



Brüssel, 29.1.2020
COM(2020) 50 final

**KOMISJONI TEATIS EUROOPA PARLAMENDILE, NÕUKOGULE, EUROOPA
MAJANDUS- JA SOTSIAALKOMITEELE NING REGIOONIDE KOMITEELE**

5G turvaline kasutuselevõtt ELis: ELi meetmepaketi rakendamine

1. Sissejuhatus

Telekommunikatsioonivõrkude viies põlvkond (5G) hakkab mängima keskset rolli Euroopa ühiskonna ja majanduse arengus. Eeldatakse, et see annab tohutud majanduslikud võimalused ja on oluline digitaalsete ja keskkonnasäästlike muutuste alus sellistes valdkondades nagu transport, energia, tootmine, tervishoid, põllumajandus ja meedia.

Niisiis on võimalik, et 5G hakkab mõjutama ELi kodanike elu enam-vähem kõiki aspekte. Seega on 5G-võrkude küberturvalisus ülimalt oluline mitte ainult liidu ja liikmesriikide majanduse, ühiskonna ja demokraatlike protsesside kaitse seisukohast, vaid ka selleks, et tagada usaldusväärne ja kõigile ELi kodanikele kasulik digipööre.

Paljude elutähtsate teenuste sõltuvus 5G-võrkudest muudaks süsteemse ja laiaulatusliku halvamise tagajärjed eriti raskeks ning sellel võiksid tulenevalt digitaalsete ökosüsteemide omavahelisest seotusest olla märkimisväärne piiriülene mõju. Ajal, mil küberründed on saenenud, keerulisemad kui kunagi varem ja nende autoriks on väga erinevad ohusubjektid (eeskätt ELi mittekuuluvad riigid või riigi toetusel tegutsevad isikud), on 5G-võrkude küberturvalisuse tagamine liidu jaoks strateegilise tähtsusega küsimus. Seoses selliste elutähtsate taristute nagu 5G turvalisusega on otsustatud esmakordselt määratleda Euroopa lähenemisviis. See lähenemisviis on täielikult kooskõlas põhimõttega, mille kohaselt ELi siseturg püsib avatuna, kui peetakse kinni ELi riskipõhistest turvanõuetest.

Euroopa Ülemkogu 22. märtsi 2019. aasta kohtumisel kutsuti üles käsitlema 5G-võrkude turvalisust kooskõlastatult. 26. märtsil 2019 võttis komisjon vastu soovitus (EL) 2019/534 5G-võrkude küberturvalisuse kohta¹. Soovitus esitati liikmesriikidele üleskutse viia lõpule riiklik riskihindamine, vaadata läbi riiklikud meetmed, teha ELi tasandil koostööd riskide koordineeritud hindamiseks ja koostada ühine võimalike leevendusmeetmete pakett. Kõnealune teatis on lahutamatu osa komisjoni laiaulatuslikust Euroopa digitaalarengu strateegiast, mida Euroopa Ülemkogu kutsus üles looma.

2. 5G kasutuselevõtt ELis

5G-võrkude taristu rajamine Euroopasse on liidu tööstusstrateegia ja konkurentsivõime jaoks äärmiselt tähtis. Komisjoni seisukoht on, et 5G-võrkude tehnoloogia juurutamine on üks peamisi elemente, mis teeb tulevased digiteenused võimalikuks. 2016. aastal võttis komisjon vastu 5G tegevuskava, mille eesmärk on tagada sellise ühenduvustaristu olemasolu liidus, mida on vaja digipöörde jaoks alates 2020. aastast ning linnapiirkondade ja suuremate transpordisõlmede laialdaseks katmiseks 2025. aastaks². Teatise gigabitiühiskonna kohta seatakse sihiks tagada juurdepääs mobiilsele andmesidele kõikjal,³ kaasa arvatud maapiirkondades ja ääremadel.

