Euroopa Liidu
Nõukogu

**Brüssel, 20. november 2017**
**(OR. en)**

**14435/17**

**CYBER 183**
**TELECOM 303**
**ENFOPOL 534**
**JAI 1055**
**MI 845**
**COSI 283**
**JAIEX 101**
**RELEX 989**
**IND 317**
**CSDP/PSDC 643**
**COPS 360**
**POLMIL 145**

**MENETLUSTE TULEMUS**

| | |
|---|---|
| Saatja: | Nõukogu peasekretariaat |
| Kuupäev: | 20. november 2017 |
| Saaja: | Delegatsioonid |
| Eelmise dok nr: | 13943/17 + COR 1 |
| Komisjoni dok nr: | 12210/17, 12211/17 |
| Teema: | Nõukogu järeldused, milles käsitletakse Euroopa Parlamendile ja nõukogule esitatud ühisteatist „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“<br>- Nõukogu järeldused (20. november 2017) |

Delegatsioonidele esitatakse lisas nõukogu järeldused, milles käsitletakse Euroopa Parlamendile ja nõukogule esitatud ühisteatist „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“, mille üldasjade nõukogu võttis vastu 20. novembril 2017.

**LISA**

**Eelnõu: nõukogu järeldused, milles käsitletakse Euroopa Parlamendile ja nõukogule esitatud ühisteatist „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“**

Euroopa Liidu Nõukogu,

1. TUNNISTADES, kui oluline on küberturvalisus ELi jõukuse, majanduskasvu ja julgeoleku tagamiseks ning meie vaba ja demokraatliku ühiskonna ja selle aluseks olevate protsesside terviklikkuse jaoks digitaalajastul, kaitstes nii õigusriigi põhimõtet kui ka iga inimese inimõigusi ja põhivabadusi;

2. RÕHUTADES vajadust käsitleda küberturvalisust riiklikul, ELi ja ülemaailmsel tasandil võetava ühtse lähenemisviisi kaudu, kuna küberohud võivad mõjutada meie demokraatiat, heaolu, stabiilsust ja julgeolekut;

3. MÄRGIB, et kübervastupidavusvõime kõrge tase kogu ELis on oluline ka selleks, et luua usaldus digitaalse ühtse turu vastu ja arendada edasi digitaalset Euroopat;

4. KORRATES, et EL jätkab avatud, ülemaailmse, vaba, rahumeelse ja turvalise küberruumi edendamist, kus nii ELi kui ka ülemaailmsel tasandil kohaldatakse ja austatakse täiel määral inimõigusi ja põhivabadusi, eeskätt sõnavabadust, juurdepääsuõigust teabele, andmekaitset, eraelu puutumatust ja turvalisust, samuti ELi põhiväärtusi ja põhimõtteid, ning RÕHUTADES, kui äärmiselt oluline on tagada asjakohane tasakaal inimõiguste ja põhivabaduste ning ELi sisejulgeolekupoliitika nõuete täitmise vahel[1];

5. TUNNISTADES, et küberruumis kehtib rahvusvaheline õigus, sealhulgas kogu ÜRO põhikiri, rahvusvaheline humanitaarõigus ja inimõigustealane õigus, ning RÕHUTADES seetõttu vajadust jätkata jõupingutusi, et tagada rahvusvahelise õiguse järgimine küberruumis;

[1] 12650/17.

6. TULETADES MEELDE oma järeldusi ELi küberjulgeoleku strateegia kohta,[2] interneti haldamise kohta,[3] Euroopa kübervastupidavusvõime tugevdamise kohta,[4] küberdiplomaatia kohta[5] ning järeldusi, mis käsitlevad ELi ühise diplomaatilise reageerimise raamistiku loomist kuritahtliku kübertegevuse suhtes,[6] samuti järeldusi küberruumi käsitleva kriminaalõigussüsteemi parandamise kohta[7], julgeoleku ja kaitse kohta ELi üldise strateegia raames[8], hübriidohtudega võitlemise ühist raamistikku[9] ning järeldusi, milles käsitletakse Euroopa Liidu sisejulgeoleku uuendatud strateegia (2015–2020) vahehindamist[10];

7. TUNNISTADES, et Euroopa Nõukogu küberkuritegevuse konventsiooni (Budapesti konventsioon) raamistik loob tugeva aluse, et mitmekesine riikide rühm saaks kasutada tõhusat õiguslikku standardit küberkuritegevust käsitlevate erinevate siseriiklike õigusaktide ja rahvusvahelise koostöö jaoks;

8. TUNNISTADES, et vaja on uuesti keskenduda 2014. aasta ELi küberkaitsepoliitika raamistiku rakendamisele ja seda ajakohastada, et veelgi enam integreerida küberturvalisus ja -kaitse ühisesse julgeoleku- ja kaitsepoliitikasse (ÜJKP) ning laiemasse julgeoleku ja kaitse tegevuskavasse;

