Euroopa Liidu
Nõukogu

Brüssel, 9. märts 2021
(OR. en)

6722/21

CYBER 55	**RECH 86**
JAI 227	**COMPET 151**
JAIEX 23	**IND 52**
EJUSTICE 25	**COTER 25**
COSI 39	**ENFOPOL 80**
DATAPROTECT 54	**COPS 79**
COPEN 103	**MI 136**
TELECOM 88	**IXIM 43**
PROCIV 21	**POLMIL 25**
CSC 85	**HYBRID 10**
CIS 35	**CSCI 34**
RELEX 168	**POLGEN 33**

I/A-PUNKTI MÄRKUS

Saatja:	Nõukogu peasekretariaat
Saaja:	Alaliste esindajate komitee / nõukogu
Teema:	Eelnõu: nõukogu järeldused, milles käsitletakse Euroopa Liidu küberturvalisuse strateegiat digikümnendi jaoks

1. Komisjon ning liidu välisasjade ja julgeolekupoliitika kõrge esindaja avaldasid 16. detsembril 2020 ühisteatise Euroopa Parlamendile ja nõukogule „ELi küberturvalisuse strateegia digikümnendi jaoks“[1]. Uue küberturvalisuse strateegia eesmärk on tugevdada Euroopa kollektiivset küberohtudega seotud vastupidavusvõimet ning tagada, et kõik kodanikud ja ettevõtjad saaksid täiel määral kasutada usaldusväärseid ja turvalisi teenuseid ja digivahendeid.

[1] 14133/20.

2. Komisjon ja Euroopa välisteenistus tutvustasid ühisteatist horisontaalse küberküsimuste töörühma 17. detsembri 2020. aasta ja 12. jaanuari 2021. aasta mitteametlikul videokonverentsil. Töörühma 17. detsembri 2020. aasta mitteametlikul videokonverentsil teatas järgmine eesistujariik Portugal kavatsusest koostada nõukogu järelduste eelnõu, milles käsitletakse Euroopa Liidu küberturvalisuse strateegiat digikümnendi jaoks.

3. Eesistujariik esitas nõukogu järelduste esimese eelnõu horisontaalse küberküsimuste töörühma 2. veebruari 2021. aasta mitteametlikul videokonverentsil. Järeldusi arutati seejärel horisontaalse küberküsimuste töörühma mitteametlikel videokonverentsidel 9. veebruaril 2021, 19. veebruaril 2021 ning 1. ja 9. märtsil 2021.

4. Kuna järelduste eelnõu sisaldab ka viidet ELi kaitsepoliitikale (punkt 30), arutas poliitilis-sõjaline töörühm asjaomast punkti oma 10. veebruari 2021. aasta koosolekul.

5. Mitmed punktid on seotud ühise välis- ja julgeolekupoliitikaga (punktid 1, 4, 7, 8, 9, 20, 23, 24, 26, 27, 28, 29, 30, 31, 32 ja 33) ning need esitati seetõttu poliitika- ja julgeolekukomiteele, kes kinnitas nimetatud punktid oma 4. märtsi 2021. aasta koosolekul.

6. Horisontaalne küberküsimuste töörühm jõudis oma 9. märtsi 2021. aasta mitteametlikul videokonverentsil kokkuleppele dokumendis 6722/21 esitatud nõukogu järelduste eelnõu suhtes.

7. Eespool toodut arvesse võttes palutakse alaliste esindajate komiteel esitada lisas esitatud nõukogu järelduste eelnõu nõukogule ja soovitada nõukogul see oma päevakorra A-punktina vastu võtta.

LISA

Eelnõu: nõukogu järeldused, milles käsitletakse Euroopa Liidu küberturvalisuse strateegiat digikümnendi jaoks

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“,[2]

- interneti haldamist,[3]

- 20. novembri 2017. aasta ühisteatist Euroopa Parlamendile ja nõukogule „Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine ELis“,[4]

- küberturvalisuse alase võimsuse ja suutlikkuse suurendamist ELis,[5]

- 5G tähendust Euroopa majandusele ning vajadust maandada 5G-ga seotud turvariske,[6]

- 2020. aasta järgse suuresti digitaliseeritud Euroopa tulevikku: „Digitaalse ja majandusliku konkurentsivõime edendamine kogu liidus ja digitaalne sidusus“,[7]

- vastupanuvõime suurendamiseks ja hübriidohtudega võitlemiseks tehtavad täiendavaid jõupingutusi,[8]

- Euroopa digituleviku kujundamist,[9]

---

2 12109/13.
3 16200/14.
4 14435/17 + COR 1.
5 7737/19.
6 14517/19.
7 9596/19.
8 14972/19.
9 8711/20.

