Euroopa Liidu
Nõukogu

Brüssel, 23. mai 2022
(OR. en)

9364/22

CYBER 183	**EUMC 170**
COPEN 202	**IPCR 54**
COPS 228	**HYBRID 46**
COSI 142	**DISINFO 45**
DATAPROTECT 166	**COTER 126**
IND 189	**CSDP/PSDC 304**
JAI 698	**CFSP/PESC 685**
JAIEX 57	**CIVCOM 93**
POLMIL 120	**RECH 262**
RELEX 681	**PROCIV 65**
TELECOM 237	

MENETLUSE TULEMUS

Saatja:	Nõukogu peasekretariaat
Kuupäev:	23. mai 2022
Saaja:	Delegatsioonid
Teema:	Nõukogu järeldused Euroopa Liidu kübervaldkonna positsiooni arendamise kohta – Nõukogu poolt 23. mai 2022. aasta istungil heaks kiidetud järeldused

Delegatsioonidele edastatakse lisas nõukogu poolt 23. mai 2022. aasta istungil heaks kiidetud nõukogu järeldused Euroopa Liidu kübervaldkonna positsiooni arendamise kohta.

LISA

Nõukogu järeldused Euroopa Liidu kübervaldkonna positsiooni arendamise kohta

EUROOPA LIIDU NÕUKOGU,

TULETADES MEELDE oma järeldusi, milles käsitletakse:

– 25. juuni 2013. aasta ühisteatist Euroopa Parlamendile ja nõukogule „Euroopa Liidu küberjulgeoleku strateegia: avatud, ohutu ja turvaline küberruum,“[1]

– ELi küberkaitsepoliitika raamistikku,[2]

– interneti haldamist,[3]

– küberdiplomaatiat,[4]

– Euroopa kübervastupidavusvõime süsteemi tugevdamist ning konkurentsivõimelise ja uuendusliku küberjulgeolekusektori toetamist,[5]

– 20. novembri 2017. aasta ühisteatist Euroopa Parlamendile ja nõukogule: „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis,“[6]

– pahatahtlikule kübertegevusele ELi ühise diplomaatilise reageerimise raamistikku („küberdiplomaatia meetmete kogum“),[7]

– ELi koordineeritud reageerimist ulatuslike küberintsidentide ja kriiside korral,[8]

– ELi välise kübersuutlikkuse suurendamise suuniseid[9],

– nõukogu 11. detsembri 2018. aasta rakendusotsust (EL) 2018/1993, mis käsitleb ELi integreeritud korda poliitiliseks reageerimiseks kriisidele,[10]

---

1 12109/13.
2 15585/14.
3 16200/14.
4 6122/15 + COR 1.
5 14540/16.
6 14435/17 + COR 1.
7 10474/17.
8 10086/18.
9 10496/18.

– küberturvalisuse alase võimsuse ja suutlikkuse suurendamist ELis,[11]

– 5G tähendust Euroopa majandusele ning vajadust maandada 5G-ga seotud turvariske[12],

– 2020. aasta järgse suuresti digitaliseeritud Euroopa tulevikku: „Digitaalse ja majandusliku konkurentsivõime edendamine kogu liidus ja digitaalne sidusus“[13],

– vastupanuvõime suurendamiseks ja hübriidohtudega võitlemiseks tehtavaid täiendavaid jõupingutusi[14],

– Euroopa digituleviku kujundamist[15],

– internetiga ühendatud seadmete küberturvalisust,[16]

– ELi küberturvalisuse strateegiat digikümnendi jaoks,[17]

– julgeolekut ja kaitset,[18]

– nõukogu järeldusi ühise küberüksuse algatuse potentsiaali uurimise kohta, täiendamaks ELi koordineeritud reageerimist ulatuslike küberintsidentide ja kriiside korral,[19]

– julgeoleku- ja kaitsevaldkonna strateegilist kompassi Euroopa Liidule, kes kaitseb oma kodanikke, väärtusi ja huve ning toetab rahvusvahelist rahu ja julgeolekut,[20]

---

10 ELT L 320, 17.12.2018, lk 28–34.
11 7737/19.
12 14517/19.
13 9596/19.
14 14972/19.
15 8711/20.
16 13629/20.
17 7290/21.
18 8396/21.
19 13048/21.
20 7371/22.

1. RÕHUTAB, et nii riiklike kui ka valitsusväliste osalejate pahatahtlik käitumine küberruumis on viimastel aastatel hoogustunud, sealhulgas on järsult ja pidevalt sagenenud pahatahtlik tegevus, mis on suunatud ELi ja selle liikmesriikide elutähtsa taristu, tarneahelate ja intellektuaalomandi vastu, samuti on suurenenud ülekandumise oht ning sagenenud lunavararünded meie ettevõtete, organisatsioonide ja kodanike vastu; MÄRGIB, et võimupoliitika taastumisega püüavad mõned riigid üha enam vaidlustada ja õõnestada reeglitel põhinevat rahvusvahelist korda küberruumis, muutes kübervaldkonna koos avamere, õhu ja avakosmosega üha enam vaidlustatavaks valdkonnaks; TUNNISTAB, et süsteemset mõju põhjustavad suuremahulised küberründed või võrgu- ja infosüsteemidesse tungimise, häirimise või hävitamise katsed on üha levinumad, võivad kahjustada meie majandusjulgeolekut, mõjutada meie demokraatlikke institutsioone ja protsesse ning näidata mõnede osalejate valmisolekut seada ohtu rahvusvahelist julgeolekut ja stabiilsust; RÕHUTAB, et Venemaa sõjaline agressioon Ukraina vastu on näidanud, et ründav kübertegevus võib toimuda hübriidstrateegiate lahutamatu osana, kombineerides hirmutamist, destabiliseerimist ja majandushäireid;

