Euroopa Liidu
Nõukogu

Brüssel, 22. mai 2023
(OR. en)

9618/23

COPS 269	**JAI 656**
POLMIL 123	**RELEX 639**
CYBER 130	**JAIEX 22**
HYBRID 31	**TELECOM 154**
EUMC 230	**IPCR 38**
CIVCOM 144	**PROCIV 35**
COPEN 162	**COTER 101**
COSI 103	**DISINFO 34**
DATAPROTECT 146	**CSC 252**
IND 256	**CSDP/PSDC 402**
RECH 191	**CFSP/PESC 748**

MENETLUSE TULEMUS

Saatja:	Nõukogu peasekretariaat
Saaja:	Delegatsioonid
Eelmise dok nr:	ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674
Teema:	Nõukogu järeldused ELi küberkaitsepoliitika kohta

Delegatsioonidele edastatakse ELi küberkaitsepoliitikat käsitlevad nõukogu järeldused, mis võeti vastu 22. mail 2023 toimunud nõukogu istungil.

Nõukogu järeldused ELi küberkaitsepoliitika kohta

1. Nõukogu tervitab ELi küberkaitsepoliitikat käsitlevat ambitsioonikat ühisteatist, mis tugineb 2014. aasta küberkaitsepoliitika raamistikule ja selle 2018. aastal ajakohastatud versioonile ning mille eesmärk on suurendada veelgi investeeringuid meie moodsatesse ja koostalitlusvõimelistesse relvajõududesse, eesrindlikesse tehnoloogiatesse ja tipptasemel küberkaitsevõimesse ning tugevdada partnerlusi ühiste probleemide lahendamiseks. Küberruumist on saanud strateegilise konkurentsi valdkond ja seda ajal, mil sõltuvus digitehnoloogiast üha kasvab. Seetõttu on oluline säilitada avatud, vaba, stabiilne ja turvaline küberruum. Selliste küberoperatsioonide kasutamine, mis on võimaldanud ja toetanud Venemaa provotseerimata ja põhjendamatut agressioonisõda Ukraina vastu, mõjutab ülemaailmset stabiilsust ja julgeolekut, kätkeb endas märkimisväärset eskaleerumise ohtu ning suurendab juba niigi märkimisväärset pahatahtliku kübertegevuse kasvu, mis on viimastel aastatel väljaspool relvakonflikte ilmnenud.

2. Sõda Ukrainas on loonud uue strateegilise konteksti ning kinnitanud, et EL, selle liikmesriigid ja nende partnerid peavad veelgi tugevdama ELi küberohtudele vastupanu võimet ning suurendama oma ühist küberjulgeolekut ja küberkaitset pahatahtliku käitumise ja agressiooni eest küberruumis. Eelmainitud ühisteatis ELi küberkaitsepoliitika kohta annab märku meie kindlameelsusest võtta koheseid ja pikaajalisi meetmeid, et tagada küberruumis tegutsemisvabadus ja reageerimine ohusubjektidele, kes üritavad näiteks tungida ELi ja tema partnerite võrgu- ja infosüsteemidesse või neid häirida või hävitada. Kõnealune ühisteatis täiendab ELi küberjulgeoleku strateegiat ja on kooskõlas strateegilise kompassiga ning kujutab endast olulist edasiminekut kogu spektrit katva lähenemisviisi poole, mida EL rakendab küberruumialase vastupanuvõime, reageerimise, konfliktide ennetamise, koostöö ja stabiilsuse suhtes. Sellega seoses rõhutab nõukogu, et EL, selle liikmesriigid ja nende partnerid peavad reageerima asjakohasel ja sidusal viisil, ning jääb ühtlasi ootama ELi küberdiplomaatia meetmete kogumi rakendussuuniste läbivaatamist, mis on järjekordne oluline samm ELi turvaoleku arengus kübervaldkonnas.

3. Nõukogu rõhutab, et hiljutised küberründed Euroopa elutähtsa taristu vastu, kiiresti arenev küberohtude keskkond ja tehnoloogia arengu kiire tempo näitavad samuti, et tsiviil- ja sõjandusvaldkonna vahelist koordineerimist ja koostööd on vaja tõhustada, ning seejuures toonitab, et tsiviil- ja militaarkogukondade vahel puudub hierarhia.
ELi küberkaitsepoliitika võimaldab ELil ja selle liikmesriikidel suurendada oma kaitse-, avastamis-, turbe- ja heidutusvõimet, kasutades sobival viisil kõiki tsiviil- ja sõjalistele kogukondadele kättesaadavaid kaitsevõimalusi ELi laiema julgeoleku ja kaitse tagamiseks kooskõlas rahvusvahelise õigusega, sealhulgas inimõigustealase õigusega ja rahvusvahelise humanitaarõigusega.