- digidiplomaatiat,[10]

- vastupanuvõime suurendamist ja hübriidohtude, sealhulgas desinformatsiooni vastu võitlemist COVID-19 pandeemia kontekstis,[11]

- küberdiplomaatiat,[12]

- ELi koordineeritud reageerimist ulatuslike küberintsidentide ja kriiside korral,[13]

- pahatahtlikule kübertegevusele ELi ühise diplomaatilise reageerimise raamistikku („küberdiplomaatia meetmete kogum“),[14]

- ELi välise kübersuutlikkuse suurendamise suunised,[15]

- dünaamilisemale, vastupanu- ja konkurentsivõimelisemale Euroopa tööstusele üleminekut edendavat taastamist,[16]

- internetiga ühendatud seadmete küberturvalisust,[17]

- Euroopa kübervastupidavusvõime süsteemi tugevdamist ning konkurentsivõimelise ja uuendusliku küberjulgeolekusektori toetamist,[18] ning

- nõukogu resolutsiooni krüpteerimise kohta – turvalisus krüpteerimise abil ja krüpteerimisest hoolimata,[19] ning ka

---

10 12804/20.
11 14064/20.
12 6122/15 + COR 1.
13 10086/18.
14 10474/17.
15 10496/18.
16 13004/20.
17 13629/20.
18 14540/16.
19 13084/1/20 REV 1.

- liikmesriikide 15. oktoobri 2020. aasta deklaratsiooni, milles käsitletakse järgmise põlvkonna pilve loomist ELi ettevõtjatele ja avalikule sektorile,

TULETADES MEELDE Euroopa Ülemkogu 1.–2. oktoobri 2020. aasta järeldusi, milles käsitletakse COVID-19 aspekte, ühtset turgu, tööstuspoliitikat, digiaspekte ja välissuhteid,[20] ning Euroopa Ülemkogu 20. juuni 2019. aasta järeldusi, milles käsitletakse desinformatsiooni ja hübriidohte ning uut strateegilist tegevuskava 2019–2024[21];

TULETADES MEELDE 28. juuni 2016. aasta Euroopa Liidu üldist välis- ja julgeolekupoliitika strateegiat – ühtne visioon, ühine tegevus: tugevam Euroopa;

TULETADES MEELDE Euroopa Komisjoni 19. detsembri 2020. aasta teatist „Euroopa digituleviku kujundamine“[22] ning 24. juuli 2020. aasta teatist ELi julgeolekuliidu strateegia kohta[23];

TULETADES MEELDE Euroopa Komisjoni ja kõrge esindaja 2. detsembri 2020. aasta ühisteatist ELi ja USA uue üleilmsete muutuste kava kohta[24];

1. RÕHUTAB asjaolu, et küberturvalisus on ülioluline vastupidava, keskkonnahoidliku ja digitaalse Euroopa ülesehitamiseks, ning PEAB TERVITATAVAKS ühisteatist Euroopa Parlamendile ja nõukogule „ELi küberturvalisuse strateegia digikümnendi jaoks“, milles kirjeldatakse uut raamistikku ELi tegevuseks vastupanuvõime, tehnoloogilise suveräänsuse ja juhtpositsiooni valdkonnas, samuti selleks, et kaitsta oma inimesi, ettevõtjaid ja institutsioone küberintsidentide ja -ohtude eest, suurendades samal ajal üksikisikute ja organisatsioonide usaldust seoses ELi suutlikkusega edendada turvalisi ja usaldusväärseid võrgu- ja infosüsteeme, taristut ja ühendatust ning edendada ja kaitsta üleilmset, avatud, vaba, stabiilset ja turvalist küberruumi, mis tugineb inimõigustel, põhivabadustel, demokraatial ja õigusriigil;

---

20 EUCO 13/20.
21 EUCO 9/19.
22 19.2.2020 COM(2020) 67 final.
23 24.7.2020 COM(2020) 605 final.
24 2.12.2020 JOIN(2020) 22 final.

2. TUNNISTAB, et COVID-19 pandeemia on meie igapäevaelus toonud esiplaanile suurenenud vajaduse usaldada info- ja kommunikatsioonitehnoloogia (IKT) vahendeid ja süsteeme ning nende turvalisust; RÕHUTAB, et küberturvalisus ning ülemaailmne ja avatud internet on väga olulised avaliku halduse ja institutsioonide toimimiseks nii riiklikul kui ka ELi tasandil ning meie ühiskonna ja majanduse jaoks tervikuna;

3. RÕHUTAB vajadust suurendada teadlikkust küberküsimustest poliitilisel ja strateegilisel otsustustasandil, andes otsustajatele asjakohaseid teadmisi ja teavet, ning RÕHUTAB vajadust suurendada üldsuse teadlikkust ja edendada küberhügieeni;