2. KORDAB, et praeguste geopoliitiliste muutustega silmitsi seistes seisneb meie liidu tugevus ühtsuses, solidaarsuses ja kindlameelsuses ning et strateegilise kompassi rakendamine suurendab ELi strateegilist autonoomiat ja tema võimet teha partneritega koostööd, et kaitsta oma väärtusi ja huve, sealhulgas kübervaldkonnas; RÕHUTAB, et julgeoleku- ja kaitsevaldkonnas tugevam ja võimekam EL annab positiivse panuse ülemaailmsesse ja Atlandi-ülesesse julgeolekusse ja täiendab NATOt, mis jääb oma liikmete kollektiivkaitse aluseks; KINNITAB TAAS ELi kavatsust suurendada reeglitel põhineva rahvusvahelise korra toetamist, mille keskmes on Ühinenud Rahvaste Organisatsioon;

3. KORDAB kooskõlas ELi küberturvalisuse strateegiat käsitlevate järelduste ja strateegilise kompassiga vajadust arendada liidu kübervaldkonna positsiooni, suurendades meie suutlikkust küberründeid ennetada võimekuse arendamise, koolituste, õppuste ja suurema kerksuse kaudu ning reageerides kõiki olemasolevaid ELi vahendeid kasutades kindlalt liidu ja selle ja liikmesriikide vastu suunatud küberrünnetele. See hõlmab ka täiendava märgu andmist ELi otsusekindlusest viivitamatult ja pikaajaliselt reageerida ohusubjektidele, kes püüavad takistada meie turvalist ja avatud juurdepääsu küberruumile ning mõjutada meie strateegilisi huve, sealhulgas meie partnerite julgeolekut; RÕHUTAB sellega seoses, et kübervaldkonna positsiooni eesmärk on ühendada erinevaid algatusi, mis on kooskõlas ELi meetmetega, millega tugevdatakse rahu ja stabiilsust küberruumis ning toetatakse avatud, vaba, ülemaailmset, stabiilset ja turvalist küberruumi, koordineerides samal ajal paremini lühiajalisi, keskmise pikkusega ja pikaajalisi meetmeid küberohtude ja -rünnete ennetamiseks, heidutamiseks, ärahoidmiseks ja neile reageerimiseks, samuti kübervõimekuse suurendamiseks; TOONITAB, et kõnealused elemendid tuleks integreerida ELi kübervaldkonna positsiooni ELi kübervaldkonna viie funktsiooni kohaselt: küberkerksuse ja kaitsesuutlikkuse suurendamine; solidaarse ja tervikliku kriisijuhtimise tõhustamine; meie küberruumi käsitleva visiooni edendamine; koostöö tõhustamine partnerriikide ja rahvusvaheliste organisatsioonidega; küberrünnete ennetamine, nende eest kaitsmine ja neile reageerimine;

I. KÜBERKERKSUSE JA KAITSESUUTLIKKUSE SUURENDAMINE

4. KORDAB vajadust tõsta ELi küberturvalisuse üldist taset, JÄÄB OOTAMA, et kiiresti võetakse vastu direktiivi eelnõu, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus (küberturvalisuse 2. direktiiv), määruse eelnõu, mis käsitleb finantssektori digitaalset tegevuskerksust (DORA), direktiivi eelnõu kriitilise tähtsusega üksuste vastupidavusvõime kohta (kriitilise tähtsusega üksuste direktiiv), ning VÕTAB TEADMISEKS määruse ettepaneku, millega kehtestatakse meetmed küberturvalisuse kõrge taseme tagamiseks liidu institutsioonides, organites ja asutustes, et edendada Euroopa Liitu, mis kaitseb oma kodanikke, avalikke teenuseid ja ettevõtteid küberruumis; ERGUTAB komisjoni viima digitaristute, -tehnoloogiate, -toodete ja -teenuste turvalisuse tagamiseks lõpule peamiste ettepanekute vastuvõtmise, et anda selge signaal sellealaste ELi ambitsioonide kohta ja et ettevõtetele saaks anda toetust väljakutsega toime tulemiseks; KUTSUB komisjoni ÜLES pakkuma välja ELi ühised küberturvalisuse nõuded ühendatud seadmetele ning nendega seotud protsessidele ja teenustele küberkerksuse õigusakti abil, mille komisjon peaks esitama enne 2022. aasta lõppu ja võttes arvesse vajadust horisontaalse ja tervikliku lähenemisviisi järele, mis hõlmaks digitoodete kogu olelusringi ning kehtivaid õigusakte, eelkõige küberturvalisuse valdkonnas;

5. PALUB asjaomastel asutustel, nt elektroonilise side Euroopa reguleerivate asutuste ametil (BEREC), Euroopa Liidu Küberturvalisuse Ametil (ENISA) ning võrgu- ja infosüsteemide turvalisuse koostöörühmal, koostada koos Euroopa Komisjoniga liikmesriikide ja Euroopa Komisjoni jaoks riskihindamisel põhinevad soovitused, et suurendada sidevõrkude ja -taristute vastupidavust Euroopa Liidus, jätkates seejuures ELi 5G meetmepaketi rakendamist;

