Euroopa Liidu
Nõukogu

Brüssel, 6. juuni 2025
(OR. en)

9794/25

Institutsioonidevaheline dokument: 2025/0036(NLE)

CYBER 157
IPCR 42
RELEX 706
JAI 738
JAIEX 54
POLMIL 138
HYBRID 63
TELECOM 178
COSI 108

MENETLUSE TULEMUS

Saatja:	Nõukogu peasekretariaat
Kuupäev:	6. juuni 2025
Saaja:	Delegatsioonid
Teema:	Nõukogu soovitus ELi küberkriiside ohjamise tegevuskava kohta – Nõukogus 6. juuni 2025. aasta istungil heaks kiidetud nõukogu soovitus

Delegatsioonidele edastatakse lisas nõukogu soovitus, mille nõukogu kiitis heaks 6. juuni 2025. aasta istungil.

LISA

NÕUKOGU SOOVITUS

ELi küberkriiside ohjamise tegevuskava kohta

EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artikleid 114 ja 292,

võttes arvesse Euroopa Komisjoni ettepanekut

ning arvestades järgmist:

(1) Digitehnoloogia ja üleilmne ühendatus on liidu majanduskasvu, konkurentsivõime ja elutähtsa taristu ümberkujundamise alus. Ent ühendatud ja üha digitaalsema majandusega käib käsikäes üha suurem küberturbeintsidentide ja küberrünnete risk. Peale selle kasvab geopoliitiliste pingete, konfliktide ja strateegilise rivaliteedi suurenemisele vastavalt ka pahatahtliku kübertegevuse mõju, maht ja keerukus. Selline tegevus võib olla hübriidkampaaniate või sõjaliste operatsioonide osa. Samuti võib see otseselt mõjutada liidu julgeolekut, majandust ja ühiskonda. Pealegi võib sellise tegevuse mõju olla tuntav ka väljaspool liitu, eriti juhul kui selle sihtmärgiks on rahvusvahelised strateegilised partnerriigid, näiteks kandidaat- või naaberriigid.

(2) Ulatuslikust küberturbeintsidendist tingitud häired võivad olla nii laialdased, et üks liikmesriik ei suuda nendega toime tulla või et need mõjutavad märkimisväärselt rohkem kui üht liikmesriiki. Selline intsident võib põhjusest ja mõjust tulenevalt eskaleeruda ning muutuda täieulatuslikuks kriisiks, mis takistab siseturu nõuetekohast toimimist või kujutab endast tõsist riski avalikule julgeolekule või turvalisusele mitme liikmesriigi või kogu liidu üksuste või kodanike jaoks. Tõhus kriisiohje on hädavajalik, et säilitada majandusstabiilsus ning kaitsta Euroopa valitsusi, elutähtsat taristut, ettevõtteid ja kodanikke, aga samuti selleks, et aidata kaasa rahvusvahelisele julgeolekule ja stabiilsusele küberruumis. Seega on küberkriiside ohjamine ELi üldise kriisiohjeraamistiku lahutamatu osa.

(3) Võttes arvesse liidu üksuste ja liikmesriikide IKT-keskkondade vastastikust sõltuvust ja omavahelist ühendatust, võib intsident liidu üksuses kujutada endast küberturberiski liikmesriikide jaoks ja vastupidi. Asjakohase teabe jagamine ja koordineerimine nii ulatuslike küberturbeintsidentide kui ka määruse (EL, Euratom) 2023/2841[1] artikli 3 punktis 8 määratletud tõsiste intsidentide korral on ELi küberkriiside ohjamise tegevuskava (edaspidi „kübervaldkonna tegevuskava“) kontekstis väga oluline.

[1] Euroopa Parlamendi ja nõukogu 13. detsembri 2023. aasta määrus (EL, Euratom) 2023/2841, millega nähakse ette meetmed küberturvalisuse ühtlaselt kõrge taseme tagamiseks liidu institutsioonides, organites ja asutustes (ELT L, 2023/2841, 18.12.2023, lk 1–27).

(4) Kriisi korral, mille jaoks on aktiveeritud nõukogu rakendusotsuse (EL) 2018/1993[2] kohane ELi integreeritud kord poliitiliseks reageerimiseks kriisidele (IPCR) (edaspidi „IPCRi kord“), peaks kübervaldkonna tegevuskava täielikult järgima koordineerimist ja reageerimist puudutavat IPCRi korda. Poliitiline ja strateegiline koordineerimine toimuks IPCRi raames. IPCRi kord on vahend horisontaalseks koordineerimiseks ja reageerimiseks liidu poliitilisel tasandil. IPCRi korra kohaselt võtab IPCRi aktiveerimise või deaktiveerimise otsuse vastu Euroopa Liidu Nõukogu eesistujariik. Komisjoni talituste ja Euroopa välisteenistuse koostatud integreeritud olukorrateadlikkuse ja analüüsi (ISAA) aruanded toetavad IPCRi tööd nii selle teabevahetuse režiimis kui ka täieliku aktiveerimise režiimis.

(5) Küberturbeintsidentide ja küberkriiside ohjamisel lasub esmane vastutus liikmesriikidel. Ent küberturbeintsidentide võimaliku piiri- ja sektoriülese olemuse tõttu on vajalik liikmesriikide ja asjaomaste liidu üksuste tehnilise, operatiivse ja poliitilise tasandi koostöö, et tegevust kõikjal liidus tulemuslikult koordineerida. Kõiki etappe hõlmav küberkriiside ohjamine tähendab valmisolekut ja ühist olukorrateadlikkust, et ulatuslikke küberturbeintsidente ennetada, avastamissuutlikkust, et teha kindlaks reageerimis- ja taastamisvahendid, mida on vaja ulatuslike küberturbeintsidentide leevendamiseks ja ohjeldamiseks, samuti reageerimisvõimet uute intsidentide ärahoidmiseks ja ennetamiseks.

[2] Nõukogu 11. detsembri 2018. aasta rakendusotsus (EL) 2018/1993, mis käsitleb ELi integreeritud korda poliitiliseks reageerimiseks kriisidele (ELT L 320, 17.12.2018, lk 28–34).

(6) Komisjoni soovituses (EL) 2017/1584[3] koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral loetletakse liikmesriikide ja liidu vahelise koostöö eesmärgid ja viisid ulatuslikele küberturbeintsidentidele ja küberkriisidele reageerimise korral. Selles kaardistati asjaomased tehnilise, operatiivse ja poliitilise tasandi osalised ja selgitati, mil viisil nad on integreeritud olemasolevatesse liidu kriisiohjemehhanismidesse, näiteks IPCRi korda. Jätkuvalt kehtivad soovituses (EL) 2017/1584 esitatud juhtpõhimõtted, nimelt subsidiaarsus, täiendavus ja teabe konfidentsiaalsus, samuti kolme tasandit (tehniline, operatiivne ja poliitiline) hõlmav lähenemisviis. Käesolev soovitus tugineb nendele juhtpõhimõtetele ja selle eesmärk on asendada soovitus (EL) 2017/1584, esitades uue raamistiku liidu küberturbekriiside ohjamiseks.

(7) Mõned käesolevas soovituses kasutatud mõisted põhinevad direktiivis (EL) 2022/2555[4] kasutatud mõistetel. Käesoleva soovituse kohaldamisala erineb siiski direktiivi (EL) 2022/2555 kohaldamisalast. Käesolevas soovituses esitatakse liidu küberkriiside ohjamise raamistik seoses ELi üldise valmisolekuga ulatuslikeks küberturbeintsidentideks ja sellistest intsidentidest tulenevateks küberkriisideks, olenemata sellest, millist sektorit või üksust see mõjutab. Mõisted põhinevad direktiivis (EL) 2022/2555 sisalduvatel mõistetel niivõrd, kuivõrd see on võimalik.

---

[3] 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 36–58).

[4] 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 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80–152).

(8) Ajakohastatud kübervaldkonna tegevuskava on vajalik, et esitada selged ja arusaadavad juhised, milles selgitatakse, mida ulatuslik küberturbeintsident või liidu tasandi küberkriis enesest kujutab, mis tingib kriisiohjeraamistiku aktiveerimise, millised on asjaomaste liidu tasandi osaliste ja mehhanismide rollid ning kuidas need osalised ja mehhanismid kogu küberkriisitsükli ulatuses koos toimivad. Kübervaldkonna tegevuskava eesmärk on toetada ELi tsiviil-sõjaliste suhete laiemat raamistikku küberkriiside ohjamise kontekstis, sealhulgas ELi ja NATO suhete süvendamise taustal, sealhulgas võimaluse korral küberkriiside ohjamisel rakendatavate kaasavate, vastastikuste ja mittediskrimineerivate tõhustatud teabevahetusmehhanismide kaudu.

(9) Tugevdada tuleks sektoriülest kriisiohjet liidu tasandil, et võimaldada integreeritud reageerimist kriisidele, eriti juhul, kui ulatuslikel küberturbeintsidentidel ja kriisidel on füüsilised tagajärjed. Käesolev soovitus täiendab IPCRi korda ja muid liidu kriisiohjemehhanisme, sealhulgas komisjoni üldine kiirhoiatussüsteem ARGUS, liidu elanikkonnakaitse mehhanism, mida toetab liidu elanikkonnakaitse mehhanismi raames elanikkonnakaitse mehhanismi käsitleva Euroopa Parlamendi ja nõukogu otsusega nr 1313/2013/EL (edaspidi „elanikkonnakaitse mehhanismi otsus“)[5] loodud hädaolukordadele reageerimise koordineerimiskeskus, Euroopa välisteenistuse kriisidele reageerimise mehhanism ning muud protsessid, nagu need, mida on kirjeldatud ELi küberdiplomaatia meetmete kogumis,[6] hübriidmeetmete kogumis[7] ja hübriidohtudega võitlemist käsitleva ELi protokolli läbivaadatud versioonis[8]. Samuti täiendab see nõukogu soovitust (EL) 2024/4371, mis käsitleb tegevuskava, mille alusel koordineerida liidu tasandi reageerimist märkimisväärse piiriülese tähtsusega elutähtsa taristu häiretele (edaspidi „ELi elutähtsa taristu tegevuskava“),[9] mis hõlmab kübermõõtmega mitteseotud füüsilist vastupanuvõimet ning on suunatud liidu tasandi reageerimise paremale koordineerimisele selles valdkonnas, ning peaks olema selle soovitusega kooskõlas.

---

5 Euroopa Parlamendi ja nõukogu 17. detsembri 2013. aasta otsus nr 1313/2013/EL liidu elanikkonnakaitse mehhanismi kohta (ELT L 347, 20.12.2013, lk 924–947).

6 Nõukogu järeldused pahatahtlikule kübertegevusele ELi ühise diplomaatilise reageerimise raamistiku kohta (9916/17).

7 Nõukogu järeldused, mis käsitlevad raamistikku ELi koordineeritud reageerimiseks hübriidkampaaniatele (22. juuni 2022).

8 Talituste ühine töödokument „Hübriidohtudega võitlemist käsitlev ELi protokoll“ (SWD(2023) 116 final).

9 ELT C, C/2024/4371, 5.7.2024.

(10) Euroopa küberkriisiga tegelevate kontaktasutuste võrgustik (EU-CyCLONe) on võrgustik, mille eesmärk on koordineerida ulatuslike küberturbeintsidentide ja -kriiside ohjamist operatiivtasandil ka sektoriüleste ulatuslike küberturbeintsidentide ja küberkriiside korral. Selleks et mitte muuta olemasolevaid raamistikke veelgi keerulisemaks, tuleks vältida selliste sektoripõhiste struktuuride loomist, mis dubleeriksid EU-CyCLONe ülesandeid. EU-CyCLONe peaks saama operatiivset küberturvalisusega seotud teavet ka sektoritelt ja toetama poliitilist tasandit.

(11) Liikmesriike innustatakse kasutama täies ulatuses ära liidu vastavatest programmidest kättesaadavaid küberturvalisuseks ette nähtud rahalisi vahendeid. Tuleks tagada, et nende programmidega kaasneks rahaliste vahendite taotlejate jaoks minimaalne halduskoormus ning et hõlbustataks liikmesriikide osalemist nendes programmides, andes asjakohaseid suuniseid sobivate rahalise toetuse võimaluste kohta.

(12) Käesolev soovitus aitab kaasa ulatuslikumatele valmisolekumeetmetele, mida liit vajab sektoriüleste kriiside korral kooskõlas ELi kriisivalmiduse strateegias sisalduvate põhimõtetega, nimelt kõiki ohte, kogu valitsemissektorit ja kogu ühiskonda hõlmava integreeritud lähenemisviisiga, eelkõige seoses teadlikkuse suurendamisega riskidest ja ohtudest ning sektoriülese kriisidele reageerimisega,

ON VASTU VÕTNUD KÄESOLEVA SOOVITUSE:

I. ELi küberkriiside ohjamise raamistiku eesmärk, kohaldamisala ja juhtpõhimõtted

Eesmärk ja kohaldamisala

1) Käesolevas soovituses ELi küberkriiside ohjamise tegevuskava kohta (edaspidi „kübervaldkonna tegevuskava“) esitatakse liidu küberkriiside ohjamise raamistik seoses ELi üldise valmisolekuga ulatuslikeks küberturbeintsidentideks ja küberkriisideks. Raamistik kajastab nii liikmesriikide kui ka liidu institutsioonide, organite ja asutuste (edaspidi „liidu üksused“) rolli nende vastava pädevuse piires, austades täielikult riigisisest õigust ja kodukordi, et tagada terviklik ja koordineeritud tegevus liidu tasandil.

2) Kübervaldkonna tegevuskava tuleks rakendada kooskõlas ELi elutähtsa taristu tegevuskavaga, eelkõige selliste intsidentide korral, mis mõjutavad nii elutähtsa taristu füüsilist vastupanuvõimet kui ka selle küberturvalisust[10].