Mis puudutab sageduste eraldamist, siis liikmesriigid on eraldanud 16 % esimestest 5G sagedusaladest⁴. Tulenevalt juriidilisest kohustusest võimaldada aasta lõpuks kõigi esimeste

¹ Soovitus (EL) 2019/534 5G-võrkude küberturvalisuse kohta (ELT L 88, 29.3.2019, lk 42–47).

² 14. juuni 2016. aasta dokument (COM (2016) 588) „5G Euroopa jaoks: tegevuskava“.

³ Dokument (COM (2016) 587) „Ühenduvus konkurentsivõimelise digitaalse ühtse turu jaoks – Euroopa gigabitiühiskonna poole“.

⁴ <http://www.5GObservatory.eu>

5G sagedusalade kasutamist on järgnevate kuude jooksul oodata mitme menetlusega seotud konsultatsioone kasutamiseõiguse andmiseks.

Euroopa on üks 5G-teenuste kommertskasutuse valdkonna eesrindlasi maailmas⁵. Praeguse seisuga peaksid esimesed 5G-teenused olema 138 Euroopa linnas kättesaadavad 2020. aasta lõpuks. Varased 5G-võrgud rajanevad praegusel neljanda põlvkonna (4G) võrgutehnoloogial ja 5G-teenuseid osutatakse ennekõike laiemale üldsusele, seda kas 4G mahu ja kiiruse suurendamise vormis või kulutõhusa traadita alternatiivina püsivõrkudele⁶.

Seoses võimalustega uute ettevõtjatevaheliste teenuste vallas näiteks energeetika-, toiduainete-, põllumajandus-, tervishoiu- tööstus- ja transpordisektoris on Euroopa teinud tublisid edusamme: investeeritud on umbes miljard eurot, sealhulgas 300 miljonit eurot ELi vahenditest programmi „Horisont 2020“ alla kuuluva avaliku ja erasektori 5G alase partnerluse raames. Nimetatud investeering hõlmab enam kui 160 suuremahulist 5G katseprojekti Euroopas, sealhulgas kümme piiriülest kiirteekoridori 5G-põhise ühendatud ja automatiseeritud liikuvuse teenuste suuremahuliseks katsetamiseks. 5G-valmidusega rakendusi katsetatakse eri valdkondades kestlikust tervishoiust, automatiseeritud liikuvusest ja ressursitõhusast põllumajandusest nutikate elektrivõrkude ja neljanda tööstusrevolutsioonini (Industry 4.0). Lisaks sellele andis EIP Euroopa Strateegiliste Investeeringute Fondi toetusel laene 5G-tehnoloogia alase teadus- ja arendustegevuse kiirendamiseks.

Euroopa elektroonilise side seadustik (edaspidi „seadustik“),⁷ mida hakatakse kohaldama 21. detsembrist 2020, on oluline alus, millele tuginedes luua 5G- ja edasistesse võrkudesse investeerimist soodustav keskkond. Lisaks sellele on 5G-võrkude tulevase kasutuselevõtu seisukohast äärmiselt olulised ka avaliku sektori rahastamisprogrammid, nagu Euroopa ühendamise rahastu digitaalvaldkonna osa⁸ või Euroopa struktuuri- ja investeerimisfondid, ennekõike kuna need viivad kokku kogukonnad ja 5G-valmidusega teenused, nagu koolid, haiglad, linnad ja kohalikud haldusasutused.

Võttes arvesse Euroopa strateegilisi võimalusi erinevatele tegevusvaldkondadele pakutavate 5G-teenuste alal, peavad ettevõtjad ja teenuseosutajad ilmtingimata investeerima tiptasemel 5G-võrkudesse ja teeninduslahendustesse. Lisaks uutele 5G-põhistele raadio juurdepääsuvõrkudele on selleks vaja ka uusi autonoomseid 5G tuumikvõrke, et teha võimalikuks 5G keerukamad funktsioonid, nagu võrkude tükeldamine⁹ ja servtöötlus¹⁰.

