|  |  |
| --- | --- |
| Euroopa Parlament  2014-2019 |  |

Istungidokument

<NoDocSe>B8‑0155/2019</NoDocSe>

<Date>{06/03/2019}6.3.2019</Date>

<TitreType>RESOLUTSIOONI ETTEPANEK</TitreType>

<TitreSuite>nõukogu ja komisjoni avalduste alusel</TitreSuite>

<TitreRecueil>vastavalt kodukorra artikli 123 lõikele 2</TitreRecueil>

<Titre>julgeolekuohtude kohta, mis on seotud Hiina järjest suurema tehnoloogilise kohaloluga ELis, ja võimalike ELi tasandi meetmete kohta nende ohtude vähendamiseks</Titre>

<DocRef>(2019/2575(RSP))</DocRef>

<RepeatBlock-By><Depute>Luděk Niedermayer, Angelika Niebler, Ivo Belet, Paul Rübig</Depute>

<Commission>{PPE}fraktsiooni PPE nimel</Commission>

</RepeatBlock-By>

B8‑0155/2019

Euroopa Parlamendi resolutsioon julgeolekuohtude kohta, mis on seotud Hiina järjest suurema tehnoloogilise kohaloluga ELis, ja võimalike ELi tasandi meetmete kohta nende ohtude vähendamiseks

(2019/2575(RSP))

*Euroopa Parlament*,

– võttes arvesse Euroopa Parlamendi ja nõukogu 11. detsembri 2018. aasta direktiivi (EL) 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik[[1]](#footnote-2),

– võttes arvesse Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiivi (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus[[2]](#footnote-3),

– võttes arvesse Euroopa Parlamendi ja nõukogu 12. augusti 2013. aasta direktiivi 2013/40/EL, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega asendatakse nõukogu raamotsus 2005/222/JSK[[3]](#footnote-4),

– võttes arvesse komisjoni ettepanekut võtta vastu Euroopa Parlamendi ja nõukogu 13. septembri 2017. aasta määrus, mis käsitleb ENISAt ehk ELi küberturvalisuse ametit, millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 ja mis käsitleb info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist („küberturvalisust käsitlev õigusakt“) (COM(2017)0477),

– võttes arvesse komisjoni ettepanekut võtta vastu Euroopa Parlamendi ja nõukogu 12. septembri 2018. aasta määrus, millega luuakse Euroopa küberturvalisuse tööstusliku, tehnoloogilise ja teadusliku pädevuse keskus ning riiklike koordineerimiskeskuste võrgustik (COM(2018)0630),

– võttes arvesse, et Hiina Rahvakongress võttis 28. juunil 2017 vastu uue riikliku luureteenistuse seaduse,

– võttes arvesse nõukogu ja komisjoni 13. veebruari 2019. aasta avaldusi julgeolekuohtude kohta, mis on seotud Hiina järjest suurema tehnoloogilise kohaloluga ELis, ja võimalike ELi tasandi meetmete kohta nende ohtude vähendamiseks,

– võttes arvesse Austraalia valitsuse poolt vastuvõetud valitsuse telekommunikatsioonisektori julgeolekureforme, mis kehtivad alates 18. septembrist 2018,

– võttes arvesse oma 14. veebruaril 2019. aastal esimesel lugemisel vastu võetud seisukohta ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus, millega luuakse Euroopa Liitu tehtavate välismaiste otseinvesteeringute taustauuringute raamistik[[4]](#footnote-5),

– võttes arvesse oma resolutsioone ELi ja Hiina suhete kohta, eriti 12. septembri 2018. aasta resolutsiooni ELi ja Hiina vaheliste suhete seisu kohta[[5]](#footnote-6),

– võttes arvesse komisjoni 14. septembri 2016. aasta teatist „5G Euroopa jaoks: tegevuskava“ (COM(2016)0588),

– võttes arvesse oma 1. juuni 2017. aasta resolutsiooni internetiühenduse kohta kasvu, konkurentsivõime ja ühtekuuluvuse suurendamiseks: Euroopa gigabitiühiskond ja 5G[[6]](#footnote-7),

– võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrust (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)[[7]](#footnote-8),

– võttes arvesse Euroopa Parlamendi ja nõukogu 11. detsembri 2013. aasta määrust (EL) nr 1316/2013, millega luuakse Euroopa ühendamise rahastu, muudetakse määrust (EL) nr 913/2010 ja tunnistatakse kehtetuks määrused (EÜ) nr 680/2007 ja (EÜ) nr 67/2010[[8]](#footnote-9),

– võttes arvesse komisjoni ettepanekut võtta vastu Euroopa Parlamendi ja nõukogu määrus, millega kehtestatakse ajavahemikuks 2021–2027 digitaalse Euroopa programm (COM(2018)0434),

– võttes arvesse kodukorra artikli 123 lõiget 2,

A. arvestades, et EL peab edasi arendama oma küberturvalisuse tegevuskava, et täita oma potentsiaal ja saada juhtivaks osalejaks küberturvalisuse valdkonnas, ning kasutada seda oma tööstuse eelisena;

B. arvestades, et 5G-võrkude haavatavust saab infotehnoloogiasüsteemide kahjustamiseks ära kasutada, mis võib tekitada nii Euroopa ja kui ka riikide majandusele tõsist kahju; arvestades, et riskide minimeerimiseks on vaja kogu väärtusahelas rakendada riskianalüüsil põhinevat lähenemisviisi;

C. arvestades, et 5G-võrgust saab ELi digitaalse taristu selgroog, mis laiendab võimalust erinevate seadmete võrkudesse ühendamiseks (asjade internet jne), ning toob ühiskonnale ja ettevõtetele uusi hüvesid ja võimalusi paljudes valdkondades, sealhulgas majanduse kriitilistes sektorites, nagu transpordi, energeetika, tervishoiu, rahanduse, telekommunikatsiooni, kaitse, kosmose ja julgeoleku sektorites;

D. arvestades, et julgeolekuprobleemide lahendamiseks sobiva reageerimismehhanismi loomine annaks ELile võimaluse astuda aktiivselt samme 5G-standardite kehtestamiseks;

E. arvestades, et on väljendatud muret seoses kolmandatest riikidest pärit seadmete müüjatega, kes võivad kujutada endast ELi jaoks julgeolekuriski oma päritoluriigi seaduste tõttu, eriti pärast Hiina riigi julgeolekuseaduste jõustumist, millega kohustatakse kõiki kodanikke, ettevõtjaid ja muid üksusi tegema riigiga koostööd, et kaitsta riigi julgeolekut; arvestades, et ei ole mingit garantiid, et see kohustus oleks seatud nõudeta kohaldada seda väljaspool oma riigi territooriumi, ning et eri riigid on reageerinud Hiina eeskirjadele erinevalt, alates julgeolekuanalüüsist kuni täieliku keelustamiseni;

F. arvestades, et detsembris 2018 avaldas Tšehhi riiklik küberjulgeolekuamet hoiatuse julgeolekuohtude eest, mida kujutavad endast Hiina äriühingute Huawei ja ZTE tehnoloogiad; arvestades, et seejärel jättis Tšehhi maksuhaldur 2019. aasta jaanuaris Huawei välja hankemenetlusest, mis toimus maksuportaali loomise eesmärgil;

G. arvestades, et on vaja põhjalikult uurida ja välja selgitada, kas asjaomased seadmed, muud seadmed või tarnijad kujutavad endast turvariske, mis tulenevad süsteemide sellistest omadustest nagu tagauksed;

H. arvestades, et lahendusi tuleks koordineerida ja nendega tegeleda ELi tasandil, et hoida ära eri tasemel julgeolek ja võimalikud lüngad küberturvalisuses; arvestades, et samas on vaja ka globaalsel tasandil koordineerida nii, et saaks jõuliselt reageerida;

I. arvestades, et ühtsest turust saadava kasuga käib kaasas kohustus järgida ELi standardeid ja õigusraamistikku, ning arvestades, et tarnijaid ei tohiks nende päritoluriigist lähtuvalt erinevalt kohelda;