4. KUTSUB ÜLES edendama ja kaitsma ELi põhiväärtusi, milleks on demokraatia, õigusriik, inimõigused ja põhivabadused, sealhulgas väljendus- ja teabevabadus, õigus kogunemis- ja ühinemisvabadusele ning õigus privaatsusele küberruumis; PEAB sellega seoses TERVITATAVAKS täiendavaid püsivaid jõupingutusi selleks, et kaitsta inimõiguste kaitsjaid, kodanikuühiskonna ja akadeemiliste ringkondade esindajaid, kes tegelevad selliste küsimustega nagu küberturvalisus, andmekaitse, jälgimine ja veebitsensuur, andes täiendavaid praktilisi suuniseid, edendades parimaid tavasid ning tõhustades ELi jõupingutusi, et ennetada inimõiguste rikkumisi ning kujunemisjärgus tehnoloogia väärkasutamist, kasutades vajadusel diplomaatilisi meetmeid ja kohaldades sellise tehnoloogia puhul ekspordikontrolli; RÕHUTAB sellega seoses, kui olulised on ELi inimõiguste ja demokraatia tegevuskava 2020–2024 ning ELi inimõigustealased suunised sõnavabaduse kohta internetis ja mujal;
5. RÕHUTAB, et strateegilise sõltumatuse saavutamine, säilitades samal ajal avatud majanduse, on liidu peamine eesmärk, et määrata ise kindlaks oma majanduskurss ja huvid. Selleks tuleb muu hulgas suurendada suutlikkust teha küberturvalisuse valdkonnas sõltumatuid valikuid, et tugevdada ELi juhtpositsiooni digitaalvaldkonnas ja strateegilist suutlikkust; TULETAB MEELDE, et see hõlmab strateegilise sõltuvuse kindlakstegemist ja sellise sõltuvuse vähendamist ning vastupanuvõime suurendamist kõige tundlikumates tööstusökosüsteemides ja konkreetsetes valdkondades; RÕHUTAB, et see võib hõlmata tootmis- ja tarneahelate mitmekesistamist, investeeringute ja tootmise soodustamist ja Euroopasse meelitamist, alternatiivsete lahenduste ja ringmajanduse mudelite uurimist ning liikmesriikide laiaulatusliku majanduskoostöö edendamist;

6. tööjõu seas valitsevat digi- ja küberturvalisuse alaste oskuste nappust silmas pidades RÕHUTAB, kui oluline on rahuldada nõudlust koolitatud tööjõu järele digi- ja küberturvalisuse valdkonnas, eelkõige arendades, hoides ja meelitades ligi tipptasemel talente, nt hariduse ja koolituse kaudu, et me suudaksime oma ühiskonda digitaliseerida küberturvaliselt; INNUSTAB naiste ja tütarlaste suuremat osalemist teaduse, tehnoloogia, inseneeria ja matemaatika valdkonna (STEM) hariduses ning IKT töökohtade digioskuste alases täiendus- ja ümberõppes ühe vahendina soolise digilõhe ületamiseks;

7. 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, et on pühendunud küberruumiga seotud rahvusvaheliste vaidluste rahumeelsete vahenditega lahendamisele ning seda, et kõik ELi diplomaatilised jõupingutused peaksid esmajärjekorras olema suunatud sellele, et edendada küberruumis julgeolekut ja stabiilsust suurema rahvusvahelise koostöö kaudu, ning IKT-intsidentidest tuleneda võiva vääritimõistmis-, eskaleerumis- ja konfliktiohu vähendamisele, ning TOETAB usaldust suurendavate meetmete edasiarendamist ja kasutuselevõtmist piirkondlikul ja rahvusvahelisel tasandil; KORDAB ÜRO Peaassamblee üksmeelselt kokku lepitud üleskutset, et ÜRO liikmesriigid juhinduksid IKT kasutamisel ÜRO valitsusekspertide rühma aruannetes esitatud soovitustest, ning KINNITAB TAAS rahvusvahelise õiguse, eriti kogu ÜRO harta kohaldamist küberruumis;

8. KINNITAB TAAS, et selliste rahvusvaheliste normide ja standardite kujundamiseks, mis puudutavad kujunemisjärgus tehnoloogiat ning interneti avaliku tuuma (*public core*) üldiseks kättesaadavuseks ja usaldusväärsuseks vajalikku tehnilist ja loogilist taristut, nii et need normid ja standardid oleksid kooskõlas universaalsete ja ELi väärtustega ning mitut sidusrühma hõlmava lähenemisviisi kaudu, on normide ja standardite edasiarendamine liidus äärmiselt oluline. Sellega tagatakse, et internet jääb üleilmseks, avatuks, vabaks, stabiilseks ja turvaliseks ning et digitehnoloogia kasutamisel ja arendamisel austatakse inimõigusi ning et digitehnoloogia kasutus on seaduslik, ohutu ja eetiline; VÕTAB TEADMISEKS tulevase standardimisstrateegia ning KOHUSTUB viima läbi tarmuka ja koordineeritud teavituskampaania, et edendada ELi juhtpositsiooni ja ELi eesmärke rahvusvahelisel tasandil, sealhulgas mitmesugustes rahvusvahelistes standardiorganisatsioonides ning tehes koostööd sarnaselt meelestatud partnerite, kodanikuühiskonna, akadeemiliste ringkondade ja erasektoriga.

9. TOETAB KINDLALT mitut sidusrühma hõlmavat interneti haldamise ja küberturvalisuse mudelit ning kohustub tugevdama rahvusvahelistel foorumitel, sealhulgas küberruumiga seotud usalduse ja turvalisuse kohta tehtud Pariisi üleskutse raames toimuvat korrapärast ja struktureeritud teabevahetust sidusrühmadega, sealhulgas erasektori, akadeemiliste ringkondade ja kodanikuühiskonnaga; EDENDAB üldist, taskukohast ja võrdset juurdepääsu internetile, et ületada digitaalsed lõhed, ning eelkõige võimestada naisi ja tütarlapsi ning haavatavas või tõrjutud olukorras olevaid isikuid nii poliitika väljatöötamisel kui ka interneti kasutamisel;