Komisjon toetab ka edaspidi 5G kasutuselevõttu ELis ning teeb selleks muu hulgas koostööd liikmesriikide ja sidusrühmadega, et kasutada ära 5G pakutavaid võimalusi. Koostöös

⁵ <http://www.5GObservatory.eu>

⁶ Mõned 5G uutest funktsioonidest juurutatakse etapiti. Esimeses etapis (väga lühikese või lühikese aja jooksul) tähendab 5G kasutuselevõtt peamiselt mitteautonoomseid võrke, mille puhul 5G-tehnoloogiale viiakse üle ainult raadio juurdepääsuvõrk ja ülejäänus tuginetakse jätkuvalt olemasolevatele 4G tuumikvõrkudele, mis pakuvad lõppkasutajatele endisest paremat mobiilset lairibaühendust. Järgmistes etappides (lühikese ja keskmise kuni pika aja jooksul) toimub autonoomsete 5G-võrkude, sealhulgas 5G tuumikvõrkude kasutuselevõtt, mis ühest küljest eeldab võrguarhitektuuri tunduvalt ulatuslikumat muutumist ning teisalt põhjustab seda aja jooksul ise.

⁷ Euroopa Parlamendi ja nõukogu direktiiv (EL) 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik (uuesti sõnastatud).

⁸ 6. juuni 2018. aasta ettepanek (COM(2018)438) määruse kohta, millega luuakse Euroopa ühendamise rahastu ning tunnistatakse kehtetuks määrused (EL) nr 1316/2013 ja (EL) nr 283/2014.

⁹ 5G-võrkude tükeldamine võimaldab ühe ja sama füüsilise võrgu erinevad teenuskihid üksteisest olulisel määral lahus hoida, suurendades seeläbi võimalusi pakkuja kogu võrgu piires diferentseeritud teenuseid.

¹⁰ Servtöötlus on üks hajustöötuse paradigma, mis viib arvutamise ja andmesalvesti lähemale paigale, kus neid vajatakse, et parandada reaktsiooniaega ja säästa edastusressursse.

asjakohaste rahvusvaheliste organisatsioonide ja teadusringkondadega võetakse ettevaatuspõhimõttest¹¹ lähtuvalt nagu kord ja kohus arvesse tervisega seotud aspekte.

3. ELi koordineeritud riskihindamine 5G-võrkude küberturvalisuse teemal

Koostöös võrgu- ja infoturbe¹² koostöörühmaga tegi iga liikmesriik oma 5G-võrkude taristu kohta riikliku riskihindamise ning saatis tulemused 2019. aasta juuli alguseks komisjonile ja Euroopa Liidu Küberturvalisuse Ametile (ENISA).

Nende riiklike riskihindamiste põhjal avaldas liikmesriikide, komisjoni ja ENISA esindajatest koosnev võrgu- ja infoturbe koostöörühm 9. oktoobril 2019 aruande, mis käsitles ELi koordineeritud riskihindamist 5G-võrkude küberturvalisuse teemal¹³. Kõnealuses aruandes on loetletud 5G-võrke puudutavad peamised ohud ja ohusubjektid, kõige tundlikumad varad ja peamised (nii tehnilised kui ka muud liiki) nõrkused. Selle põhjal nimetati aruandes ka terve hulk ELi seisukohast strateegilise tähtsusega riske, näitlikustades need konkreetsete riskistsenaariumidega, mis kajastavad eri parameetrite (nõrgad kohad, ohud ja ohusubjektid) asjaomaseid kombinatsioone eri varade puhul (vt liide).

Aruande täiendamiseks ja lisapanusena meetmepaketti koostas ENISA spetsiaalse ohtude kaardi,¹⁴ mis kujutab enesest teatavate tehniliste aspektide üksikasjalikku analüüsi ja kus on ennekõike esitatud võrguvarad ja neid mõjutavad ohud.