9. TUNNISTADES, et ülemaailmselt konkurentsivõimeline Euroopa tööstus on oluline element, et saavutada küberturvalisuse kõrge tase riiklikult ja kogu ELis;

10. TULETADES MEELDE, et ELi lepingu artikli 4 lõike 2 kohaselt on riigi julgeolek iga liikmesriigi ainuvastutuses,

---

2 Dok 12109/13 ja dok 6225/13 (ühisteatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele: Euroopa Liidu küberjulgeoleku strateegia: avatud, ohutu ja turvaline küberruum (COM JOIN(2013) 1 final)).

3 Dok 16200/14 ja dok 6460/14 (komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide komiteele: Internet – põhimõtted ja juhtimine. Euroopa roll interneti haldamise tuleviku kujundamisel (COM(2014) 72 final)).

4 Dok 14540/16 ja dok 11013/16 (komisjoni teatis Euroopa Parlamendile, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide komiteele: „Euroopa kübervastupidavusvõime süsteemi tugevdamine ning konkurentsivõimelise ja uuendusliku küberjulgeolekutööstuse soodustamine“ (COM 2016(410) final)).

5 6122/15.

6 9916/17.

7 10007/16.

8 9178/17.

9 Dok 7688/16 (ühisteatis Euroopa Parlamendile ja nõukogule: Hübriidohtudega võitlemise ühine raamistik: Euroopa Liidu lahendus).

10 12650/17.

**KÄESOLEVAGA**

11. TERVITAB Euroopa Parlamendile ja nõukogule esitatud ühisteatist „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“ seoses ELi küberturvalisuse suurendamise ambitsioonika eesmärgi seadmisega. Samuti aitab see suurendada ELi strateegilist sõltumatust, nagu on osutatud nõukogu järeldustes Euroopa Liidu üldise välis- ja julgeolekupoliitika strateegia kohta[11], seades eesmärgiks luua digitaalne Euroopa, mis oleks turvalisem, usaldusväärsem, oma tugevatest külgedest teadlikum, konkurentsivõimelisem ja maailmale avatum ning austaks ELi ühiseid väärtusi avatud, vabas, rahumeelses ja turvalises ülemaailmses internetis, saavutades seeläbi suurema vastupidavusvõime küberohtude ennetamiseks, ära hoidmiseks, avastamiseks ja neile reageerimiseks ning selleks, et olla võimeline küberohuolukordadele kogu ELis ühiselt reageerima;

12. KUTSUB liikmesriike ning ELi institutsioone, ameteid ja organeid ÜLES tegema käesolevates järeldustes esitatud strateegilisi eesmärke silmas pidades koostööd, austades üksteise pädevusvaldkondi ning subsidiaarsuse ja proportsionaalsuse põhimõtet, ja

13. RÕHUTAB, et EL, selle liikmesriigid ja erasektor peavad tagama piisava rahastamise olemasolevate vahendite piires, et toetada kübervastupidavusvõime ja -turvalisuse suurendamise alast teadus- ja arendustegevust kogu ELis ning tugevdada koostööd, et ennetada, ära hoida ja avastada küberohte ning neile reageerida ning olla võimeline ühiselt reageerima ulatuslikele küberintsidentidele ja kuritahtlikule kübertegevusele kogu ELis;

---

[11] 13202/16.

**I peatükk**

**ELi TULEMUSLIKU KÜBERVASTUPIDAVUSVÕIME JA DIGITAALSE ÜHTSE TURU USALDAMISE TAGAMINE**

14. RÕHUTAB, et iga liikmesriik kannab esmast vastutust oma küberturvalisuse suurendamise ning küberturbeintsidentidele ja -kriisidele reageerimise tagamise eest, samal ajal kui EL saab pakkuda suurt lisaväärtust liikmesriikide koostöö toetamisel. Sellega seoses RÕHUTAB vajadust, et kõik liikmesriigid teeksid küberturvalisuse eest vastutavatele riiklikele ametiasutustele kättesaadavaks vajalikud ressursid, et tagada küberturbeintsidentide ja -kriiside ennetamine, avastamine ja neile reageerimine kogu ELis;