6. KUTSUB ELi ja selle liikmesriike ÜLES suurendama jõupingutusi üldise küberturvalisuse taseme tõstmiseks, hõlbustades näiteks usaldusväärsete küberturvalisuse teenuste osutajate teket ning RÕHUTAB, et selliste teenuseosutajate arengu soodustamine peaks olema ELi küberturvalisuse valdkonna tööstuspoliitika prioriteet. Selleks et paremini vastu seista võimaliku süsteemse mõjuga küberrünnetele ja nende vastu võidelda, tuginedes seejuures Solarwindsi, Microsoft Exchange'i ja Apache Log4J haavatavuste käsitlemisel saadud kogemustele, KUTSUB komisjoni ÜLES esitama ettepanekuid võimaluste kohta, millega ergutada usaldusväärse küberturvalisuse teenuste sektori teket, tugevdada IKT tarneahela küberturvalisust, tegeleda tarkvara haavatavuste võimaliku mõjuga ELi ja selle liikmesriikide jaoks, sealhulgas pidades silmas tulevast küberkerksuse õigusakti, ning parandada küberohtude avastamise ja jagamise suutlikkust liikmesriikides ja nende vahel;

7. KINNITADES TAAS, et investeerimine innovatsiooni ning tsiviiltehnoloogia parem kasutamine on meie tehnoloogilise suveräänsuse suurendamise võti, sealhulgas kübervaldkonnas, KUTSUB komisjoni ÜLES tegema küberturvalisuse valdkonna Euroopa pädevuskeskus kiiresti operatiivseks, et töötada välja tugev Euroopa küberuuringute, tööstuse ja tehnoloogia ökosüsteem**,** RÕHUTAB vajadust hoogustada teadusuuringuid ja innovatsiooni ning investeerida rohkem tsiviil- ja kaitsevaldkondadesse, et tugevdada ELi kaitsesektori tehnoloogilist ja tööstuslikku baasi (EDTIB) ning arendada ELi ja selle liikmesriikide kübervõimekust, sealhulgas strateegilist toetusvõimekust; RÕHUTAB, kui oluline on kasutada intensiivselt uusi, eelkõige kvantandmetöötluse, tehisintellekti ja suurandmete tehnoloogialahendusi, et saavutada suhtelisi eeliseid, sealhulgas küberreageerimisoperatsioonide valdkonnas;

8. TUNNISTADES, et meie küberturvalisuse edendamine on viis, kuidas suurendada meie jõupingutuste tõhusust ja turvalisust maismaal, õhus, merel ja avakosmoses, RÕHUTAB, kui oluline on küberturvalisusega seotud kaalutluste integreerimine kõikidesse ELi avaliku sektori poliitikavaldkondadesse, sealhulgas küberturvalisuse 2. direktiivi täiendavatesse valdkondlikesse õigusaktidesse, ning KUTSUB komisjoni ÜLES uurima võimalusi küberturvalisuse suurendamiseks ELi kaitsesektori tehnoloogilise ja tööstusliku baasi (EDTIB) kogu tarneahelas;

9. TUNNISTAB, et piisavate rahaliste ja inimressursside tagamine küberturvalisuse jaoks ning meetmed, mille eesmärk on luua erasektori konkurentsivõimelisust soodustav keskkond, on ELi kübervaldkonna positsiooni arendamiseks olulised ning et küberturvalisuse stabiilse ja pikaajalise rahastamise küsimusega tuleks tegeleda ka ELi tasandil, töötades välja ja rakendades horisontaalset mehhanismi, milles on ühendatud mitu rahastamisallikat, hõlmates ka kõrge kvalifikatsiooniga inimressursiga seotud kulusid; KUTSUB seetõttu komisjoni ÜLES uurima enne 2022. aasta lõppu võimalusi sellise mehhanismi loomiseks, mida hakatakse arutama asjaomastes nõukogu organites;

10. RÕHUTAB vajadust tugevdada jõupingutusi ja suurendada koostööd võitluses rahvusvahelise küberkuritegevuse, eelkõige lunavara vastu, kasutades selleks EMPACTi (kuritegevusega seotud ohte käsitlev valdkondadevaheline Euroopa platvorm) mehhanismi, vahetades teavet küberturvalisuse, õiguskaitse ja diplomaatiliste sektorite vahel ning suurendades õiguskaitsealast võimekust küberkuritegevuse uurimisel ja selle eest vastutusele võtmisel; KORDAB oma kohustust teavitada üldsust küberohtudest ning kõnealuste ohtude vastu riiklikul ja ELi tasandil võetud meetmetest, kaasates kodanikuühiskonda, erasektorit ja akadeemilisi ringkondi, et suurendada teadlikkust ning soodustada küberkaitse ja küberhügieeni tõstmist asjakohasele tasemele; RÕHUTAB vajadust keskenduda ELi ja liikmesriikide tasandil kodanike küberturvalisusega seotud oskustele ja võimetele ning vajadust kaasata kasutajaid hoolitsema aktiivselt oma turvalisuse eest;

