SOOVITUSED

KOMISJONI SOOVITUS (EL) 2019/534,

26. märts 2019

5G-võrkude küberturvalisus

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 292,

ning arvestades järgmist:

(1) Komisjon peab viienda põlvkonna (5G) võrgutehnoloogiate kasutuselevõttu tulevaste digiteenuste arengu mootoriks ja on seadnud selle digitaalse ühtse turu strateegia prioriteediks. Komisjon võttis vastu 5G tegevuskava, et tagada liidule ühenduvustaristu, mida on vaja digitaaltehnoloogiale üleminekuks alates 2020. aastast ([1]).

(2) 5G-võrgud arendavad edasi praeguseid neljanda põlvkonna (4G) võrgutehnoloogiaid, pakkudes uusi teenindusvõimsusi ja muutudes liidu majanduse suurte osade jaoks keskseks taristuks ja arengumootoriks. Kui 5G-võrgud on kasutusele võetud, on need aluseks väga paljudele teenustele, mis on olulised siseturu toimimiseks ning ühiskonna ja majanduse eluliselt tähtsate funktsioonide (nt energeetika, transport, pangandus, tervishoid ja tööstuslikud juhtimissüsteemid) hooldamiseks ja toimimiseks. Ka demokraatlike protsesside (nt valimised) korraldus tugineb üha rohkem digitaristule ja 5G-võrkudele.

(3) Paljude kriitilise tähtsusega teenuste sõltuvus 5G-võrkudest muudaks süsteemse ja laiaulatusliku halvamise tagajärjed eriti raskeks. Seepärast on 5G-võrkude küberturvalisuse tagamine liidu jaoks strateegilise tähtsusega küsimus ajal, mil küberrünnakud on sagenenud ja keerulisemad kui kunagi varem.

(4) Digitaalse ökosüsteemi aluseks olevate taristute omavaheline seotus ja riigiülesus ning asjaomaste ohtude piiriülesus tähendab, et kõik 5G-võrkudega seotud olulised nõrgad kohad ja/või ühes liikmesriigis toimuvad küberturvalisuse intsidendid mõjutaksid liitu tervikuna. Seepärast tuleks ette näha meetmed, et toetada 5G-võrkude küberturvalisuse ühtlaselt kõrget taset.

(5) Vajadust liidu tasandi meetmete järgi on kinnitanud liikmesriigid. 21. märtsi 2019. aasta järeldustes kutsus Euroopa Ülemkogu komisjoni üles esitama soovitust 5G-võrkude turvalisuse tagamise kooskõlastatud lähenemisviisi kohta ([2]).

(6) Euroopa suveräänsuse tagamine peaks olema oluline eesmärk, mille poole püüeldes tuleb täielikult austada Euroopa väärtusi, nagu avatus ja sallivus ([3]). ELi julgeolekut võivad ohustada ka välisinvesteeringud strateegilistes sektorites, kriitilise tähtsusega varade, tehnoloogia ja taristu omandamine liidus ning kriitilise tähtsusega seadmete tarnimine.

(7) 5G-võrkude küberturvalisus on liidu strateegilise sõltumatuse tagamisel esmatähtis, nagu on tunnistatud ühisteatises „ELi ja Hiina suhete strateegilised väljavaated“ ([4]).

(8) Ka Euroopa Parlamendi resolutsioonis julgeolekuohtude kohta, mis on seotud Hiina järjest suurema tehnoloogilise kohaloluga liidus, kutsutakse komisjoni ja liikmesriike üles võtma meetmeid liidu tasandil ([5]).

(9) Käesolevas soovituses käsitletakse 5G-võrkude küberturvalisuse riske, esitades suunised riiklikul tasandil võetavate asjakohaste riskianalüüsi- ja riskijuhtimismeetmete kohta, Euroopa koordineeritud riskihindamise väljatöötamise kohta ja ühiste parimate riskijuhtimismeetmete kogumi väljatöötamise protsessi kehtestamise kohta.

(10) Elektroonilise side võrkude kaitsmiseks on liidus kehtestatud tugev õigusraamistik.