15. RÕHUTAB, et võimaluse korral on vaja kasutada ELi tasandil olemasolevaid mehhanisme, struktuure ja organisatsioone;

16. TUNNUSTAB

- liikmesriikide edusamme võrgu- ja infoturbe direktiivi ülevõtmisel ning RÕHUTAB vajadust saavutada 2018. aasta maiks selle täielik ja tulemuslik rakendamine, nagu on ette nähtud kõnealuses direktiivis[12];
- võrgu- ja infoturbe koostöörühma tööd liikmesriikidevahelise strateegilise koostöö ja teabevahetuse tõhustamisel;
- küberturbe intsidentide lahendamise üksuste võrgustiku tööd, eeskätt osas, mis tugevdab liikmesriikide operatiivkoostööd, suurendab usaldust ja kindlustunnet, kui jagatakse teavet ulatuslike küberturbeintsidentide käsitlemise korral, ning panustab liikmesriikide riiklikele järeldustele tuginedes Euroopa tasandi ühise olukorrateadlikkuse suurendamisse;
- küberturvalisuse alase lepingulise avaliku ja erasektori partnerluse kontekstis tehtud tööd;

[12] Ilma et see piiraks liikmesriikide pädevust võrgu- ja infoturbe direktiivi ülevõtmiseks, eelkõige seoses oluliste teenuste operaatoritega.

17. PEAB TERVITATAVAKS, et ühisteatises kinnitatakse, et tugev ja usaldusväärne krüpteerimine on äärmiselt oluline inimõiguste ja põhivabaduste korrektseks tagamiseks ELis ning avalikkuse usalduse jaoks digitaalse ühtse turu vastu, võttes samas arvesse õiguskaitseasutuste vajadust saada juurdepääs oma uurimiste jaoks vajalikele andmetele, ning kinnitatakse, et turvaline digitaalne tuvastamine ja suhtlus on mõlemad väga olulised tõhusa küberturvalisuse tagamiseks ELis;

18. TUNNEB HEAMEELT ühisteatises esitatud plaani üle suurendada korrapäraselt läbiviidavate üleeuroopaliste küberturvalisuse õppuste eesmärke, tuginedes Cyber Europe õppustel saadud kogemustele ja kombineerides eri tasanditel reageerimist, kuna see on oluline element, et suurendada liikmesriikide ja ELi institutsioonide valmisolekut reageerida laiaulatuslikele küberturbeintsidentidele;

19. KUTSUB ELi ja selle liikmesriike ÜLES korraldama korrapäraseid strateegilisi küberturvalisuse õppuseid erinevates nõukogu koosseisudes, tuginedes EU CYBRID 2017 õppusel saadud kogemustele, ja

20. Ilma et see piiraks õigusloome protsessi tulemusi:

- TERVITAB ettepanekut anda ENISAle tugev ja alaline volitus, mille esmane eesmärk on toetada ja arendada tihedamat koostööd liikmesriikide vahel, et suurendada nende suutlikkust ja tugevdada usaldust digitaalse Euroopa vastu;

- KINNITAB TAAS, et tulevane ENISA peaks tuginema liikmesriikide ja ELi kogemustele ja eriteadmistele ning toetama olemasolevate ja tulevaste küberturvalisust käsitlevate ELi poliitikameetmete ja õigusnormide järjepidevat edasiarendamist ja rakendamist, tagades samal ajal, et kõiki ENISA pädevusi arendatakse välja liikmesriikide pädevuste täiendamiseks;

- KINNITAB TAAS eesmärki suurendada usaldust digitaalse Euroopa vastu, suurendades usaldust ja kindlustunnet digitaalsete lahenduste ja innovatsiooni, sealhulgas asjade interneti, e-kaubanduse ja e-valitsuse suhtes, eriti maailmatasemel Euroopa küberturvalisuse sertifitseerimise raamistiku[13] osas. See on peamine eeltingimus usalduse ja turvatunde suurendamiseks digitaalsete toodete ja teenuste suhtes, kaitstes esmatähtsaid infrastruktuure ning valitsuse, kodanike ja ettevõtjate andmeid, ning aitab võtta lõimitud turvalisuse lähenemisviisi toodete, teenuste ja protsesside suhtes digitaalsel ühtsel turul;

- RÕHUTAB, et küberturvalisuse sertifitseerimise tugevdamiseks ELi tasandil tehtav seadusandlik töö peab vastama turu ja kasutajate vajadustele, põhinema sertifitseerimissuutlikkuse alal saadud kogemustel ja ELis olemasolevatel protsessidel (nt SOG-IS raamistik) ning pakkuma raamistikku, mis suudaks kiiresti kohanduda digitaalvaldkonna tulevaste arengutega;

