Euroopa Liidu
Nõukogu

**Brüssel, 20. oktoober 2021**
**(OR. en)**

**13048/21**

**CYBER 263**
**JAI 1117**
**TELECOM 384**
**CSC 362**
**CIS 116**
**RELEX 874**
**ENFOPOL 370**
**COPS 373**
**COSI 190**
**HYBRID 62**
**CSCI 133**
**POLGEN 177**
**DATAPROTECT 244**

**MENETLUSE TULEMUS**

| | |
|---|---|
| Saatja: | Nõukogu peasekretariaat |
| Kuupäev: | 19. oktoober 2021 |
| Saaja: | Delegatsioonid |
| Eelmise dok nr: | 12534/21 |
| Teema: | Nõukogu järeldused ühise küberüksuse algatuse potentsiaali uurimise kohta, täiendamaks ELi koordineeritud reageerimist ulatuslike küberintsidentide ja kriiside korral<br>– Nõukogu järeldused (19. oktoober 2021) |

Delegatsioonidele esitatakse lisas nõukogu järeldused ühise küberüksuse algatuse potentsiaali uurimise kohta, täiendamaks ELi koordineeritud reageerimist ulatuslike küberintsidentide ja kriiside korral, mille nõukogu võttis vastu 19. oktoobril 2021.

**LISA**

**Nõukogu järeldused ühise küberüksuse algatuse potentsiaali uurimise kohta, täiendamaks ELi koordineeritud reageerimist ulatuslike küberintsidentide ja kriiside korral**

EUROOPA LIIDU NÕUKOGU,

TULETADES MEELDE oma järeldusi, milles käsitletakse:

– ELi küberturvalisuse strateegiat digikümnendi jaoks,[1]

– ELi koordineeritud reageerimist ulatuslike küberintsidentide ja kriiside korral,[2]

– küberdiplomaatiat,[3]

– pahatahtlikule kübertegevusele ELi ühise diplomaatilise reageerimise raamistikku („küberdiplomaatia meetmete kogum“),[4]

– julgeolekut ja kaitset,[5]

– ELi küberkaitsepoliitika raamistikku,[6]

– Euroopa digituleviku kujundamist,[7]

– nõukogu 11. detsembri 2018. aasta rakendusotsust (EL) 2018/1993, mis käsitleb ELi integreeritud korda poliitiliseks reageerimiseks kriisidele,

---

1 7290/21.
2 10086/18.
3 6122/15 + COR 1.
4 10474/17.
5 8396/21.
6 15585/14.
7 8711/20.

– Euroopa Parlamendile ja nõukogule esitatud ühisteatist „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis,“[8]

– küberturvalisuse alase võimsuse ja suutlikkuse suurendamist ELis,[9]

1. TOONITAB küberturvalisuse tähtsust vastupidava, digitaalse ja rohelise Euroopa ülesehitamisel; RÕHUTAB, et küberturvalisus on hädavajalik ELi ja selle liikmesriikide, kodanike, ettevõtjate ja asutuste jõukuse ja julgeoleku tagamiseks ning meie vaba ja demokraatliku ühiskonna terviklikkuse säilitamiseks;

2. TUNNISTAB paljude küberohtude piiri- ja sektoriülest olemust ning mõjukama, keerukama, suunatuma, komplekssema, püsivama ja/või läbivama pahatahtliku kübertegevuse jätkuvate kampaaniatega kaasnevaid riske ja nende võimalikku mõju[10]. COVID-19 pandeemia on toonud veelgi rohkem esile meie ühiskondade haavatavuse ja ulatuslikest küberintsidentidest tekkida võiva kahju majandusele, demokraatiale, esmatähtsatele teenustele ja elutähtsale taristule, eelkõige tervishoiusektoris. Samuti on see suurendanud ühenduvuse tähtsust ja ühiskonna sõltuvust töökindlatest, usaldusväärsetest ja turvalistest võrgu- ja infosüsteemidest. Lõppkokkuvõttes on see rõhutanud vajadust ülemaailmse, avatud, vaba, stabiilse ja turvalise interneti järele, samuti usalduse järele info- ja kommunikatsioonitehnoloogia (IKT) toodete, protsesside ja teenuste ning nende turvalisuse suhtes, hõlmates vastupidava tarneahela tagamise vajadust;

---

8 14435/17 + COR 1.
9 7737/19.
10 ENISA ohtude kaardistamise aruanne 2020.