10. RÕHUTAB, et küberturvalisus tuleb lähiaastatel integreerida digitaalsetesse investeeringutesse ja algatustesse ning et järjepidevalt tuleb kaasa aidata küberturvalisuse valdkonnas võrdsete tingimuste loomisele, VÕTAB samuti TEADMISEKS komisjoni kavatsuse suurendada avaliku sektori kulutusi ja võimendada erasektori investeeringuid küberturvalisuse valdkonnas; TOONITAB väikeste ja keskmise suurusega ettevõtjate (VKEde) tähtsust küberturvalisuse ökosüsteemis ning TÕDEB, et mitmeaastase finantsraamistiku 2021–2027 ning taaste- ja vastupidavusrahastu kaudu on saadaval asjakohased rahastamisvahendid, millega digipöörde raames küberturvalisust tõhusalt toetada;

11. JÄÄB OOTAMA küberturvalisuse valdkonna tööstuse, tehnoloogia ja teadusuuringute Euroopa pädevuskeskust ning riiklike koordineerimiskeskuste võrgustikku käsitleva määruse kiiret rakendamist, sealhulgas Bukarestis asuva Euroopa küberturvalisuse pädevuskeskuse kiiret rajamist ja tööle rakendamist. Selle tegevuskava kiire vastuvõtmine aitab maksimeerida investeeringute mõju, et tugevdada liidu juhtpositsiooni ja strateegilist sõltumatust küberturvalisuse valdkonnas ning toetada tehnoloogilist suutlikkust ja oskusi ning suurendada liidu ülemaailmset konkurentsivõimet küberturvalisuse sektori ja akadeemiliste ringkondade, sealhulgas VKEde ja teaduskeskuste kaasabil, mis saavad kasu süstemaatilisemast, kaasavamast ja strateegilisemast koostööst, võttes arvesse liidu ja kõigi selle liikmesriikide ühtekuuluvust;

12. TUNNEB HEAMEELT, et ENISA juhtimisel toimub koos liikmesriikide ja huvitatud sidusrühmadega töö selle nimel, et koostada ELi jaoks IKT toodete, teenuste ja protsesside sertifitseerimiskavad, mis peaksid aitama kaasa üldise küberturvalisuse taseme tõstmisele digitaalsel ühtsel turul; JÄÄB sellega seoses OOTAMA liidu jooksvat tööprogrammi, mille eesmärk on töötada küberturvalisuse määruse raames välja ELi küberturvalisuse sertifitseerimise kavad; TUNNISTAB sellega seoses ELi keskset rolli selliste standardite väljatöötamisel, millega saab küberturvalisuse keskkonda mõjutada ja mis aitavad tagada ausat konkurentsi ELis ja ülemaailmsel tasandil, edendades turulepääsu ja käsitledes turvariske, tagades samal ajal ELi õigusraamistiku kohaldatavuse;

13. KORDAB, kui oluline on hinnata pikas perspektiivis vajadust horisontaalsete õigusaktide järele, täpsustades ka vajalikud turulelaskmise tingimused, et käsitleda ühendatud seadmete küberturvalisuse kõiki asjakohaseid aspekte, nagu kättesaadavus, terviklikkus ja konfidentsiaalsus. TERVITAB sellega seoses arutelu, et uurida selliste õigusaktide kohaldamisala ja selle seoseid küberturvalisuse sertifitseerimise raamistikuga, nagu on kindlaks määratud küberturvalisuse määruses, eesmärgiga tõsta turvalisuse taset digitaalsel ühtsel turul; RÕHUTAB, et küberturvalisuse nõuded tuleks kindlaks määrata kooskõlas asjakohaste liidu õigusaktidega, sealhulgas küberturvalisuse määrusega, uue õigusraamistikuga, Euroopa standardimist käsitleva määrusega ja võimalike tulevaste horisontaalsete õigusaktidega, et vältida õigusaktide mitmetimõistetavust ja killustatust;

14. TUNNISTAB, kui oluline on liidus küberturvalisuse puhul järgida terviklikku ja horisontaalset lähenemisviisi, austades samal ajal täielikult liikmesriikide pädevusi ja vajadusi, ning kui oluline on jätkuvalt toetada tehnilist abi ja koostööd liikmesriikide suutlikkuse arendamiseks; VÕTAB küberohtude arengut arvesse võttes TEADMISEKS küberturvalisuse direktiivile tugineva uue direktiivi ettepaneku, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ning kordab oma toetust riiklike küberturvalisuse raamistike tugevdamisele ja ühtlustamisele ning liikmesriikidevahelisele püsivale koostööle; RÕHUTAB lisaks sellele vajadust kõnealuse valdkonna õigusaktide vastavusse viimise ja sidususe järele;