II. SOLIDAARSE JA TERVIKLIKU KRIISIJUHTIMISE TÕHUSTAMINE

11. RÕHUTAB, tuginedes iga-aastastele küberõppustele, muudele kübermõõdet hõlmavatele õppustele ning õppusele EU CyCLES 2022, kui oluline on luua korrapäraste kogukondadevaheliste ja mitmetasandiliste küberõppuste programm, et testida ja arendada ELi-sisest ja -välist reageerimist ulatuslikele küberintsidentidele; programmis osalevad nõukogu, Euroopa välisteenistus, komisjon ja asjaomased sidusrühmad, nt ENISA ja erasektor, ning seda arendatakse edasi ja sellega antakse panus ELi üldisesse õppuste poliitikasse; RÕHUTAB õppuste Cyber Europe'i ja BlueOLExi edasiarendamise tähtsust, kombineerides eri tasanditel reageerimist; TUNNISTAB vajadust hinnata ja konsolideerida olemasolevaid õppusi ning uurida võimalusi täiendavateks õppusteks kübervaldkonna konkreetsetes segmentides, eelkõige CERTi sõjalist õppust ning ELi institutsioonide ja ametite vahelisele kriisikoostööle suunatud õppust; TUNNISTAB, et liidu kübervaldkonna positsioon tugevdab meie suutlikkust ennetada küberründeid mitmesuguste meetmete, sealhulgas koolituse abil, ning KUTSUB seetõttu liikmesriike ÜLES tõhustama tsiviil-sõjalist koostööd küberkoolituste ja ühisõppuste valdkonnas;

12. TOONITAB vajadust täiendavalt testida ja tugevdada operatiivkoostööd ja ühist olukorrateadlikkust liikmesriikide vahel, sealhulgas selliste väljakujunenud võrgustike kaudu nagu CSIRTide võrgustik ja küberkriisi kontaktasutuste võrgustik (EU - CyCLONe), et edendada ELi valmisolekut tulla toime ulatuslike küberintsidentidega; TOONITAB, kui oluline on töötada liikmesriikide ja ELi institutsioonide ja ametite vahel välja ühine, poliitilisel tasandil toimuvaks aruteluks kohandatud keelekasutus, et soodustada konsolideeritud hinnangu koostamist asjaomaste küberintsidentide tõsiduse ja mõju ning vajaduse korral võimalike arengustsenaariumide ja nendest tulenevate vajaduste kohta; RÕHUTAB sellega seoses vajadust parandada ühiste olukorra hindamise aruannete (sealhulgas EU - CyCLONe aruanded laiaulatuslike küberintsidentide mõju ja tõsiduse kohta ELi liikmesriikides ning ELi küberdiplomaatia meetmete kogumi raames ELi luure- ja situatsioonikeskuse EU INTCEN poolt esitatavad ohuhinnangud) vastastikust täiendavust; KUTSUB komisjoni, kõrget esindajat ning võrgu- ja infoturbe koostöörühma ÜLES viima koostöös asjaomaste tsiviil- ja sõjaväeorganite ja ametite ning väljakujunenud võrgustike, sealhulgas EU - CyCLONe'ga 2022. aasta lõpuks läbi riskihindamise ja koostama küberturvalisusealased riskistsenaariumid olukorraks, kus liikmesriigid või partnerriigid on ohustatud või võimaliku rünnaku all, ning esitama need asjaomastele nõukogu organitele; RÕHUTAB vajadust asjakohase ja koordineeritud üldsuse teavitamise järele ELi reageerimise kohta ulatuslikele küberintsidentidele;

13. RÕHUTAB, et ulatusliku küberintsidendi korral on vaja tugevdada koordineerimist ja asjakohasel juhul meie intsidentidele reageerimise suutlikkuse vabatahtlikku koondamist liikmesriikide vahel, tuginedes seejuures PESCO küberturbe kiirreageerimisrühmade edusammudele ja tehtud tööle, võttes ühtlasi arvesse CSIRTide võrgustiku ja EU - CyCLONe tööd; TUNNISTAB, et sidemete arendamine erasektoriga võib suurendada avaliku sektori suutlikkust, võttes eelkõige arvesse kogu ELis valitsevat oskuse nappust, ning et erasektori partnerite kindlakstegemine ja koordineerimine võib ulatuslike intsidentide korral tulemust mõjutada; KUTSUB komisjoni ÜLES esitama 2022. aasta kolmanda kvartali lõpuks ettepaneku uue küberturvalisuse kiirreageerimisfondi kohta, et valmistuda põhjalikult ulatuslikeks küberintsidentideks;

14. KORDAB kooskõlas strateegilise kompassiga vajadust jätkata panustamist vastastikuse abi andmisse vastavalt Euroopa Liidu lepingu artikli 42 lõikele 7 ja solidaarsusesse vastavalt Euroopa Liidu toimimise lepingu artiklile 222, eelkõige sagedaste õppuste kaudu; RÕHUTAB sellega seoses vajadust jätkata tööd kahepoolse tsiviil- ja/või sõjalise toetuse andmiseks ja koordineerimiseks, selgitades sealhulgas välja sellise toetuse võimalusi, mida EL annab liikmesriikide selgesõnalise taotluse korral, ning asjakohaste reageerimismeetmete kindlaksmääramiseks, sealhulgas koordineeritud kommunikatsioonistrateegia koostamise kaudu, pidades silmas artikli 42 lõike 7 rakendamist; MÄRGIB, et see peaks hõlmama ka seoste uurimist olemasolevate ELi kriisiohjemehhanismide ja ELi elanikkonnakaitse mehhanismiga;