([1]) COM(2016)588 final.
([2]) Euroopa Ülemkogu 21. ja 22. märtsi 2019. aasta järeldused.
([3]) Euroopa Liidu olukord 2018. aastal – Euroopa suveräänsuse aeg, 12. september 2018.
([4]) JOIN (2019) 5 final.
([5]) www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//ET.

(11) Elektroonilise side valdkonna liidu raamistik ([6]) edendab konkurentsi, siseturgu ja lõppkasutajate huve ning püüdleb koos Euroopa elektroonilise side seadustikuga ([7]) täiendava ühenduvuseesmärgi poole, mida iseloomustab järgmine tulemus: kõigile liidu kodanikele ja ettevõtjatele pakutav laialdane juurdepääs ülikiirele püsi- ja mobiilsideühendusele ning selliste ühenduste laialdane kasutuselevõtt, kaitstes samal ajal kodanike huve. Direktiiviga 2002/21/EÜ on ette nähtud, et liikmesriigid tagavad üldkasutatavate sidevõrkude terviklikkuse ja turvalisuse ning on kohustatud tagama, et üldkasutatavaid sidevõrke või üldkasutatavaid elektroonilise side teenuseid pakkuvad ettevõtjad võtavad tehnilisi ja korralduslikke meetmeid, et asjakohaselt maandada võrkude ja teenuste turvalisusega seotud riske. Samuti on selles sätestatud, et pädevatel riigi reguleerivatel asutustel on volitused, sealhulgas õigus esitada siduvaid suuniseid, et tagada selliste kohustuste täitmine.

(12) Lisaks on Euroopa Parlamendi ja nõukogu direktiivi 2002/20/EÜ ([8]) kohaselt liikmesriikidel õigus lisada üldloale tingimusi, mis käsitlevad üldkasutatavate võrkude turvalisust loata juurdepääsu seisukohast, et kaitsta side konfidentsiaalsust kooskõlas Euroopa Parlamendi ja nõukogu direktiiviga 2002/58/EÜ ([9]).

(13) Liit on loonud mitmeid koostööorganeid, et toetada nende kohustuste täitmist. Võrgu- ja infoturbeamet (ENISA), komisjon, liikmesriigid ja riikide reguleerivad asutused on töötanud riikide reguleerivate asutuste jaoks välja tehnilised suunised intsidentidest teatamise, turvameetmete, ohtude ja varade kohta ([10]). Euroopa Parlamendi ja nõukogu direktiiviga (EL) 2016/1148 ([11]) loodud koostöörühm toob kokku pädevad asutused, et toetada ja hõlbustada koostööd eelkõige selliste strateegiliste juhiste andmisega küberturbe intsidentide lahendamise üksuste võrgustiku tegevuse kohta, mis hõlbustavad operatiivkoostööd tehnilisel tasandil.

(14) Tulevane Euroopa küberturvalisuse sertifitseerimise raamistik ([12]) peaks moodustama olulise toetava vahendi turvalisuse ühtse taseme edendamiseks. See peaks võimaldama välja töötada küberturvalisuse sertifitseerimise kavad, et reageerida 5G-seadmete ja tarkvara kasutajate vajadustele. Need taristud on kriitilise tähtsusega ja seepärast peaks peamine prioriteet olema asjakohaste Euroopa küberturvalisuse sertifitseerimise kavade väljatöötamine 5G võrkudes kasutatavate info- ja kommunikatsioonitehnoloogia toodete, teenuste või protsesside jaoks. Liikmesriigid ja turuosalised peaksid aktiivselt osalema selliste sertifitseerimiskavade väljatöötamises, sealhulgas toetama 5G-võrkude konkreetsete kaitseprofiilide kindlaksmääramist.

(15) Kuna liidu tasandil ei ole õigusnorme ühtlustatud, võivad liikmesriigid näha liidu õiguse kohaselt vastu võetud riiklike tehniliste normidega ette, et Euroopa küberturvalisuse sertifitseerimise kava on kohustuslik. Liikmesriigid saavad Euroopa küberturvalisuse sertifitseerimise kavasid kasutada ka riigihangete ja Euroopa Parlamendi ja nõukogu direktiivi 2014/24/EL ([13]) kontekstis ning võiksid toetada selliste abimehhanismide (nt abikeskus) väljatöötamist, mis on suunatud küberturvalisuse lahendusi hankivatele avaliku sektori hankijatele.