- RÕHUTAB, et küberturvalisuse sertifitseerimise tugevdamisel ELis tuleks hõlmata kõiki turvanõudeid, sealhulgas kõige kõrgemaid, kui tuleb tõendada vastupanuvõimet ründajate suutlikkusele. Põhilisteks eduteguriteks on tagada turvalisuse sertifitseerimise usaldusväärne, läbipaistev ja sõltumatu protsess, et edendada usaldatavate ja turvaliste seadmete, tarkvara ja teenuste kättesaadavust ühtsel turul ja väljaspool seda; tunnustada Euroopa ja rahvusvaheliste standardite kaudu[14] Euroopa tööstuse, valitsuste ja hindamisspetsialistide vastavaid eriteadmisi; austada liikmesriikide rolli sertifitseerimisprotsessis, eelkõige kõrgematel turvalisustasemetel hindamise osas ja eeskätt seoses oluliste julgeolekuvajaduste ja oskuste hindamisega. Selline sertifitseerimisraamistik peaks ka tagama, et igasugune kogu ELi hõlmav sertifitseerimissüsteem on proportsionaalne asjaomaste IKT toodete, teenuste ja/või süsteemide kasutamiseks vajaliku usaldusväärsuse tasemega, ning see võimaldab igas suuruses ettevõtjatel piiriülest kauplemist, et välja töötada ja müüa uusi tooteid nii ELi sees kui ka väljaspool;

---

**13** Ülemaailmsete standardite kaudu, mis töötatakse välja kooskõlas WTO tehniliste kaubandustõkete heade tavade koodeksiga.

**14** Euroopa ja ülemaailmsete standardite kaudu, mis on välja töötatud kooskõlas WTO tehniliste kaubandustõkete heade tavade koodeksiga.

21. TERVITAB kavatsust luua küberturbe pädevuskeskuste võrgustik, et stimuleerida küberturvalisuse tehnoloogiate väljatöötamist ja kasutuselevõtmist ning anda täiendavat hoogu ELi tööstussektori innovatsioonile ülemaailmses plaanis järgmise põlvkonna ja murranguliste tehnoloogiate, näiteks tehisintellekti, kvantarvutite, plokiahela tehnoloogia ja turvaliste digitaalsete identiteetide väljatöötamisel;

22. RÕHUTAB, et küberturbe pädevuskeskuste võrgustik peab kaasama kõik liikmesriigid ja nende olemasolevad tipp- ja pädevuskeskused ning pöörama erilist tähelepanu vastastikusele täiendavusele, ning seda silmas pidades MÄRGIB ÄRA kavandatud Euroopa küberturvalisuse ja teadusuuringute keskuse, mis peaks eeskätt keskenduma vastastikuse täiendavuse tagamisele ning dubleerimise vältimisele küberturbe pädevuskeskuste võrgustikus ja muude ELi ametitega;

23. RÕHUTAB, et küberturbe pädevuskeskuste võrgustik peaks käsitlema mitmesuguseid küsimusi alates teadusuuringutest kuni tööstuseni ning aitama seega muu hulgas saavutada Euroopa strateegilise sõltumatuse eesmärki;

24. Pidades silmas kavandatavat küberturbe pädevuskeskuste võrgustikku, KINNITAB TAAS, et EL peab oma liikmesriikide kaudu töötama välja Euroopa suutlikkuse hinnata krüptograafia tugevust, mida kasutatakse kodanikele, ettevõtjatele ja valitsustele kättesaadavates toodetes ja teenustes digitaalsel ühtsel turul, tunnistades samas, et krüptograafiat käsitlevad poliitikameetmed on riikliku julgeoleku võtmetähtsusega aspekt ja kuuluvad seega liikmesriikide pädevusse;

25. KUTSUB kõiki asjaomaseid sidusrühmi ÜLES suurendama investeeringuid uue tehnoloogia rakendamisse küberturvalisuse valdkonnas, et aidata tagada küberturvalisus Euroopa kõigis majandussektorites;

26. RÕHUTAB, kui oluline on küberturvalisuse tagamise teenuste usaldusväärne, kindel ja koordineeritud osutamine ELi institutsioonide jaoks, ning KUTSUB komisjoni ja teisi ELi institutsioone ÜLES arendama edasi CERT-EU rühma vastavalt neile eesmärkidele ning tagama selleks ka piisavad vahendid;

27. TERVITAB üleskutset tunnustada kolmandatest isikutest turbeuurijate olulist rolli olemasolevate toodete ja teenuste nõrkade kohtade kindlakstegemisel ning KUTSUB liikmesriike ÜLES vahetama parimaid tavasid kooskõlastatult turvalünkadest teadaandmiseks;

28. RÕHUTAB igaühe vastutust küberturvalisuse vallas ning KUTSUB ELi ja selle liikmesriike ÜLES edendama digitaalseid oskusi ja meediapädevust, et aidata kasutajatel kaitsta oma digitaalset teavet internetis ja suurendada nende teadlikkust isikuandmete internetti panekuga seotud ohtudest;

29. TUNNEB HEAMEELT, et ühisteatises pannakse rõhku haridusele, küberhügieenile ja teadlikkusele liikmesriikides ja ELis;

