ta vastab määruse XX/XXXX (küberkerksuse määrus) artiklis X sätestatud nõuetele***;

Muudatusettepanek 58

Ettepanek võtta vastu määrus
Artikkel 16 – lõige 2 – punkt j a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	ja) suure riskiga kolmandast riigist pärit teenuseosutajatel ei ole lubatud teenuseid osutada.

Muudatusettepanek 59

Ettepanek võtta vastu määrus
Artikkel 16 – lõige 2 – punkt j b (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	jb) teenuseosutaja teeb võimaluse korral tihedat koostööd asjaomaste VKEdega;

Muudatusettepanek 60

Ettepanek võtta vastu määrus
Artikkel 17 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. Kolmandad riigid võivad taotleda ELi küberreservist toetust, kui ***see on ette nähtud assotsieerimislepinguga, mis on sõlmitud seoses nende osalemisega programmis „Digitaalne Euroopa“.***	1. Kolmandad riigid võivad taotleda ELi küberreservist toetust, kui ***a) see on ette nähtud assotsieerimislepinguga, mis on sõlmitud seoses nende osalemisega programmis „Digitaalne Euroopa“;*** ***b) tegu on selliste kolmandate riikidega, kuhu lähetatakse ÜJKP missioon, millel on erivolitused, et tugevdada vastupidavusvõimet hübriidohtudele, sealhulgas küberohtudele, või kus on vastu võetud Euroopa rahutagamisrahastu abimeede riigi kübervastupidavusvõime tugevdamiseks.***

Muudatusettepanek 61

Ettepanek võtta vastu määrus
Artikkel 17 – lõige 2

Komisjoni ettepanek	*Muudatusettepanek*
2. ELi küberreservist antakse toetust kooskõlas käesoleva määrusega ja järgides konkreetseid tingimusi, mis on sätestatud lõikes 1 osutatud assotsieerimislepingus.	2. ELi küberreservist antakse toetust kooskõlas käesoleva määrusega ja järgides konkreetseid tingimusi, mis on sätestatud lõikes 1 osutatud assotsieerimislepingus***, välja arvatud lõike 1 punkti b sätetega hõlmatud kolmandate riikide puhul***.

Muudatusettepanek 62

Ettepanek võtta vastu määrus
Artikkel 18 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
1. ENISA vaatab läbi ja hindab komisjoni, EU-CyCLONe või CSIRTide võrgustiku taotlusel konkreetse olulise või ulatusliku küberintsidendiga seotud ohte, nõrkusi ja leevendusmeetmeid. Pärast intsidendi läbivaatamist ja hindamist esitab ENISA CSIRTide võrgustikule, EU-CyCLONe-le ja komisjonile läbivaatamisaruande, et toetada neid nende ülesannete, eelkõige direktiivi (EL) 2022/2555 artiklites 15 ja 16 sätestatud ülesannete täitmisel. Asjakohasel juhul jagab komisjon aruannet kõrge ***esindajaga***.	1. ENISA vaatab läbi ja hindab komisjoni, EU-CyCLONe või CSIRTide võrgustiku taotlusel konkreetse olulise või ulatusliku küberintsidendiga seotud ohte, nõrkusi ja leevendusmeetmeid. Pärast intsidendi läbivaatamist ja hindamist esitab ENISA CSIRTide võrgustikule, EU-CyCLONe-le ja komisjonile läbivaatamisaruande, et toetada neid nende ülesannete, eelkõige direktiivi (EL) 2022/2555 artiklites 15 ja 16 sätestatud ülesannete täitmisel. Asjakohasel juhul***, eriti kui intsident on seotud kolmanda riigiga,*** jagab komisjon aruannet kõrge ***esindaja ja Euroopa välisteenistusega***.

Muudatusettepanek 63

Ettepanek võtta vastu määrus
Artikkel 18 – lõige 3 a (uus)

Komisjoni ettepanek	*Muudatusettepanek*
	3a. Aruannet jagatakse Euroopa Parlamendiga kooskõlas liidu või riigisisese õigusega, mis käsitleb tundliku salastatud teabe kaitset.