15. VÕTAB TEADMISEKS komisjoni ettepaneku toetada liikmesriike turbekeskuste loomisel ja tugevdamisel, et luua kogu ELis turbekeskuste võrgustik, et täiendavalt jälgida ja prognoosida signaale võrgustike vastu suunatud rünnete kohta; OOTAB sellega seoses komisjoni üksikasjalikke kavasid turbekeskuste võrgustiku kohta, austades samal ajal liikmesriikide pädevusi; TULETAB MEELDE ELi toetusel tehtud liikmesriikide jõupingutusi valdkondlike, riiklike ja piirkondlike küberturbe intsidentide lahendamise üksuste (CSIRTide) ning teabe jagamise ja analüüsimise riiklike või Euroopa keskuste loomiseks liidu küberturvalisuse partnerluste tõhusa võrgustiku osana; JÄÄB OOTAMA võimalust uurida kõnealuse võrgustiku potentsiaali turbekeskuste tugevdamiseks ning nende vastastikuse täiendavuse ja koordineerituse suurendamiseks olemasolevate võrgustike ja osalejatega (eelkõige CSIRTide võrgustikuga), et edendada tõhusat, turvalist ja usaldusväärset teabejagamiskultuuri; RÕHUTAB, et nimetatud protsess tugineb tehisintellekti ja kõrgjõudlusega andmetöötluse algatuste raames tehtud tööle ning Euroopa digitaalse innovatsiooni keskuste tööle;

16. VÕTAB TEADMISEKS Euroopa kvantkommunikatsioonitaristul (EuroQCI) ja Euroopa Liidu valitsuste satelliitsidel (GOVSATCOM) põhineva turvalise ühenduvussüsteemi võimalikku väljatöötamist ning TUNNISTAB, et mis tahes tulevane võimalik areng peaks põhinema kindlal küberturvalisuse raamistikul ja võtma arvesse kogu elektroonilise side taristut, hõlmates kosmose-, maismaa- ja veealuseid võrgusüsteeme;

17. JÄÄB OOTAMA arutelusid komisjoni, ENISA, kahe ELi domeeninimede süsteemi juurserveri operaatori ja mitut sidusrühma hõlmava kogukonnaga, et hinnata milline roll on nendel kahel ELi domeeninimede süsteemi juurserveri operaatoril selles, et internet jääks ülemaailmselt kättesaadavaks ja killustamata; PEAB TERVITATAVAKS edasist arutelu, mis on seotud komisjoni kavatsusega töötada välja alternatiivne Euroopa teenus juurdepääsuks ülemaailmsele internetile (algatus „DNS4EU“), mis põhineb läbipaistval mudelil, mis vastab viimastele turva-, andmekaitse- ja lõimprivaatsuse ning privaatsuse vaikesätete standarditele ja -normidele, et aidata suurendada vastupanuvõimet, säilitades ja tõhustades samas kõigi liikmesriikide rahvusvahelist ühendatust;

18. TUNNISTAB vajadust komisjoni ja liikmesriikide ühiste jõupingutuste järele, et kiirendada peamiste internetistandardite, sealhulgas IPv6 ning hästi toimivate internetiturvalisuse standardite kasutuselevõttu, kuna need on üliolulised ülemaailmse interneti turvalisuse, töökindluse, avatuse ja koostalitlusvõime üldise taseme tõstmiseks, suurendades samal ajal ELi tööstuse ja eelkõige internetitaristuettevõtjate konkurentsivõimet;

19. RÕHUTAB kooskõlastatud lähenemisviisi ning tõhusate meetmete väljatöötamise ja rakendamise tähtsust riiklikul tasandil 5G-võrkude küberturvalisuse tugevdamiseks; TOETAB edasisi samme 5G-võrkude küberturvalisuse valdkonnas, mis on esitatud ELi küberturvalisuse strateegia lisas ning mis põhinevad 5G-võrkude turvalisust käsitleva komisjoni soovituse mõju käsitleva aruande tulemustel, näiteks seoses kogu 5G väärtusahelat ja ökosüsteemi hõlmava pikaajalise ja tervikliku lähenemisviisi määratlemisega; selleks et veelgi tugevdada 5G-võrkude turvalisusega seotud kooskõlastatud lähenemisviisi, KUTSUB liikmesriike, ELi institutsioone ja teisi asjaomaseid sidusrühmi TUNGIVALT ÜLES jätkama oma korrapärast hindamist koos teabe ja parimate tavade vahetamisega võrgu- ja infoturbe koostöörühmas seoses töörühma spetsiaalse 5G-küberturvalisuse töösuunaga ning andma nõukogule korrapäraselt aru tehtud edusammudest; TOONITAB, rõhutades samal ajal liikmesriikide vastutust riikliku julgeoleku kaitsmise eest, oma kindlat pühendumust ELi 5G meetmepaketi meetmete kohaldamisele ja nende rakendamise kiirele lõpuleviimisele, samuti jõupingutuste jätkamisele 5G-võrkude turvalisuse tagamiseks ja võrkude tulevaste põlvkondade arendamiseks. Liikmesriikide, komisjoni ja ENISA tihe koostöö 5G-võrkude turvalisuse valdkonnas võiks olla eeskujuks muude küberturvalisuse valdkonna küsimuste puhul, austades samas liikmesriikide pädevusi ning subsidiaarsuse ja proportsionaalsuse põhimõtet;