4. Kuigi riiklik julgeolek, sealhulgas kübervaldkonnas, jääb iga liikmesriigi ainupädevusse, nagu on märgitud ELi lepingu artikli 4 lõikes 2, rõhutab nõukogu siiski, et on vaja teha ulatuslikke investeeringuid nii individuaalselt kui ka koostöös, et tugevdada vastupanuvõimet ja asuda kasutama küberkaitsevõimalusi kogu nende spektri ulatuses ning rakendada ELi koostööraamistikke ja finantsstiimuleid. Nõukogu rõhutab, et on vaja veelgi tugevdada liikmesriikide ning ELi institutsioonide, organite ja asutuste tegevust, kaitsmaks liitu, meie kodanikke, ELi institutsioone, organeid ja asutusi ning ÜJKP missioone ja operatsioone küberruumis. Lisaks toonitab nõukogu, et küberruumis on oluline tagada ELi vastupanuvõime, arendades küberkaitsevõimet ja tõhustades koostööd usaldusväärse erasektori ökosüsteemiga.

I. **Ühine tegutsemine tugevama küberkaitse nimel**

5. Nõukogu kordab, et järkjärguline, läbipaistev ja kaasav protsess on oluline usalduse suurendamiseks, mis on omakorda hädavajalik ELi küberturvalisuse kriisireguleerimise raamistiku edasiarendamiseks, mida tuleb teha kooskõlas nõukogus välja töötatud küberkriiside ohjamise tegevuskavaga. Nõukogu kordab, et meil on vaja jätkata enda küberrünnetealase kaitse-, avastamis-, turbe- ja heidutusvõime suurendamist olukorrateadlikkuse parandamise, suutlikkuse suurendamise, võimete arendamise, koolituste ja õppuste korraldamise ja vastupanuvõime tugevdamise kaudu ning reageerides kindlameelselt kõigi asjakohaste vahendite abil ELi, selle liikmesriikide, ELi institutsioonide, organite ja asutuste ning ÜJKP missioonide ja operatsioonide vastu korraldatud küberrünnetele. Seejuures julgustab nõukogu kõrget esindajat ja komisjoni vähendama kübervaldkonnas keerukust, vältima tarbetut dubleerimist ning tagama koostöö ja koostoime olemasolevate algatustega. On tarvis tugevdada koostööd ja koordineerimist küberkaitses osalejate vahel ELis ja liikmesriikides, sõjandus- ja tsiviilvaldkonna küberkogukondade vahel ning avaliku ja usaldusväärse erasektori ökosüsteemi vahel. Sellega seoses julgustatakse liikmesriike veelgi uurima ja tugevdama tsiviil- ja sõjandusvaldkonna riiklikke koordineerimismehhanisme, hõlbustama ühist vabatahtlikku teabevahetust, jagama saadud kogemusi, aitama kaasa koostalitlusstandardite väljatöötamisele ning teostama riskihindamisi ja koostama riskistsenaariume, samuti korraldama ühisõppusi eelkõige Euroopa tasandil, järgides täielikult nõudeid, mis on sätestatud direktiivis, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus (küberturvalisuse 2. direktiiv).

6. Tunnustades jõupingutusi suurendada veelgi liidu vastupanuvõimet suurendamiseks küberturvalisuse 2. direktiivi ja elutähtsa teenuse osutajate toimepidevuse direktiivi abil, kordab nõukogu oma soovitust rakendada elutähtsa taristu toimepidavuse tugevdamiseks kogu ELi hõlmavat kooskõlastatud lähenemisviisi[1]. Nõukogu kutsub üles võtma meetmeid elutähtsa teenuse osutajate, taristu ning digitoodete ja -teenuste vastupidavuse edasiseks suurendamiseks, märkides samas, et küberturvalisuse 2. direktiivi nõuetekohane rakendamine on jätkuvalt kõige olulisem samm. Kuigi see kuulub peamiselt tsiviilvaldkonna vastutusalasse, aitab see kaasa ka küberkaitse tugevdamisele. Sellega seoses julgustatakse ELi institutsioone, organeid ja asutusi ning liikmesriike toetama uute ja olemasolevate ELi koordineerimismehhanismide, riskihindamiste ja stsenaariumide, ühise vabatahtliku teabevahetuse ja õppuste edasiarendamist ja rakendamist viisil, mis annab lisaväärtust ja hoiab ära olemasolevate algatuste tarbetu dubleerimise.