Muudatusettepanek 64

Ettepanek võtta vastu määrus
Artikkel 19 – lõik 1 – punkt 1 – alapunkt a – punkt 1
Määrus (EL) 2021/694
Artikkel 6 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
aa) toetada ELi küberkilbi arendamist, sealhulgas riiklike ja piiriüleste infoturbekeskuste loomist, kasutuselevõttu ja käitamist, mille tulemusel paranevad liidus olukorrateadlikkus ja	aa) toetada ELi küberkilbi arendamist, sealhulgas riiklike ja piiriüleste infoturbekeskuste loomist, kasutuselevõttu ja käitamist, mille tulemusel paranevad liidus olukorrateadlikkus ja küberohuteadmus ***ning väheneb liidu***

küberohuteadmus;	***sõltuvus kriitilise tähtsusega küberturvalisuse seadmete või komponentide suure riskiga tarnijatest, kes oleks vastuolus liidu ja selle liikmesriikide julgeoleku- ja kaitsehuvidega, mis on kehtestatud ÜVJP raames vastavalt ELi lepingu V jaotisele***;

Muudatusettepanek 65

Ettepanek võtta vastu määrus
Artikkel 20 – lõige 1

Komisjoni ettepanek	*Muudatusettepanek*
Komisjon esitab Euroopa Parlamendile ja nõukogule hiljemalt ***[neli*** aastat pärast käesoleva määruse kohaldamise ***alguskuupäeva]*** aruande käesoleva määruse hindamise ja läbivaatamise kohta.	Komisjon esitab Euroopa Parlamendile ja nõukogule hiljemalt ***[kolm*** aastat pärast käesoleva määruse kohaldamise ***alguskuupäeva ja pärast seda iga kahe aasta tagant]*** aruande käesoleva määruse hindamise ja läbivaatamise kohta.

NÕUANDVA KOMISJONI MENETLUS

Pealkiri	Meetmed, et tugevdada liidus solidaarsust ja suurendada suutlikkust küberohtude ja -intsidentide avastamiseks, nendeks valmistumiseks ja neile reageerimiseks
Viited	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Vastutav komisjon istungil teada andmise kuupäev	ITRE 1.6.2023
Arvamuse esitajad istungil teada andmise kuupäev	AFET 1.6.2023
Arvamuse koostaja nimetamise kuupäev	Dragoş Tudorache 16.6.2023
Läbivaatamine parlamendikomisjonis	18.9.2023
Vastuvõtmise kuupäev	24.10.2023
Lõpphääletuse tulemus	+: 39 –: 4 0: 0
Lõpphääletuse ajal kohal olnud liikmed	Alexander Alexandrov Yordanov, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Włodzimierz Cimoszewicz, Katalin Cseh, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Bernard Guetta, Sandra Kalniete, Dietmar Köster, Andrius Kubilius, David Lega, Leopoldo López Gil, Jaak Madison, Pedro Marques, David McAllister, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Matjaž Nemec, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Jordi Solé, Sergei Stanishev, Tineke Strik, Dominik Tarczyński, Dragoş Tudorache, Thomas Waitz, Bernhard Zimniok, Željana Zovko
Lõpphääletuse ajal kohal olnud asendusliikmed	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

NIMELINE LÕPPHÄÄLETUS NÕUANDVAS KOMISJONIS

39	+
ECR	Lars Patrick Berg, Dominik Tarczyński
ID	Anna Bonfrisco, Jaak Madison
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Michael Gahler, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Leopoldo López Gil, David McAllister, Vangelis Meimarakis, Francisco José Millán Mon, Željana Zovko
Renew	Petras Auštrevičius, Katalin Cseh, Bernard Guetta, Georgios Kyrtsos, Dragoş Tudorache
S&D	Attila Ara-Kovács, Włodzimierz Cimoszewicz, Dietmar Köster, Pedro Marques, Sven Mikser, Matjaž Nemec, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Sergei Stanishev
Verts/ALE	Sergey Lagodinsky, Jordi Solé, Tineke Strik, Thomas Waitz

4	-
ID	Bernhard Zimniok
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Mick Wallace

0	0

Kasutatud tähised:
+ : poolt
- : vastu
0 : erapooletu