Aruandes ELi koordineeritud riskihindamise kohta juhitakse tähelepanu mitmele 5G-võrkude jaoks olulisele aspektile. Eriti rõhutatakse järgmist.

a) 5Gga kaasnevate tehnoloogiliste muudatustega tekib kokkuvõttes rohkem ründevõimalusi ja suureneb ründajate potentsiaalsete sissepääsupunktide arv:

– kuna võrreldes eelnevate mobiilsidevõrkude põlvkondadega on võrgu servades rohkem funktsioone ja võrgu arhitektuur on hajusam, võidakse mõned tuumikvõrgu funktsioonid integreerida võrkude muudesse osadesse, mistõttu suureneb vastavate seadmete tundlikkus (nt tugijaamad või MANO funktsioonid);

– tarkvara endisest suurem roll 5G-võrgu seadmetes suurendab riske, mis on seotud tarkvara arendamise ja uuendamise protsessidega, põhjustab uusi konfiguratsioonivigade riske ning tähendab, et iga mobiilsideoperaatori poolt võrgu kasutuselevõtu etapis tehtud valikutel hakkab olema julgeolekuanalüüsis olulisem koht.

b) Need uued tehnoloogilised võimalused suurendavad mobiilsideoperaatorite sõltuvust kolmandast isikust tarnijatest ja viimaste rolli 5G tarneahelas.

See omakorda loob uusi ründevõimalusi, mida võivad ära kasutada ohusubjektid – eriti ELi mittekuuluvad riigid või riigi toetusel tegutsevad isikud, kellel on suutlikkus (kavatsused ja

¹¹ Nõukogu 12. juuli 1999. aasta soovitus 1999/519/EÜ üldsuse kokkupuute piiramise kohta elektromagnetväljadega (0 Hz kuni 300 GHz).

¹² 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 (küberturvalisuse direktiiv). Võrgu- ja infoturbe koostöörühm loodi küberturvalisuse direktiiviga, et tagada ELi liikmesriikide küberturvalisuse alane strateegiline koostöö ja teabevahetus.

¹³ <https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security>

¹⁴ ENISA „5G ohtude kaardistamise aruanne“ <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks>.

vahendid) ELi liikmesriikide telekommunikatsioonivõrkude ründamiseks – , ja suurendab selliste rünnete potentsiaalset negatiivset mõju.

Pidades silmas kolmandast isikust tarnijate kaudu sooritatavate rünnete suurenenud ohtu, muutub eriti oluliseks individuaalsete tarnijate riskiprofiil, eriti juhul, kui asjaomasel tarnijal on võrgus või piirkonnas oluline kohalolu.

c) Suur sõltuvus ühest tarnijast suurendab avatust selle tarnija äritegevuse võimaliku ebaõnnestumisega kaasnevatele probleemidele ja selle võimalikke tagajärgi. Samuti tähendab see, et nõrkadel kohtadel või haavatavustel võivad olla tõsisemad tagajärjed ja et suureneb nende võimaliku kuritarvitamise oht ohusubjektide poolt, eelkõige juhul, kui satutakse sõltuvusse suure riskiga tarnijast.

d) Kui mõned 5G jaoks kavandatud kasutusviisid realiseeruvad, saab 5G-võrkudest lõpuks paljude elutähtsate IT-rakenduste tarneahela oluline osa, mis mitte lihtsalt ei mõjuta konfidentsiaalsus- ja privaatsusnõudeid, vaid tähendab, et nende võrkude terviklusest ja käideldavusest saab tõsine turvalisusprobleem nii riikide kui ka ELi jaoks.

Allikas: ELi koordineeritud riskihindamine.

ELi koordineeritud riskihindamise aruandes nenditakse lisaks sellele, et need probleemid loovad uue turvalisusparadigma, mistõttu tuleb ümber hinnata 5G-sektori ja selle tegutsemiskeskonna suhtes praegu kohaldatav poliitika- ja turvalisusraamistik ning muuta hädavajalikuks liikmesriikide poolsed vastavad leevendusmeetmed.