7. Selleks et veelgi suurendada usaldust, tugevdada koostööd ja hõlbustada õigeaegset teabevahetust kaitsesüsteeme mõjutavate oluliste ja ulatuslike küberintsidentide kohta, tervitab nõukogu algatust arendada edasi ELi küberväejuhatuste ülemate konverentsi, mille korraldab iga ELi nõukogu eesistujariik Euroopa Kaitseagentuuri toetusel ja Euroopa välisteenistuse osalusel. Nõukogu julgustab kõiki liikmesriike nendel kohtumistel osalema. Tugevdamaks ELi vastupanuvõimet ulatuslike küberintsidentide suhtes, kutsub nõukogu ELi küberkriisi kontaktasutuste võrgustikku (EU-CyCLONe) ja ELi küberväejuhatuste ülemate konverentsi üles tegema kindlaks võimalikud viisid koostöö korraldamiseks ning ühisest sõjalisest ja tsiviilperspektiivist kasu saamiseks.

[1] Ettepanek: nõukogu soovitus, milles käsitletakse liidu kooskõlastatud lähenemisviisi elutähtsa taristu vastupidavuse tugevdamisele (COM/2022/551).

8. Selleks et edendada jõulisemat ja koordineeritumat reageerimist ELi tasandil, tervitab nõukogu ELi sõjaliste infoturbeintsidentidega tegelevate rühmade operatiivvõrgustiku (MICNET) loomist ja jääb ootama selle esialgse operatsioonivõime saavutamist 2024. aasta keskpaigaks, et tõhustada osalevate liikmesriikide vahelist tehnilise teabe jagamist kaitsesüsteeme mõjutavate küberintsidentide kohta. Nõukogu julgustab kõiki liikmesriike MICNETis osalema, et tagada võrgustiku hea toimivus. Lisaks kutsub nõukogu liikmesriike üles tuginema küberturbe intsidentide lahendamise üksuste (CSIRT) võrgustikust saadud kogemustele ning kutsub tungivalt üles looma sobival ajal nende kahe võrgustiku vahele hästitoimiva koostöö ja koordineerimise mehhanismi, võttes täielikult arvesse iga üksuse juhtimismehhanisme ja ülesehitust.

9. Võttes arvesse riiklike ja valitsusväliste osalejate pahatahtliku kübertegevuse kasvu ELi ÜJKP missioonidel ja operatsioonidel, kutsub nõukogu ELi ja selle liikmesriike üles tugevdama oma suutlikkust kaitsta ÜJKP missioone ja operatsioone ning tagada nende julgeolek. Sellega seoses tervitab nõukogu eesmärke edendada veelgi ELi sõjaliste võrgustike ja struktuuride kaitset kooskõlas muu hulgas ELi sõjalise visiooniga ja strateegiaga küberruumi kui tegevusvaldkonna jaoks[2].

[2] EEAS(2021) 706 REV4.

10. Nõukogu kordab oma 2022. aasta mai järeldusi[3] ja vajadust investeerida ELi lepingu artikli 42 lõikes 7 ning ELi toimimise lepingu artiklis 222 esitatud solidaarsusklausli kohasesse vastastikusesse abisse. Nõukogu rõhutab, et on oluline veelgi süvendada ELi ja selle liikmesriikide ühist arusaama artikli 42 lõike 7 rakendamisest, sealhulgas küberründega seotud keerukates olukordades, kooskõlas asjakohaste rahvusvahelises õiguses sätestatud põhimõtetega. Nõukogu tervitab võimalust, et küberründe korral saab liikmesriik või saavad liikmesriigid selgesõnalise taotluse esitamisel ELilt toetust, ilma et see piiraks teatavate liikmesriikide julgeoleku- ja kaitsepoliitika eripära.

11. Nõukogu toonitab, et alaliste struktureeritud koostöö (PESCO) küberturbe kiirreageerimisrühmade ja küberjulgeolekualase vastastikuse abi projekti raames on tehtud edusamme ning nõukogu on valmis tegutsema taotluse korral liikmesriikide ja ELi vajaduste rahuldamise nimel, et toetada ÜJKP missioone ja operatsioone ning abistada ELi partnereid. Nõukogu tervitab PESCO küberturbe kiirreageerimisrühmade suutlikkuse, riiklike küberturbe reageerimisrühmade ja asjakohastel juhtudel täiendavate intsidentidele reageerimise üksuste edasiarendamist, näiteks hübriidohtudega tegelevate kiirreageerimisrühmade loomist, nagu on ette nähtud strateegilises kompassis, sealhulgas edendades nende koordineerimist ja koostööd ELi tasandil.

[3] Nõukogu järeldused Euroopa Liidu kübervaldkonna positsiooni arendamise kohta (23. mai 2022, dok 9364/22).