3. KORDAB, kui oluline on kübervastupidavusvõime ja ELi küberturvalisuse kriisiohjeraamistiku[11] edasiarendamine, et reageerida ELi tasandil tõhusalt ja õigeaegselt ulatuslikele küberintsidentidele ja -kriisidele ning integreerida see senisest enam olemasolevatesse horisontaalsetesse ja valdkondlikesse ELi kriisidele reageerimise mehhanismidesse; RÕHUTAB nõukogu ning kriisidele poliitilist reageerimist käsitleva ELi integreeritud korra (IPCR) rolli selles, et tagada liidu poliitilisel tasandil toimuv õigeaegne koordineerimine ja reageerimine ulatusliku mõju või poliitilise tähtsusega kriisidele, olenemata sellest, kas need on tekkinud liidus või sellest väljaspool; TOONITAB, kui oluline on selliste raamistike ja mehhanismide katsetamine korrapärastel õppustel;

4. TULETAB MEELDE, et ulatuslike küberintsidentide ja -kriisidega seotud tegevus ELi tasandil toimub kooskõlas subsidiaarsuse, proportsionaalsuse, vastastikuse täiendavuse, dubleerimise vältimise ja konfidentsiaalsuse põhimõtetega; KORDAB, et esmane vastutus liikmesriike mõjutavatele ulatuslikele küberintsidentidele ja kriisidele reageerimise eest lasub neil endil; TULETAB MEELDE, kui oluline on austada liikmesriikide pädevusi ja nende ainuvastutust riikliku julgeoleku eest vastavalt Euroopa Liidu lepingu artikli 4 lõikele 2, sealhulgas küberturvalisuse valdkonnas;

5. TULETAB samal ajal MEELDE, kui oluline on austada ELi institutsioonide, organite ja asutuste pädevusi ja volitusi. Kõrgel esindajal, komisjonil ning teistel ELi institutsioonidel, organitel ja asutustel on samuti oluline roll, mis tuleneb liidu õigusest, sealhulgas potentsiaalse mõju tõttu, mis ulatuslikel küberturvalisuse intsidentidel ja -kriisidel on ühtsele turule ning samuti ELi institutsioonide, organite ja asutuste toimimisele;

[11] 10086/18.

6. RÕHUTAB, et ELi küberturvalisuse kriisijuhtimise raamistiku edasiarendamisel tuleb vältida tarbetut dubleerimist ning püüelda vastastikuse täiendavuse ja lisaväärtuse poole, tagades ka kooskõla olemasolevate mehhanismide, algatuste, võrgustike, protsesside ja menetlustega riiklikul ja Euroopa tasandil; TOONITAB, kui oluline on olemasolevate protsesside ja struktuuride optimeerimine keerukuse vähendamiseks, samuti liidu ühtekuuluvuse huvides juurdepääsu ja reageerimisvõime parandamine abi ja solidaarsust otsivate isikute jaoks;

7. TUNNISTAB rahvusvahelise õiguse, sealhulgas kogu ÜRO põhikirja ning rahvusvahelise humanitaarõiguse ja inimõigustealase õiguse kohaldatavust küberruumis, ning INNUSTAB järgima vabatahtlikke mittesiduvaid norme, reegleid ja põhimõtteid, mis käsitlevad riikide vastutustundlikku käitumist küberruumis, mille on heaks kiitnud kõik ÜRO liikmesriigid;

8. VÄLJENDAB HEAMEELT nõukogus viimastel aastatel tehtud edusammude üle, eelkõige horisontaalses küberküsimuste töörühmas ja teistes asjaomastes nõukogu töörühmades, samuti muude liikmesriikidevaheliste koostöö- ja teabejagamisalgatuste, -võrgustike ja -mehhanismide loomise üle, nt Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiviga (EL) 2016/1148 loodud võrgu- ja infoturbe koostöörühma ja CSIRTide võrgustiku, küberkriisi kontaktasutuste võrgustiku (CyCLONe) üle, samuti alalise struktureeritud koostöö (PESCO) raames käivitatud asjaomaste küberkaitsega seotud projektide,[12] ühise küberkuritegevuse vastase rakkerühma (J-CAT), Euroopa küberkuritegevuse vastase õigusalase koostöö võrgustiku (EJCN) ja liikmesriikide vabatahtlike panuste üle ELi luure- ja situatsioonikeskusesse (EU SITCEN) ning küberdiplomaatia meetmete kogumi raames tehtava koordineerimise ja koostöö üle;

[12] Eelkõige Leedu koordineeritav küberturbe kiirreageerimisrühmade ja küberturvalisuse alase vastastikuse abistamise projekt, Saksamaa koordineeritav küber- ja teabevaldkonna koordinatsioonikeskus ning Kreeka koordineeritav küberohtudele ja -intsidentidele reageerimise teabevahetuse platvorm.