(16) Kõrgetasemeline andmekaitse ja privaatsus on olulised tegurid 5G-võrkude turvalisuse tagamisel. Liidu tasandil on kehtestatud õigusnormid, millega tagatakse isikuandmete töötlemise turvalisus, sealhulgas elektroonilise side puhul. Isikuandmete kaitse üldmäärusega ([14]) on kehtestatud kohustus töödelda isikuandmeid viisil, mis tagab nende turvalisuse, sealhulgas hoiab ära loata juurdepääsu isikuandmetele ja nende töötlemiseks kasutatavatele seadmetele loata juurdepääsu ja nende loata kasutamise. Eraelu puutumatust ja elektroonilist sidet käsitlevas

([6]) Euroopa Parlamendi ja nõukogu 7. märtsi 2002. aasta direktiiv 2002/21/EÜ elektrooniliste sidevõrkude ja -teenuste ühise reguleeriva raamistiku kohta (raamdirektiiv) (EÜT L 108, 24.4.2002, lk 33) ja eridirektiivid.

([7]) Euroopa Parlamendi ja nõukogu 11. detsembri 2018. aasta direktiiv (EL) 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik (ELT L 321, 17.12.2018, lk 36).

([8]) Euroopa Parlamendi ja nõukogu 7. märtsi 2002. aasta direktiiv 2002/20/EÜ elektrooniliste sidevõrkude ja -teenustega seotud lubade andmise kohta (loadirektiiv) (EÜT L 108, 24.4.2002, lk 21).

([9]) Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (EÜT L 201, 31.7.2002, lk 37).

([10]) https://resilience.enisa.europa.eu/article-13.

([11]) Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.7.2016, lk 1).

([12]) Ettepanek: Euroopa Parlamendi ja nõukogu 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) 477 final - 2017/0225 (COD).

([13]) Euroopa Parlamendi ja nõukogu 26. veebruari 2014. aasta direktiiv 2014/24/EL riigihangete kohta ja direktiivi 2004/18/EÜ kehtetuks tunnistamise kohta (ELT L 94, 28.3.2014, lk 65).

([14]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

direktiivis on sätestatud konkreetsed õigusnormid side ja lõppkasutajate lõppseadmete konfidentsiaalsuse kaitse kohta. Samuti nähakse sellega teenuseosutajatele ette kohustus võtta oma teenuste turvalisuse tagamiseks asjakohaseid tehnilisi ja korralduslikke meetmeid.

(17) Samuti on liit võtnud vastu õigusakti, millega kaitstakse elutähtsaid taristuid ja tehnoloogiaid, näiteks neid, mida kasutatakse sides, võimaldades liikmesriikidel teha julgeoleku või avaliku korra huvides taustauuringuid välismaiste otseinvesteeringute kohta ning luues koostöömehhanismi, mille raames saavad liikmesriigid ja komisjon vahetada teavet ja tõstatada küsimusi seoses konkreetsete investeeringutega ([15]).

(18) Liikmesriigid ja ettevõtjad teevad praegu olulisi ettevalmistusi 5G-võrkude ulatuslikuks kasutuselevõtuks. Mitu liikmesriiki on väljendanud muret seoses 5G-võrkude võimalike turvariskidega, mis tulenevad 5G-võrkude jaoks määratud raadiospektri sagedusalade kasutamise õiguste andmise menetlustest, ([16]) ja analüüsinud meetmeid nende riskide maandamiseks.