12. Nõukogu tervitab PESCO küber- ja teabevaldkonna koordinatsioonikeskuse (CIDCC) tööd, mille eesmärk on pakkuda sõjalist võimet koguda ja analüüsida ühise operatiiv-küberpildi jaoks olulist teavet. Lisaks tervitab nõukogu ettepanekut integreerida see kontseptsioonitõend (kui keskus osutub edukaks teabekoordineerimiskeskuseks) alates 2025. aastast ELi küberkaitse koordineerimiskeskusesse (EUCDCC), et tõhustada koordineerimist ja olukorrateadlikkust, eelkõige ELi ÜJKP missioonide ja operatsioonide ülemate puhul, ning ELi laiema juhtimise ühendstruktuuri tugevdamist. Nõukogu kutsub kõrget esindajat üles esitama kontseptsiooni ja tegevuskava EUCDCC loomiseks, tuginedes sarnastelt rahvusvahelistelt üksustelt saadud kogemustele, tehes kindlaks vajalikud ressursid, vältides tarbetut dubleerimist ja püüdes saavutada vastastikuse täiendavuse laiema ELi küberturvalisuse raamistikuga.

13. Nõukogu tõstab esile küberohtude ja -tegevuse alase strateegilise luurekoostöö tähtsust ning kutsub liikmesriike üles jätkama oma pädevate asutuste kaudu panustamist ELi luure- ja situatsioonikeskuse, Euroopa Liidu sõjalise staabi luuredirektoraadi ning liikmesriikide töösse ühtse luureandmete analüüsivõime (SIAC) raames. Lisaks tõstab nõukogu esile tõsiasja, et on oluline tugevdada meie küberluurealast suutlikkust, parandamaks meie küberkerksust ja reageerimist ning toetamaks tulemuslikult meie ÜJKP tsiviil- ja sõjalisi missioone ja operatsioone, samuti meie relvajõude ja SIACi suutlikkust kübervaldkonnas, tuginedes liikmesriikide vabatahtlikele luurealastele panustele, piiramata seejuures nende pädevust.

14. Nõukogu võtab teadmiseks Euroopa Komisjoni küberolukorra ja -analüüsi keskuse, mille eesmärk on suurendada komisjoni olukorrateadlikkust. Nõukogu rõhutab, et selle keskuse ja teiste ELi institutsioonide, organite ja asutuste, eelkõige Euroopa Liidu Küberturvalisuse Ameti (ENISA) ja Euroopa Liidu institutsioonide, organite ja asutuste infoturbeintsidentidega tegeleva rühma (CERT-EU) vahel on oluline tagada vastastikku kasulik koostöö. Nõukogu toonitab, et olukorrateadlikkuse arendamisel on oluline tagada tihe koostöö ELi koostöövõrgustikega ning austada konfidentsiaalsust. Nõukogu märgib, et on vaja tugevdada ühist olukorrateadlikkust ELi tasandil ja arendada edasi ELi küberturvalisuse kriisireguleerimise raamistikku, vältides samal ajal jõupingutuste tarbetut dubleerimist.

15. Nõukogu tuletab meelde, et kübervaldkonna õpe, koolitused ja õppused on valmisoleku ja tulemuslikkuse tagamiseks üliolulised, ning tervitab riiklikku tegevust, samuti tegevust, mida EL korraldab Euroopa Julgeoleku- ja Kaitsekolledži (ESDC), Euroopa Kaitseagentuuri, ENISA ja käimasolevate PESCO projektide kaudu, nagu küberharjutusväljade liidud ning ELi küberakadeemia ja innovatsioonikeskus (CAIH). Nende jõupingutuste edasiseks tõhustamiseks jääb nõukogu ootama küberkaitseõppuste sünkroniseerimiseks ja toetamiseks Euroopa Kaitseagentuuri raamprojekti CyDef-X loomist. Nõukogu julgustab Euroopa Kaitseagentuuri uurima tihedas koostöös liikmesriikide ja Euroopa välisteenistusega, kuidas CyDef-X saaks veelgi toetada selliseid õppusi nagu CYBER PHALANX, sealhulgas ELi lepingu artikli 42 lõike 7 kohase vastastikuse abi alaseid ja ELi toimimise lepingu artikli 222 kohase solidaarsusklausli alaseid õppusi, ning komisjoni ja ENISAga sama küsimust tsiviilvaldkonna õppuste osas. Lisaks julgustab nõukogu CyDef-Xis kasutama ja edasi arendama olemasolevaid küberkaitse testimis- ja õppuste keskkondi, näiteks küberharjutusväljade liite. Nõukogu toonitab, et küberkriisi korral kiire ja tõhusa otsustusprotsessi tagamiseks on oluline korraldada liikmesriikide otsustustasandi jaoks korrapäraseid lauaõppusi.