20. TUNNISTAB, et küberturvalisuse täiendav integreerimine ELi kriisidele reageerimise mehhanismidesse ja nende testimine asjakohaste õppuste käigus on asjakohane, ning TOONITAB, kui oluline on tõhustada koostööd ja teabevahetust ELi eri küberkogukondade vahel ning ühendada ulatuslike ja piiriüleste küberintsidentide ja -ohtude puhul olemasolevad algatused, struktuurid ja menetlused (nt ELi integreeritud kord poliitiliseks reageerimiseks kriisidele (IPCR), CSIRTide võrgustik, võrgu- ja infoturbe koostöörühm, küberkriisi kontaktasutuste võrgustik (CyCLONe), küberkuritegevuse vastase võitluse Euroopa keskus, ELi luure- ja situatsioonikeskus (EU INTCEN) ja muud asjaomased ELi organid); VÕTTES ARVESSE selles valdkonnas juba tehtud edusamme, JÄÄB OOTAMA komisjoni ettepanekut ühise küberüksuse kindlaksmääramise protsessi, vahe-eesmärkide ja ajakava kohta, et pakkuda lisaväärtust ja selget fookust ning ühtlustada ELi küberturvalisuse kriisiohjeraamistikku, sealhulgas valmisoleku, ühise olukorrateadlikkuse, koordineeritud reageerimise ja õppuste tugevdamise kaudu, tehes seda läbipaistval viisil ja järk-järgult, vältides samas dubleerimist ja kattumist ning austades liikmesriikide pädevusi;

21. RÕHUTAB, kui oluline on edendada koostööd ja teabevahetust asjaomaste küberturvalisuse valdkonna osalejate ning julgeoleku ja kriminaalõiguse valdkonna pädevate asutuste, nt õiguskaitse- ja õigusasutuste vahel, samuti vajadust suurendada ja parandada nende asutuste küberkuritegude uurimise ja nende eest vastutusele võtmise suutlikkust ning rõhutab vajadust edendada rahvusvahelisi läbirääkimisi ja ELi reegleid, mis käsitlevad piiriülest juurdepääsu elektroonilistele tõenditele. Igapäevasest tehnoloogilisest keskkonnast sõltumata on äärmiselt oluline säilitada pädevate asutuste volitused julgeoleku ja kriminaalõiguse valdkonnas, andes neile seadusliku juurdepääsu oma ülesannete täitmiseks vastavalt õiguses ette nähtule ja lubatule. Sellistes täitmisvolitusi sätestavates õigusaktides tuleb alati täielikult järgida nõuetekohast menetlust ja muid kaitsemeetmeid, samuti põhiõigusi, eelkõige õigust eraelu ja -suhtluse puutumatusele ning õigust isikuandmete kaitsele;

22. KINNITAB TAAS oma toetust tugeva krüpteerimise kui põhiõiguste ning kodanike, valitsuste, tööstuse ja ühiskonna digitaalse turvalisuse kaitsmiseks vajaliku vahendi arendamisele, rakendamisele ja kasutamisele ning TUNNISTAB samal ajal vajadust tagada julgeoleku ja kriminaalõiguse valdkonna pädevate asutuste, nt õiguskaitse- ja õigusasutuste suutlikkus kasutada oma seaduslikke volitusi nii internetis kui ka mujal, et kaitsta meie ühiskondi ja kodanikke. Pädevatel asutustel peab olema andmetele seaduslik ja eesmärgipärane juurdepääs, austades täielikult põhiõigusi ja asjakohaseid andmekaitsealaseid õigusnorme ja tagades seejuures küberturvalisuse; RÕHUTAB, et kõigi võetavate meetmete puhul peavad need huvid olema hoolikalt tasakaalustatud vajalikkuse, proportsionaalsuse ja subsidiaarsuse põhimõttega;

23. TOETAB ja EDENDAB Budapesti küberkuritegevuse konventsiooni ning tööd, mida tehakse kõnealuse konventsiooni teise lisaprotokolliga; jätkab lisaks sellele osalemist mitmepoolses teabevahetuses küberkuritegevuse teemal, sealhulgas protsessides, mis on seotud Euroopa Nõukogu, ÜRO narkootikumide ja kuritegevuse büroo (UNODC) ning kuriteoennetuse ja kriminaalõigusemõistmise komisjoniga, et tagada tõhustatud rahvusvaheline koostöö küberkuritegevuse vastu võitlemisel, sealhulgas parimate tavade ja tehniliste teadmiste vahetamine ning suutlikkuse suurendamise toetamine, austades, edendades ja kaitstes samal ajal inimõigusi ja põhivabadusi;

24. TUNNISTAB, kuigi riigi julgeolek jääb iga liikmesriigi ainuvastutusse, et strateegiline luurekoostöö küberohtude ja -tegevuse vallas on väga oluline, ning KUTSUB liikmesriike ÜLES aitama oma pädevate asutuste kaudu jätkuvalt kaasa ELi küberküsimustega seotud olukorrateadlikkuse ja ohuhinnangute keskusena toimiva ELi luure- ja situatsioonikeskuse (EU INTCEN) tööle ning uurima ettepanekut liikmesriikide küberluure töörühma võimaliku loomise kohta, et tugevdada nimetatud keskuse eriotstarbelist suutlikkust kõnealuses valdkonnas, tuginedes liikmesriikide vabatahtlikele luurealastele panustele, piiramata seejuures nende pädevust;