(19) 5G-võrkude küberturvalisuse riskidega tegelemisel tuleks võtta arvesse nii tehnilisi kui ka muid tegureid. Tehniliste tegurite hulka võivad kuuluda küberturvalisuse nõrkused, mida võidakse ära kasutada, et saada loata juurdepääs teabele (küberspionaaž, olgu see majanduslikel või poliitilistel põhjustel), või muudel kuritegelikel eesmärkidel (küberründed, mille eesmärk on süsteemide ja andmete halvamine või hävitamine). Tuleks kaaluda vajadust kaitsta võrke kogu nende kasutusaja jooksul ja hõlmata kõik asjaomased seadmed nii 5G-võrkude projekteerimis-, arendus-, hanke-, kasutuselevõtu-, käitamis- kui ka hooldusetapis.

(20) Muud tegurid võivad hõlmata info- ja kommunikatsioonitehnoloogia seadmete tarnijatele kehtestatud regulatiivseid või muid nõudeid. Selliste tegurite olulisuse hindamisel tuleks muu hulgas arvesse võtta kolmanda riigi poolse mõjutamise üldist riski, eelkõige seoses tema juhtimismudeliga, küberjulgeolekualaste koostöökokkulepete või sarnaste andmekaitsealaste kokkulepete (nt kaitse piisavuse otsused) puudumist liidu ja asjaomase kolmanda riigi vahel või seda, kas kõnealune riik on osaline mitmepoolsetes, rahvusvahelistes või kahepoolsetes lepingutes, mis käsitlevad küberjulgeolekut, küberkuritegevuse vastast võitlust või andmekaitset.

(21) 5G-võrkude küberturvalisuse alase liidu lähenemisviisi väljatöötamise olulise sammuna tuleks riikide tasandil läbi viia riskihindamine. Riskihindamise tulemuste põhjal saaksid liikmesriigid kohandada turvanõudeid ja riskijuhtimist käsitlevaid siseriiklikke meetmeid.

(22) Välja tuleks töötada koordineerimiskord, et tagada küberturvalisuse riskide maandamise meetmete tõhusus, pidades silmas, et need meetmed on esmatähtsad siseturu tõrgeteta toimimiseks ning isikuandmete ja privaatsuse kaitseks.

(23) Riikide riskihindamised peaksid olema aluseks liidu koordineeritud riskihindamisele, mis koosneb ohtude kaardistamisest ja ühisest läbivaatamisest, mille teevad liikmesriigid komisjoni toel ja koos Euroopa Liidu Küberturvalisuse Ametiga (ENISA).

(24) Võttes arvesse liikmesriikide ja liidu riskihindamise tulemusi, peaks koostöörühm koostama meetmete kogumi, mille abil määratakse kindlaks küberturvalisuse riskide ja riskide maandamise võimalike meetmete liigid näiteks sertifitseerimise, testimise ja juurdepääsu kontrollimise valdkonnas. Samuti peaks see määrama kindlaks võimalikud erimeetmed, mis sobivad ühe või mitme liikmesriigi tuvastatud riskide maandamiseks. Koostöörühma peaks toetama Euroopa Liidu Küberturvalisuse Amet (ENISA), Europol, Elektroonilise Side Euroopa Reguleerivate Asutuste Ühendatud Amet (BEREC) ja ELi luure- ja situatsioonikeskus. See meetmete kogum peaks toimima komisjoni jaoks abinõuna, mille alusel töötada välja ühised miinimumnõuded 5G-võrkude küberturvalisuse kõrge taseme tagamiseks kogu liidus.

(25) Kui võetakse meetmeid küberturvalisuse riskide maandamiseks, tuleks kaaluda küberturvalisuse edendamist seeläbi, et mis tahes üheainsa võrgu loomisel kasutatakse erinevaid tarnijaid.

([15]) Euroopa Parlamendi ja nõukogu 19. märtsi 2019. aasta määrus (EL) 2019/452, millega luuakse liitu tehtavate välismaiste otseinvesteeringute taustauuringute raamistik (ELT L 79I, 21.3.2019, lk 1).

([16]) 2019. aastal kavatsetakse vähemalt ühe sagedusalaga seotud enampakkumismenetlus korraldada 11 liikmesriigis: Austria, Belgia, Tšehhi, Prantsusmaa, Saksamaa, Kreeka, Ungari, Iirimaa, Madalmaad, Leedu, Portugal. 2020. aastaks on kavandatud veel kuus enampakkumist järgmistes riikides: Hispaania, Malta, Leedu (erinevad sagedused), Slovakkia, Poola, Ühendkuningriik. Allikas: http://5gobservatory.eu/observatory-overview/observatory-reports/.