16. Nõukogu võtab teadmiseks kübersolidaarsuse määruse ettepaneku ning kavatsuse suurendada ELis küberohtude ja -intsidentide avastamise ja neile reageerimise suutlikkust. Nõukogu toonitab, et selle valdkonna ettepanekud saavad olla tulemuslikud ainult siis, kui need on kooskõlas liikmesriikide kriisiohjeraamistike ja vajadustega. Nõukogu toonitab, et elutähtsat taristut on oluline võimalike nõrkade kohtade suhtes testida, kui seda peetakse kasulikuks, riikliku pädevuse raames, võttes arvesse kättesaadavaid ELi riskihinnanguid.

17. Nõukogu võtab teadmiseks komisjoni ettepaneku luua küberhädaolukorra mehhanism, mis võiks toetada usaldusväärsete erasektori teenuseosutajate pakutavate küberturvalisuse teenuste kättesaadavust, et aidata taotluse korral liikmesriike ulatuslikele küberturvalisuse intsidentidele reageerimisel, ning toonitab samal ajal, et Euroopa küberturvalisuse tööstust, mis on kõnealuse mehhanismi toimimise oluline alustala, on vaja küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskuse (ECCC) abiga laiendada. Nõukogu toonitab iga liikmesriigi keskset rolli oma vajaduste seiramisel ja hindamisel.

II. **ELi kaitseökosüsteemi kindlustamine**

18. Nõukogu tuletab meelde, et on julgustanud liikmesriike arendama edasi oma suutlikkust korraldada küberkaitseoperatsioone, sealhulgas asjakohasel juhul ennetavaid kaitsemeetmeid küberrünnete eest kaitsmiseks, küberrünnete avastamiseks, küberrünnete vastu turvamiseks ja küberrünnetevastaseks heidutuseks. Võttes arvesse, et küberturvalisuse 2. direktiivi ei kohaldata kaitsevaldkonnas tegutsevate avalike haldusüksuste suhtes, kutsub nõukogu Euroopa Kaitseagentuuri üles aitama liikmesriikidel töötada komisjoni ja asjakohasel juhul Euroopa välisteenistuse toetusel välja õiguslikult mittesiduvad vabatahtlikud soovitused, mis on inspireeritud küberturvalisuse 2. direktiivist, et suurendada küberturvalisust kaitsevaldkonnas, ning kutsub kõiki liikmesriike üles sellealastes jõupingutustes aktiivselt osalema. Nimetatud soovitustes tuleks silmas pidada muudes raamistikes ette võetud sarnaseid jõupingutusi.

19. Strateegilises kompassis tunnistatakse, et ELi tegutsemisvõime sõltub tema võimest vähendada oma strateegilist sõltuvust küberkaitsevõime ja tarneahelate osas ning arendada eesrindlikke küberkaitsetehnoloogiaid ja omandada täielikult selliste tehnoloogiate kasutamise oskused. See hõlmab Euroopa kaitsesektori tehnoloogilise ja tööstusliku baasi (EDTIB) tugevdamist kogu ELis, samuti ELi võimekust teha sarnaselt meelestatud partneritega kogu maailmas vastastikkusel põhinevat koostööd, et tagada vastastikune kasu. Seetõttu kutsub nõukogu küberturvalisuse ja küberkaitse tööstusharusid üles tegema tihedat koostööd, et luua koostoimet eesmärgiga arendada välja ja tagada kogu spektrit kattev küberkaitsevõime. Nõukogu kutsub komisjoni üles toetama tihedas koostöös ECCCga asjakohastel juhtudel veelgi rohkem tugeva, paindliku, üleilmselt konkurentsivõimelise ja uuendusliku Euroopa küberkaitse tööstusliku ja tehnoloogilise baasi, sealhulgas väikeste ja keskmise suurusega ettevõtjate (VKEd) arendamist täiendavate investeeringute ja poliitikameetmete abil.

20. Võttes arvesse küberkaitsevõimealase koostalitlusvõime ja ühtsuse tähtsust, sealhulgas seoses järgmise põlvkonna küberkaitsevõime ühise väljaarendamisega, kutsub nõukogu Euroopa Kaitseagentuuri ja ELi sõjalist staapi üles töötama välja ELi küberkaitsevaldkonna koostalitlusvõime nõuded, mis tugineksid olemasolevatele põhimõtetele, protsessidele ja standarditele, mis on kehtestatud eelkõige Põhja-Atlandi Lepingu Organisatsiooni (NATO) raamistikus, ning oleksid nendega kooskõlas. Lisaks kutsub nõukogu liikmesriike üles uurima Euroopa kaitsestandardite komitee raames, kas kaitsesüsteemide jaoks võiks olla tarvis konkreetseid vabatahtlikke standardeid, tehes seda tihedas koostöös kõigi asjaomaste sidusrühmadega, sealhulgas asjakohastel juhtudel Euroopa standardiorganisatsioonide ja NATOga.