30. KUTSUB KOMISJONI ÜLES esitama kiiresti mõjuhinnangu ja tegema 2018. aasta keskpaigaks ettepaneku asjakohaste õigusaktide vastuvõtmiseks, et viia ellu algatus luua küberturbe pädevuskeskuste võrgustik ning Euroopa küberturvalisuse uurimis- ja pädevuskeskus;

31. KUTSUB liikmesriike ÜLES:

- seadma küberteadlikkust esmatähtsale kohale teavituskampaaniates ning suurendama küberturvalisuse käsitlemist akadeemilistes, haridus- ja kutseõppe programmides. Erilist tähelepanu tuleks pöörata noorte haridusele ja digitaalsete oskuste suurendamisele, et kujundada tulevikus hästi hakkama saavaid spetsialiste, kes tulevad toime turvalisuse, majanduse ja teenustega seotud probleemidega;

- suurendama jõupingutusi kõrgetasemeliste küberturbealaste eriprogrammide avamiseks, et vastata praegusele küberturbespetsialistide puudusele ELis;

- looma hariduse kontaktpunktide tõhusa koostöövõrgustiku ENISA egiidi all. Selle võrgustiku eesmärk peaks olema tõhustada liikmesriikide vahel küberturvalisusalase hariduse ja teadlikkuse suurendamise, samuti koolituse, õppuste ja suutlikkuse suurendamise valdkonnas parimate tavade koordineerimist ja vahetamist;

- kaaluma võrgu- ja infoturbe direktiivi normide kohaldamist ka nende haldusasutuste suhtes, mis osalevad kriitilise tähtsusega ühiskondlikus või majandustegevuses, kui need ei ole juba hõlmatud siseriiklike õigusaktidega ja kui seda peetakse vajalikuks, ning pakkuma küberturvalisusalast koolitust ka haldusasutustele, arvestades nende rolli meie ühiskonnas ja majanduses.

**II peatükk.**

**ELi SUUTLIKKUSE SUURENDAMINE PAHATAHTLIKU KÜBERTEGEVUSE ENNETAMISEKS, TAKISTAMISEKS JA TUVASTAMISEKS NING SELLELE REAGEERIMISEKS**

32. RÕHUTAB, et eriti raske küberintsident või -kriis võib liikmesriigi jaoks olla piisav põhjus ELi solidaarsusklausli[15] ja/või vastastikuse abi klausli[16] kohaldamiseks;

33. TERVITAB pahatahtlikule kübertegevusele ELi ühise diplomaatilise reageerimise raamistiku vastuvõtmist, millega antakse panus konfliktide ennetamisse, koostöösse ja stabiilsusesse küberruumis, sätestades ÜVJP raames meetmed, sealhulgas piiravad meetmed, mida saab kasutada pahatahtliku kübertegevuse ennetamiseks ja sellele reageerimiseks ning KUTSUB Euroopa välisteenistust ja liikmesriike ÜLES viima läbi korrapäraseid õppusi seoses kõnealuse raamistikuga;

---

15 Euroopa Liidu toimimise lepingu artikkel 222.
16 Euroopa Liidu toimimise lepingu artikli 42 lõige 7.

34. RÕHUTAB vajadust reageerida ELi tasandil tulemuslikult ulatuslikele küberintsidentidele ja -kriisidele, austades samal ajal liikmesriikide pädevusi, ning vajadust integreerida küberturvalisus ELi tasandil olemasolevatesse kriisiohjemehhanismidesse[17]. KUTSUB selle saavutamiseks ÜLES korraldama korrapäraseid õppusi seoses ELi tasandil reageerimisega ulatuslikele küberintsidentidele – alates diplomaatilis-strateegilisest reageerimisest kuni tehnilise reageerimiseni –, tuginedes asjakohastele raamistikele ja menetlustele ning vajaduse korral täiustades neid[18];

35. RÕHUTAB, kui olulised on eri kogukondade, sealhulgas asjaomaste ELi asutuste ja liikmesriikide ametiasutuste vahelised hästi integreeritud reageerimis- ja teabevahetusmehhanismid, mis on otsustava tähtsusega küberturvalisuse tagamiseks Euroopas. Selliseid mehhanisme tuleb katsetada ja kontrollida ELi tasandi küberturvalisuse õppuste raames ning vormistada vajaduse korral vastavate lepingutega;

36. MÄRGIB võimalust analüüsida, kui komisjon peaks esitama ettepaneku luua küberturvalisuse kiirreageerimisfond lisaks liikmesriikide olemasolevatele jõupingutustele ja arvestades olemasolevate ressurssidega (eriti ELi mitmeaastase finantsraamistiku raames), et aidata liikmesriikidel reageerida ulatuslikele küberintsidentidele ja neid leevendada, tingimusel et liikmesriigid on enne intsidendi toimumist loonud usaldusväärse küberturvalisuse süsteemi, mis hõlmab võrgu- ja infoturbe direktiivi täielikku rakendamist, hästi väljaarendatud riskihaldust ja riikliku tasandi järelevalveraamistikke;