15. TOONITAB, et ELi tugevdatud kübervaldkonna positsioon nõuab side turvalisuse suurendamist ja KINNITAB sellega seoses TAAS strateegilises kompassis esitatud sellekohaseid suuniseid ning KUTSUB komisjoni ja teisi asjaomaseid institutsioone, organeid ja asutusi ÜLES kaardistama 2022. aasta lõpuks olemasolevad kübervaldkonna turvalise side vahendid, mida hakatakse arutama asjaomastes nõukogu organites ja asjakohaste koostöörühmade, nt CIRTSide võrgustiku ja EU - CyCLONe'ga;

III. KÜBERRUUMI KÄSITLEVA VISIOONI EDENDAMINE

16. TULETAB MEELDE, et küberdiplomaatia puhul järgitava ELi ühise ja tervikliku lähenemisviisi eesmärk on anda panus konfliktide ennetamisse, küberohtude leevendamisse ja suuremasse stabiilsusesse rahvusvahelistes suhetes; KINNITAB sellega seoses TAAS ELi pühendumust küberruumis ilmnevate rahvusvaheliste vaidluste lahendamisele rahumeelsete vahenditega ning rahvusvahelise õiguse, sealhulgas rahvusvahelise inimõigustealase õiguse ja rahvusvahelise humanitaarõiguse kohaldamist riikide tegevusele küberruumis; TOONITAB ELi ja selle liikmesriikide pühendumust tegutseda kooskõlas küberruumis riikide vastutustundlikku käitumist käsitlevate vabatahtlike mittesiduvate normidega, milles on kokku leppinud kõik ÜRO liikmesriigid; RÕHUTAB, kui oluline on avatud, vaba, ülemaailmne, stabiilne ja turvaline küberruum, kus kohaldatakse täielikult inimõigusi, põhivabadusi ja õigusriigi põhimõtet meie vabade ja demokraatlike ühiskondade sotsiaalse heaolu, majanduskasvu, jõukuse ja terviklikkuse tagamiseks, ning KINNITAB TAAS ELi ja selle liikmesriikide kohustust jätkata nende väärtuste ja põhimõtete edendamist; RÕHUTAB, et peamiste küberruumi sidusrühmadega peetava konstruktiivse, ausa ja avatud dialoogi jaoks mõeldud kanalite väljatöötamiseks on oluline , et küberküsimustest, sealhulgas ELi küberdiplomaatia meetmete kogumist, saaks liidu ühinemisläbirääkimiste ning nii rahvusvaheliste partnerite kui ka konkurentidega peetavate ELi strateegiliste ja poliitiliste dialoogide lahutamatu osa, ning KUTSUB samal ajal kõrget esindajat ÜLES olemasolevaid kahepoolseid küberdialooge läbi vaatama ja tegema vajaduse korral ettepaneku sarnase koostöö alustamiseks teiste riikide või asjaomaste rahvusvaheliste organisatsioonidega;

17. TULETAB MEELDE, kui oluline on mitut sidusrühma hõlmav koostöö, sest küberturvalisuse eest vastutavad ka teised sidusrühmad, eelkõige rahvusvahelistel ja piirkondlikel foorumitel tehtud soovituste ja otsuste rakendamisel; KUTSUB ELi ja selle liikmesriike ÜLES täiendavalt edendama meie küberruumi ja interneti mudelit, tuginedes mitut sidusrühma hõlmavale lähenemisviisile ja kasutades selliseid algatusi nagu Pariisi üleskutse usalduse ja turvalisuse tagamiseks küberruumis ning avaldus interneti tuleviku kohta, rõhutades küberruumi stabiilsusest tulenevat ühist kasu ja suurendades ülemaailmset teadlikkust ohtudest, mis tulenevad interneti riigikesksest ja autoritaarsest visioonist, ning KUTSUB ELi ja selle liikmesriike ÜLES veelgi tugevdama koostööd mitut sidusrühma hõlmava kogukonnaga, kasutades sealhulgas ära selliseid asjakohaseid projekte, nagu ELi välispoliitika vahendite hulka kuuluv ELi küberdiplomaatia algatus;

18. KOHUSTUB järjepidevalt osalema asjaomastes rahvusvahelistes organisatsioonides, eelkõige ÜRO esimese ja kolmanda komiteega seotud protsessides, rõhutades samas, et kehtivat rahvusvahelist õigust kohaldatakse reservatsioonideta küberruumis ja sellega seoses; RÕHUTAB, et tähtis on jätkata jõupingutuste tegemist riikide vastutustundliku käitumist käsitleva ÜRO raamistiku järgimiseks ja edendamiseks, ning RÕHUTAB, et EL ja selle liikmesriigid teevad aktiivselt tööd selle rakendamise tugevdamiseks, kehtestades sealhulgas tegevuskava riikide vastutustundliku käitumise edendamiseks küberruumis; TOONITAB, et EL ja selle liikmesriigid osalevad aktiivselt läbirääkimistel tulevase ÜRO konventsiooni üle, mis peaks toimima õiguskaitse- ja õigusasutuste tõhusa vahendina ülemaailmses küberkuritegevuse vastases võitluses, võttes täielikult arvesse selle valdkonna rahvusvaheliste ja piirkondlike vahendite olemasolevat raamistikku, eelkõige Budapesti küberkuritegevuse konventsiooni; RÕHUTAB, kui oluline on täiendavalt toetada usaldust suurendavate meetmete väljatöötamist ja kasutuselevõtmist piirkondlikul ja rahvusvahelisel tasandil ning täiendavalt ergutada olemasolevate kübervaldkonna usaldust suurendavate meetmete kasutamist OSCEs, sealhulgas rahvusvaheliste pingete ajal;