21 Nõukogu tervitab komisjoni jõupingutusi esitada kava olemasolevate standardite kasutamise edendamiseks tsiviilvaldkonna küberturvalisuse ja küberkaitse rakendustes, samuti uute vabatahtlike standardite väljatöötamist. Nõukogu rõhutab, et küberturvalisuse ja küberkaitse standardid on vaja asjakohastel juhtudel ühtlustada. Nõukogu tunnistab, et sellised vabatahtlikud standardid võivad ELi küberturvalisuse ja küberkaitse tööstusharude jaoks olla kasulikud, ning kutsub tsiviil- ja kaitsevaldkonna standardimisasutusi üles tegema omavahel tihedamat koostööd.

22. Nõukogu kutsub üles töötama kiiresti välja soovitused, mis põhinevad komisjoni ja asjaomaste institutsioonide teostatud kübervaldkonnas olemasolevate turvalise side vahendite kaardistamisel. Võimaluse korral tuleks soovitused viia kooskõlla olemasolevate teabevahetuse algatustega ning võtta arvesse ka riske, mida kujunemisjärgus ja murrangulised tehnoloogiad põhjustavad praegustele krüpteerimismeetoditele.

23. Nõukogu tervitab ka esialgset tööd, mis on ette võetud riskihindamise ja -stsenaariumide asjus, mille väljatöötamisega komisjon, kõrge esindaja ning võrgu- ja infoturbe koostöörühm tegelevad nõukogu taotlusel esmalt seoses energeetika- ja telekommunikatsioonisektoriga. Nõukogu teadvustab, et ettevalmistamisel on ka sihipärased ELi sidetaristu ja -võrkude küberturvalisuse riskihindamised. Nõukogu kordab, et on äärmiselt oluline, et nii liikmesriigid kui ka ELi institutsioonid, organid ja asutused saaksid küberintsidentide võimalikest mõjudest aru ühtemoodi. Seetõttu kutsub nõukogu eespool nimetatud osalejaid üles tagama, et ELi ja asjakohasel juhul riiklikul tasandil võetaks meetmete ja toetuse kindlaksmääramisel ja prioriseerimisel arvesse riskihindamisi ja -stsenaariume ning neist johtuvaid soovitusi. Lisaks kutsub nõukogu kõiki asjaomaseid osalejaid üles võtma riskistsenaariume arvesse nii riskihindamisprotsessides kui ka küberõppuste kavandamisel.

III. **Investeeringud küberkaitsevõimesse**

24. Nõukogu julgustab liikmesriike suurendama oma investeeringuid koostalitlusvõimelise küberkaitsevõime loomiseks, säilitamiseks ja edasiarendamiseks. Nõukogu toetab vabatahtlike kohustuste väljatöötamist liikmesriikide küberkaitsevõime edasiarendamiseks, mille juures võetakse arvesse teistes raamistikes ette võetud sarnaseid jõupingutusi.

25. Nõukogu kutsub liikmesriike ja Euroopa Kaitseagentuuri üles kasutama võimearendusplaani läbivaatamise võimalust, et seada ELi tasandi koostööpõhise küberkaitse arendamiseks kõrged eesmärgid. Lisaks julgustab nõukogu liikmesriike tuginema ajakohastatud prioriteetidele ja oma PESCO raames võetud kohustustele suurendada oma osalemist ELi küberkaitsevõime arendamise koostööprojektides, tunnistades, et ELi tasandi koostööprojektid aitavad otseselt toetada riikliku küberkaitsevõime arendamist.

26. Nõukogu tervitab teadusalast ELil tasandil tehtavat koostööd, et uurida kujunemisjärgus ja murranguliste tehnoloogiate võimalikke rakendusi kaitsealastes süsteemides, ning märgib ka vajadust tagada, et sellised edasiminekud tehnoloogias lõimitaks kiiresti olemasolevatesse ja tulevastesse võimetesse. Nõukogu julgustab liikmesriike ja ELi tööstussektorit kasutama parimal viisil ära võimalusi ELi tasandil teadusalase koostöö tegemiseks, näiteks Euroopa Kaitseagentuuri raamistikus, käimasolevates PESCO projektides, nagu ELi küberakadeemia ja innovatsioonikeskus (CAIH), ning Euroopa Kaitsefondi ja asjakohastel juhtudel programmi „Euroopa horisont“ ja programmi „Digitaalne Euroopa“ raames kahesuguse kasutusega projektide jaoks. Lisaks tervitab nõukogu sihtotstarbeliste raamistike, eelkõige ELi kaitseinnovatsiooni kava ja Euroopa kaitseinnovatsiooni keskuse rakendamist kaitsealase innovatsiooni toetamiseks tsiviilvaldkonna *spin-in*'e kasutades. Lisaks julgustab nõukogu ECCCd ja Euroopa Kaitseagentuuri töötama välja töökorra, millega hõlbustada asjaomaste töötajate vahel teabe vahetamist tsiviilkasutuse, kahesuguse kasutusega kaupade ja kaitsetehnoloogia prioriteetide kohta, et luua koostoimet ja vältida dubleerimist.