Selleks et kindlakstehtud riskidele tulemuslikult reageerida ning 5G-võrkude turvalisust ja vastupanuvõimet suurendada, on vaja terviklikku lähenemisviisi, mis tähendab, et kasutusele võetakse põhimeetmed ja nendega seotud toetavad tegevused, mille varal saab riske käsitleda üheaegselt. ELi koordineeritud riskihindamine lõi aluse, millest lähtudes määrata kindlaks riskileevendamismeetmed, mida saab rakendada riiklikul ja Euroopa tasandil.

Nõukogu 3. detsembri 2019. aasta järeldustes avaldati toetust koordineeritud riskihindamise järeldustele ja rõhutati „koordineeritud lähenemisviisi ja soovitusliku rakendamise tähtsust ühtse turu killustumise vältimiseks“¹⁵. Sel eesmärgil kutsus nõukogu liikmesriike, komisjoni ja ENISAd üles võtma „oma pädevuse piires kõiki vajalikke meetmeid, et tagada elektroonilise side võrkude, eriti 5G-võrkude turvalisus ja terviklus, ning jätkama kooskõlastatud lähenemisviisi tugevdamist 5G-tehnoloogiatega seotud turvalisuse alaste mureküsimumuste lahendamiseks.“

4. 5G-võrkude küberturvalisust käsitlevate ELi meetmete pakett

29. jaanuaril 2020 avaldas võrgu- ja infoturbe koostöörühm ELi riskileevendamismeetmete paketi¹⁶. Selles käsitletakse kõiki koordineeritud riskihindamise aruandes loetletud riske.

ELi meetmepaketis on loetletud ja kirjeldatud strateegilisi ja tehnilisi meetmeid, samuti nende juurde käivaid toetavaid tegevusi meetmete tulemuslikkuse suurendamiseks, mis võidakse

¹⁵ Nõukogu järeldused, milles käsitletakse 5G tähendust Euroopa majandusele ning vajadust leevendada 5G-ga seotud turvariske. 3. detsember 2019, 14517/19 <https://data.consilium.europa.eu/doc/document/ST-14517-2019-INIT/et/pdf>.

¹⁶ 5G-võrkude küberturvalisus: ELi riskileevendamismeetmete pakett, 29. jaanuar 2020 (<https://ec.europa.eu/digital-single-market/en/nis-cooperation-group>).

kehtestada kindlakstehtud riskide leevendamiseks. **Strateegilised meetmed** hõlmavad meetmeid, mis puudutavad ametiasutuste suuremaid reguleerimisvolutusi, et kontrollida võrkude hankemenetlusi ja kasutuselevõttu, erimeetmeid muude kui tehniliste nõrkustega seotud riskidega tegelemiseks, samuti võimalikke algatusi 5G tarne- ja väärtusahela kestlikkuse ja mitmekesisuse edendamiseks, vältimaks süsteemset pikaajalise sõltuvuse riski. **Tehniliste meetmete** seas on meetmed 5G-võrkude ja seadmete turvalisuse suurendamiseks tehnoloogiast, protsessidest ning inim- ja füüsilistest teguritest tulenevate riskide käsitlemise kaudu. Lisaks sellele on iga ELi koordineeritud riskihindamises nimetatud riskivaldkonna kohta esitatud **riskileevendamiskava**, mis põhineb kõige kõrgema tulemuslikkuse astmega meetmetel.

Nende seas on ELi meetmepaketi järeldustes vastavalt võrgu- ja infoturbe koostöörühmas kokkulepitule esitatud kõigile liikmesriikidele ja komisjonile soovitus rakendada teatavad **põhimeetmed**, mis on järgmised.

ELi meetmepaketi järeldused

ELi meetmepaketis on esitatud hulk meetmeid ja tegevusi, mis moodustavad nende sobiliku kombineerimise ja tulemusliku rakendamise korral aluse selle valdkonna kooskõlastatud lähenemisviisile. Arvestades ELi koordineeritud riskihindamises loetletud riskivaldkondade suurt arvu ja mitmekesisust, ei piisa üht liiki meetmetest – kõigi peamiste riskivaldkondadega tegelemiseks on vaja kasutada erinevaid meetmeid, neid omavahel sobilikult kombineerides.