19. TULETAB MEELDE, et inimõigustel põhineva ennetava lähenemisviisi kasutuselevõtmine rahvusvaheliste standardite järgimise tagamiseks kujunemisjärgus tehnoloogiate ja interneti põhiarhitektuuri valdkonnas kooskõlas demokraatlike väärtuste ja põhimõtetega on ülioluline tagamaks, et internet jääb ülemaailmseks, killustamata ja avatuks, ning TOETAB põhimõtet, et tehnoloogia kasutamisel ja arendamisel järgitakse inimõigusi ja eraelu puutumatust ning et selle kasutus on seaduslik, ohutu ja eetiline; ERGUTAB kõrget esindajat ja komisjoni töötama välja strateegilist visiooni digivaldkonna tehniliste küsimuste kohta, millel on välispoliitiline mõju ning mis võivad mõjutada küberruumi ja eelkõige interneti stabiilsust, sealhulgas spetsialiseerunud rahvusvahelistes organisatsioonides (nt Rahvusvaheline Telekommunikatsiooni Liit);

IV. KOOSTÖÖ TÕHUSTAMINE PARTNERRIIKIDE JA RAHVUSVAHELISTE ORGANISATSIOONIDEGA

20. RÕHUTAB vajadust siduda ELi kübersuutlikkuse suurendamise strateegia paremini ÜRO normidega, mis käsitlevad riikide vastutustundlikku käitumist küberruumis, töötades sealhulgas välja kohandatud koostöö- ja suutlikkuse suurendamise programme, et toetada kolmandaid riike nende rakendamispüüdlustes, jätkates ja laiendades seejuures meetmeid, millega edendada riikide vastutustundlikku küberkäitumist edendavat ÜRO tegevusprogrammi; RÕHUTAB, kui oluline on täielikult integreerida kübersuutlikkuse suurendamine ELi kui julgeoleku tagaja pakkumisse, koordineerides asjakohaselt liikmesriikide ning ELi institutsioonide, organite ja asutuste meetmeid, ning PEAB eriti TERVITATAVAKS koostööd nii liikmesriikide vahel kui ka avaliku ja erasektori partneritega, eelkõige ELi kübersuutlikkuse suurendamise võrgustiku EU CyberNeti ja kübervaldkonna erialateadmiste üleilmse foorumi (GFCE) kaudu, et tagada koordineerimine ja vältida dubleerimist;

KUTSUB kõrget esindajat ja komisjoni ÜLES looma 2022. aasta kolmandaks kvartaliks *kübersuutlikkuse suurendamise nõukogu* ja pidama horisontaalses küberküsimuste töörühmas korrapärast mõttevahetust; KUTSUB komisjoni ja kõrget esindajat ÜLES senisest enam kasutama ära naabruspiirkonna, arengu- ja rahvusvahelise koostöö instrumenti, ühinemiseelse abi rahastamisvahendit (IPA III) ja muid rahastamisvahendeid, nt Euroopa rahutagamisrahastut ja algatust Global Gateway, et toetada meie partnerite vastupanuvõime tugevdamist, nende suutlikkust küberohtusid tuvastada ja nendega tegeleda ning

küberkuritegusid uurida ja nende eest vastutusele võtta, samuti koostööprojektide arendamist, kaasa arvatud kriiside kontekstis; INNUSTAB eelkõige koostöö tegemist Lääne-Balkani ning ELi ida- ja lõunanaabruse partneritega, samuti ELi ja liikmesriikide ekspertide lähetamist, et pakkuda küberkriisides tuge, võttes arvesse olemasolevaid õiguslikke volitusi;

21. RÕHUTAB vajadust teha rohkem jõupingutusi, et kujundada struktureeritud ja avatud ELi teavitustegevuse lähenemisviis selle suhtes, kuidas edendada üleilmset ühist arusaama rahvusvahelise õiguse kohaldamisest küberruumis, riikide vastutustundliku käitumist küberruumis käsitlevat ÜRO raamistikku, sealhulgas algatust tegevuskava koostamiseks riikide vastutustundliku käitumise edendamiseks küberruumis, ning samuti ELi ja selle liikmesriikide seisukoha suhtes käimasolevatel läbirääkimistel ÜRO küberkuritegevuse konventsiooni üle, ning PALUB kõrgel esindajal kõnealuste jõupingutuste osana esitada nõukogule teavituskava 2022. aasta lõpuks; ERGUTAB kõrget esindajat ja komisjoni talitusi kasutama täielikult ja süstemaatiliselt ära oma 145 delegatsiooni ning arendama kavandatava ELi küberdiplomaatia võrgustiku egiidi all korrapärast ja viljakat koostööd nende ja kolmandates riikides asuvate liikmesriikide saatkondade vahel; KUTSUB kõrget esindajat ÜLES moodustama 2022. aasta kolmandaks kvartaliks ELi küberdiplomaatia võrgustiku, mis edendab teabevahetust, ELi ja liikmesriikide töötajate ühist koolitust, sidusaid suutlikkuse suurendamise meetmeid ning tugevdab riikide vastutustundlikku käitumist käsitleva ÜRO raamistiku rakendamist ja liikmeriikidevahelisi usaldust suurendavaid meetmeid;