9. TULETAB MEELDE olemasolevaid ELi institutsioonide, organite ja asutuste vahelisi koostööraamistikke, nt ENISA ja CERT-EU struktureeritud koostöö ning ENISA, Euroopa Kaitseagentuuri (EDA), Europoli küberkuritegevuse vastase võitluse Euroopa keskuse (EC3) ja CERT-EU vaheline vastastikuse mõistmise memorandum; RÕHUTAB, kui oluline on jätkata korrapärast teabevahetust nõukoguga seoses kõnealuste koostööraamistike edasise arenguga;

10. TOONITAB, kui oluline on tõhustada koostööd ja teabevahetust ELi ja selle liikmesriikide erinevate küberkogukondade vahel kõigil vajalikel tasanditel, nii tehnilisel, operatiivsel kui ka strateegilisel/poliitilisel tasandil, ning ühendada olemasolevad kriisiohjemehhanismid, -võrgustikud, -struktuurid, -protsessid ja -menetlused, kui see toetab ja parandab laiaulatuslike küberintsidentide ja kriisidega toimetulemist;

11. TUNNISTAB edusamme, mida liikmesriikide rühm on teinud ühise operatiivse kübervõime, nn küberturbe kiirreageerimisrühmade loomisel alalise struktureeritud koostöö (PESCO) raames, eesmärgiga süvendada vastastikuse abi kaudu vabatahtlikku koostööd kübervaldkonnas, sealhulgas ulatuslikele küberintsidentidele ja kriisidele reageerimisel;

12. TUNNISTAB õiguskaitseasutuste kogemusi ja ööpäevaringset reageerimisvõimet operatiivkoostöö ja turvalise teabevahetuse valdkonnas võitluses suurte piiriüleste küberrünnetega ELi hädaolukordades õiguskaitsealase reageerimise protokolli kaudu;

13. TUNNISTAB pahatahtlikule kübertegevusele ELi ühise diplomaatilise reageerimise raamistiku (küberdiplomaatia meetmete kogum) jätkuvat rakendamist; TULETAB MEELDE, et igal liikmesriigil on vabadus teha pahatahtliku kübertegevuse omistamisega seoses juhtumipõhiselt oma suveräänne otsus; TULETAB MEELDE, et pahatahtlikule kübertegevusele ELi ühise diplomaatilise reageerimise raamistikus võetavad meetmed peaksid põhinema ühisel olukorrateadlikkusel, milles on liikmesriikide vahel kokku lepitud; EU INTCENil on keskne roll keskusena, mis võimaldab tagada ELis olukorrateadlikkuse ja hindab küberküsimustega seotud ohte, tuginedes liikmesriikide vabatahtlikule luureandmete kogumisele ja piiramata seejuures nende pädevust;

14. KORDAB vastastikuse abi ja solidaarsuse tähtsust kooskõlas Euroopa Liidu lepingu artikli 42 lõikega 7 ja Euroopa Liidu toimimise lepingu artikliga 222 ning KUTSUB ÜLES jätkama kübermõõtmega õppusi; TULETAB MEELDE vajadust kaaluda ELi küberturvalisuse kriisiohjeraamistiku, küberdiplomaatia meetmete kogumi ja eespool osutatud artiklite sätete omavahelist seotust ulatuslike küberintsidentide või -kriiside korral; lisaks TULETAB MEELDE, et liikmesriikidele Euroopa Liidu lepingu artikli 42 lõikest 7 tulenevad kohustused ei mõjuta teatavate liikmesriikide julgeoleku- ja kaitsepoliitika eripära; TULETAB samuti MEELDE, et NATO liikmeks olevate riikide jaoks on kollektiivse kaitse alus endiselt NATO;

15. TUNNISTAB ELi ja NATO koostööd küberturvalisuse ja -kaitse valdkonnas, sealhulgas teabe jagamist CERT-EU ja NATO küberturbeintsidentidele reageerimise üksuse (NCIRC) vahel, austades täielikult läbipaistvuse, vastastikkuse ja kaasatuse põhimõtteid ning mõlema organisatsiooni sõltumatust otsuste tegemisel;