37. TUNNISTAB tihenevaid sidemeid küberturvalisuse ja -kaitse vahel ning KUTSUB ÜLES tugevdama koostööd küberkaitse valdkonnas, sealhulgas ergutades koostööd intsidentidele reageerivate tsiviil- ja sõjaväeliste kogukondade vahel, ning jätkama ÜJKP missioonide ja operatsioonide küberturvalisuse tugevdamist;

---

17 C(2017) 6100 final.
18 Dok 9916/17 ja C(2017)6100 final.

38. RÕHUTAB vajadust kasutada võimaluse korral kavandatud kaitsealaseid algatusi täiel määral, et kiirendada piisava kübersuutlikkuse väljatöötamist Euroopas ja TUNNISTAB võimalusi, mis peituvad küberkaitseprojektide võimalikus väljatöötamises alalise struktureeritud koostöö (PESCO) kaudu, kui seda peavad vajalikuks PESCOs osalevad liikmesriigid, ning TUNNUSTAB Euroopa kaitsesektori tehnoloogilise ja tööstusliku baasi (EDTIB) ning laiema tsiviilvaldkonna küberturvalisuse tööstusbaasi rolli, millega antakse liikmesriikidele vahendid oma kübervaldkonnaga seotud turvalisus- ja kaitsehuvide edendamiseks;

39. MÄRGIB komisjoni ettepanekut luua 2018. aastaks küberkaitsealase koolituse ja hariduse platvorm ning RÕHUTAB, et platvorm peaks laiendama koolitus- ja haridusvõimalusi liikmesriikides ning tagama täiendavuse teiste ELi jõupingutuste ja algatustega, eeskätt Euroopa Julgeoleku- ja Kaitsekolledži ning Euroopa Kaitseagentuuriga;

40. KUTSUB ELi ja selle liikmesriike ÜLES olema reageerimisvõimelised info- ja kommunikatsioonitehnoloogial põhineva intellektuaalomandi varguse ohule, mis hõlmab ärisaladuste ja muu konfidentsiaalse äriteabe varguse ohtu, eesmärgiga pakkuda ettevõtetele või kaubandussektoritele konkurentsieeliseid;

41. TUNNISTAB vajadust tegeleda kuritegevuse probleemiga küberruumis, sealhulgas pimeveebis, laste seksuaalse ärakasutamise probleemiga internetis ning mittesularahaliste maksevahenditega seotud pettuste ja võltsimisega, seades eesmärgiks luua parem luureteave, viia läbi ühiseid uurimisi ja jagada operatiivtuge;

42. TERVITAB ELi ja selle liikmesriikide tehtud tööd selliste väljakutsetega tegelemisel, mis tulenevad süsteemidest, mis võimaldavad kurjategijatel ja terroristidel suhelda viisil, millele pädevatel asutustel puudub juurdepääs; RÕHUTAB, et selle töö puhul tuleb meeles pidada, et tugev ja usaldusväärne krüpteerimine on väga oluline küberturvalisuse ning digitaalse ühtse turu usaldamise jaoks ning inimõiguste ja põhivabaduste austamise tagamiseks;

43. TOONITAB, et oluline on anda õiguskaitseasutustele vahendid, mis võimaldavad avastada ja uurida küberkuritegusid ning esitada nende eest süüdistusi, et küberruumis toime pandud kuriteod ei jääks märkamata või karistamata ning VÄLJENDAB HEAMEELT Euroopa küberkuritegevuse vastase õigusalase koostöö võrgustiku panuse üle kuritegevuse vastasesse võitlusesse õigusasutuste koostöö kaudu;

44. RÕHUTAB, et kooskõlastatud ELi seisukoha tagamine on oluline, et tulemuslikult kujundada interneti Euroopa ja ülemaailmse halduse otsuseid paljudest sidusrühmadest koosnevas kogukonnas, näiteks tagades kiirelt kättesaadavad ja täpsed WHOIS andmebaasid IP-aadresside ja domeeninimede kohta, et kindlustada õiguskaitsealase suutlikkuse ja avalike huvide kaitse;

45. RÕHUTAB IPv6 internetiprotokolli kasutuselevõtu tähtsust, mis on hädavajalik asjade interneti arenguks suures mahus ning selleks, et parandada küberruumis kuritegude toimepanijate kindlakstegemist;