22. RÕHUTAB oma pühendumust täiendavale koostööle rahvusvaheliste organisatsioonide ja partnerriikidega, et edendada ühist arusaama küberohtudest, arendada koostöömehhanisme ja teha proaktiivselt kindlaks koostööl põhinevaid diplomaatilisi lahendusi; TULETADES MEELDE ELi ja NATO küberturvalisuse alase koostöö peamisi saavutusi 2016. aasta Varssavi ja 2018. aasta Brüsseli ühisdeklaratsioonide rakendamise raames, austades täielikult mõlema organisatsiooni sõltumatust otsuste tegemisel ja nende menetlusi ning tuginedes läbipaistvuse, vastastikkuse ja kaasatuse põhimõtetele, RÕHUTAB vajadust veelgi tugevdada NATOga tehtavat küberkoostööd õppuste, teabe jagamise ja ekspertide vahetuse kaudu, sealhulgas seoses võimekuse arendamise, partnerite suutlikkuse suurendamise, missioonide ja operatsioonide, samuti rahvusvahelise õiguse ja riikide vastutustundlikku käitumist küberruumis käsitlevate ÜRO normide kohaldatavuse ning võimaliku koordineeritud reageerimisega pahatahtlikule kübertegevusele;

V. KÜBERRÜNNETE ENNETAMINE, NENDE EEST KAITSMINE JA NEILE REAGEERIMINE

23. TUNNISTAB, et küberruum on muutunud geopoliitilise konkurentsi areeniks, ja KORDAB seetõttu, et EL peab olema suuteline küberrünnetele, nt ELi ja selle liikmesriikide vastu suunatud riiklikult toetatavale pahatahtlikule kübertegevusele, kiiresti ja jõuliselt reageerima ning peab seetõttu tugevdama ELi küberdiplomaatia meetmete kogumit ja kasutama täiel määral ära kõiki selle vahendeid, sealhulgas olemasolevaid poliitilisi, majanduslikke, diplomaatilisi, õiguslikke ja strateegilisi kommunikatsioonivahendeid, et pahatahtlikku kübertegevust ennetada, heidutada, ära hoida ja sellele reageerida; RÕHUTAB, et vaenulikud osalejad peavad olema teadlikud sellest, et liikmesriikide ja ELi institutsioonide vastu suunatud küberründed avastatakse varakult, tuvastatakse kiiresti ning et neile reageeritakse kõigi vajalike vahendite ja poliitikatega; tuginedes eelkõige nendes sisalduva kübervaldkonna positsiooni elementidele ning kogemustele, mis on saadud küberdiplomaatia meetmete kogumi rakendamisest alates selle algatamisest ja EU CyCLES õppustest, KUTSUB liikmesriike ja kõrget esindajat ÜLES töötama komisjoni toetusel 2023. aasta esimese kvartali lõpuks välja ELi küberdiplomaatia meetmete kogumi rakendussuuniste muudetud versiooni, eelkõige uurides täiendavaid reageerimismeetmeid;

24. RÕHUTAB vajadust vahetada korrapäraselt teavet küberohtude keskkonna kohta nõukogu asjaomastes organites ja komiteedes, tehes samal ajal korrapäraselt koostööd erasektoriga ning tuginedes hiljutiste intsidentide mõju ja tõsiduse hindamisele, et suurendada üldist teadlikkust ja valmisolekut ELi küberdiplomaatia meetmete kogumi edasiseks kohaldamiseks ning töötada välja täiendavaid vahendeid selle rakendamise toetamiseks; kuigi riiklik julgeolek jääb iga liikmesriigi ainuvastutusse, MÄRGIB vajadust tugevdada luureandmete ja teabe jagamist ning koostööd nii liikmesriikide vahel kui ka ELi luure- ja situatsioonikeskusega EU INTCEN, et oleks võimalik jagada luureandmeid otsustusprotsessi alguses, sealhulgas omistamise küsimuses, ning seega võimaldada kiiret, tõhusat ja põhjendatud reageerimist ELi ja selle partnerite vastu suunatud pahatahtlikule kübertegevusele; KORDAB, kui oluline on tugevdada EU INTCENi suutlikkust kübervaldkonnas, tuginedes liikmesriikide vabatahtlikele luurealastele panustele, piiramata seejuures nende pädevust, ning kaaluda ettepanekut luua liikmesriikide küberluure töörühm;

25. TUNNISTADES, et ELi küberdiplomaatia meetmete kogumi raames tehtud ELi deklaratsioonid ja kehtestatud piiravad meetmed on saatnud tugeva sõnumi selle kohta, et ELile, selle liikmesriikidele ja partneritele välist ohtu kujutav pahatahtlik kübertegevus on vastuvõetamatu, ning aitavad seega kaasa pahatahtliku kübertegevuse ennetamisele, heidutamisele, ärahoidmisele ja sellele reageerimisele, KORDAB oma pühendumust kõnealuste meetmete kasutamisele selleks, et tuletada meelde rahvusvahelise õiguse alusel küberruumile kohaldatavaid kohustusi, sealhulgas ÜRO hartat tervikuna, ning edendada riikide vastutustundliku käitumist küberruumis käsitlevat ÜRO raamistikku, sealhulgas kõigi riikide hoolsuskohustust, mille kohaselt nad teadlikult ei võimaldaks kasutada oma territooriumi info- ja kommunikatsioonitehnoloogia abil rahvusvaheliste õigusrikkumiste toimepanemiseks, et arendada edasi ja edendada ELi ühist seisukohta rahvusvahelise õiguse kohaldamise kohta küberruumis; märkides, et asjakohased ja kiired sõnumid vähendavad eskaleerumise ohtu ja võivad heidutada ründajaid, kes on Euroopa huvid sihikule võtnud, KUTSUB kõrget esindajat ÜLES töötama välja ja esitama liikmesriikidele sidusa kommunikatsioonistrateegia ELi küberdiplomaatia kogumi kasutamise kohta;