16. TUNNISTAB, et asjakohasel juhul on oluline teha koostööd erasektoriga teabe jagamise õppuste ning asjaomaste eksperditeadmiste, samuti usaldusväärsete lahenduste ja teenuste pakkumise osas, sealhulgas näiteks intsidentidele reageerimise toetamisel ja eri küberkogukondade olukorrateadlikkuse suurendamisel;

17. RÕHUTAB turvaliste sidekanalite tähtsust salastatud ja tundliku teabe vahetamisel; TOOB ESILE vajaduse edasiste edusammude järele;

sellega seoses ja eespool toodut arvesse võttes:

18. TUNNUSTAB komisjoni soovitust ühise küberüksuse loomise kohta kui algatust, mida tuleb kaaluda ELi küberturvalisuse kriisiohjeraamistiku edasiarendamisel[13];

19. KUTSUB ELi ja selle liikmesriike ÜLES jätkama jõupingutusi terviklikuma ja tõhusama ELi küberturvalisuse kriisiohjeraamistiku loomiseks, tuginedes olemasolevatele mehhanismidele ja juba saavutatud edusammudele, ning võtma arvesse ühise küberüksuse algatuse potentsiaali neid mehhanisme täiendada, rakendades järkjärgulist lähenemisviisi; RÕHUTAB, et järkjärguline, läbipaistev ja kaasav protsess on oluline usalduse suurendamiseks ning seetõttu on see ELi küberturvalisuse kriisiohjeraamistiku edasisel arendamisel otsustava tähtsusega. Selles protsessis tuleks arvesse võtta liikmesriikide ning ELi institutsioonide, organite ja asutuste olemasolevaid rolle, pädevusi ja volitusi, samuti käesolevates järeldustes esitatud põhimõtteid, sealhulgas proportsionaalsuse, subsidiaarsuse, kaasavuse, täiendavuse, dubleerimise vältimise ja teabe konfidentsiaalsuse põhimõtteid; samal ajal TOONITAB, et liikmesriikide mis tahes võimalik osalemine või panus potentsiaalses ühises küberüksuses on vabatahtlik;

[13] C(2021)4520 final (11155/21 ja 11155/21 ADD1).

20. RÕHUTAB vajadust kehtestada asjakohased töömeetodid ja asjakohane juhtimine, et võimaldada kõigi liikmesriikide kaasamine ja osalemine aruteludes, arendamises ja tõhusates otsustusprotsessides, mis on seotud ELi küberturvalisuse kriisiohjeraamistiku, sealhulgas potentsiaalse ühise küberüksuse algatusega; KUTSUB ÜLES austama aluslepingutest tulenevaid nõukogu õigusi ja lojaalse koostöö põhimõtet;

21. TOONITAB, kui oluline on teha kindlaks ja kaasata kõik asjaomased küberkogukonnad ELis ja selle liikmesriikides, võttes samal ajal arvesse nende erinevaid rolle ja kohustusi eri liiki ulatuslike küberintsidentide ja -kriiside korral; RÕHUTAB nõukogu olulist rolli, eelkõige horisontaalse küberküsimuste töörühma (HWPCI) kaudu, poliitika kujundamisel ja koordineerimisel seoses ELi küberturvalisuse kriisiohjeraamistiku edasiarendamisega; PALUB seetõttu selles protsessis osaleda liikmesriikidel, komisjonil, Euroopa välisteenistusel, EU INTCENil, CERT-EU-l, ENISA-l, Europolil (EC3), Eurojustil (EJCN), küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskusel, samuti küberturbe intsidentide lahendamise üksuste võrgustiku, CyCLONe, võrgu- ja infoturbe koostöörühma, Euroopa Kaitseagentuuri ja asjaomaste PESCO projektide esindajatel ning muudel võimalikel sidusrühmadel. Nagu komisjoni soovituses välja pakutud, võiks põhjalikumalt uurida võimaliku töörühma loomist, tagades kõigi liikmesriikide piisava esindatuse ja tegutsedes nõukogu poliitiliste suuniste kohaselt, et see toimiks ajutise foorumina, mis toob kokku kõigi asjaomaste küberkogukondade esindajad liikmesriikides ja ELis. Selline töörühm peaks oma tegevusest korrapäraselt aru andma ning esitama võimalikud ettepanekud nõukogule arutamiseks, kinnitamiseks ja täiendavate suuniste andmiseks. Lisaks võiks luua muid kogukondadesiseseid ja -vahelisi dialoogivorme, sealhulgas õpikodade, seminaride, ühiste koolituste ja õppuste kaudu;