J. arvestades, et välismaiste otseinvesteeringute taustauuringute määruses, mis peaks jõustuma 2020. aasta lõpuks, tugevdatakse liikmesriikide võimet kontrollida julgeoleku ja avaliku korra kaalutlustel välisinvesteeringuid ning luuakse koostöömehhanism, mis võimaldab komisjonil ja liikmesriikidel teha üheskoos tööd tundlike välisinvesteeringute poolt tekitatud julgeolekuriskide, sealhulgas küberturvalisusriskide hindamisel, ning et see hõlmab ka liidule huvi pakkuvaid projekte ja programme, nagu üleeuroopalised telekommunikatsioonivõrgud ja „Horisont 2020”;

1. on veendunud, et liit peab asuma küberturvalisuse valdkonnas esirinda, kasutades ühist lähenemisviisi, mis põhineb ELi, liikmesriikide ja selle sektori eksperditeadmiste tulemuslikul ja tõhusal kasutamisel, kuna digitaalse ühtse turu jaoks oleks kahjulik, kui iga riik võtaks omaette vastu erinevaid otsuseid;

2. väljendab sügavat muret hiljutiste väidete pärast, et Hiina ettevõtete poolt välja töötatud 5G-seadmed võivad sisaldada tagauksi, mis lasevad tootjatel ja ametivõimudel ELi kodanike ja ettevõtjate andmetele ja elektroonilisele sidele loata juurde pääseda;

3. on samuti mures, et kui nende tootjate poolt välja arendatud 5G-seadmed võetakse lähiaastatel kasutusele seoses 5G-võrkude käivitamisega, võivad need seadmed sisaldada olulisi turvaauke;

4. rõhutab, et võrkude ja seadmete turvalisusele avalduv mõju on kogu maailmas sarnane, ning palub ELil teha olemasolevate kogemuste põhjal järeldused, et saaks tagada kõrgeimad küberturvalisuse standardid; kutsub komisjoni üles töötama välja strateegia, mis asetaks Euroopa küberturvalisuse tehnoloogia valdkonnas juhtpositsioonile ja mille eesmärk oleks vähendada Euroopa sõltuvust välismaisest tehnoloogiast küberturvalisuse valdkonnas;

5. kutsub liikmesriike üles teavitama komisjoni kõikidest riiklikest meetmetest, mida nad kavatsevad vastu võtta, et koordineerida liidu reageerimist nii, et kogu liidus oleks tagatud kõrgeim küberturvalisuse tase, ning kordab, kui oluline on mitte kehtestada ebaproportsionaalseid ühepoolseid meetmeid, mis killustaksid ühtset turgu;

6. kordab, et kõik üksused, kes pakuvad ELis seadmeid või teenuseid peavad sõltumata nende päritoluriigist täitma põhiõiguste alaseid kohustusi ning austama ELi ja liikmesriikide õigust, sealhulgas eraelu puutumatust, andmekaitset ja küberjulgeolekut käsitlevat õigusraamistikku;

7. kutsub komisjoni üles hindama, kas liidu õigusraamistik on piisavalt tugev, reageerimaks murele, et strateegilistes sektorites ja tuumtaristus leidub haavatavaid seadmeid; nõuab tungivalt, et komisjon esitaks algatused, sealhulgas vajadusel ka seadusandlikud ettepanekud tuvastatud puudujääkide kiireks kõrvaldamiseks, arvestades, et EL on pidevas protsessis, et teha kindlaks küberturvalisuse probleeme ja neid lahendada ning suurendada ELis küberturvalisuse alast vastupanuvõimet;

8. nõuab tungivalt, et liikmesriigid, kes ei ole veel täielikult üle võtnud direktiivi 2016/1148/EL (võrgu- ja infosüsteemide turvalisuse kohta), teeksid seda viivitamata ja palub, et komisjon jälgiks seda ülevõtmist hoolikalt, et tagada kõnealuse direktiivi sätete nõuetekohane kohaldamine ja jõustamine ning ELi kodanike jaoks tugevam kaitse välisjulgeoleku ohtude eest;