(26) Käesolev soovitus ei tohiks piirata liikmesriikide pädevust seoses tegevusega, mis on seotud avaliku julgeoleku, riigikaitse, riigi julgeoleku ja riigi tegevusega kriminaalõiguse valdkonnas, sealhulgas liikmesriikide õigusega jätta pakkujad või tarnijad oma turgudelt riigi julgeoleku huvides välja.

ON VASTU VÕTNUD KÄESOLEVA SOOVITUSE:

I. **EESMÄRGID**

1. Selleks et toetada liidu lähenemisviisi väljatöötamist 5G-võrkude küberturvalisuse tagamiseks, määratakse käesolevas soovituses kindlaks meetmed, mis tuleks võtta, et:

   a) liikmesriigid saaksid hinnata 5G-võrke mõjutavaid küberturvalisuse riske riigi tasandil ja võtta vajalikke turvameetmeid;

   b) liikmesriigid ja asjaomased liidu institutsioonid, asutused ja muud organid saaksid ühiselt välja kujundada liidu koordineeritud riskihindamise, mis põhineb riikide riskihindamisel;

   c) direktiivi (EL) 2016/1148 alusel loodud koostöörühm saaks kindlaks määrata võimalikud ühised meetmed, mida võtta, et maandada digitaalse ökosüsteemi aluseks olevate taristutega, eelkõige 5G-võrkudega seotud küberturvalisuse riske.

II. **MÕISTED**

2. Käesolevas soovituses kasutatakse järgmisi mõisteid:

   a) „5G-võrgud“ – kõigi selliste asjaomaste võrgutaristu elementide kogum, mida kasutatakse mobiil- ja traadita side tehnoloogiates täiustatud käitamisnäitajatega (näiteks ülisuur andmeedastuskiirus ja läbilaskevõime, lühikese latentsusajaga ühendused ning ülisuur töökindlus) ühenduvusteenuste ja lisaväärtusega teenuste jaoks või paljude omavahel ühendatud seadmete töö toetamiseks. Need võivad hõlmata pärandvõrgu elemente, mis põhinevad varasema põlvkonna mobiil- ja traadita side tehnoloogial (nt 4G või 3G). 5G-võrkude mõiste peaks hõlmama kõiki võrgu asjaomaseid osi;

   b) „digitaalse ökosüsteemi aluseks olev taristu“ – taristu, mida kasutatakse kriitilise tähtsusega rakenduste kaudu majanduse ja ühiskonna digitaliseerimiseks.

III. **RIIKIDE TASANDIL VÕETAVAD MEETMED**

3. Liikmesriigid peaksid 30. juuniks 2019 teostama 5G-võrgutaristu riskihindamise ning tegema muu hulgas kindlaks kõige tundlikumad elemendid, kus turvarikkumistel oleks märkimisväärne negatiivne mõju. Samuti peaksid liikmesriigid samaks kuupäevaks läbi vaatama ka riiklikul tasandil kohaldatavad turvanõuded ja riskijuhtimismeetodid, et võtta arvesse küberohtusid, mis võivad tuleneda i) tehnilistest teguritest, nagu 5G-võrkude spetsiifilised tehnilised omadused, ja ii) muudest teguritest, nagu õigus- ja poliitikaraamistik, mida võidakse info- ja kommunikatsioonitehnoloogia seadmete tarnijate suhtes kohaldada kolmandates riikides.