3) Kübervaldkonna tegevuskavas antakse suuniseid ulatuslikele küberturbeintsidentidele või küberkriisidele reageerimiseks ning seda tuleks kasutada lisaks mis tahes asjakohastele valdkondlikele reageerimismehhanismidele, näiteks II lisas loetletud mehhanismidele. Asjaomased küberturvalisuse sidusrühmad peaksid aitama saavutada nende valdkondlike mehhanismide eesmärke nii riiklikul kui ka liidu tasandil.

4) Kogu ELi hõlmava küberaspektidega sektoriülese kriisi korral, mille jaoks IPCR aktiveeritakse, peaks reageerimist liidu poliitilisel tasandil koordineerima nõukogu, kasutades IPCRi korda. Kui IPCR on aktiveeritud, peaks kübervaldkonna tegevuskava kohaste meetmetega toetama ELi reageerimist poliitilisel tasandil, pakkudes konkreetset tuge küberturvalisuse valdkonnas.

[10] Üksikasjalikumalt on koordineerimist sellistel juhtudel kirjeldatud ELi elutähtsa taristu tegevuskava lisa I osa 4. jaos.

Juhtpõhimõtted

5) Liidu tasandil kohaldatakse küberkriiside ohjamise suhtes järgmisi juhtpõhimõtteid:

a) *proportsionaalsus:*enamik liikmesriike mõjutavatest küberturbeintsidentidest ei ole oma olemuselt sellised, et neid saaks käsitada riikliku või liidu tasandi ulatusliku küberturbeintsidendi või küberkriisina. Küberturbeintsidentide ja -ohtude korral teevad liikmesriigid koostööd ja vahetavad teavet vabatahtlikult ja korrapäraselt küberintsidentidele reageerimise üksuste võrgustikus (edaspidi „CSIRTide võrgustik“) ja EU-CyCLONe-s kooskõlas nende võrgustike standardse töökorraga;

b) *subsidiaarsus:* esmane vastutus liikmesriike mõjutatavatele küberturbeintsidentidele, ulatuslikele küberturbeintsidentidele või küberkriisidele reageerimise ja nende lahendamise eest lasub liikmesriikidel. Võimalikku piiriülest mõju arvesse võttes peaksid nõukogu, komisjon, kõrge esindaja, Euroopa Liidu Küberturvalisuse Amet (ENISA), liidu institutsioonide, organite ja asutuste küberturvalisuse teenistus (CERT-EU), Europol ja kõik muud asjaomased liidu üksused tegema koostööd kogu kriisitsükli jooksul. See roll tuleneb liidu õigusest ja kajastab seda, kuidas ulatuslikud küberturbeintsidendid ja küberkriisid mõjutavad ühtse turu üht või mitut majandustegevuse sektorit, liidu julgeolekut ja rahvusvahelisi suhteid ning institutsioone endid;

c) *täiendavus:* käesolevas soovituses võetakse täielikult arvesse olemasolevaid liidu tasandi kriisiohjemehhanisme, mis on loetletud II lisas, eelkõige IPCRi korda, ARGUSt ja Euroopa välisteenistuse kriisidele reageerimise mehhanismi. Käesolevas soovituses võetakse arvesse CSIRTide võrgustiku ja EU-CyCLONe volitusi, samuti määrust (EL, Euratom) 2023/2841. Kui IPCR aktiveeritakse, peaks asjaomaste võrgustike, üksuste ja aktiveeritud valdkondlike mehhanismide töö jätkuma ning andma panuse IPCRis toimuvasse poliitilisse ja strateegilisse koordineerimisse ja seda toetama;

d) *teabe konfidentsiaalsus:* kogu käesoleva soovituse raames toimuv teabevahetus peaks olema kooskõlas kohaldatavate julgeolekunormidega ja isikuandmete kaitse normidega. Asjakohasel juhul tuleks arvesse võtta mitteametlikke mitteavaldamise kokkuleppeid, näiteks fooritulede analoogial põhinevat protokolli teabe tundlikkuse märgistamiseks. Salastatud teabe vahetamiseks, olenemata kasutatavast salastusmärkest, tuleks lisaks olemasolevatele akrediteeritud vahenditele kohaldada olemasolevaid salastatud teabe töötlemist käsitlevaid siduvaid norme ja kokkuleppeid.

6) Kooskõlas eelnimetatud juhtpõhimõtetega peaksid liikmesriigid ja liidu üksused süvendama omavahelist küberkriiside ohjamise alast koostööd, suurendades vastastikust usaldust ning kasutades ära olemasolevaid võrgustikke ja mehhanisme. Sellele kübervaldkonna tegevuskava raamistikus tehtavale koostööle aitab kaasa määruse (EL, Euratom) 2023/2841 artiklite 22 ja 23 rakendamine. Eelkõige aitab määruse (EL, Euratom) 2023/2841 artikli 23 alusel koostatud küberkriiside ohjamise kava muu hulgas kaasa asjakohase teabe korrapärasele vahetamisele liidu üksuste vahel ja liikmesriikidega ning selles määratakse kindlaks liidu üksuste vahelise koordineerimise ja teabevoo kord.

II. Mõisted

7) Käesolevas kübervaldkonna tegevuskavas kasutatakse järgmisi mõisteid:

a) „intsident“ – sündmus, mis kahjustab salvestatavate, edastatavate või töödeldavate andmete või võrgu- ja infosüsteemi kaudu pakutavate või juurdepääsetavate teenuste kättesaadavust, autentsust, terviklust või konfidentsiaalsust;

b) „oluline intsident“ – intsident, mis on:

a. põhjustanud või võib põhjustada asjaomase üksuse teenuste osutamisel tõsiseid tegevushäireid või rahalist kahju;

b. mõjutanud või võib mõjutada teisi füüsilisi või juriidilisi isikuid, põhjustades märkimisväärset materiaalset või mittemateriaalset kahju;

c) „ulatuslik küberturbeintsident“ – intsident, mille põhjustatud häired on niivõrd laialdased, et üks liikmesriik ei suuda nendega toime tulla või millel on märkimisväärne mõju vähemalt kahele liikmesriigile;

d) „küberkriis“ – ulatuslik küberturbeintsident, mis eskaleerus täieulatuslikuks kriisiks, mis takistab siseturu nõuetekohast toimimist või kujutab endast mitme liikmesriigi või kogu liidu üksustele või kodanikele tõsist avaliku julgeoleku- või turvalisusriski.

III. Riiklikud küberkriiside ohjamise struktuurid ja kohustused

8) Esmane vastutus liikmesriike mõjutavatele ulatuslikele küberturbeintsidentidele või küberkriisidele reageerimise eest lasub liikmesriikidel. Igal liikmesriigil on kooskõlas direktiiviga (EL) 2022/2555 üks või mitu küberkriiside ohjamise asutust ning üks või mitu CSIRTi.

9) Direktiivi (EL) 2022/2555 ning muude küberturvalisust käsitlevate õigusaktide ja muude kui seadusandlike vahendite vastuvõtmisega on liikmesriigid oma küberturberaamistikke omavahel vastavusse viinud, kehtestades miinimumnormid koordineeritud õigusraamistiku toimimise kohta, kehtestades igas liikmesriigis mehhanismid vastutavate asutuste vaheliseks tõhusaks koostööks ning nähes ette tõhusad õiguskaitsevahendid ja täitemeetmed, mis on kõnealuste kohustuste tulemusliku täitmise tagamiseks keskse tähtsusega.

10) Direktiivi (EL) 2022/2555 artikli 9 lõike 4 kohaselt peaksid liikmesriigid vastu võtma riiklikud ulatuslike küberturbeintsidentide ja kriiside lahendamise kavad. Need kavad hõlmavad muu hulgas riiklikke valmisolekumeetmeid, küberkriisi ohjamise menetlusi ning liikmesriigi menetlusi ja korda riiklike asutuste ja organite vahel, et tagada nende tulemuslik osalemine ulatuslike küberturbeintsidentide ja küberkriiside koordineeritud ohjamisel liidu tasandil ning selle ohjamise toetamine. Küberkriiside ohjamise menetlused hõlmavad ka sätteid, mis käsitlevad selliste menetluste lõimimist üldisesse riiklikku kriisiohjeraamistikku ja teabevahetuskanalitesse.

11) Direktiivi (EL) 2022/2555 artikli 9 lõike 1 kohaselt peaksid liikmesriigid tagama sidususe oma olemasolevate üldiste kriisiohjeraamistikega. IPCRi aktiveerimise korral peaksid riiklikud kriisiohjeasutused koguma IPCRi teavitamiseks teavet küberkriisi ohjamise asutustelt ja riiklikelt valdkondlikelt kriisimehhanismidelt.

12) Kooskõlas direktiivi (EL) 2022/2555 artikli 9 lõikega 5 peaks EU-CyCLONe asjaomase liikmesriigi taotlusel vahetama teavet riiklike ulatuslike küberturbeintsidentide ja kriiside lahendamise kavade asjakohaste osade ja eelkõige nende sätete kohta, millega tagatakse tulemuslik osalemine ulatuslike küberturbeintsidentide ja küberkriiside koordineeritud ohjamises liidu tasandil ja selle toetamine, selleks et vahetada parimaid tavasid ja kaaluda, kas üldine raamistik praktikas toimiks.

13) EU-CyCLONe-l ja institutsioonidevahelisel küberturvalisuse nõukojal palutakse asjakohasel juhul vahetada teavet selle kohta, kas selle nõukoja poolt määruse (EL, Euratom) 2023/2841 artikli 23 kohaselt koostatud kriiside haldamise kava on kooskõlas riiklike ulatuslike küberturbeintsidentide ja kriiside lahendamise kavadega.

14) EU-CyCLONe peaks ENISA kui oma sekretariaadi toetusel haldama ajakohastatud loetelu riiklikest küberkriisi ohjamise asutustest koos EU-CyCLONe ametnike ja juhtide kontaktandmetega ning tegema selle kättesaadavaks EU-CyCLONe liikmetele.

IV. ELi küberkriiside ohjamise ökosüsteemi peamised võrgustikud ja osalejad

15) CSIRTide võrgustik on peamine tehniline võrgustik, mis vahetab asjakohast teavet intsidentide kohta, eelkõige käesoleva soovituse kohaldamisalas, kooskõlas direktiivi (EL) 2022/2555 artikli 15 lõikes 3 kirjeldatud asjakohaste ülesannetega. See aitab suurendada usaldust ja kindlustunnet ning edendab kiiret ja tõhusat operatiivkoostööd liikmesriikide vahel. CSIRTide võrgustiku eesistuja võib osaleda institutsioonidevahelises küberturvalisuse nõukojas vaatlejana.

16) CERT-EU on küberturvalisuse teenistus kõigi liidu üksuste jaoks. CERT-EU tegutseb liidu üksuste küberturvalisuse alase teabevahetuse ja intsidentidele reageerimise koordineerimise keskusena kooskõlas määruse (EL) 2023/2841 artikliga 13. CERT-EU on CSIRTide võrgustiku liige ja toetab komisjoni EU-CyCLONe-s. CERT-EU tegutseb tehnilisel tasandil ja vastutab liidu üksusi mõjutavate tõsiste intsidentide haldamise koordineerimise eest.

17) EU-CyCLONe tegutseb tehnilise ja poliitilise tasandi vahel vahendajana, eelkõige ulatuslike küberturbeintsidentide ja küberkriiside ajal. EU-CyCLONe toetab ulatuslike küberturbeintsidentide ja küberkriiside koordineeritud ohjamist operatiivtasandil ning tagab asjakohase teabe korrapärase vahetamise liikmesriikide ning liidu institutsioonide, organite ja asutuste vahel kooskõlas direktiivi (EL) 2022/2555 artikliga 16. EU-CyCLONe eesistuja võib osaleda institutsioonidevahelises küberturvalisuse nõukojas vaatlejana.

18) ENISA on liidu amet, mis täidab määrusega (EL) 2019/881[11] määratud ülesandeid, et saavutada küberturvalisuse kõrge ühine tase kogu liidus, muu hulgas toetades aktiivselt liikmesriike ning liidu institutsioone, organeid ja asutusi. ENISA tagab muu hulgas CSIRTide võrgustiku ja EU-CyCLONe sekretariaaditeenused, olukorrateadlikkuse teenused ning abistab liikmesriike, korraldades korrapäraselt küberturvalisuse õppusi liidu tasandil. Kooskõlas direktiiviga (EL) 2022/2555 ja määrusega (EL) 2024/2847[12] saab ENISA teavet oluliste piiriüleste intsidentide ning digitooteid mõjutavate aktiivselt ärakasutatavate nõrkuste ja intsidentide kohta.

19) Euroopa Liidu Nõukogu (edaspidi „nõukogu“) on institutsioon, kellel on Euroopa Liidu lepingu (edaspidi „ELi leping“) artikli 16 kohaselt poliitika kujundamise ja koordineerimise funktsioonid ning kellele on usaldatud IPCRi kohaldamine, mis puudutab koordineerimist ja reageerimist liidu poliitilisel tasandil. Nõukogu tegutseb nõukogu koosseisude, alaliste esindajate komitee ja asjaomaste nõukogu ettevalmistavate organite, eelkõige horisontaalse küberküsimuste töörühma ning asjakohasel juhul IPCRi korra kaudu.

---

[11] 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 15–69).

[12] Euroopa Parlamendi ja nõukogu 23. oktoobri 2024. aasta määrus (EL) 2024/2847, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrusi (EL) nr 168/2013 ja (EL) 2019/1020 ning direktiivi (EL) 2020/1828 (küberkerksuse määrus) (ELT L, 2024/2847, 20.11.2024, lk 1–81).