26. INNUSTAB töötama välja järk-järgulisi, sihipäraseid ja püsivaid lähenemisviise ja reageerimist pahatahtlikule kübertegevusele, kasutades ELi küberdiplomaatia meetmete kogumis ette nähtud mitmesuguseid vahendeid, sealhulgas ELi kübersanktsioonide korda, ning kavandama lisameetmeid; RÕHUTAB vajadust suurendada võimalust võtta juhtumipõhiselt kasutusele kõik olemasolevad sisemised ja välised vahendid, et küberründe ennetada, heidutada, ära hoida ja neile reageerida, rakendades kõnealuseid vahendeid kiiresti, tõhusalt, järk-järgult, sihipäraselt ja püsivalt, lähtudes pikaajalisest strateegilisest tegevusest; KUTSUB kõrget esindajat ÜLES koostöös komisjoniga tegema kõikides valdkondades kindlaks võimalikud ELi ühised vastused küberrünnetele, sealhulgas karistusvõimalused, et olla vajaduse korral valmis võtma kiireid ja tõhusaid meetmeid, ning esitama need 2023. aasta esimese kvartali lõpuks nõukogule;

27. märkides, et küberkaitse kuulub peamiselt liikmesriikide vastutusalasse, INNUSTAB liikmesriike edasi arendama oma võimekust viia läbi küberkaitseoperatsioone, sealhulgas võtta ennetavaid meetmeid küberrünnete eest kaitsmiseks, nende avastamiseks ja ärahoidmiseks, ehk isegi teiste liikmesriikide ja ELi toetamiseks; kõiki liikmesriike ergutatakse vajaduse korral suurendama oma suutlikkust anda ja saada abi ja toetust; RÕHUTAB, et kõnealuse võimekuse edasiarendamine peaks olema ELi tulevase küberkaitsepoliitika üks põhieesmärke; MÄRGIB, et ELi küberkaitsepoliitikas tuleks rohkem võtta arvesse rolli, mida asjaomased ELi institutsioonid ja organid võivad etendada koostöö suurendamisel ELi ja liikmesriikide asjaomaste küberkaitse valdkonna osalejate vahel, samuti nende endi võimekuse arendamisel kooskõlas nende vastavate volitustega; PALUB kõrgel esindajal aidata koos komisjoniga kaasa ELi kübervaldkonna positsiooni väljatöötamisele, esitades 2022. aastal ambitsioonika ELi küberkaitsepoliitikat käsitleva ettepaneku, mis sillutaks teed ELi kübervaldkonna positsiooni edasiarendamisele nõukogus;

28. RÕHUTAB vajadust suurendada koostegutsemisvõimet ja teabevahetust sõjaliste infoturbeintsidentidega tegelevate rühmade (mil CERT) vahelise koostöö kaudu; KUTSUB liikmesriike ÜLES Euroopa Kaitseagentuuri (EDA) tehtud tööle tuginedes töötama koostöö arendamiseks ja teabevahetuse hõlbustamiseks välja mil CERTi võrgustiku, mis ühtlasi aitaks edendada koordineerimist teiste küberkogukondadega, samuti looma sõjaväe küberjuhtide võrgustiku, et tugevdada strateegilist koostööd ELi küberüksuste või muude vastavate asutuste vahel. Nimetatud võrgustike loomine ja PESCO kübervaldkonna projektid aitaksid tugevdada küberkaitset ELi tasandil; RÕHUTAB kavandatava mil CERTi võrgustiku ja juba olemasoleva tsiviilvõrgustiku (CSIRTide võrgustiku) vahelise koostöö tähtsust teabevahetuse tõhustamiseks ja olukorrateadlikkuse parandamiseks;

29. tuginedes ELi sõjalisele visioonile ja strateegiale küberruumi kui tegevusvaldkonna jaoks ning võttes teadmiseks ELi juhitavate sõjaliste operatsioonide ja missioonide küberkaitsealase sõjalise kontseptsiooni käimasolevat väljatöötamist, KINNITAB TAAS vajadust integreerida kübermõõde ÜJKP missioonide ja operatsioonide kavandamisse ja läbiviimisesse, sealhulgas nende kübervõimekuse suurendamise kaudu, ning RÕHUTAB, et see aitab parandada küberolukorrateadlikkust ELi tasandil;

30. MÄRGIB kokkuvõtteks, et kübervaldkonna positsioon on samm edasi küberruumis tegutsemist käsitleva ELi doktriini kehtestamise suunas, mis põhineb nii suuremal vastupanuvõimel, võimekusel ja parematel reageerimisvõimalustel kui ka ühisel seisukohal rahvusvahelise õiguse kohaldamise kohta küberruumis; TEEB 2023. aastal KOKKUVÕTTE käesolevate järelduste rakendamisel tehtud edusammudest, et tagada ELi kübervaldkonna positsiooni edasiarendamine.