9. nõuab tungivalt, et komisjon ja liikmesriigid tagaksid küberturvalisuse direktiivis kehtestatud aruandlusmehhanismide nõuetekohase kohaldamise; märgib, et komisjon ja liikmesriigid peaksid võtma põhjalikke järelmeetmeid seoses turvaintsidentidega või tarnijate sobimatu reageerimisega nii, et saaks likvideerida avastatud lüngad;

10. kutsub komisjoni üles hindama vajadust laiendada küberturvalisuse direktiivi kohaldamisala ka muudele elutähtsatele sektoritele ja teenustele, nagu võrgutaristu, mis ei ole hõlmatud konkreetsete õigusaktidega;

11. väljendab heameelt ja toetab küberturvalisuse direktiivi osas saavutatud kokkulepet, ning Euroopa Liidu Võrgu- ja Infoturbeameti (ENISA) volituste tugevdamist, et paremini toetada liikmesriike küberturvalisuse ohtude ja rünnakute vastu võitlemisel;

12. tuletab meelde, et küberturvalisuseks on vaja täita kõrgeid turvanõudeid; nõuab, et võrgud oleksid juba kavandatult ja vaikimisi turvalised; nõuab tungivalt, et liikmesriigid uuriksid koos komisjoniga kõiki kättesaadavaid vahendeid, et tagada turvalisuse kõrge tase.

13. nõuab tungivalt, et komisjon volitaks ENISAt töötama eelisjärjekorras välja 5G-seadmete sertifitseerimissüsteemi, tagamaks, et 5G-tehnoloogia kasutuselevõtmine liidus vastab kõrgeimatele turvastandarditele, on vastupidav nn tagauste ja suuremate turvaaukude suhtes, mis võivad ohustada liidu telekommunikatsioonivõrkude ja neist sõltuvate teenuste turvalisust; soovitab pöörata erilist tähelepanu üldiselt kasutatavatele protsessidele, toodetele ja tarkvarale, millel on juba oma laiaulatuslikkuse tõttu oluline mõju nii kodanike igapäevaelule kui ka majandusele;

14. väljendab suurt heameelt seoses ettepanekutega, mis puudutavad küberturvalisuse pädevuskeskusi ja riiklike koordineerimiskeskuste võrgustikku, mille eesmärk on aidata ELil säilitada ja arendada küberjulgeoleku alast tehnoloogilist ja tööstuslikku suutlikkust, mida on vaja tema digitaalse ühtse turu kindlustamiseks;

15. kinnitab oma seisukohta digitaalse Euroopa programmi suhtes, millega kehtestatakse turvanõuded ja komisjoni järelevalve selliste üksuste üle, mis on asutatud ELis, kuid mida kontrollitakse kolmandatest riikidest, eelkõige seoses küberturvalisusega seotud meetmetega;

16. kutsub liikmesriike üles tagama, et avaliku sektori asutused ja eraettevõtjad, kes on seotud elutähtsate taristuvõrkude, nagu telekommunikatsiooni-, energia-, tervishoiu- ja sotsiaalsüsteemide nõuetekohase toimimise tagamisega, teostaksid asjakohaseid riskianalüüsi hindamisi, võttes arvesse julgeolekuohte, mis on konkreetselt seotud vastava süsteemi tehniliste omadustega, ning arvestaksid sõltuvust riist- ja tarkvara tehnoloogiate liiduvälistest tarnijatest;

17. tuletab meelde, et praegune telekommunikatsiooni õigusraamistik volitab liikmesriike tagama, et sideoperaatorid järgiksid üldkasutatavate elektrooniliste sidevõrkude terviklikkuse ja kättesaadavuse nõuet; rõhutab, et vastavalt Euroopa elektroonilise side seadustiku sätetele on liikmesriikidel kõik vajalikud volitused uurida ja kohaldada mitmesuguseid parandusmeetmeid juhul, kui ELi turul olevad tooted ei vasta nõuetele;