20) Komisjon kui liidu üldisi huve edendav institutsioon, kes teeb sel eesmärgil asjakohaseid algatusi ning tagab aluslepingute ja institutsioonide poolt ELi lepingu artikli 17 alusel vastu võetud meetmete kohaldamise, vastutab teatavate liidu tasandi üldiste valmisolekumeetmete ja teatavate olukorrateadlikkuse meetmete eest, sealhulgas hädaolukordadele reageerimise koordineerimiskeskuse ning ühise hädaolukordade side- ja infosüsteemi haldamise eest kooskõlas liidu elanikkonnakaitse mehhanismi otsusega. Ta aitab kaasa asjaomaste liidu tasandi kriisile reageerimise meetmete sidususele ja koordineerimisele operatiivtasandil. Komisjoniga peetakse nõu, kui ta otsustab IPCRi aktiveerimise või deaktiveerimise üle. Komisjoni talitused koos Euroopa välisteenistusega koostavad ISAA aruandeid. Komisjon on EU-CyCLONe liige sellise võimaliku või käimasoleva ulatusliku küberturbeintsidendi korral, millel on või võib olla märkimisväärne mõju direktiivi (EL) 2022/2555 kohaldamisalasse kuuluvatele teenustele ja tegevustele, ning osaleb EU-CyCLONe-s vaatlejana muudel juhtudel. Ta on EU-CyCLONe jaoks kontaktpunkt institutsioonidevahelises küberturvalisuse nõukojas. Komisjon on vaatleja CSIRTide võrgustikus.

21) Liidu välisasjade ja julgeolekupoliitika kõrge esindaja (edaspidi „kõrge esindaja“), keda abistab Euroopa välisteenistus, viib ellu liidu ühist välis- ja julgeolekupoliitikat (ÜVJP) ning aitab oma ettepanekutega kaasa selle poliitika, sealhulgas ühise julgeoleku- ja kaitsepoliitika (ÜJKP) arendamisele. See hõlmab diplomaatilisi, luure- ja sõjalisi struktuure ja mehhanisme, eelkõige ühtset luureandmete analüüsivõimet (SIAC), mis on ühtne liikmesriikide luureandmete sisestamise koht, ELi sõjalist staapi (ELSS), mis on sõjaliste eksperditeadmiste allikas, ELi küberdiplomaatia meetmete kogumit ning ELi delegatsioonide võrgustikku, mis võivad välismõõtme aspektist kriisiohjele kaasa aidata. Euroopa välisteenistus koostab samuti koos komisjoniga ISAA aruandeid.

22) II lisas kirjeldatakse asjaomaste liidu tasandi osalejate rolle ja pädevusi seoses küberkriiside ohjamisega, sealhulgas peamisi võrgustikke ja osalisi.

V. Ulatuslikeks küberturbeintsidentideks ja küberkriisiks valmistumine

Ohumaastik

23) Tunnistades, et ohumaastik ja intsidendipõhine olukorrateadlikkus nõuavad erinevaid toimimisviise, peaksid liikmesriigid ja asjaomased liidu üksused võtma olukorrateadlikkuse suurendamiseks vajalikke meetmeid. Liikmesriikidel ja asjaomastel liidu üksustel tuleks teha koostööd, mis põhineb kontrollitud ja usaldusväärsetel andmetel, sealhulgas intsidentide, taktika, meetodite ja menetluste suundumustel ning aktiivselt ärakasutatavatel nõrkustel.

24) Liikmesriigid peaksid ELi tasandil teavet jagades kõigiti ära kasutama olemasolevaid tehnilise ja operatiivkoostöö platvorme, näiteks neid, mida kasutavad CSIRTide võrgustik ja EU-CyCLONe.

25) Ühise olukorrateadlikkuse suurendamiseks ja ELi mõju hindamise hõlbustamiseks peaksid EU-CyCLONe ja CSIRTide võrgustik ENISA toetusel kasutama asutustesiseselt kokku lepitud aruandlusmehhanismi, et koostada riikide tasandil kogutud teabe põhjal ELi ülevaade tehnilisest ja operatiivtegevusest.

26) EU-CyCLONe ja CSIRTide võrgustik peaksid:

a) tegema koostööd tehnilise ja operatiivtasandi vahelise teabevahetuse ja kogu olukorrateadlikkuse parandamiseks;

b) jätkama usaldusliku õhkkonna loomist oma liikmete ja võrgustike vahel;

c) kasutama ENISA toetusel täielikult ära olemasolevaid teabejagamisvahendeid, arutama nende vahendite parandamise võimalusi ja tagama võrkude koostalitlusvõime.

27) EU-CyCLONe, CSIRTide võrgustik ja IICB peaksid tegema koostööd, et tagada asjakohase teabe tõhus vahetamine.

28) ENISA-l kui CSIRTide võrgustiku ja EU-CyCLONe sekretariaadil on keskne roll liikmesriikide ning liidu institutsioonide, organite ja asutuste toetamisel eesmärgiga saavutada ELi ühine olukorrateadlikkus tehnilisel ja operatiivtasandil, selleks et toetada ulatuslikeks küberturbeintsidentideks ja kriisideks valmistumist.

29) Kooskõlas direktiiviga (EL) 2022/2555 ja määrusega (EL) 2019/881 peaksid liikmesriigid ja asjaomased liidu üksused koordineerima oma tegevust erasektoriga, sealhulgas avatud lähtekoodiga tarkvara kogukondade ja tootjatega, et parandada teabevahetust. Eelkõige ENISA peaks sellega seoses kasutama oma partnerlusprogrammi. Lisaks võiksid liikmesriigid ja asjaomased liidu üksused tugineda olemasolevatele ELi ja riikliku tasandi teabe jagamise ja analüüsimise keskustele (ISACid), et suurendada kübervõimsust ja reageerida küberturbeintsidentidele, sealhulgas erasektori ja EU-CyCLONe või erasektori ja CSIRTide võrgustiku ühiste kohtumiste kaudu.

30) Selleks et tõhustada teabe jagamist võrgustikes ja nende vahel ning selgitada vastastikuseid ootusi sellise jagamise suhtes, peaks EU-CyCLONe ENISA kui sekretariaadi toetusel ning pärast CSIRTide võrgustiku ja võrgu- ja infoturbe koostöörühmaga konsulteerimist leppima 24 kuu jooksul alates käesoleva soovituse vastuvõtmisest kokku intsidentide raskusastmete ühtses ühtlustatud taksonoomias. See taksonoomia peaks võimaldama intsidentide raskusastme võrdlemist liikmesriikide vahel, võttes arvesse nende mõju teenuste osutamisele, mõjutatud üksuste arvu ja nende vastavat asjakohasust, mõju muudele teenustele ja taristule ning tekitatud rahalist ja mainekahju ning poliitilist kahju. See peaks tuginema asjakohastele olemasolevatele skaaladele või taksonoomiatele, nagu võrdlusintsidentide klassifitseerimise taksonoomia.

Tehniline tasand

31) CSIRTide võrgustik on kõigi liikmesriikide vahelise ning CERT-EU kaudu liidu üksustega tehtava tehnilise koostöö ja teabe vahetamise platvorm.

32) Vastavalt direktiivile (EL) 2022/2555 on iga CSIRTi ülesanne jälgida ja analüüsida küberohte, nõrkusi ja intsidente riiklikul tasandil. CSIRTid peaksid nii CSIRTide võrgustikus kui ka kahepoolselt vahetama intsidentide, ohuolukordade, küberohtude, riskide ja nõrkuste kohta asjakohast teavet, et saavutada ühine olukorrateadlikkus.

33) Et tõhustada operatiivkoostööd liidu tasandil, peaks CSIRTide võrgustik kaaluma võimalust kutsuda oma töös osalema küberturvalisuse poliitika kujundamisega seotud asjaomased liidu asutused ja ametid, näiteks Europoli.

34) Kooskõlas määrusega (EL) 2023/2841 peaks CERT-EU koguma, haldama, analüüsima ja jagama liidu institutsioonide, organite ja asutustega teavet küberohtude, nõrkuste ja intsidentide kohta salastamata IKT-taristus ning esitama vajaduse korral IICB-le konkreetsed ettepanekud suuniste ja soovituste kohta liidu institutsioonide, organite ja asutuste jaoks. CERT-EU peaks tegema koostööd ja vahetama teavet liikmesriikide vastavate asutustega, sealhulgas CSIRTide võrgustiku kaudu.

Operatiivtasand

35) Kooskõlas direktiiviga (EL) 2022/2555 peaks EU-CyCLONe toimima liikmesriikide küberkriisi ohjamise asutuste vahelise ja komisjoni kaudu asjaomaste liidu üksustega tehtava koostöö platvormina, mille eesmärk on suurendada valmisolekut ulatuslike küberturbeintsidentide ja küberkriiside ohjamiseks ning arendada ühist olukorrateadlikkust ulatuslike küberturbeintsidentide ja küberkriiside kohta.

36) Kooskõlas direktiiviga (EL) 2022/2555 ja määrusega (EL) 2024/2847 saab ENISA teavet oluliste piiriüleste intsidentide ning digitooteid mõjutavate aktiivselt ärakasutatavate nõrkuste ja intsidentide kohta. Sekretariaadina tegutsev ENISA peaks CSIRTide võrgustikku ja EU-CyCLONe-t nõustama, et toetada võrgustikke edasiste meetmete võtmise üle otsustamisel ja anda oma panus ühisesse olukorrateadlikkusse.

Poliitiline tasand

37) Liikmesriigid ja asjaomased liidu üksused peaksid jälgima küberturvalisust mõjutavaid rahvusvahelisi suundumusi (sealhulgas küberohte, hübriidohte ning välisriigist lähtuvaid infomanipulatsioone ja sekkumisi, sealhulgas desinformatsiooni, kui see on asjakohane). Arvesse tuleks võtta selliseid algatusi nagu küberturvalisuse tehnilise olukorra aruanded, SIACi esitatud analüüsid ja muud asjakohased tooted, mis annavad spetsiifilisi teadmisi.

38) Kõrge esindaja peaks liikmesriike jätkuvalt teavitama ja kaasama neid küberohtudega seotud liidu diplomaatilistesse meetmetesse, eelkõige nendesse, mis hõlmavad riiklikke osalejaid, oma koostöösse kolmandate riikide ja rahvusvaheliste organisatsioonidega, sealhulgas NATOga, ning diplomaatiliste meetmete, sealhulgas piiravate meetmete rakendamisse.

39) Euroopa Liidu Nõukogu eesistujariik võib algatada IPCRi veebiplatvormil järelevalvelehekülje, kus liikmesriigid ning ELi institutsioonid ja organid saavad vahetada teavet tõenäoliselt areneva kriisi kohta.

Ühisõppused

40) Komisjon peaks koostöös kõrge esindajaga, keda toetab ENISA, pärast EU-CyCLONe-ga ja CSIRTide võrgustikuga konsulteerimist koostama tõhusa iga-aastase küberõppuste jooksva programmi, et valmistuda küberkriisideks ja suurendada organisatsioonilist tõhusust. Küberõppuste jooksvas programmis tuleks arvesse võtta liidu elanikkonnakaitse mehhanismi õppusi ja muid liidu tasandi kriisidele reageerimise mehhanismide õppusi, sealhulgas ELi elutähtsa taristu tegevuskavas kirjeldatud õppust. Esimene jooksev programm tuleks välja töötada 12 kuu jooksul pärast kübervaldkonna tegevuskava vastuvõtmist ning järgnevad programmid tuleks lõpule viia iga aasta 31. märtsiks. Jooksev programm tuleks teavitamise eesmärgil esitada nõukogule.

41) Jooksev programm peaks hõlmama ka õppusi, mis on välja töötatud, kasutades ELi koordineeritud riskihindamise stsenaariume. See peaks hõlmama õppusi, millesse on kaasatud kõik asjaomased osalejad, eelkõige erasektor ja NATO.

42) ENISA peaks CSIRTide võrgustiku ja EU-CyCLONe sekretariaadina tagama õppustest saadud kogemuste süstemaatilise kogumise ning sellest tulenevate meetmete kindlakstegemise ja nende rakendamise viiside väljapakkumise, et tagada nende tulemuslik elluviimine ja positiivne mõju ELi ühisele kerksusele, sealhulgas vastavad püsitoimingud.

43) Kõik osalejad ja võrgustikud peaksid õppustest saadud õppetundide põhjal parandama koordineerimist ulatusliku küberturbeintsidendi või küberkriisi korral. Eelkõige peaksid EU-CyCLONe ja CSIRTide võrgustik tegelema õppuste käigus kindlaks tehtud kitsaskohtadega, et parandada koordineerimist, eelkõige sellistega, mis on seotud võrgustike koostööga, ning vajaduse korral kiiresti püsitoiminguid kohandama.

44) Võrgu- ja infoturbe koostöörühm peaks kutsuma CSIRTide võrgustikku, EU-CyCLONe-t ja ENISAt üles tutvustama õppustest saadud kogemusi ning sellest tulenevate meetmete kindlaksmääramist ja kavandatavat rakendamisviisi.

45) Nõukogu võib kutsuda CSIRTide võrgustiku, EU-CyCLONe ning võrgu- ja infoturbe koostöörühma eesistujad ja ENISA juhi tutvustama, kuidas õppustel saadud kogemusi rakendati.

46) ENISA-l palutakse koostöös komisjoni ja kõrge esindajaga korraldada õppus, et katsetada kübervaldkonna tegevuskava järgmise õppuse „Cyber Europe“ (Euroopa küberõppus) käigus. Õppusele tuleks kaasata kõik asjaomased osalejad, sealhulgas poliitiline tasand. ENISA-l palutakse kooskõlastada poliitilise tasandi kaasamine Euroopa Liidu Nõukogu eesistujariigiga. Õppusele võib kaasata ka erasektori ja NATO.