46. INNUSTAB käimasolevat tööd elektroonilistele tõenditele piiriülese juurdepääsu vallas, käsitledes andmete säilitamist, ning kriminaalmenetlustele avalduvate väljakutsete vallas, mis tulenevad süsteemidest, mis võimaldavad kurjategijatel ja terroristidel suhelda viisil, millele pädevatel asutustel puudub juurdepääs, pidades silmas vajadust austada inimõigusi ja põhivabadusi ning andmekaitset;

47. KUTSUB komisjoni ÜLES:

- esitama 2017. aasta detsembriks eduaruannet praktiliste meetmete rakendamise kohta, millega parandatakse piiriülest juurdepääsu elektroonilistele tõenditele;
- esitama 2018. aasta alguses seadusandlikku ettepanekut, et parandada piiriülest juurdepääsu elektroonilistele tõenditele;

48. KUTSUB Europoli, ENISAt ja Eurojusti:

- jätkuvalt tugevdama küberkuritegevuse vastase võitluse alast koostööd nii omakeskis kui ka teiste asjakohaste sidusrühmadega, sealhulgas CSIRTide kogukonna, Interpoli, erasektori ja akadeemiliste ringkondadega, tagades sünergia ja vastastikuse täiendavuse vastavalt oma volitustele ja pädevustele;

- panustama üheskoos liikmesriikidega koordineeritud lähenemisviisi ELi õiguskaitsealaseks reageerimiseks ulatuslikele küberintsidentidele ja -kriisidele, et täiendada asjaomastes raamistikes[19] kirjeldatud menetlusi;

49. KUTSUB ELi ja selle liikmesriike ÜLES jätkama tööd, et:

- kõrvaldada takistused küberruumis toimepandavate kuritegude uurimisel ja tulemuslikul õigusemõistmisel kriminaalasjades ning suurendada rahvusvahelist koostööd ja koordineerimist kuritegevuse vastu võitlemisel küberruumis;

- tegeleda probleemidega, mis tulenevad anonümiseerimistehnoloogiast, pidades silmas, et tugev ja usaldusväärne krüpteerimine on väga oluline küberturvalisuse ja digitaalse ühtse turu usaldamise jaoks;

- kujundada interneti haldamisega seotud otsuseid, mis mõjutavad õiguskaitseasutuste suutlikkust võidelda kuritegevusega küberruumis;

[19] Dok 9916/17 ja C(2017)6100 final.

**III peatükk.**

**RAHVUSVAHELISE KOOSTÖÖ TUGEVDAMINE AVATUD, VABA, RAHUMEELSE JA TURVALISE ÜLEMAAILMSE KÜBERRUUMI NIMEL**

50. TUNNISTAB, et küberturvalisuse tagamine on ülemaailmne väljakutse, mis eeldab tulemuslikku ülemaailmset koostööd kõigi osalejate vahel, ning TUNNISTAB, et erilist rõhku tuleb asetada demokraatlike väärtuste ning avatud, vaba, rahumeelse ja turvalise ülemaailmse küberruumi põhimõtete toetamisele, ning seda silmas pidades:

51. KUTSUB ELi ja selle liikmesriike ÜLES soodustama küberruumis konfliktide ennetamist, koostööd ja stabiilsust käsitleva strateegilise raamistiku loomist, mis põhineb kehtiva rahvusvahelise õiguse ning eelkõige ÜRO põhikirja kohaldamisel tervikuna, riikide vastutustundliku käitumise üldkehtivate normide väljatöötamisel ja rakendamisel ning riikidevahelistel piirkondliku usalduse suurendamise meetmetel;

52. TUNNISTAB ÜRO rolli riikide vastutustundlikku käitumist küberruumis käsitlevate normide edasiarendamisel ja tuletab meelde, et ÜRO valitsusekspertide rühmas aastate jooksul toimunud arutelude tulemusel on sõnastatud konsensuslik normide ja soovituste kogu,[20] mida ÜRO Peaassamblee on korduvalt heaks kiitnud ning mille riigid peaksid võtma aluseks riigi vastutustundlikule käitumisele küberruumis;

53. TUNNISTAB, et need riigi vastutustundliku käitumise normid hõlmavad seda, et riik ei tohiks teadvalt lubada kasutada oma territooriumi rahvusvahelisteks õigusrikkumisteks, riik peaks reageerima teise riigi asjakohastele abitaotlustele, kui selle riigi elutähtis taristu on sattunud pahatahtliku info- ja kommunikatsioonitehnoloogiaalase tegevuse sihtmärgiks, mis lähtub taotluse saanud riigi territooriumilt ning riik peaks võtma asjakohaseid meetmeid, et kaitsta oma elutähtsat taristut info- ja kommunikatsioonitehnoloogia alaste ohtude eest;