25. TOONITAB, kui tähtis on tugev ja järjekindel julgeolekuraamistik, et kaitsta kõiki ELi töötajaid, andmeid, sidevõrke ja infosüsteeme ning otsuste tegemise protsesse, tuginedes terviklikele, järjekindlatele ja ühtsetele normidele. Eelkõige tuleks selleks edendada ELi küberohtudega seotud vastupanuvõimet ja julgeolekukultuuri ning tugevdada ELi salastatud ja salastamata võrkude turvalisust, tagades samal ajal nõuetekohase juhtimise ning piisavate vahendite ja piisava suutlikkuse kättesaadavuse, sealhulgas ELi institutsioonide ja ametite infoturbeintsidentidega tegelev rühm (CERT-EU) volituste tugevdamise kontekstis; PEAB sellega seoses TERVITATAVAKS ühiste infoturbenormide kehtestamise üle toimuvaid arutelusid, võttes nõuetekohaselt arvesse ELi salastatud teabe kaitset käsitlevaid nõukogu julgeolekueeskirju ning kõigile ELi institutsioonidele, organitele ja asutustele ühiste siduvate küberturvalisuse eeskirjade määratlemist;

26. TUGINEDES ELi jõupingutustele küberdiplomaatia vallas, VÕTAB KOHUSTUSE suurendada küberdiplomaatia meetmete kogumi tulemuslikkust ja tõhusust ning JÄÄB OOTAMA arutelude süvendamist selle kohaldamisala ja kasutamise kohta, lähtudes kõnealuse vahendi senise kohaldamise käigus saadud kogemustele. Arutelud peaksid aitama edendada julgeolekut rahvusvahelisel tasandil, soodustades dialoogi ja edendades ühist arusaama küberturvalisusega seotud küsimustest, tugevdades ennetamist, stabiilsust ja koostööd, edendades usaldust ja suutlikkuse suurendamist ning kohaldades vajaduse korral piiravaid meetmeid, et ennetada, heidutada ja tõkestada ELi ja selle liikmesriikide terviklikkuse ja julgeoleku vastu suunatud pahatahtlikku kübertegevust ja sellele reageerida, aidates seeläbi kaasa rahvusvahelisele julgeolekule ja stabiilsusele ning ELi positsiooni tugevdamisele kübervaldkonnas, austades täielikult riikide pädevusi ja eelisõigusi. Eelkõige tuleks pöörata erilist tähelepanu selliste süsteemse mõjuga küberrünnete ennetamisele ja nende vastu võitlemisele, mis võivad mõjutada meie tarneahelaid, elutähtsaid taristuid, olulisi teenuseid ning demokraatlikke institutsioone ja protsesse või kahjustada meie majanduslikku julgeolekut, hõlmates küberruumi kasutades toime pandud intellektuaalomandi vargusi. Liikmesriigid ja ELi institutsioonid peaksid samuti täiendavalt tähelepanu pöörama ELi küberturvalisuse kriisiohjeraamistike, küberdiplomaatia meetmete kogumi ning ELi lepingu artikli 42 lõike 7 ja ELi toimimise lepingu artikli 222 sätete sidususele, eelkõige stsenaariumipõhise töö kaudu, et luua ühine arusaam ELi lepingu artikli 42 lõike 7 rakendamise praktilisest korrast;

27. TUNNISTAB, kui oluline on tugevdada koostööd rahvusvaheliste organisatsioonide ja partnerriikidega, et edendada ühist arusaama küberohtudest, arendada dialooge ja koostöömehhanisme, määrata vajaduse korral kindlaks koostööl põhinevad diplomaatilised meetmed ning parandada teabe jagamist, sealhulgas hariduse, koolituse ja õppuste kaudu; TOONITAB eelkõige, et tugev Atlandi-ülene partnerlus küberturvalisuse valdkonnas aitab suurendada meie ühist julgeolekut, stabiilsust ja jõukust ning VÕTAB TEADMISEKS ELi ja Ühendkuningriigi kaubandus- ja koostöölepingus sisalduvad küberturvalisuse alase koostöö sätted; TULETADES MEELDE ELi ja NATO küberturvalisuse alase koostöö peamisi saavutusi 2016. aasta Varssavi ja 2018. aasta Brüsseli ühisdeklaratsioonide rakendamise raames; kordab taas, kui oluline on tõhustatud, vastastikku tugevdav ja kasulik koostöö hariduse, koolituse, õppuste ja pahatahtlikule kübertegevusele koordineeritud reageerimise kaudu, austades täielikult mõlema organisatsiooni sõltumatust otsuste tegemisel ja nende menetlusi, tuginedes läbipaistvuse, vastastikkuse ja kaasatuse põhimõtetele;

28. selleks et aidata kaasa ülemaailmsele, avatud, vabale, stabiilsele ja turvalisele küberruumile, mis omab meie ühiskondade jätkuva jõukuse, majanduskasvu, turvalisuse, heaolu, ühenduvuse ja terviklikkuse seisukohast üha suuremat tähtsust, KOHUSTUB pidevalt osalema rahvusvahelistes organisatsioonide raames toimuvates normide kehtestamise protsessides, eelkõige ÜRO esimese komiteega seotud protsessides, edendades ja aidates kaasa rahvusvahelise õiguse kohaldamise tunnustamisele küberruumis ning riikide vastutustundliku käitumise normide, reeglite ja põhimõtete kohaldamisele küberruumis, sealhulgas edendades riikide vastutustundliku küberruumis käitumise edendamise tegevuskava kiiret kehtestamist konstruktiivse, kaasava ja konsensusepõhise järelmeetmena ÜRO valitsusekspertide rühma ja tähtajata töörühma praegustele protsessidele;