VI. Sellise intsidendi avastamine, mis võib kasvada ulatuslikuks küberturbeintsidendiks või küberkriisiks

47) Kõik osalejad peaksid vastavalt oma volitustele ja tuginedes kõiki ohte hõlmavale lähenemisviisile edastama võimalikust ulatuslikust küberturbeintsidendist või küberkriisist märku andva teabe asjaomastele võrgustikele.

48) Kui piiriülesed küberkeskused saavad võimaliku või käimasoleva ulatusliku küberturbeintsidendiga seotud teavet, peaksid nad vastavalt määrusele (EL) 2025/38[13] tagama ühise olukorrateadlikkuse eesmärgil, et asjakohane teave edastatakse põhjendamatu viivituseta liikmesriikide ametiasutustele ning komisjonile EU-CyCLONe ja CSIRTide võrgustiku kaudu.

[13] Euroopa Parlamendi ja nõukogu 19. detsembri 2024. aasta määrus (EL) 2025/38, millega nähakse ette meetmed, et tugevdada liidus solidaarsust ja suurendada suutlikkust küberohtude ja intsidentide avastamiseks, nendeks valmistumiseks ja neile reageerimiseks, ning millega muudetakse määrust (EL) 2021/694 (kübersolidaarsuse määrus) (ELT L, 2025/38, 15.1.2025; ELI: http://data.europa.eu/eli/reg/2025/38/oj).

49) Kui märgatakse olulist intsidenti, millel on eelkõige vahetu mõju, võidakse sellest teatada CSIRTile ning liikmesriikide küberkriiside ohjamise asutustele või muudele konkreetse valdkonna asutustele või nad võivad sellise intsidendi ise avastada. Liikmesriike julgustatakse jagama selliste intsidentidega seotud teavet võrgustikes, mis peaksid kaaluma asjakohaste meetmete võtmist. CSIRTide võrgustiku ja EU-CyCLONe aktiveerimine võivad olla üksteisest sõltumatud, sõltudes intsidendi laadist ja vajalikust reageerimisest. Siiski julgustatakse mõlemat võrgustikku jätkama omavahelist koostööd kokkulepitud menetluskorra alusel. Aktiveerimise otsus sõltub ainuüksi ja sõltumatult igast vastavast võrgustikust.

50) CSIRTide võrgustik peaks EU-CyCLONe-le teatama, kas täheldatud küberturbeintsidenti võib käsitada võimaliku või käimasoleva ulatusliku küberturbeintsidendina.

51) Nagu on osutatud direktiivis (EL) 2022/2555, peaksid CSIRTide võrgustik ja EU-CyCLONe võimaliku või käimaoleva ulatusliku küberturbeintsidendi puhuks leppima viivitamatult kokku menetluskorra, mille eesmärk on tagada tehnilis-operatiivne koordineerimine ning asjaomase teabe õigeaegne edastamine poliitilisele tasandile.

VII. Ulatuslikule küberturbeintsidendile või küberkriisile reageerimine liidu tasandil

Reageerimine ulatuslikule küberturbeintsidendile või küberkriisile, mille korral IPCR ei ole täielikult aktiveeritud

52) Tõhus reageerimine ulatuslikele küberturbeintsidentidele või küberkriisidele ELi tasandil sõltub tõhusast tehnilisest, operatiivsest ja poliitilisest koostööst kogu valitsemissektorit hõlmava lähenemisviisi kohaselt, sealhulgas võimaluse korral õiguskaitse valdkonnas.

53) Igal tasandil peaksid asjaomased osalejad võtma konkreetseid meetmeid, et saavutada ühine olukorrateadlikkus ja koordineeritud reageerimine. Selliste meetmetega tagatakse teabe korrapärane ja tõhus levitamine.

54) Reageerimine peaks olema asjakohane, võttes arvesse ulatusliku küberturbeintsidendi või küberkriisi mõju. Vastavalt direktiivile (EL) 2022/2555 peaksid liikmesriikide küberkriiside ohjamise asutused tagama eri valdkondades küberkriisile reageerimisel lahenduste sidususe ja koordineerimise oma riigis.

55) Ulatusliku küberturbeintsidendi või küberkriisi korral peaksid kõik osalejad ja võrgustikud reageerima tihedas koostöös, tehes järgmist.

a) Tehnilisel tasandil:

i. peaksid mõjutatud liikmesriigid ja nende CSIRTid tegema mõjutatud üksustega koostööd, et reageerida intsidentidele ja anda vajaduse korral abi;

ii. peaksid CSIRTid tegema CSIRTide võrgustiku kaudu koostööd, et jagada intsidendi kohta asjakohast tehnilist teavet; CSIRTid teevad koostööd oma püüdlustes analüüsida intsidendiga seotud kättesaadavaid tehnilisi artefakte ja muud tehnilist teavet, et teha kindlaks selle põhjus ja võimalikud tehnilised leevendusmeetmed;

iii. kutsutakse CSIRTi või liikmesriigi küberkriisi ohjamise asutust, juhul kui nad saavad teada olulisest intsidendist, üles jagama seda teavet CSIRTide võrgustikus või EU-CyCLONe-s.

iv. peaks CSIRTide võrgustik ENISA toetusel koostama CSIRTide poolt esitatud liikmesriikide aruannete kokkuvõtte, mis tuleks esitada EU-CyCLONe-le;

v. peaks CSIRTide võrgustik, juhul kui küberturbeintsident võib kasvada ulatuslikuks küberturbeintsidendiks või küberkriisiks, jagama EU-CyCLONe-ga asjakohast teavet. EU-CyCLONe peaks kasutama seda teavet nõukogu informeerimiseks;

vi. peaks CSIRTide võrgustik olema Europoliga tihedas kontaktis, et tagada asjakohase tehnilise teabe vahetamine. CSIRTide võrgustik ja Europol peaksid looma kontaktpunktid, et tõhustada teabe jagamist, kui see on ulatusliku küberturbeintsidendi korral asjakohane.

b) Operatiivtasandil:

i. peaksid liikmesriigid peaksid asjakohaste meetmete abil leevendama intsidendi mõju riigi tasandil;

ii. peaks CSIRTide võrgustik pakkuma EU-CyCLONe-le käimasolevaid intsidente käsitlevaid tehnilisi hinnanguid, mida EU-CyCLONe saab kasutada;

iii. peaks EU-CyCLONe hindama asjaomaste ulatuslike küberturbeintsidentide ja küberkriiside tagajärgi ja mõju ning pakkuma välja võimalikud leevendusmeetmed, toetama ulatuslike küberturbeintsidentide ja küberkriiside koordineeritud ohjamist ning otsuste tegemist poliitilisel tasandil;

iv. kui ulatusliku valdkonnaülese mõjuga küberturbeintsidendi korral on vaja aktiveerida liidu tasandi reageerimismeetmed, eelkõige II lisas loetletud asjakohased liidu tasandi horisontaalsed ja valdkondlikud kriisiohjemehhanismid, siis:

a) võivad asjaomased osalejad sõltuvalt liidu tasandi valdkondlike kriisiohjemehhanismide liigist nõuda kõnealuse mehhanismi aktiveerimist;

b) toetavad asjaomased üksused sellise valdkondliku mehhanismi aktiveerimise korral konkreetse valdkonna üksusi intsidendi mõju leevendamisel;

c) peaks komisjon hõlbustama vajaliku teabe liikumist II lisas loetletud asjaomaste horisontaalsete ja valdkondlike liidu tasandi kriisimehhanismide ja EU-CyCLONe kontaktpunktide vahel ning peaks jätkama integreeritud valdkonnaülest analüüsi ja pakkuma välja sobiva integreeritud kriisilahenduskava võimalusi;

d) peaks komisjon vajaduse korral EU-CyCLONe kaudu ja koostöös kõrge esindajaga tagama kübervaldkonnas võetavate ELi tasandi operatiivmeetmete sidususe ja koordineerimise seonduvate tasandi reageerimismeetmetega, eelkõige seoses liidu elanikkonnakaitse mehhanismi kaudu esitatud abitaotlustega;

e) tuleks, juhul kui intsidendi kohta on algatatud IPCRi seireleht, selle mõju ja võetud meetmete kohta liikmesriikide ja liidu üksuste vahel IPCRi veebiplatvormi kaudu ka teavet jagada;

v. liikmesriigid võivad taotleda ELi küberreservist teenuseid kooskõlas määruse (EL) 2025/38 artikliga 15. Ilma et see piiraks kõnealuse määruse kohaste tulevaste rakendusaktide kohaldamist, tuleks ELi küberreservi teenused kasutusele võtta 24 tunni jooksul alates taotluse esitamisest.

c) Poliitilisel tasandil:

i. võib nõukogu nõuda ülevaateid peamistelt sidusrühmadelt, eelkõige komisjonilt, kõrgelt esindajalt ja EU-CyCLONe-lt, et võtta asjakohaseid poliitilisi ja strateegilisi meetmeid;

ii. võiks nõukogu, keda toetavad komisjon ja kõrge esindaja, otsustada, millised on asjakohased ulatuslikule küberturbeintsidendile reageerimise meetmed, sealhulgas võimalikud diplomaatilised meetmed kooskõlas IX peatükiga;

iii. võivad liikmesriigid sõltuvalt intsidendi laadist ja mõjust aktiveerida täiendavaid küberkriisi ohjamise mehhanisme või vahendeid;

iv. kui IPCR aktiveeritakse teabevahetuse režiimis, käivitub ISAA tugivõime, mis suurendab teabevahetust IPCRi veebiplatvormi kaudu ja tagab ühise olukorraülevaate. EU-CyCLONe ja CSIRTide võrgustiku olukorraülevaated peaksid jääma peamisteks vahenditeks, mis kajastavad ühist olukorrateadlikkust vastavalt operatiivtasandil ja tehnilisel tasandil. Need aruanded võivad olla ISAA aruannete alus;

v. peaks nõukogu koostöös komisjoni ja kõrge esindajaga tagama küberturbekriisile reageerimise ja sellega seotud liidu tasandi kriisilahendusmeetmete sidususe ja koordineerimise sellise intsidendi korral, mis nõuab liidu tasandi kriisilahendusmeetmete, eelkõige II lisas loetletud asjakohaste liidu tasandi horisontaalsete ja valdkondlike kriisiohjemehhanismide aktiveerimist;

vi. peaksid komisjoni talitused ja asjakohasel juhul Euroopa välisteenistus, samuti asjaomased nõukogu organid, eelkõige horisontaalne küberjulgeoleku töörühm (HWPCI) ning vastupanuvõime suurendamise ja hübriidohtudega võitlemise horisontaalne töörühm (HWP-ERCHT), juhul kui taotletakse asjakohaste mehhanismide käivitamist, eelkõige küberreservi teenuseid, vajaduse korral koordineerima meetmete kavandamist ja rakendamist ning lisameetmete jaoks asjakohast otsustusprotsessi kooskõlas hübriidmeetmete kogumiga[14], juhul kui pahatahtlik kübertegevus on osa laiemast hübriidkampaaniast.

Reageerimine ulatuslikule küberturbeintsidendile või küberkriisile, mille korral IPCR on täielikult aktiveeritud

56) Rakendada tuleks eespool jaos „Reageerimine ulatuslikule küberturbeintsidendile või küberkriisile, mille korral IPCR ei ole täielikult aktiveeritud“ loetletud samme.

57) Kui IPCR on täielikult aktiveeritud, aitavad ISAA aruanded tagada poliitilisel tasandil ühise olukorrateadlikkuse. EU-CyCLONe ja CSIRTide võrgustiku olukorraülevaated peaksid jääma peamisteks vahenditeks, mis kajastavad ühist olukorrateadlikkust vastavalt operatiivtasandil ja tehnilisel tasandil. Need aruanded võivad olla ISAA aruannete alus.

58) Ulatusliku küberturbeintsidendi või küberkriisi korral, mille tulemusel on IPCR täielikult aktiveeritud, peaksid kõik osalejad reageerima tihedalt koordineerides kogu valitsemissektorit hõlmava lähenemisviisi kohaselt järgmiselt:

a) nõukogu koordineerib liidu poliitilisel tasandil reageerimist, kasutades IPCRi korda;

14 Hübriidmeetmete kogum on raamistik koordineeritud reageerimiseks ELi ja tema liikmesriike mõjutavatele hübriidkampaaniatele ja see hõlmab näiteks ennetus-, koostöö-, stabiilsus-, piiramis- ja taastemeetmeid ning toetab solidaarsust ja vastastikust abi.

b) EU-CyCLONe peaks koostöös CSIRTide võrgustikuga esitama poliitilisele tasandile selge teabe intsidendi mõju, võimalike tagajärgede ning selle suhtes võetud reageerimis- ja parandusmeetmete kohta, sealhulgas osaledes ISAA aruande koostamisel;

c) lisaks ISAA võimele kutsub Euroopa Liidu Nõukogu eesistujariik kokku IPCRi ümarlauakohtumised, et võimaldada ELi reageerimise poliitilist ja strateegilist koordineerimist, kasutades kübervaldkonna tegevuskava meetmeid ja asjakohaste valdkondlike mehhanismide tööd, mis toetavad IPCRi tööd. Ümarlauakohtumistel saab kindlaks teha ka konkreetsed reageerimise puudused ning paluda konkreetsetel ELi osalejatel nendega tegeleda ja anda nende kohta aru tulevastel ümarlauakohtumistel, et toetada poliitilist ja strateegilist koordineerimist IPCRis;

d) Euroopa Liidu Nõukogu eesistujariik peaks kaaluma EU-CyCLONe kutsumist asjakohastele kohtumistele, sealhulgas IPCRi raames toimuvatele ümarlauakohtumistele ja muudele asjakohastele nõukogu istungitele;

e) liikmesriikide kriisiohjeasutused, mida toetavad küberkriisi ohjamise asutused, peaksid tagama valdkondlike küberkriisile reageerimise meetmete vahelise sidususe ja koordineerimise;

f) võimalik diplomaatiline reageerimine tuleks läbi arutada ja ellu viia kooskõlas IX peatükiga.