54. TUNNISTAB ühiseid küberohte ja -riske, millega EL, NATO ja nende liikmesriigid silmitsi seisavad, ning KORDAB, et oluline on jätkata ELi ja NATO küberturvalisuse ja -kaitse koostööd, austades läbinisti selliseid põhimõtteid nagu kaasamine, vastastikkus ja ELi sõltumatus otsuste tegemisel ning kooskõlas oma 6. detsembri 2016. aasta järeldustega Euroopa Ülemkogu eesistuja, Euroopa Komisjoni presidendi ja Põhja-Atlandi Lepingu Organisatsiooni peasekretäri ühisdeklaratsiooni rakendamise kohta[20];

55. KUTSUB ELi ja selle liikmesriike ÜLES toetama ja innustama piirkondliku usalduse suurendamise meetmete väljatöötamist, mis on oluline element koostöö ja läbipaistvuse suurendamiseks ning konfliktiohu vähendamiseks. Küberturvalisuse alal usaldust suurendavate meetmete rakendamine OSCEs ja muudes piirkondlikes koosseisudes suurendab riigi käitumise ennustatavust ja aitab veelgi stabiliseerida küberruumi;

56. KORDAB, et EL jätkab oma põhiväärtuste toetamist inimõiguste ja põhivabaduste kaitsmisel, tuginedes ELi inimõigustealastele suunistele sõnavabaduse kohta internetis. EL rõhutab ka, et interneti haldamisse on oluline kaasata kõik sidusrühmad, nende seas akadeemilised ringkonnad, kodanikuühiskond ja erasektor;

57. KUTSUB ELi ja selle liikmesriike üles edendama kübersuutlikkuse suurendamist kolmandates riikides, seades esmatähtsale kohale ELi naaberriigid ja arengumaad, kus interneti kasutamine kiiresti kasvab, tegeledes küberkuritegevuse probleemiga ja luues kübervastupidavusvõimet vastavalt ELi põhiväärtustele. Selles valdkonnas ELi jõupingutuste edendamiseks tuleks välja arendada ELi kübersuutlikkuse suurendamise võrgustik ja ELi kübersuutlikkuse suurendamise suunised, mis peaksid täiendama olemasolevaid mehhanisme ja struktuure;

[20] 15283/16.

58. RÕHUTAB edusamme, mis on saavutatud ELi ja NATO küberkaitse ja -turvalisuse alases koostöös ning selle arendamises väljaõppe, hariduse ja kontseptsioonide vallas, vältides samas tarbetut topelttööd seal, kus nõuded kattuvad, samuti edendades koostalitlusvõimet küberkaitsenõuete ja -standardite kaudu ning KUTSUB ÜLES jätkama koostööd küberkaitseõppuste alal (töötajate tasandil) ning jagama häid tavasid seoses kriisiohjega, vältides samas tarbetut topelttööd seal, kus nõuded kattuvad, austades täielikult ELi õppuste läbiviimise poliitikat ning selliseid põhimõtteid nagu kaasamine, vastastikkus ja ELi sõltumatus otsuste tegemisel;

59. TUNNISTAB, et Euroopa Nõukogu küberkuritegevuse konventsioon (Budapesti konventsioon) annab toimiva õigusliku standardi, et täiendada riiklikke õigusakte küberkuritegevuse vallas; KUTSUB kõiki riike ÜLES koostama asjakohased riiklikud raamistikud ja edendama koostööd Budapesti konventsiooni pakutavas, olemasolevas rahvusvahelises raamistikus;

60. TULETAB MEELDE kahepoolsete ELi küberdialoogide pidamisel tehtud saavutusi ja kutsub üles tegema täiendavaid jõupingutusi, et lihtsustada küberturvalisuse alast koostööd kolmandate riikidega;

61. TULETAB MEELDE, et ELil on olemas stabiilne ja õiguslikult siduv ekspordikontrolli mehhanism, mis põhineb otsustel ja headel tavadel, mis on töötatud välja tuumarelva leviku tõkestamise rahvusvahelise korra raames, ning MÄRGIB nõukogus käimasolevat arutelu, mille eesmärk on leida parim viis, kuidas veelgi parandada selle kontrolli toimimist ning PALUB liikmesriikidel asjakohase rahvusvahelise ekspordikontrolli korra raames (nt Wassenaari kokkulepe) jätkata tegelemist uue tehnoloogia elutähtsate küberturvalisuse rakendustega, et tagada tulemuslik kontroll väga oluliste küberturvalisuse tulevikutehnoloogiate üle;

62. Jätkuna Euroopa Ülemkogu 19. oktoobri 2017. aasta järeldustele[21] rakendatakse käesolevaid järeldusi tegevuskava abil, mille nõukogu võtab vastu 2017. aasta lõpuks. Nõukogu vaatab tegevuskava korrapäraselt läbi pidevalt areneva dokumendina ja ajakohastab seda.

---

[21] EUCO 14/17.