Lähtudes võimalike riskileevendamiskavade hindamisest ja kõige tulemuslikumate meetmete kindlakstegemisest, soovitatakse meetmepaketis järgmist.

1. Kõik liikmesriigid peaksid tagama, et nad on võtnud meetmed – sealhulgas andnud riiklikele asutustele pädevuse – reageerida asjakohaselt ja proportsionaalselt praeguseks kindlakstehtud ja tulevastele riskidele, ning ennekõike tagama, et nad on suutelised kehtestama riskipõhist lähenemisviisi järgides piiranguid, keelde ja/või erinõudeid või -tingimusi 5G-võrkude seadmete tarnimise, paigaldamise ja käitamise suhtes turvalisusega seotud kaalutlustel.

Eelkõige peaksid nad:

*karmistama mobiilsideoperaatorite suhtes kohaldatavaid **turvanõudeid** (nt range juurdepääsukontroll, turvalise käitamise ja järelevalve nõuded, piirangud konkreetsete funktsioonide allhankimise suhtes jne);*

*hindama tarnijate riskiprofiili ja sellest tulenevalt **kohaldama kõrgeks hinnatava riskitasemega tarnijate suhtes sobilikke piiranguid** (sealhulgas vajalikke erandeid riskide tulemuslikuks leevendamiseks) selliste **põhivarade puhul**, mis on määratletud ELi koordineeritud riskihindamises kriitiliste ja tundlikena (näiteks tuumvõrgu funktsioonid, võrguhalduse ja võrgu orkestreerimise funktsioonid ning juurdepääsuvõrgu funktsioonid);*

*tagama, et igal operaatoril on asjakohane mitme teenuseosutajaga strateegia, et **vältida või piirata suurt sõltuvust** ühest tarnijast (või sarnase riskiprofiiliga tarnijatest), tagada tarnijate nõuetekohane tasakaal riiklikul tasandil ja **vältida sõltuvust kõrgeks hinnatava riskitasemega tarnijatest**. Selleks tuleb samuti vältida seotust ühe tarnijaga, sealhulgas edendades seadmete suuremat koostalitlusvõimet.*

2. Euroopa Komisjon koos liikmesriikidega peaks aitama:

säilitada pikaajalise sõltuvuse vältimiseks **mitmekesist ja kestlikku 5G tarneahelat**, muu hulgas:

o kasutades täielikult ära olemasolevaid ELi vahendeid, eriti uurides 5G põhivarasid puudutavate võimalike välismaiste otseinvesteeringute tausta ja vältides võimalikust dumpingust või subsideerimisest tulenevaid moonutusi 5G tarnete turul, ning

o tugevdades veelgi ELi suutlikkust 5G- ja 5G-järgse tehnoloogia valdkonnas, kasutades selleks asjakohaseid ELi programme ja rahastamist;

lihtsustada liikmesriikide vahelist kooskõlastamist **standardimise** valdkonnas, et saavutada konkreetset turvaeesmärgid ja töötada välja asjakohased kogu ELi hõlmavad **sertifitseerimissüsteemid**, et aidata kaasa toodete ja protsesside suuremale turvalisusele.

3. Selleks et tagada kooskõlastatud lähenemisviisi ajas kestma jäämine, tuleks laiendada võrgu- ja infoturbe koostöörühma volitusi, samuti koostööd teiste asjaomaste asutuste ja üksustega, ennekõike selleks, et:

vaadata komisjoni ja ENISA toetusel korrapäraselt läbi 5G- ja sellele järgnevate põlvkondade võrkude turvalisust käsitlevad **riiklikud ja ELi riskihindamised**, kasutatud hindamismetoodikat edasi arendades, seda kohandades ja pidades sammu areneva 5G-tehnoloogiaga;

kontrollima ja hindama liikmesriikide struktureeritud aruandluse põhjal üksikasjalikult ja korrapäraselt meetmepaketi **rakendamist**;

koordineerima ja toetama selliste **toetavate tegevuste** rakendamist, milleks on vaja ELi tasandi koostööd, eriti mis puudutab suuniste väljatöötamist ja erinevate meetmetega seotud heade tavade vahetamist;

toetama vajaduse korral täiendavat ELi tasandi koordineerimist, kui see on asjakohane, eriti eesmärgiga lähendada **operaatorite suhtes kehtivaid tehnilisi ja organisatsioonilisi turvanõudeid**.