VIII. Avaliku kommunikatsiooni meetmed

59) Kuigi liikmesriigi elanikkonna teavitamine jätkuvast ulatuslikust küberturbeintsidendist või küberkriisist, sealhulgas teadlikkuse suurendamise osana, kuulub liikmesriikide pädevusse, peaksid liikmesriigid, komisjon ja kõrge esindaja püüdma oma avaliku kommunikatsiooni meetmeid võimalikult suures ulatuses koordineerida. Vajaduse korral võib kaasata IPCRi mitteametliku kriisist teavitamise võrgustiku.

60) Ulatuslikeks küberturbeintsidentideks ja küberkriisideks valmistumiseks kutsutakse liikmesriike ning vajaduse korral komisjoni ja CERT-EUd üles oma kommunikatsioonialaste jõupingutuste kohta EU-CyCLONe ja CSIRTide võrgustiku raames teavet vahetama, sealhulgas selliste parimate tavade kohta nagu nõuanded või teadlikkuse suurendamise kampaaniad. ENISA peaks pakkuma sellist teabevahetust toetavaid ja lihtsat juurdepääsu tagavaid vahendeid.

61) Ulatusliku küberturbeintsidendi või küberkriisi korral kutsutakse liikmesriike ühise teadlikkuse suurendamiseks ja meetmete koordineerimiseks üles jagama oma avaliku kommunikatsiooni meetmeid puudutavat teavet EU-CyCLONe raames. EU-CyCLONe võib omal algatusel või nõukogu taotlusel jagada nõukoguga ülevaadet sellistest lähenemisviisidest.

IX. Diplomaatiline reageerimine ja koostöö strateegiliste partneritega

62) Kõrge esindaja peaks tihedas koostöö komisjoni ja liidu teiste asjaomaste üksustega tegema järgmist:

a) toetama nõukogus otsuste tegemist, sealhulgas analüüside, aruannete ja ettepanekute kaudu, võimalike meetmete kasutamise kohta ELi küberdiplomaatia meetmete kogumi osana. See võimaldab kasutada pahatahtliku kübertegevuse ennetamiseks, selle toimepanijate heidutamiseks ja sellele reageerimiseks kõiki kättesaadavaid liidu vahendeid, kindlustades liidu kübervaldkonna turvaolekut ja aidates kaasa rahvusvahelisele rahule ning turvalisusele ja stabiilsusele küberruumis;

b) kui asjaomane intsident on kindlaks tehtud, soodustama vajaliku teabe liikumist strateegiliste partnerite (sealhulgas asjakohasel juhul ka NATO) vahel;

c) alaliste ohusubjektide toime pandud pahatahtlikule kübertegevusele reageerimisel parandama koordineerimist strateegiliste partneritega, kaasa arvatud asjakohasel juhul NATOga, eriti juhul, kui kasutatakse ELi küberdiplomaatia meetmete kogumit, nagu on ette nähtud selle rakendussuunistes.

63) Liikmesriigid, kõrge esindaja, komisjon ja muud liidu asjaomased üksused peaksid tegema strateegiliste partnerite ja rahvusvaheliste organisatsioonidega koostööd, et propageerida häid tavasid ja riikide vastutustundlikku käitumist küberruumis ning tagada kiire ja koordineeritud reageerimine võimalikele või ulatuslikele küberturbentsidentidele.

64) Euroopa Liidu ja NATO koostöö peaks toimuma kooskõlas kokkulepitud juhtpõhimõtetega, milleks on kaasatus, vastastikkus ja läbipaistvus, ning täielikult liidu autonoomset otsustusprotsessi austades.

65) Võttes arvesse selliseid kehtivaid kokkuleppeid nagu CERT-EU ja NATO vahel 2016. aastal sõlmitud tehniline kokkulepe, peaksid komisjon ja kõrge esindaja looma kontaktpunktid tegevuse koordineerimiseks NATOga küberkriisi korral, et vahetada vajalikku teavet olukorra ja kriisidele reageerimise mehhanismide kasutamise kohta, selleks et tihendada reageerimise valdkonnas koostööd ja suurendada reageerimise tõhusust. Selleks peaks liit uurima võimalusi, kuidas parandada teabe jagamist NATOga kaasaval, vastastikusel ja mittediskrimineerival viisil, eelkõige tagades vahendid turvaliseks teabevahetuseks, võttes samal ajal arvesse eri liikmesriikide teabevahetusstandardeid.

66) Osana eespool V peatükis osutatud liidu küberõppuste jooksvast programmist peaksid komisjoni talitused ja Euroopa välisteenistus kaaluma töötajate tasandil õppuse korraldamist NATOga, et testida tsiviil- ja sõjaliste üksuste vahelist koostööd ulatusliku küberturbeintsidendi või küberkriisi korral, kui liikmesriigid või NATO liitlased püüavad reageerida nende julgeolekut mõjutavale küberründele. Õppus tuleks läbi viia kaasaval ja mittediskrimineerival viisil ning täielikult ELi ja NATO koostöö parameetreid puudutavaid kokkulepitud põhimõtteid järgides. Õppus tuleks läbi viia ELi integreeritud kriisilahenduse õppuse (nn paralleelne ja koordineeritud õppus, PACE) raames. Tuleks võtta kõik vajalikud meetmed, et tagada kõigi kübervaldkonna tegevuskavas osutatud osalejate osalemine.

67) Samuti tuleks kaaluda ühiseid liidu tasandi küberõppusi Lääne-Balkani riikide, Moldova Vabariigi, Ukraina ning muude strateegiliste partnerite ja sarnaselt meelestatud kolmandate riikidega, konsulteerides nõukogu, komisjoni ja kõrge esindajaga.

X. Küberkriiside ohjamise koordineerimine sõjaliste osalejatega ELi tasandil

68) Liikmesriigid peaksid jätkama tsiviil- ja sõjaliste kübervaldkonna osalejate vahelise koostöö tugevdamist liikmesriikide tasandil.

69) EU-CyCLONe ja CSIRTide võrgustik peaksid tegema kindlaks võimalikud viisid ja menetlused koostöö tegemiseks asjaomaste ELi sõjaliste osalejatega, nagu ELi küberväejuhatuste ülemate konverents ning sõjaliste infoturbeintsidentidega tegelevate rühmade operatiivvõrgustik (MICNET), et saada kasu ühisest sõjalisest ja tsiviilperspektiivist, eelkõige ühiste kohtumiste kaudu. EU-CyCLONe ja CSIRTide võrgustik peaksid teavitama nõukogu sellist koostööd puudutavatest edusammudest.

70) Juhul kui mõjutatud liikmesriik kasutab ulatusliku küberturbeintsidendi või küberkriisi korral asjakohaseid riiklikke või rahvusvahelisi sõjalisi reageerimisvõimekusi, palutakse tal sellest teavitada EU-CyCLONe-t ja Euroopa välisteenistust ning sellise teabe esitamine lepitakse kokku sellise reageerimisvõimekuse kasutaja ja pakkuja vahel.

71) Osana eespool V peatükis osutatud liidu küberõppuste jooksvast programmist peaksid komisjon ja kõrge esindaja kaaluma ühisõppuse korraldamist, et testida nii tsiviil- kui ka sõjaliste kübervaldkonna osalejate vahelist koostööd liikmesriike mõjutava ulatusliku küberturbeintsidendi korral.

XI. Küberkriisist taastumine ja saadud õppetunnid

72) Liikmesriigid, asjaomased liidu üksused ja võrgustikud peaksid tegema küberkriisijärgses taastamisetapis koostööd, et tagada põhifunktsioonide kiire taastamine. Sellisesse koostöösse tuleks vajaduse korral kaasata ka õiguskaitse ringkonnad. Selles etapis on väga oluline koostöö erasektoriga, eelkõige andmete taastamise ja süsteemide taaskäivitamise hõlbustamisel. Sidusrühmade vahelisel tõhusal koordineerimisel peaks seadma prioriteediks häirete minimeerimise ja toimepidevuse tagamise.

73) Liikmesriigid, asjaomased liidu üksused ja võrgustikud peaksid taastamisetapis koostööd tegema, tuginedes õppetundidele, mis on saadud minevikus toimunud küberkriiside käigus või hallatud küberturbeintsidentide käigus, ning intsidentide kohta koostatud aruannete põhjal, eriti määrusega (EL) 2025/38 loodud Euroopa küberintsidentide läbivaatamise mehhanismi kontekstis.

74) EU-CyCLONe peaks CSIRTide võrgustikule, võrgu- ja infoturbe koostöörühmale ja nõukogule esitama põhjaliku loetelu küberkriisidest või ohjatud küberturbeintsidentidest saadud õppetundidest ja parimatest tavadest. ENISA peaks tagama, et saadud õppetunde võetakse nõuetekohaselt arvesse tulevastes valmisolekumeetmetes ja tulevaste õppuste kavandamisel.

XII. Turvaline side

75) Olemasolevate turvaliste sidevahendite kaardistamise põhjal[15] peaks komisjon 2026. aasta lõpuks tegema ettepaneku koostalitlusvõimeliste turvaliste sidelahenduste kohta. Nõukogu, komisjon, kõrge esindaja, EU-CyCLONe ja CSIRTide võrgustik peaksid selles kokku leppima 2027. aasta lõpuks. Nende lahenduste puhul tuleks kasutada turvalise side valdkonna meetmeid, mida ELi institutsioonid võiksid võtta ELi kriisivalmiduse strateegia raames, ning need peaksid hõlmama kõiki vajalikke suhtlusviise (kõne, andmed, videokonverentsid, sõnumivahetus, koostöö ning dokumentide jagamine ja konsulteerimine). Need lahendused peaksid vastama ühiselt määratletud salastamata, kuid tundliku teabe kaitse nõuetele. Kasutada tuleks avatud protokollil põhinevaid, avatud lähtekoodiga rakendusi omavaid lahendusi, mis sobivad reaalajas suhtlemiseks ja mida haldab ELi residendist üksus.

76) EU-CyCLONe ja CSIRTide võrgustik peaksid tasemel RESTREINT UE/EU RESTRICTED salastatud teabe vahetamiseks saama vajaduse korral kasutada omavahel ja liikmesriikidega salastatud teabe vahetamiseks ELi institutsioonidele, organitele ja asutustele tagatud turvalisi sidekanaleid.

[15] WK 862/2023.

77) Ilma et see mõjutaks tulevast mitmeaastast finantsraamistikku, peaks määruse (EL) 2021/887[16] alusel loodud küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus kaaluma võimalust kasutada turvaliste sidevahendite kasutuselevõtul liikmesriikide aitamiseks programmi „Digitaalne Euroopa“ rahastust. Vältida tuleks koostalitlusvõimelistesse turvalistesse süsteemidesse tehtavate investeeringute dubleerimist.

78) Ennekõike peaksid ELi üksused ja liikmesriigid välja töötama erivahendid tõsiste kriiside puhuks, kui Internetil või telekommunikatsioonivõrkudel põhinevad tavalised sidekanalid on häiritud või ei ole kättesaadavad.

79) Tulemuslikuks küberkriisile reageerimiseks tuleks luua õiguskaitse ja küberturbevõrgustike vahelised side- ja teabevahetusmehhanismid, ennekõike tehnilisel tasandil. Need mehhanismid peaksid arvestama kõigi osaliste rolliga ja mitte sekkuma käimasolevatesse operatsioonidesse ning tagama alternatiivsed kommunikatsioonivõimalused. Praegu väljatöötamisel olev Euroopa elutähtsa teabevahetuse süsteem (EUCCS) võib aidata kaasa ühisele reageerimisele asjaomaste küberkogukondadega.

XIII. Lõppsätted

80) EU-CyCLONe peaks koostöös CSIRTide võrgustiku ja muude ELi küberkriiside ohjamise ökosüsteemi peamiste osalejatega, keda toetab ENISA, töötama ühe aasta jooksul pärast soovituse avaldamist välja üksikasjalikud protsessikirjeldused, milles kirjeldatakse asjaomaste osalejate vahelist teabe liikumist, otsustusprotsesse ja aruandeid, mis on välja töötatud käesolevas soovituses kirjeldatud ulatusliku küberturbeintsidendi või küberkriisi ohjamise käigus. Protsessikirjeldused peaksid hõlmama eri koostööviise ja -kihte. Neid tuleks vastavalt vajadusele ajakohastada.

[16] Euroopa Parlamendi ja nõukogu 20. mai 2021. aasta määrus (EL) 2021/887, millega luuakse küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus ning riiklike koordineerimiskeskuste võrgustik (ELT L 202, 8.6.2021, lk 1–31).

81) Läbivaadatud kübervaldkonna tegevuskava tõhusa kohaldamise toetamiseks ja selle alusel läbi viidud ühiste küberõppuste käigus saadud õppetundidele tuginedes võib nõukogu vajaduse korral välja töötada rakendussuunised. Neid suunistes võiks käsitleda õppuste käigus kindlaks tehtud praktilisi probleeme ning kõrvaldada koordineerimises, teabevahetuses ja operatiivkoostöös tuvastatud lüngad ja puudused.