29. TULETAB MEELDE oma kindlat pühendumust tõhusale mitmepoolsusele ja reeglitel põhinevale maailmakorrale, mille keskmes on ÜRO, ning oma otsustavust tugevdada koostööd ja koordineerimist rahvusvaheliste ja piirkondlike organisatsioonidega, nimelt ÜRO süsteemi, NATO, Euroopa Nõukogu, OSCE, OECD, Aafrika Liidu, Ameerika Riikide Organisatsiooni, ASEANi, ASEANi piirkondliku foorumi, Pärsia lahe koostöönõukogu (GCC) ja Araabia Riikide Liigaga seoses kübervaldkonna küsimusi käsitlevate aruteludega, samuti kolmandate riikidega peetavate struktureeritud ELi küberdialoogide ja konsulteerimiste jätkamisele ja laiendamisele; RÕHUTAB oma aktiivset toetust ÜRO-le, eelkõige seoses selle kestliku arengu tegevuskavaga aastani 2030, sealhulgas kestliku arengu eesmärkidega, ning PEAB TERVITATAVAKS ÜRO peasekretäri digikoostöö tegevuskava ja ÜRO peasekretäri desarmeerimiskava, millega edendatakse vastutust ja normide järgimist küberruumis ning aidatakse kaasa küberruumis toimuvast pahatahtlikust tegevusest tulenevate konfliktide ennetamisele ja rahumeelsele lahendamisele; PEAB TERVITATAVAKS liidu välisasjade ja julgeolekupoliitika kõrge esindaja ettepanekut luua mitteametlik ELi küberdiplomaatia võrgustik, et arendada nii ELi kui ka liikmesriikide osalemist ja eksperditeadmisi rahvusvahelistes küberküsimustes, et tugevdada koordineeritud teavituskampaaniat;

30. JÄÄB OOTAMA eelseisvat ettepanekut küberkaitsepoliitika raamistiku läbivaatamiseks ning KOHUSTUB jätkama jõupingutusi küberturvalisuse ja küberkaitse mõõtmete tugevdamiseks, et tagada nende täielik integreerimine laiemasse julgeoleku- ja kaitsevaldkonda, eelkõige strateegilise kompassiga seotud töö raames; ON SEISUKOHAL, et tulevane „Sõjaline visioon ja strateegia küberruumi kui tegevusvaldkonna jaoks“ aitab neid arutelusid edendada; PEAB TERVITATAVAKS Euroopa Kaitseagentuuri (EDA) algatust edendada koostööd sõjaliste CERTide vahel ning TOETAB jõupingutusi, mida on tehtud tsiviil-sõjalise koostoime suurendamiseks ning küberkaitse ja küberturvalisuse, sealhulgas kosmosega seotud aspektide koordineerimiseks, sealhulgas eriotstarbeliste PESCO projektide kaudu;

31. PEAB TERVITATAVAKS ettepanekuid ELi välise kübersuutlikkuse suurendamise tegevuskava koostamiseks ja ELi kübersuutlikkuse suurendamise nõukogu loomiseks, samuti ELi kübersuutlikkuse suurendamise võrgustiku (EU CyberNet) loomist ja rakendamist, et suurendada kübervastupidavusvõimet ja -suutlikkust kogu maailmas; PEAB sellega seoses TERVITATAVAKS koostööd liikmesriikidega ning avaliku ja erasektori partneritega, eelkõige kübervaldkonna erialateadmiste üleilmse foorumi ja muude asjaomaste rahvusvaheliste kehamitega, et tagada koordineerimine ja vältida dubleerimist; JULGUSTAB eelkõige tegema koostööd partneritega Lääne-Balkani piirkonnas ning ELi ida- ja lõunanaabruses;

32. selleks, et kõik riigid saaksid kasu internetist ja tehnoloogia kasutamisest tulenevatest sotsiaalsetest, majanduslikest ja poliitilistest hüvedest, KOHUSTUB aitama partnerriikidel võidelda pahatahtlikust kübertegevusest tingitud kasvavate probleemidega, eelkõige sellistega, mis kahjustavad nende majanduse arengut, ühiskonda ning demokraatlike süsteemide terviklikkust ja turvalisust, sealhulgas kooskõlas Euroopa demokraatia tegevuskava raames tehtavate jõupingutustega;

33. selleks et tagada ELi küberturvalisuse strateegias esitatud ettepanekute väljatöötamine, rakendamine ja järelevalve ning võttes arvesse mõnede algatuste mitmeaastast iseloomu, INNUSTAB komisjoni ning liidu välisasjade ja julgeolekupoliitika kõrget esindajat koostama üksikasjaliku rakenduskava, milles on määratud kindlaks kavandatavate meetmete prioriteedid ja ajakava; JÄLGIB käesolevate järelduste rakendamisel tehtavaid edusamme tegevuskava abil, mille nõukogu korrapäraselt läbi vaatab ja ajakohastab tihedas koostöös Euroopa Komisjoni ja kõrge esindajaga.