Allikas: ELi meetmepakett.

Meetmepaketi järelused annavad tunnistust liikmesriikide kindlast nõust astuda 5G-võrkude turvalisusega seotud väljakutsetele vastu üheskoos. Sellel on põhimõtteline tähtsus nii liikmesriikide sisese kui ka kogu ELi turvalisuse, liikmesriikide majanduse, aga ka ELi siseturu ja Euroopa tehnoloogilise sõltumatuse seisukohast. Nii ELi koordineeritud riskihindamine kui ka ELi meetmepakett annavad tunnistust sellest, kui väärtuslikku ühistööd on võrgu- ja infoturbe koostöörühmas väsimatult teinud kõigi liikmesriikide, komisjoni ja ENISA esindajad.

Meetmepakett teeb võimalikuks ELi ühise lähenemisviisi 5G küberturvalisusele, toetades ELi poliitika ja koordineerimise varal järjepidevust kogu ühtsel turul, samuti liikmesriikide poolset oma pädevuse kasutamist ennekõike seoses riikliku julgeolekuga. Selles sisalduvad riskileevendamismeetmed ja -kavad võimaldavad anda 5G küberturvalisusega seotud ühistele probleemidele ELi tasandil asjakohase, tulemusliku ja proportsionaalse vastulöögi.

Komisjon tervitab 5G küberturvalisust puudutavate ELi meetmete paketi avaldamist ja toetab täielikult kõiki selle eespool esitatud järeldusi.

Komisjon kutsub liikmesriike ning asjaomaseid liidu institutsioone, ameteid ja muid asutusi üles:

- i) tagama tõhusate ja sobilike riskileevendamistrateegiatega kiire rakendamise kooskõlas ELi meetmepaketiga kõikjal ELis;
- ii) astuma kõik edasised sammud, mis on vajalikud liidu tasandi koordineerimiseks, muu hulgas jätkates tööd võrgu- ja infoturbe koostöörühmas ning võttes kasutusele töökindla mehhanismi ELi meetmepaketi rakendamise järelevalveks, et tagada meetmete tulemuslikkus ja siseturu sujuv toimimine.

5. Meetmepaketi rakendamine

5G turvalisust puudutava Euroopa lähenemisviisi usutavuse ja edu pant on liikmesriikide otsustavus meetmepaketi igakülgsel kasutamisel. Ehkki liikmesriigid otsustavad konkreetse meetme sobivuse üle oma riigis valitsevate olude põhjal, on kindlakstehtud riskidega tegelemiseks hädavajalik, et **kõigis liikmesriikides ja teatavate meetmete puhul ELi tasandil oleksid olemas võrgu- ja infoturbe koostöörühma soovitusel (vt eespool meetmepaketi järeldused) tuginevad põhimeetmed.**

Komisjon on valmis pakkuma ka järgmistes etappides oma täielikku toetust ja kutsub liikmesriike üles:

- astuma **30. aprilliks 2020** konkreetsed ja mõõdetavad sammud, et rakendada ELi meetmepaketi järeldustes soovitatud põhimeetmed;
- koostama **30. juuniks 2020** iga liikmesriigi kohta põhimeetmete rakendamist puudutava võrgu- ja infoturbe koostöörühma aruande, tuginedes korralisele aruandlusele ja järelevalvele, mida tehakse ennekõike võrgu- ja infoturbe koostöörühmas komisjoni ja ENISA toetusel.