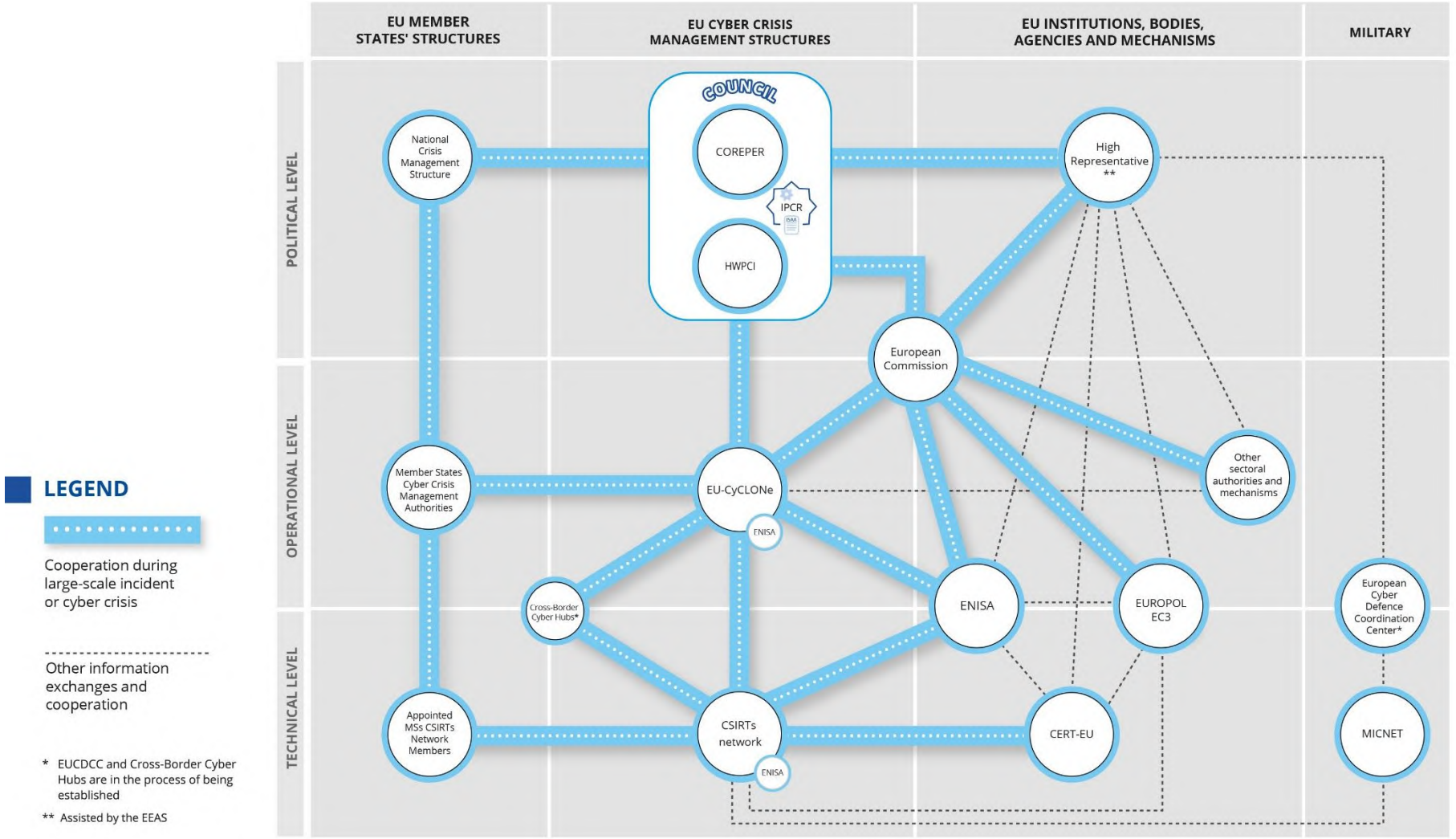
82) Komisjon peaks käesoleva soovituse koostöös liikmesriikidega läbi vaatama vähemalt iga nelja aasta järel pärast selle avaldamist. Pärast iga läbivaatamist peaks komisjon avaldama aruande ja esitama selle nõukogule. Komisjon ja liikmesriigid peaksid võtma eelkõige arvesse muutuva ohumaastiku mõju, ühisõppuste tulemusi ja seadusandlikke muudatusi, eelkõige määruse (EL) 2019/881 läbivaatamisest tulenevaid võimalikke muudatusi.

Brüssel,

Nõukogu nimel

eesistuja

I. LISA. Küberturbekriisile reageerimise liidu tegevuskava



II LISA. ASJAOMASED LIIDU TASANDI OSALEJAD (ÜKSUSED JA VÕRGUSTIKUD) JA KRIISIOHJEMEHHANISMID

(1) Peamiste osalejate kaasamine küberkriisi ohjamise tsükli jooksul (ulatuslikud küberturbeintsidendid ja küberkriisid)

	Valmisolek	Avastamine	Reageerimine ulatuslikule küberturbeintsidendile või küberkriisile			Avalikkuse teavitamine	Taastamine ja saadud kogemused
			tehnilisel tasandil	operatiivtasandil	poliitilisel tasandil		
Liikmesriigid	X	X	X	X	X	X	X
Komisjon	X			X	X	X	
Kõrge esindaja, keda abistab Euroopa välisteenistus	X			X	X	X	
Nõukogu	X				X	X	X
ENISA	X		X	X			
CERT-EU	X	X	X	X		X	X
CSIRTide võrgustik	X	X	X				X
EU-CyCLONe	X			X	X		X

(2) Asjaomaste liidu tasandi osalejate ja mehhanismide (inglise keeles tähestikuline järjestus) roll ja pädevus küberkriisi ohjamisel

Osaleja	Tasand	Roll ja pädevus	Aluseks olev õigusakt
CERT-EU	Tehniline/operatiivne	Koordineerib kriisile reageerimist tehnilisel tasandil ja liidu üksusi mõjutavate tõsiste intsidentide ohjamist. Peab loendit olemasolevatest tehnilistest eksperditeadmistest, mida oleks vaja tõsiste intsidentide korral intsidendile reageerimiseks, ning aitab IICB-l koordineerida liidu üksuste küberkriiside ohjamise kavasid tõsiste intsidentide käsitlemiseks. Kuulub CSIRTide võrgustikku. Toetab komisjoni EU-CyCLONe-s ulatuslike küberturbeintsidentide ja kriiside koordineeritud ohjamisel. Tegutseb küberturvalisust puudutava teabe vahetamist ja intsidentidele reageerimist koordineeriva keskusena, hõlbustades intsidente, küberohtusid, nõrkuste ja napilt ära hoitud intsidente puudutava teabe	Määrus (EL, Euratom) 2023/2841 Määrus (EL) 2025/38

Osaleja	Tasand	Roll ja pädevus	Aluseks olev õigusakt
		vahetamist liidu üksuste ja nende vastaspoolte vahel. Taotleb liidu üksuste nimel ELi küberreservi kasutuselevõtmist. Teeb koostööd NATO küberturvalisuse keskusega nendevahelise tehnilise kokkuleppe alusel.	
Euroopa Liidu Nõukogu	Poliitiline	Poliitika kujundamise ja koordineerimise funktsioonid. Talle on tehtud ülesandeks IPCR, mis käsitleb koordineerimist ja reageerimist liidu poliitilisel tasandil.	Euroopa Liidu lepingu artikkel 16
Euroopa Liidu Nõukogu eesistujariik	Poliitiline	Otsustab (välja arvatud juhul, kui tuginetakse Euroopa Liidu toimimise lepingu artikli 222 kohasele solidaarsusklauslile) IPCRi aktiveerimise üle, konsulteerides vastavalt vajadusele mõjutatud liikmesriikide ning komisjoni ja kõrge esindajaga.	Euroopa Liidu lepingu artikkel 16 Nõukogu rakendusotsus (EL) 2018/1993
Piiriülesed küberkeskused	Tehniline	Piiriülene küberkeskus on mitut riiki hõlmav, kirjaliku konsortsiumikokkuleppega loodud platvorm, mis	Määrus (EL) 2025/38

Osaleja	Tasand	Roll ja pädevus	Aluseks olev õigusakt
		koondab koordineeritud võrgustikku vähemalt kolme liikmesriigi riiklikud küberkeskused ning mis on loodud eesmärgiga tõhustada küberohtude seiret, avastamist ja analüüsimist, ennetada intsidente ning toetada küberohuteadmuse kogumist, eelkõige vahetades asjassepuutuvaid ja asjakohasel juhul anonüümseks muudetud andmeid ja teavet, jagades tipptasemel vahendeid ning arendades usaldusväärses keskkonnas ühiselt küberohtude ja intsidentide avastamise, analüüsimise ja ennetamise suutlikkust ning kaitsevõimet. Teevad teabevahetuse eesmärgil tihedat koostööd CSIRTide võrgustikuga. Edastavad liikmesriikide ametiasutustele ja komisjonile EU-CyCLONe ja CSIRTide võrgustiku kaudu teavet, mis on seotud võimaliku või käimasoleva ulatusliku küberturbeintsidendiga.	
CSIRTide võrgustik	Tehniline	Aitab suurendada usaldust ja kindlustunnet ning edendab kiiret operatiivkoostööd liikmesriikide vahel.	Direktiiv (EL) 2022/2555 Määrus (EL) 2025/38

Osaleja	Tasand	Roll ja pädevus	Aluseks olev õigusakt
		Tegemist on peamise võrgustikuga asjakohase teabe vahetamiseks intsidentide, napilt ära hoitud intsidentide, küberohtude, riskide ja nõrkuste kohta. Intsidendist potentsiaalselt mõjutatud liikme taotlusel vahetab ja arutab võrgustik teavet intsidendi ja sellega seotud küberohtude kohta. Võrgustik võib lisaks sellele hõlbustada koordineeritud reageerimist intsidendile, mis on tuvastatud taotluse esitanud liikme jurisdiktsioonis. Abistab liikmesriike piiriüleste intsidentide ohjamisel ja uurib täiendavaid koostöövorme, sealhulgas vastastikuse abi andmist. Saab liikmesriikidelt teavet nende poolt ELi küberreservile esitatud taotluste kohta.	
Küberväejuhatuse ülemate konverents		Liikmesriigi tasandi küberväejuhatuse ülemate foorum, mille eesmärk on teha koostööd ja vahetada olulist teavet	Ühisteatis ELi küberkaitsepoliitika kohta (2022)

Osaleja	Tasand	Roll ja pädevus	Aluseks olev õigusakt
		käimasolevate küberruumi operatsioonide kohta ning ulatuslike küberintsidentide mõju leevendamise strateegiate kohta. Seda korraldab Euroopa Liidu Nõukogu rotatsiooni korras vahetuv eesistujariik Euroopa Kaitseagentuuri ja Euroopa välisteenistuse, sealhulgas Euroopa Liidu sõjalise staabi toetusel.	
Komisjon	Operatiivne/poliitiline	Euroopa Liidu täitevorgan. Tagab siseturu sujuva toimimise. Hõlbustab asjaomaste liidu tasandi kriisidele reageerimise meetmete sidusust ja koordineerimist. Teatavad üldised liidu tasandi valmisolekumeetmed vastavalt liidu elanikkonnakaitse mehhanismi käsitlevale otsusele, sealhulgas hädaolukordadele reageerimise koordineerimiskeskuse ja ühise hädaolukordade side- ja infosüsteemi haldamine. Osaleb EU-CyCLONe-s vaatlejana ning selle	Euroopa Liidu lepingu artikkel 17 Rakendusotsus (EL) 2018/1993 Otsus nr 1313/2013/EL Direktiiv (EL) 2022/2555 Määrus (EL) 2025/38 Määrus (EL, Euratom) 2023/2841

Osaleja	Tasand	Roll ja pädevus	Aluseks olev õigusakt
		liikmena sellise võimaliku või käimasoleva ulatusliku intsidendi korral, millel on või võib olla märkimisväärne mõju direktiivi (EL) 2022/2555 kohaldamisalasse kuuluvatele teenustele ja tegevustele. Osaleb CSIRTide võrgustikus vaatlejana. Kannab üldist vastutust ELi küberreservi rakendamise eest. Institutsioonidevahelise küberturvalisuse nõukoja kontaktpunkt tõsiste intsidentidega seotud olulise teabe jagamiseks EU-CyCLONe-le. Nõukogu eesistujariik konsulteerib temaga IPCRi aktiveerimise või deaktiveerimise otsuste tegemisel (välja arvatud juhul, kui tuginetakse ELi toimimise lepingu artikli 222 kohasele solidaarsusklauslile). Komisjoni talitused koostavad koos Euroopa välisteenistusega ISAA aruanded.	