27. Nõukogu tervitab komisjoni kavatsust töötada koostöös Euroopa Kaitseagentuuri ja ECCCga nende vastavate volituste kohaselt, koostöös liikmesriikidega ja konsulteerides asjaomaste sidusrühmadega, näiteks tööstuse esindajatega, välja elutähtsa kübertehnoloogia tegevuskava, mis tänu elutähtsate kübertehnoloogiate ning kindlakstegemisele ning tehnoloogiate arengu ja strateegiliste sõltuvuste kaardistamisele loob võimalusi nende sõltuvuste vähendamiseks ning seega toetab ELi strateegilist autonoomiat ja tehnoloogilist suveräänsust, säilitades samal ajal avatud majanduse. Nõukogu märgib, et elutähtsa kübertehnoloogia tegevuskava võib anda teavet ELi rahastamisvahendite osas strateegiliste prioriteetide seadmiseks, olles samal ajal kooskõlas nende jaoks kehtiva korraga. Nõukogu tuletab meelde, et EL peaks ellu viima ambitsioonikat ja jõulist Euroopa tööstuspoliitikat, et luua kestlik, atraktiivne ja konkurentsivõimeline ettevõtluskeskkond, mis võib samuti võimaldada Euroopa üksustel kübervaldkonnas kasvada.

28. Nõukogu hindab kõrgelt kavatsust tegeleda küberturvalisuse oskuste märkimisväärse nappusega, meelitades ligi uusi spetsialiste, sealhulgas naisi, toetades täiendõpet ja ümberõpet ning investeerides koolitustesse ja õppustesse ning korraldades koolitusi ja õppusi, et luua mitmekesine ja kaasav kübervaldkonna töötajaskond. Tunnistades ELi ees seisvaid probleeme seoses inimkapitaliga küberturvalisuse ja küberkaitse valdkonnas, tervitab nõukogu küberturvalisusoskuste akadeemia algatust, mis võib olla kasulik ka küberkaitsetöötajatele.

29. Nõukogu kutsub liikmesriike üles vahetama teavet parimate tavade kohta, et õpetada välja kvalifitseeritud küberturvalisuse spetsialiste, võimendades sünergiat sõjaliste, tsiviil- ja õiguskaitsealgatuste vahel, ning kutsub ESDCd üles kaaluma Euroopa Kaitseagentuuri ja ENISA abiga võimalusi, kuidas tõhustada parimate tavade vahetamist ja luua täiendavat koostoimet sõjaliste ja tsiviilvaldkondade vahel seoses koolitamisega ja kübervaldkonna kaitseoskuste arendamisega.

30. Nõukogu toonitab, et küberturvalisuse tööturul esinevate puudujääkide kindlakstegemiseks ja nendega tegelemiseks on oluline omada küberturvalisuse tööjõu koosseisust ja asjaomastest oskustest ühtset arusaama ning et on vaja suhelda kõigi sidusrühmadega, sealhulgas liikmesriikidega ja tööstuse esindajatega. Nõukogu tunnistab, et küberturvalisuse tööturu seiramiseks näitajate kehtestamine aitaks teha kindlaks küberturvalisuse valdkonna oskustega seotud vajadused ja suunata rahalisi vahendeid asjakohasel viisil, andes samal ajal panuse poliitikaga seotud, eelkõige küberturvalisuse 2. direktiivist tulenevate kohustuste täitmisse. Nõukogu tervitab ettepanekut küberkaitseoskuste sertifitseerimise raamistiku kohta ning kutsub kõrget esindajat üles arendama seda ESDC juhi ametikohustuste raames koostöös Euroopa välisteenistuse, komisjoni ja liikmesriikidega tsiviilalgatuste toel.