22. TOONITAB küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse ning riiklike koordineerimiskeskuste võrgustiku rolli seoses potentsiaalse ühise küberüksusega, eriti arvestades selle rolli märkimisväärselt suurendada liidu tehnoloogilist suutlikkust, tehnoloogilisi lahendusi ning suutlikkust ja oskusi küberturvalisuse valdkonnas;

23. PALUB ELil ja selle liikmesriikidel jätkata ELi küberturvalisuse kriisiohjeraamistiku edasiarendamist, sealhulgas uurides ühise küberüksuse algatuse potentsiaali, määrates kindlaks ja määratledes protsessi, sealhulgas selle etapid ja ajakava, ning selgitades eesmärke ning võimalikke rolle ja kohustusi; TOONITAB vajadust esmajärjekorras tugevdada olemasolevaid võrgustikke ja suhtlust igas kogukonnas ning koostada põhjalik ülevaade võimalikest lünkadest ja vajadustest seoses teabejagamisega küberkogukondades ja nende vahel, samuti Euroopa institutsioonide, organite ja asutuste sees ja vahel, ning leppida seejärel kokku potentsiaalse ühise küberüksuse võimalikes esmastes eesmärkides ja prioriteetides; ilma et see mõjutaks tulemust, RÕHUTAB vajadust keskenduda teabe jagamise vajaduste kindlakstegemisele, et luua kõigi asjaomaste kogukondade seas ühine olukorrateadlikkus. Teabejagamisega seotud lünkade ja vajaduste kindlakstegemisel, sealhulgas virtuaalsete platvormide võimalikul kasutamisel, tuleks jätkuvalt pöörata nõuetekohast tähelepanu turvalistele sidekanalitele salastatud ja tundliku teabe vahetamiseks, RÕHUTADES samas, et oluline on kasutada juba olemasolevat taristut. Järkjärgulise lähenemisviisi kasutuselevõtmise eesmärk on suurendada usaldust ja luua alus võimalikele edasistele meetmetele seoses valmisoleku ja operatiivkoostöö tõhustamisega; TUNNISTAB, et erinevad eesmärgid võivad nõuda erinevaid lahendusi ning ELis ja selle liikmesriikides asjaomaste küberkogukondade erinevate esindajate osalemist;

24. KUTSUB ÜLES täiendavalt kaaluma potentsiaalse ühise küberüksuse õiguslikku alust kogu protsessi vältel, sealhulgas hinnates selle üksuse ülesandeid ja rolli võrreldes soovituses ENISA-le antud ülesannete ja rolliga, pidades silmas Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määruse (EL) 2019/881 artiklit 7; KUTSUB ÜLES täiendavalt kaaluma ühist küberüksust käsitleva soovituse üksikuid elemente, sealhulgas seoses ELi küberturvalisuse kiirreageerimisrühmade ideega ning ELi küberintsidentidele ja -kriisidele reageerimise kavaga; RÕHUTAB, et potentsiaalne ühine küberüksus peab austama oma võimalike tulevaste osalejate pädevusi, mandaati ja õiguslikke volitusi;

25. KUTSUB ELi ja selle liikmesriike ÜLES kaaluma ühise küberüksuse algatuse potentsiaali, seda ka ELi institutsioonide, organite ja asutuste seisukohast, et täiendada praeguseid jõupingutusi liikmesriikide tasandil; TERVITAB komisjoni kavatsust tugevdada asjaomaste ELi institutsioonide, organite ja asutuste vastupanuvõimet oma peatse määruse ettepanekuga, milles käsitletakse ELi institutsioonidele, organitele ja asutustele kehtivaid ühiseid siduvaid küberturvalisuseeskirju;

26. kokkuvõtteks KINNITAB TAAS oma pühendumust kübervastupidavusvõime suurendamisele ja ELi küberturvalisuse kriisiohjeraamistiku väljaarendamisele ning JÄLGIB KORRAPÄRASELT edusamme ja annab täiendavaid suuniseid ELi küberturvalisuse kriisiohjeraamistiku täiendamiseks.