Osaleja	Tasand	Roll ja pädevus	Aluseks olev õigusakt
Euroopa Liidu Küberturvalisuse Amet (ENISA)	Tehniline/operatiivne	Täidab ülesandeid, mille eesmärk on saavutada küberturvalisuse kõrge tase kogu liidus, sealhulgas toetades aktiivselt liikmesriike ja liidu institutsioone. Tagab CSIRTide võrgustiku ja EU-CyCLONe sekretariaaditeenused. Koostab intsidentide ja küberohtude kohta korrapäraselt ELi küberturvalisuse tehnilise olukorra aruande (koos küberkuritegevuse vastase võitluse Euroopa keskuse ja CERT-EUga ning tihedas koostöös liikmesriikidega). Aitab välja töötada ühised reageerimismeetmed ulatuslikele piiriülestele intsidentidele või kriisidele, tehes peamiselt järgmist: – koondab ja analüüsib riiklikelt allikatelt saadud aruandeid; – tagab teabe liikumise tehnilise, operatiivse ja poliitilise tasandi vahel;	Direktiiv (EL) 2022/2555 Määrus (EL) 2019/881 Määrus (EL) 2025/38 Määrus (EL) 2024/2847

Osaleja	Tasand	Roll ja pädevus	Aluseks olev õigusakt
		– taotluse korral hõlbustab intsidentide käsitlemist; – toetab liidu üksusi avalikkuse teavitamisel; – taotluse korral toetab liikmesriike avalikkuse teavitamisel; – testib intsidentidele reageerimise suutlikkust ja korraldab korrapäraselt küberturvalisuse õppusi. Tegutseb avaliku sektori hankijana, kui talle on tehtud ülesandeks ELi küberreservi osaline või täielik käitamine ja haldamine. Korraldab iga kahe aasta tagant liidu tasandil ulatuslikke kõikehõlmavaid küberturvalisuse õppusi, mis hõlmavad tehnilisi, operatiivseid või strateegilisi elemente. Koostab koostöös asjaomase liikmesriigi ja muude asjaomaste sidusrühmadega intsidendi kohta	

Osaleja	Tasand	Roll ja pädevus	Aluseks olev õigusakt
		läbivaatamisaruande, et hinnata intsidendi põhjuseid, mõju ja leevendamist (komisjoni või EU-CyCLONe taotlusel ja asjaomase liikmesriigi heakskiidul). Teavitab EU-CyCLONe-d, kui küberkerksuse määruse aruandluskohustuste alusel esitatud teave on asjakohane ulatuslike küberturbeintsidentide ja kriiside koordineeritud ohjamiseks operatiivtasandil.	
Euroopa küberkriisiga tegelevate kontaktasutuste võrgustik (EU-CyCLONe)	Operatiivne	Toetab ulatuslike küberturbeintsidentide ja kriiside koordineeritud ohjamist operatiivtasandil. Tagab asjakohase teabe korrapärase vahetamise liikmesriikide ning liidu institutsioonide, organite ja asutuste vahel. Koordineerib ulatuslike küberturbeintsidentide ja kriiside ohjamist ning toetab selliste intsidentide ja kriisidega seotud otsuste tegemist poliitilisel tasandil. Hindab asjaomaste ulatuslike küberturbeintsidentide ja kriiside tagajärgi ja mõju	Direktiiv (EL) 2022/2555 Määrus (EL) 2025/38

Osaleja	Tasand	Roll ja pädevus	Aluseks olev õigusakt
		ning pakub välja võimalikud leevendusmeetmed. Arutab asjaomase liikmesriigi taotlusel riiklikke ulatuslikule küberturbeintsidendile ja kriisile reageerimise kavasid. Töötab koos ENISA ja komisjoniga välja näidisvormi, et hõlbustada ELi küberreservist toetuse saamise taotluste esitamist. Saab liikmesriikidelt teavet nende poolt ELi küberreservile esitatud taotluste kohta. Saab piiriülestelt küberkeskustelt või CSIRTide võrgustikult võimaliku või käimasoleva ulatusliku küberturbeintsidendiga seotud teavet.	
Liidu välisasjade ja julgeolekupoliitika kõrge esindaja, keda abistab Euroopa välisteenistus	Poliitiline	Juhib ja koordineerib hübriid- ja küberohtude valdkonna välisjulgeolekuohtude vastast liidu tegevust. Vastutab liidu küberdiplomaatia ja küberkaitsevahendite eest eesmärgiga väliseid ohte heidutada ja neile reageerida, sealhulgas	Nõukogu otsus 2010/427/EL

Osaleja	Tasand	Roll ja pädevus	Aluseks olev õigusakt
		kasutades liidu hübriid- ja küberdiplomaatia meetmete kogumit. Suhtleb välispartneritega, muu hulgas ühise julgeoleku- ja kaitsepoliitika raames. Tagab kriisivalmiduse liidule ja liikmesriikidele hübriid- ja küberohtude alase olukorrateadlikkuse ja reageerimissuutlikkuse, näiteks praktiliste õppuste, koolituse ja võrgustike abil. Tegeleb liidu kosmosevarade mõjuga julgeolekule ja kaitsele, eriti liidu ühise julgeoleku- ja kaitsepoliitika raames. Toetab ELi küberväejuhatuste ülemate konverentsi. Toetab ELi sõjaliste infoturbeintsidentidega tegelevate rühmade operatiivvõrgustikku (MICNET). Nõukogu eesistujariik konsulteerib temaga IPCRi aktiveerimise või deaktiveerimise otsuste tegemisel (välja arvatud juhul, kui tuginetakse ELi toimimise lepingu artikli 222 kohasele	

Osaleja	Tasand	Roll ja pädevus	Aluseks olev õigusakt
		solidaarsusklauslile). Euroopa välisteenistus koos komisjoni talitustega koostab ISAA aruanded.	
ELi küberkaitse koordineerimiskeskus	Horisontaalne	Selle esmane eesmärk on ennekõike parandada liidu ja selle liikmesriikide ühist olukorrateadlikkust küberruumis toimuva pahatahtliku tegevuse kohta, eelkõige mis puudutab ÜJKP sõjalisi missioone ja operatsioone.	Ühisteatis ELi küberkaitse-poliitika kohta (2022)
Europol	Operatiivne	Pakub liikmesriikide pädevatele asutustele operatiivset ja tehnilist tuge küberkuritegevuse ennetamiseks ja heidutuseks. Liikmesriikide pädevate asutuste taotluse korral abistab neid kuritegeliku päritolu kahtlusega küberrünnetele reageerimisel.	Määrus (EL) 2016/794, sealhulgas kõik selle muudatused
Institutsioonide-vaheline küberturvalisuse nõukoda		Töötab välja küberkriiside ohjamise kava, et operatiivtasandil toetada liidu üksusi mõjutavate	Määrus (EL, Euratom) 2023/2841

Osaleja	Tasand	Roll ja pädevus	Aluseks olev õigusakt
		tõsiste intsidentide koordineeritud ohjamist ja aidata kaasa asjakohase teabe korrapärasele vahetamisele. Koordineerib liidu eri üksuste küberkriiside ohjamise kavade vastuvõtmist. Võtab CERT-EU ettepaneku alusel vastu suunised või soovitused koostöö kohta intsidentidele reageerimisel liidu üksusi puudutavate oluliste intsidentide korral.	
Sõjaliste infoturbe-intsidentidega tegelevate rühmade operatiivvõrgustik (MICNET)	Tehniline	Edendab jõulisemat ja koordineeritumat reageerimist küberohtudele, mis mõjutavad liidu kaitsesüsteeme, sealhulgas neid, mida kasutatakse ÜJKP sõjalistes missioonides ja operatsioonides; seda toetab Euroopa Kaitseagentuur.	Ühisteatis küberkaitsepoliitika kohta (2022)

Osaleja	Tasand	Roll ja pädevus	Aluseks olev õigusakt
Ühtne luureandmete analüüsivõime (SIAC)		Koosneb 1) ELi luure- ja situatsioonikeskuse (EU INTCEN) ning 2) ELi sõjalise staabi luuredirektoraadi (EUMS INT) ühtsest luureandmete analüüsivõimest. Annab strateegilist luureteavet välispoliitika, terrorismi ning küber- ja hübriidohtude kohta ning käsitleb sõjalist luureteavet ÜJKP missioonideks ning toetab liidu kaitse- ja kriisiohjeoperatsioone. Kuulub kõrge esindaja alluvusse.	Euroopa Liidu lepingu artiklid 38 ja 42–46

(3) Asjakohased liidu tasandi kriisiohjemehhanismid ja platvormid

Mehhanism	Horisontaalne/ valdkondlik/kübervaldkonnaspetsiifiline	Kirjeldus	Aluseks olev õigusakt
ARGUS	Horisontaalne	Komisjoni koordineerimisprotsess ja üldine hoiatussüsteem ühtseks reageerimiseks ulatusliku piiriülese kriisi korral, mille puhul on vaja tegutseda ELi tasandil. See koondab kõik asjaomased talitused ja kabinetid, et otsustada meetmete üle ja neid koordineerida. Võimaldab komisjonil vahetada asjakohast teavet mitut valdkonda hõlmava kriisi tekkimisel või selle ennustatava või vahetu ohu korral, mille puhul on vaja tegutseda liidu tasandil.	Komisjoni teatis (2005)662
Euroopa välisteenistuse kriisidele reageerimise keskus	Horisontaalne	Euroopa välisteenistuse ühtne kontaktpunkt kõigis kriisidega seotud küsimustes ja ööpäevaringselt töötav alaline kriisidele reageerimise võimekus selliste hädaolukordade puhuks, mis ähvardavad ELi delegatsioonide töötajate turvalisust, ja/või selleks et reageerida kriisidele, mis mõjutavad liidu kodanikke väljaspool ELi. See koondab julgeoleku-, konsulaartöö ja	Julgeoleku- ja kaitsevaldkonna strateegiline kompass Euroopa Liidule, kes kaitseb oma kodanikke, väärtusi ja huve ning toetab rahvusvahelist rahu ja julgeolekut (21. märts 2022)

Mehhanism	Horisontaalne/ valdkondlik/kübervaldkonnaspetsiifiline	Kirjeldus	Aluseks olev õigusakt
		olukorrateadlikkuse eksperte ning tugineb samas liidu delegatsioonides kohapeal töötavatele pühendunud spetsialistidele.	
Elutähtsa taristu tegevuskava	Horisontaalne	Selle alusel koordineeritakse liidu tasandi reageerimist märkimisväärse piiriülese tähtsusega elutähtsa taristu häiretele.	Nõukogu soovitus C/2024/4371
Kübertuvalisuse hoiatussüsteem	Kübervaldkonna spetsiifiline	Tagab liidu täiustatud suutlikkuse, eesmärgiga suurendada liidus küberohtudega seotud avastamis-, analüüsi- ja andmetöötlussuutlikkust ning intsidentide ennetamist.	Määrus (EL) 2025/38
Küberdiplomaatia meetmete kogum (pahatahtlikule kübertegevusele ELi ühise diplomaatilise reageerimise raamistik)	Kübervaldkonna spetsiifiline	Võimaldab liidu ühist diplomaatilist reageerimist pahatahtlikule kübertegevusele, aidates kaasa konfliktide ennetamisele, küberohtude leevendamisele ja rahvusvahelistes suhetes suurema stabiilsuse saavutamisele.	Nõukogu 19. juuni 2017. aasta järeldused Läbivaadatud rakendussuunised, 10289/23, 8. juuni 2023
ELi küberreserv	Kübervaldkonna spetsiifiline	Kaasab kriiside käigus küberturvalisuse eksperte ja ressursse, et toetada liikmesriike, liidu institutsioone, organeid ja asutusi kriisile reageerimisel.	Määrus (EL) 2025/38

Mehhanism	Horisontaalne/ valdkondlik/kübervaldkonnaspetsiifiline	Kirjeldus	Aluseks olev õigusakt
Võrgueeskiri piiriüleste elektrivoogude küberturvalisust käsitlevate sektoripõhiste normide kohta	Valdkondlik	Sellega on kehtestatud elektrisektori küberriskide hindamise järjepidev protsess liidu, liikmesriigi, piirkonna ja üksuse tasandil. Sisaldab sätteid, mis käsitlevad kriisiohjet ning koostööd CSIRTide ja EU-CyCLONe-ga juhtudel, kui ulatuslik küberturbeintsident mõjutab teisi sektoreid, mis sõltuvad elektrivarustuskindlusest.	Komisjoni delegeeritud määrus (EL) 2024/1366
Hübriidmeetmete kogum	Horisontaalne	Sisaldab sätteid, mille eesmärk on tagada ülevaade ELi tasandil kättesaadavatest vahenditest mis tahes liiki hübriidohtudele reageerimiseks ja nende koordineeritud kasutamine, tagades sidususe kõigis valdkondades võetavate liidu meetmete vahel. Hübriidmeetmete kogum aitab tagada, et otsuste tegemise aluseks on terviklik olukorrateadlikkus ja saadud kogemused.	Nõukogu järeldused, mis käsitlevad raamistikku ELi koordineeritud reageerimiseks hübriidkampaaniatele (22. juuni 2022). Rakendussuunised, mis käsitlevad raamistikku ELi koordineeritud reageerimiseks hübriidkampaaniatele (14. detsember 2022)

Mehhanism	Horisontaalne/ valdkondlik/kübervaldkonnaspetsiifiline	Kirjeldus	Aluseks olev õigusakt
Hübriidohtudega tegelevad kiirreageerimisrühmad	Horisontaalne	ELi hübriidmeetmete kogumi osana tuginevad hübriidohtudega tegelevad ELi kiirreageerimisrühmad asjakohasele valdkondlikule riiklikule ning ELi tsiviilalasele ja sõjalisele eksperditeabele, et pakkuda liikmesriikidele, ühise julgeoleku- ja kaitsepoliitika missioonidele ja operatsioonidele ning partnerriikidele kohandatud ja sihipärast lühiajalist abi hübriidohtude ja -kampaaniate vastu võitlemisel.	Suunav raamistik hübriidohtudega tegelevate ELi kiirreageerimisrühmade praktikas moodustamiseks (21. mai 2024) Tegevussuunised hübriidohtudega tegelevate kiirreageerimisrühmade siirmiseks, heaks kiidetud COREPERi poolt 4. detsembril 2024
IPCR	Horisontaalne	Toetab kiiret ja koordineeritud otsuste tegemist liidu poliitilisel tasandil tõsiste ja keerukate kriiside korral. Otsuse selle aktiveerimise või desaktiveerimise kohta teeb nõukogu eesistujariik, konsulteerides (välja arvatud juhul, kui tuginetakse solidaarsusklauslile) mõjutatud liikmesriikide, komisjoni ja kõrge esindajaga. Samuti võivad nõukogu peasekretariaat, komisjoni talitused ja Euroopa välisteenistus leppida eesistujariigiga konsulteerides	Nõukogu rakendusotsus (EL) 2018/1993

Mehhanism	Horisontaalne/ valdkondlik/kübervaldkonnaspetsiifiline	Kirjeldus	Aluseks olev õigusakt
		kokku, et IPCR aktiveeritakse teabevahetuse režiimil. IPCRi töö tugineb ISAA aruannetele, mille koostavad komisjoni talitused ja Euroopa välisteenistus. Selliste aruannete aluseks on asjakohane teave ja analüüs, mille esitavad liikmesriigid (nt asjaomased riiklikud kriisikeskused) ning vastavad liidu asutused ja organid.	
ELi protokoll õiguskaitsealase reageerimise kohta hädaolukordades	Horisontaalne	Vahend, mis toetab liidu õiguskaitseasutusi tõsistele piiriülestele küberrünnetele viivitamatul reageerimisel, võimaldades anda kiire hinnangu, jagada kriitilise tähtsusega teavet turvaliselt ja õigeaegselt ning koordineerida tulemuslikult oma uurimiste rahvusvahelisi aspekte.	Nõukogu järeldused ELi koordineeritud reageerimise kohta ulatuslike küberintsidentide ja kriiside korral (26. juuni 2018)
PESCO küberturbe kiirreageerimisrühmad	Kübervaldkonna spetsiifiline	PESCO küberturbe kiirreageerimisrühmad on ühiselt välja töötatud ELi liikmesriikide tsiviil-sõjaline küberkaitsevõime, et reageerida kiiresti küberintsidentidele ja küberkriisidele ning võtta ennetavaid meetmeid, nagu nõrkuste hindamine ja valimiste jälgimine. PESCO küberturbe	Euroopa Liidu lepingu artikli 42 lõige 6, artikkel 46 ja protokoll nr 10

Mehhanism	Horisontaalne/ valdkondlik/kübervaldkonnas petsiifiline	Kirjeldus	Aluseks olev õigusakt
		kiirreageerimisrühmade ülesanne on pakkuda taotluse korral kübervaldkonnas tuge ELi liikmesriikidele, ELi institutsioonidele, organitele ja asutustele, ELi ÜJKP sõjalistele missioonidele ja operatsioonidele ning partnerriikidele.	