4. Kõnealuse riikliku riskihindamise ja läbivaatamise põhjal ning võttes arvesse liidu tasandil koordineeritavaid meetmeid, peaksid liikmesriigid:

   a) ajakohastama 5G-võrkude puhul kohaldatavaid turvanõudeid ja riskijuhtimismeetodeid;

   b) ajakohastama asjaomaseid kohustusi, mis on kehtestatud üldkasutatavaid sidevõrke või üldkasutatavaid elektroonilise side teenuseid pakkuvatele ettevõtjatele vastavalt direktiivi 2002/21/EÜ artiklitele 13a ja 13b;

   c) lisama üldloale tingimusi, mis käsitlevad üldkasutatavate võrkude turvalisust loata juurdepääsu seisukohast ja nõudma, et ettevõtjad, kes osalevad mis tahes tulevases 5G sagedusalade raadiosageduste kasutamise õiguste andmise menetluses, võtaksid kohustuse täita võrkude turvalisusega seotud nõudeid vastavalt direktiivile 2002/20/EÜ;

   d) rakendama muid ennetavaid meetmeid, mille eesmärk on maandada võimalikke küberturvalisuse riske.

5. Punktis 4 osutatud meetmed peaksid hõlmama tarnijate ja ettevõtjate rangemat kohustust tagada võrkude tundlike osade turvalisus ning vajaduse korral muid kohustust, näiteks anda riigi pädevatele asutustele asjakohast teavet seoses kavandatavate muudatustega elektroonilise side võrkudes, ja nõuet, mille kohaselt peavad riiklikud auditeerimis- ja sertifitseerimislaborid turvalisuse ja usaldusväärsuse huvides konkreetseid infotehnoloogia-komponente ja -süsteeme eelnevalt testima.

6. Näiteks juhul kui sama ettevõtja käitab või ehitab võrgutaristut rohkem kui ühes liikmesriigis või kui võrgu konfiguratsioonides on suuri sarnasusi, peaksid ühiseid turvalisusalaseid läbivaatamisi tegema kaks või enam liikmesriiki, kes kasutavad ja jagavad asjakohaseid tehnilisi teadmisi ja vahendeid, mis on seotud digitaalse ökosüsteemi ja 5G-võrkude aluseks oleva taristuga. Euroopa Liidu Küberturvalisuse Amet (ENISA), Europol ja Elektroonilise Side Euroopa Reguleerivate Asutuste Ühendatud Amet (BEREC) peaksid seadma selles valdkonnas liikmesriikide esitatud abitaotlused prioriteediks. Kõnealuste läbivaatamiste tulemused tuleks edastada koostöörühmale ja küberturbe intsidentide lahendamise üksuste võrgustikule.

IV. **LIIDU TASANDIL KOORDINEERITAVAD MEETMED**

7. Selleks et töötada välja ühine lähenemisviis 5G-võrkude küberturvalisusriskide maandamiseks, peaksid liikmesriigid alustama 30. aprilliks 2019 koostöörühmas tööd spetsiaalses töösuunas. Vajaduse korral peaksid liikmesriigid kutsuma asjaomaseid asutusi osalema koostöörühma töös.

Euroopa koordineeritud riskihindamine

8. Liikmesriigid peaksid vahetama omavahel ja asjaomaste liidu asutustega teavet, et suurendada ühist teadlikkust 5G-võrkudega seotud olemasolevatest ja võimalikest küberturvalisuse riskidest.

9. Liikmesriigid peaksid edastama oma riiklikud riskihinnangud komisjonile ja Euroopa Liidu Küberturvalisuse Ametile (ENISA) 15. juuliks 2019.

10. Euroopa Liidu Küberturvalisuse Amet (ENISA) peaks koostama eraldi 5G-võrkude ohtude kaardistamise aruande. Seda protsessi peaksid toetama direktiivi (EL) 2016/1148 kohaselt loodud koostöörühm ja küberturbe intsidentide lahendamise üksuste võrgustik.

11. Võttes arvesse kõiki neid elemente, peaksid liikmesriigid komisjoni toel ja koos Euroopa Liidu Küberturvalisuse Ametiga (ENISA) viima 1. oktoobriks 2019 lõpule digitaalse ökosüsteemi ja eelkõige 5G-võrkude aluseks oleva taristuga seotud kogu liitu hõlmavate riskide ühise läbivaatamise.