18. kutsub komisjoni ja liikmesriike üles muutma julgeoleku nii ELi kui ka riiklikul tasandil kõikides asjaomase taristu riigihankemenetlustes kohustuslikuks aspektiks;

19. kutsub komisjoni ja liikmesriike üles suurendama läbipaistvust ja turvalisust, töötades välja mitmefaasilised hankemenetlused IKT taristu jaoks, mis võimaldaks teha vahet pakkumiste vahel, mis on esitatud nende süsteemide ülesehituseks, tootmiseks, käitamiseks ja hoolduseks ning samuti teha vahet üksikute tehnoloogiapakkujate vahel;

20. tuletab liikmesriikidele meelde, et nad on ELi kriminaalõigusest tulenevalt kohustatud kehtestama karistused, eelkõige kriminaalõiguslikud ja muud trahvid juriidilistele isikutele, kes on infosüsteemide vastu suunatud rünnete vallas toime pannud kuritegusid, nagu ebaseaduslikku süsteemi häirimist, ebaseaduslikku andmetesse sekkumist ja ebaseaduslikku pealtkuulamist; rõhutab, et liikmesriigid peaksid kasutama ka võimalust kehtestada neile juriidilistele isikutele muid sanktsioone, näiteks ajutine või alaline ettevõtluskeeld;

21. eeldab, et riiklikud andmekaitseasutused ja Euroopa andmekaitseinspektor uurivad põhjalikult juhtumeid, kus on alust kahtlustada, et liiduväline müüja on pannud toime andmetega seotud rikkumise, ning kohaldavad kooskõlas Euroopa andmekaitseõigusega asjakohaseid karistusi ja sanktsioone;

22. väljendab heameelt, et peatselt jõustub määrus, millega julgeoleku ja avaliku korra kaalutlustel kehtestatakse välismaiste otseinvesteeringute taustauuringute raamistik, ning rõhutab, et selle määrusega kehtestatakse esmakordselt loetelu valdkondadest ja teguritest, sh kommunikatsioon ja küberturvalisus, mis on ELi tasandil julgeoleku ja avaliku korra seisukohast olulised;

23. kordab, et EL peab toetama küberturvalisust kogu väärtusahela ulatuses, alates teadusuuringutest kuni peamiste tehnoloogiate kasutuselevõtu ja juurutamiseni, levitama asjakohast teavet ja edendama küberhügieeni ja küberturvalisuse alaseid õppekavasid, ning on veendunud, et muude meetmete seas on selleks tõhus vahend digitaalse Euroopa programm;

24. nõuab tungivalt, et komisjon ja liikmesriigid astuksid vajalikke samme, et luua ELis innovatsioonisõbralik keskkond, mis peaks olema kättesaadav kõigile ELi digitaalmajanduse ettevõtetele, sealhulgas väikestele ja keskmise suurusega ettevõtjatele; nõuab lisaks tungivalt, et selline keskkond laseks Euroopa müüjatel töötada välja uusi tooteid, teenuseid ja tehnoloogiaid, mis võimaldaks neil olla konkurentsivõimelised;

25. teeb presidendile ülesandeks edastada käesolev resolutsioon nõukogule ja komisjonile.

1. ELT L 321, 17.12.2018, lk 36. [↑](#footnote-ref-2)
2. ELT L 194, 19.7.2016, lk 1. [↑](#footnote-ref-3)
3. ELT L 218, 14.8.2013, lk 8. [↑](#footnote-ref-4)
4. Vastuvõetud tekstid, P8\_TA(2019)0121. [↑](#footnote-ref-5)
5. Vastuvõetud tekstid, P8\_TA(2018)0343. [↑](#footnote-ref-6)
6. ELT C 307, 30.8.2018, lk 144. [↑](#footnote-ref-7)
7. ELT L 119, 4.5.2016, lk 1. [↑](#footnote-ref-8)
8. ELT L 348, 20.12.2013, lk 129. [↑](#footnote-ref-9)