Kosmoseohtudele reageerimise struktuur	Valdkondlik (kosmoseohud, sealhulgas kui need on seotud kübervaldkonnaga)	Kosmoseohtudele reageerimise struktuur, mis käsitleb nõukogu ja kõrge esindaja täidetavaid kohustusi sellise ohu kõrvaldamiseks, mis tuleneb liidu kosmoseprogrammi raames loodud süsteemide ja pakutavate teenuste kasutuselevõtmisest, toimimisest või kasutamisest.	Nõukogu otsus (ÜVJP) 2021/698
Süsteemsete küberintsidentide koordineerimisraamistik	Valdkondlik	Väljatöötamisel olev side- ja koordineerimisraamistik, mille kaudu käsitletakse ja hallatakse potentsiaalseid süsteemseid kübersündmusi finantssektoris. See tugineb ühele rollidest, mis on määruse (EL) 2022/2554 kohaselt kavandatud Euroopa järelevalveasutustele: võimaldada järk-järgult tõhusat koordineeritud reageerimist liidu tasandil info- ja kommunikatsioonitehnoloogiaga seotud olulise piiriülese intsidendi või seonduva ohu korral, millel on süsteemne mõju liidu finantssektorile tervikuna.	Euroopa Süsteemsete Riskide Nõukogu 2. detsembri 2021. aasta soovitus seoses üleeuroopalise süsteemsete küberintsidentide koordineerimisraamistikuga asjaomastele asutustele (ESRN/2021/17)
Liidu elanikkonnakaitse mehhanism	Horisontaalne	Tagab elanikkonnakaitse alase koostöö, et parandada suurõnnetuste ennetamist, nendeks valmisolekut ja neile reageerimist.	Otsus 1313/2013

Ühine teabejagamiskeskkond (CISE)	Merendusspetsiifiline, hõlmab seitset sektorit	CISE on võrgustik, mis ühendab mereseire eest vastutavate ELi/EMP asutuste süsteeme. CISE võimaldab asjakohase teabe sujuvat ja automaatset vahetamist piirüleselt ja eri sektorite vahel.	Julgeoleku- ja kaitsevaldkonna strateegiline kompass Euroopa Liidule, kes kaitseb oma kodanikke, väärtusi ja huve ning toetab rahvusvahelist rahu ja julgeolekut (21. märts 2022)

(4) Kriitilise tähtsusega sektorid ja muud kriitilise tähtsusega sektorid vastavalt direktiivile (EL) 2022/2555 ning liidu tasandi valdkondlikud kriisimehhanismid (kui see on asjakohane)		
Sektor	**Allsektor**	**Kohaldatavad valdkondlikud kriisimehhanismid**
Energeetika	Elekter	Elektrivaldkonna koordineerimise rühm
	Kaugküte ja -jahutus	Puuduvad
	Nafta	Nafta koordineerimisrühm Euroopa Liidu avameretegevust reguleerivate asutuste rühm (EUOAG)
	Gaas	Gaasikoordineerimisrühm
	Vesinik	Puuduvad
Transport	Lennutransport	Euroopa lennunduskriiside koordineerimisüksus (EACCC)
	Raudteetransport	Puuduvad

	Veetransport	Euroopa Kalanduskontrolli Amet (EFCA) SafeSeaNet Integreeritud merendusteenused Laevade kaugtuvastuse ja kaugseire andmekeskus Euroopa Meresõiduohutuse Ameti merenduse tugiteenused
	Maanteetransport	Puuduvad
	Horisontaalne	Transpordisektori hädaolukorra lahendamise plaaniga (COM(2022) 211) loodud transpordiasutuste kontaktpunktide võrk
Pangandus		Üleeuroopaline süsteemsete küberintsidentide koordineerimisraamistik (EU-SCICF)
Finantsturutaristud		Üleeuroopaline süsteemsete küberintsidentide koordineerimisraamistik (EU-SCICF) Euroopa finantsstabiilsusmehhanism

Tervishoid		Varajase hoiatamise ja reageerimise süsteem (EWRS) Tervisealaste hädaolukordade lahendamise üksus (HEOF) Kudede, rakkude ja verekomponentide kiirhoiatussüsteem (RATC/RAB) Tervisealase hädaolukorra raamistik Kemikaaliintsidentide kiirhoiatussüsteem (RASCHEM) Nakkushaiguste Euroopa seireportaal ELi tervisealasteks hädaolukordadeks valmisoleku ja neile reageerimise asutus (HERA) Meditsiinilise järelevalve süsteem (MediSys) Meditsiiniseadmete nappuse juhtrühm (MDSSG) Ravimiohutuse järelevalve kiirhoiatussüsteem ELi tervishoiu rakkerühm (EUHTF) Terviseohutuse komitee

Joogivesi		Puuduvad
Reovesi		Puuduvad
Digitaristu		Puuduvad
IKT-teenuste haldus		Puuduvad
Avalik haldus		Puuduvad
Kosmos		Kosmoseohtudele reageerimise struktuur (STRA)
Posti- ja kulleriteenused		Puuduvad
Jäätmekäitlus		Puuduvad
Kemikaalide valmistamine, tootmine ja levitamine		Kemikaaliintsidentide kiirhoiatussüsteem (RASCHEM)

Toiduainete tootmine, töötlemine ja turustamine		Euroopa põllumajanduskultuuride seiresüsteem Üleilmse põllumajandustoodangu anomaaliate tulipunktide tuvastamine (ASAP) Euroopa taimetervisealaste teabesüsteemide võrgustik (EUROPHYT) ELi veterinaariaalane hädaabirühm (EUVET) Toidu- ja söödaalane kiirhoiatussüsteem (RASFF) Euroopa toiduga kindlustatuse kriisiks valmisoleku ja kriisile reageerimise mehhanism (EFSCM) Siseturu hädaolukorra ja vastupanuvõime määrus
Töötlev tööstus	Meditsiiniseadmed	Puuduvad
	Arvutid, elektroonika- ja optikaseadmed	Puuduvad
	Masinad ja seadmed	Puuduvad
	Mootorsõidukite, haagiste ja poolhaagiste tootmine	Puuduvad
	Muude transpordivahendite tootmine	Puuduvad

Digiteenuste osutajad		Puuduvad
Teadustegevus		Puuduvad

III LISA. ELi küberturvalisuse kriisireguleerimise raamistik ja sellega seotud vahendid

Alates 2017. aastast on liit kujundanud oma küberturvalisuse raamistikku mitme õigusaktiga, mis sisaldavad küberturbekriisi ohjamist käsitlevaid sätteid:

- Euroopa Parlamendi ja nõukogu määrus (EL) 2019/881[1],
- Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555[2],
- komisjoni rakendusmäärus (EL) 2024/2690[3], Euroopa Parlamendi ja nõukogu määrus (EL, Euratom) 2023/2841[4],
- Euroopa Parlamendi ja nõukogu määrus (EL) 2021/887[5],
- Euroopa Parlamendi ja nõukogu määrus (EL) 2024/2847[6] ning
- Euroopa Parlamendi ja nõukogu määrus (EL) 2025/38 (kübersolidaarsuse määrus)[7].

Konkreetsed valdkondlikud meetmed küberturbekriiside puhuks on muu hulgas esitatud komisjon delegeeritud määruses (EL) 2024/1366[8] ning tulevases süsteemsete küberintsidentide koordineerimisraamistikus (EU-SCICF) Euroopa Parlamendi ja nõukogu määruse (EL) 2022/2554[9] kontekstis.

Küberrünnetega seotud kuritegeliku tegevuse määratlemisel saab lähtuda direktiivist 2013/40/EL[10] ning pärast seda, kui hakatakse rakendama liidu norme elektrooniliste tõendite piiriülese kättesaadavuse kohta, eelkõige Euroopa Parlamendi ja nõukogu määrust (EL) 2023/1543[11], muutub õiguskaitsetegevus selles valdkonnas oluliselt hõlpsamaks.

ELi küberkaitsepoliitikas[12] kirjeldatakse ELi sõjaliste infoturbeintsidentidega tegelevate rühmade operatiivvõrgustiku (MICNET) ja ELi küberväejuhatuste ülemate konverentsi rolli ning nähakse ette ELi küberkaitse koordineerimiskeskuse (EUCDCC) loomine.

Mõnes kriitilise tähtsusega sektoris, mis on loetletud direktiivi (EL) 2022/2555 I ja II lisas, on olemas muud olukorrateadlikkuse ja kriisidele reageerimise mehhanismid, mis ei ole kübermõõtmega seotud.

Nõukogu soovituses tegevuskava kohta, mille alusel koordineerida liidu tasandi reageerimist märkimisväärse piiriülese tähtsusega elutähtsa taristu häiretele[13], on ette nähtud asjaomaste osalejate koostöö juhul, kui intsident mõjutab nii elutähtsa taristu füüsilisi aspekte kui ka küberturvalisust.

[1] 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, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

[2] 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 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[3] Komisjoni 17. oktoobri 2024. aasta rakendusmäärus (EL) 2024/2690, millega kehtestatakse seoses domeeninimede süsteemi teenuse osutajate, tippdomeeninimede registrite, pilvandmetöötlusteenuse osutajate, andmekeskusteenuse osutajate, sisulevivõrgu pakkujate, hallatud teenuse osutajate, turbetarnijate ning internetipõhiste kauplemiskohtade, internetipõhiste otsingumootorite, sotsiaalvõrguteenuse platvormide ja usaldusteenuse pakkujatega direktiivi (EL) 2022/2555 kohaldamise eeskirjad, mis puudutavad küberturvalisuse riskijuhtimismeetmete tehnilisi ja metoodilisi nõudeid ja selliste juhtude täpsemat kindlaksmääramist, mille korral peetakse intsidenti oluliseks (ELT L, 2024/2690, 18.10.2024). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

[4] Euroopa Parlamendi ja nõukogu 13. detsembri 2023. aasta määrus (EL, Euratom) 2023/2841, millega nähakse ette meetmed küberturvalisuse ühtlaselt kõrge taseme tagamiseks liidu institutsioonides, organites ja asutustes (ELT L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

[5] Euroopa Parlamendi ja nõukogu 20. mai 2021. aasta määrus (EL) 2021/887, millega luuakse küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskus ning riiklike koordineerimiskeskuste võrgustik (ELT L 202, 8.6.2021, lk 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[6] Euroopa Parlamendi ja nõukogu 23. oktoobri 2024. aasta määrus (EL) 2024/2847, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrusi (EL) nr 168/2013 ja (EL) 2019/1020 ning direktiivi (EL) 2020/1828 (küberkerksuse määrus) (ELT L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] Euroopa Parlamendi ja nõukogu 19. detsembri 2024. aasta määrus (EL) 2025/38, millega nähakse ette meetmed, et tugevdada liidus solidaarsust ja suurendada suutlikkust küberohtude ja intsidentide avastamiseks,

nendeks valmistumiseks ja neile reageerimiseks, ning millega muudetakse määrust (EL) 2021/694 (kübersolidaarsuse määrus) (ELT L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

[8] Komisjoni 11. märtsi 2024. aasta delegeeritud määrus (EL) 2024/1366, millega täiendatakse Euroopa Parlamendi ja nõukogu määrust (EL) 2019/943 ning kehtestatakse võrgueeskiri piiriüleste elektrivoogude küberturvalisust käsitlevate sektoripõhiste normide kohta (ELT L, 2024/1366, 24.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

[9] 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 (ELT L 333, 27.12.2022, lk 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[10] 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, ELI: http://data.europa.eu/eli/dir/2013/40/oj).

[11] Euroopa Parlamendi ja nõukogu 12. juuli 2023. aasta määrus (EL) 2023/1543, mis käsitleb Euroopa andmeesitamismäärust ja Euroopa andmesäilitamismäärust elektrooniliste tõendite hankimiseks kriminaalmenetluses ja kriminaalmenetluse järgsete vabadusekaotuslike karistuste täitmisele pööramiseks, ning Euroopa Parlamendi ja nõukogu 12. juuli 2023. aasta direktiiv (EL) 2023/1544, millega kehtestatakse määratud majandusüksuste määramise ja esindajate nimetamise ühtlustatud normid elektrooniliste tõendite kogumiseks kriminaalmenetluses (ELT L 191, 28.7.2023, lk 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

[12] JOIN(2022) 49 final. https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52022JC0049

[13] *ELT C, C/2024/4371, 5.7.2024.* https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=OJ:C_202404371