12. Kõnealuse ühise läbivaatamise puhul tuleks eelkõige analüüsida riske, millele on avatud 5G-võrkude põhielementides sisalduvad eriti tundlikud või haavatavad elemendid, operatsiooni- ja hoolduskeskus, samuti 5G-juurdepääsuvõrgu elemendid, mida kasutatakse tööstuslikes rakendustes.

13. Teises etapis tuleks kõnealust ühist läbivaatamist laiendada digitaalse väärtusahela muudele strateegilistele elementidele.

Liidu ühine meetmete kogum riskide maandamiseks

14. Koostöörühma töö raames tuleks kindlaks teha punkti 4 kohased riikide tasandil rakendatavad parimad tavad. Riikide parimate tavade alusel tuleks 31. detsembriks 2019 kokku leppida asjakohaste, tulemuslike ja proportsionaalsete riskijuhtimismeetmete kogum, millega saab maandada liikmesriigi ja liidu tasandil tuvastatud küberturvalisuse riske, et anda komisjonile nõu ühiste miinimumnõuete väljatöötamiseks, et tagada 5G-võrkude küberturvalisuse kõrge tase kogu liidus.

15. See meetmete kogum peaks hõlmama järgmist:

a) selliste turvariskiliikide loetelu, mis võivad mõjutada 5G-võrkude küberturvalisust (nt tarneahela risk, tarkvara haavatavuse risk, juurdepääsukontrolli risk ning riskid, mis tulenevad õigus- ja poliitikaraamistikust, mida võidakse info- ja kommunikatsioonitehnoloogia seadmete tarnijate suhtes kohaldada kolmandates riikides); ning

b) võimalike maandavate meetmete loetelu (nt kolmanda isiku teostatav riistvara, tarkvara või teenuste sertifitseerimine, ametlikud riistvara ja tarkvara testid või vastavuskontroll ning protsessid, millega tagatakse juurdepääsukontrolli korra olemasolu ja selle järgimine, selliste toodete, teenuste või tarnijate kindlakstegemine, mida võib pidada ebaturvalisteks jne). Need meetmed peaksid käsitlema igat liiki turvariske, mis on pärast riskihindamist kindlaks tehtud ühes või mitmes liikmesriigis.

16. Pärast seda, kui on välja töötatud 5G-võrkude jaoks asjakohased Euroopa küberturvalisuse sertifitseerimise kavad, peaksid liikmesriigid kooskõlas liidu õigusega võtma vastu riiklikud tehnilised normid, millega nähakse ette kõnealuste kavadega hõlmatud info- ja kommunikatsioonitehnoloogia toodete, teenuste või süsteemide kohustuslik sertifitseerimine.

17. Liikmesriigid peaksid koos komisjoniga määrama kindlaks tingimused, mis käsitlevad üldkasutatavate võrkude turvalisust loata juurdepääsu seisukohast ja mis lisatakse üldloale, ning võrkude turvanõuded, mille alusel nõutakse, et ettevõtjad, kes osalevad 5G sagedusalade raadiosageduste kasutamise õiguste andmise menetluses, võtaksid kohustuse täita direktiivi 2002/20/EÜ nõudeid. Võimaluse korral peaksid need kajastuma punkti 4 alapunkti c kohaselt võetud meetmetes.

18. Liikmesriigid peaksid tegema komisjoniga koostööd, et töötada välja konkreetsed turvanõuded, mida saaks kohaldada 5G-võrkudega seotud riigihangete puhul. See peaks hõlmama kohustuslikke nõudeid küberturvalisuse sertifitseerimise kavade rakendamiseks riigihangete puhul, kui sellised kavad ei ole veel kõigi tarnijate ja ettevõtjate jaoks siduvad.

V. **LÄBIVAATAMINE**

19. Liikmesriigid peaksid tegema komisjoniga koostööd, et hinnata käesoleva soovituse mõju 1. oktoobriks 2020, et määrata kindlaks asjakohased edasised sammud. Hindamisel tuleks arvesse võtta liidu kooskõlastatud riskihindamise ja liidu meetmete kogumi rakendamise tulemusi.

Strasbourg, 26. märts 2019

Komisjoni nimel

komisjoni liige

Julian KING