IV. **Partner ühiste probleemide lahendamisel**

31. Nõukogu kutsub kõrget esindajat ja komisjoni üles tugevdama ja edendama oma koostööd ning uurima vastastikku kasulikke ja kohandatud partnerlusi küberkaitsepoliitika valdkonnas, sealhulgas Euroopa rahutagamisrahastu kaudu küberkaitsealase suutlikkuse suurendamise valdkonnas. Selleks tuleks küberkaitse teema lisada ELi kübervaldkonna dialoogidesse ja konsultatsioonidesse, partneritega peetavatesse üldistesse julgeoleku- ja kaitsealastesse konsultatsioonidesse. Lisaks tuleks tõhustada dialoogi ja koostööd erasektoriga. Nõukogu toonitab, et rahvusvaheline koostöö küberturvalisuse standardite ja sertifitseerimise valdkonnas annaks Euroopa tööstusele lisaväärtust. Seetõttu tervitab nõukogu komisjoni võetud kohustust muuta see ELi ning kolmandate riikide ja rahvusvaheliste organisatsioonide vaheliste kübervaldkonda käsitlevate dialoogide oluliseks osaks.

32. Nõukogu rõhutab, et rahvusvaheline koostöö on tähtis selleks, et ennetada või vähendada konfliktiohtu küberruumis, eelkõige usaldust suurendavate meetmete edasiarendamise ja rakendamise kaudu piirkondlikul ja rahvusvahelisel tasandil, sealhulgas ÜROs, ning olemasolevate usaldust suurendavate kübervaldkonna meetmete kasutamise julgustamise kaudu, näiteks Euroopa Julgeoleku- ja Koostööorganisatsioonis (OSCE), sealhulgas rahvusvaheliste pingete ajal.
EL ja selle liikmesriigid rõhutavad, et kehtivat rahvusvahelist õigust kohaldatakse ka küberruumis ning et on oluline jätkata jõupingutusi riikide vastutustundlikku käitumist käsitleva ÜRO raamistiku järgimiseks ja edendamiseks ning tööd selle rakendamise nimel, sealhulgas kehtestades tegevuskava riikide vastutustundliku käitumise edendamiseks küberruumis.

33. Kooskõlas ELi ja NATO koostööd käsitlevate ühisdeklaratsioonidega kutsub nõukogu kõrget esindajat, muu hulgas kui Euroopa Kaitseagentuuri juhti, ja komisjoni üles tugevdama, süvendama ja laiendama partnerlust NATOga kübervaldkonnas nii, et seejuures austatakse täielikult kaasatuse, vastastikkuse, vastastikuse avatuse ja läbipaistvuse põhimõtteid ning mõlema organisatsiooni sõltumatust otsuste tegemisel. Võttes arvesse vajadust tagada vastastikku täiendavad ja koordineeritud jõupingutused, milles osalevad võimalikult suurel määral liikmesriigid, kes ei ole NATO liikmed, ning vältida tarbetut dubleerimist, kutsub nõukogu üles looma asjaomastel tasanditel sidemeid ELi ja NATO vahel koolituste, hariduse, olukorrateadlikkuse, õppuste ning teadus- ja arendustegevuse platvormide valdkonnas ning otsima võimalikku koostoimet vastavate vabatahtlike kohustuste vahel seoses riikliku küberkaitsevõime arendamisega ja kriisiohjeraamistike väljatöötamisega ning elutähtsa taristu kaitsega, samuti olukorrateadlikkuse alase teabevahetuse, pahatahtlikule kübertegevusele koordineeritult reageerimise ning suutlikkuse suurendamise jõupingutuste tõhustamisega kolmandates riikides. See hõlmab tehnilise korra kokkulepet NATO küberturbeintsidentidele reageerimise üksuse (NCIRC) ja ELi infoturbeintsidentidega tegeleva rühma (CERT-EU) vahel ning tõhustatud poliitilist dialoogi küberkaitseküsimustes kõigil tasanditel.

V. **Lõppsõna**

34. Tuginedes nõukogu järeldustele ELi küberkaitsepoliitika kohta, kutsub nõukogu kõrget esindajat ja komisjoni üles töötama 2023. aasta teiseks kvartaliks välja kõnealuse poliitika rakenduskava, mille liikmesriigid peavad seejärel heaks kiitma. Samuti kutsub nõukogu liikmesriike üles andma vabatahtlikult teada oma küberkaitsealastest ambitsioonidest ja meetmetest ELi küberkaitsepoliitika kontekstis ning kasutama täielikult ära õiguslikult mittesiduvaid vabatahtlikke soovitusi ja kohustusi, et tõhustada oma riiklikke ja rahvusvahelisi küberkaitsealaseid jõupingutusi eesmärgiga maksimeerida ELi tasandil avalduvat mõju. Kõrgel esindajal, komisjonil ja liikmesriikidel palutakse hiljemalt alates 2024. aasta teisest kvartalist anda igal aastal aru ühisteatise elementide ja selle rakenduskava kohaldamisel tehtud edusammude kohta ning neid arutada.