5.1. 5G tarnijate riskipõhine kooskõlastatud käsitlusviis

Kuna lõppkokkuvõttes on eesmärk tagada 5G-võrkude turvalisus ja vastupanuvõime ning nende kestlikkus, leppisid liikmesriigid kokku, et on vaja hinnata iga konkreetse tarbija riskiprofiili ja sellest tulenevalt seada kõrgeks hinnatava riskitasemega tarnijatele põhivarade puhul kohased piirangud, sealhulgas vajalikud erandid riskide tulemuslikuks leevendamiseks põhivarade puhul, lähtudes meetmepaketist. Komisjon on valmis liikmesriike nende meetmete rakendamisel toetama.

Meetmete rakendamise toetamiseks kõikjal liidus on ELi koordineeritud riskihindamises ja ELi meetmepaketis esitatud suunised, mis puudutavad 1) tarnijate riskiprofiili hindamist¹⁷ ning 2) võrguelementide ja -funktsioonide,¹⁸ samuti muude varade tundlikkust. Nii ELi

¹⁷ ELi kooskõlastatud riskihindamise punkt 2.37.

¹⁸ ELi kooskõlastatud riskihindamise punktis 2.21 on esitatud elementide ja funktsioonide põhikategooriad ja nende tundlikkuse üldine tase ning loetletud iga kategooria puhul terve hulk liikmesriikide kindlaks tehtud põhielemente,

koordineeritud riskihindamine kui ka meetmepaketi meetmed käsitlevad riske, mis on seotud 5G võrguseadmete ja võrguteenuste tarnijatega. Need ei puuduta muid tooteid või teenuseid, mida need või muud tarnijad võivad pakkuda.

ELi koordineeritud riskihindamise punkti 2.37 kohaselt võib konkreetse tarnija riskiprofiili hinnata mitme teguri põhjal.

Tarnijate riskiprofiile tuleks hinnata ainuüksi turvalisuskaalutlustel ja hindamine peaks põhinema objektiivsetel kriteeriumidel. Selleks et hõlbustada kooskõlastatud lähenemisviisi nende meetmete rakendamisele, on meetmepaketis soovitatud, et liikmesriigid vahetaksid teavet riiklike lähenemisviiside ja heade tavade kohta. Lisaks sellele on komisjon seisukohal, et selline tegevus peaks olema võrgu- ja infoturbe koostöörühmas koos komisjoni ja ENISAGA tehtava töö järgmise etapi üks prioriteete.

Kõrgeks hinnatava riskitasemega tarnijatele seatavad piirangud, sealhulgas riskide tulemuslikuks leevendamiseks vajalikud erandid, samuti meetmed sõltuvuse vältimiseks sellistest tarnijatest, tuleb ilmtingimata rakendada õigeaegselt. Kui seda tehakse kõige varasemas etapis, sealhulgas võimaluse korral 5G-sageduste litsentsimise kontekstis, muudab see olukorra turuosaliste jaoks paremini prognoositavaks, aidates nii kaasa 5G-võrkude kiirele kasutuselevõtule ning tagades 5G-võrkude pikaajalise turvalisuse ja 5G tarneahela vastupidavuse.

Samal ajal võib nende meetmete rakendamine riiklikul tasandil ette kirjutada erinevad ajakavad, kui see on vajalik ja õigustatud, eriti juhul, kui juba sõltutakse suurel määral kõrgeks hinnatava riskitasemega tarnijate seadmetest või teenustest (nt võttes arvesse seadmete uuendamistsükleid, eriti üleminekut mitteautonoomsetelt 5G-võrkudelt autonoomsetele 5G-võrkudele). Liikmesriigid võiksid kaaluda selliste rakenduskavade visandamist, mis näeksid asjaomaste võrguoperaatorite puhul ette kohased üleminekuperioodid. Sellega seoses tuleks üleminekuperioodid määratleda selliselt, et säiliks või isegi suureneksid stiimulid investeerida ajakohastesse võrguseadmetesse, sealhulgas kiirendades iseseisvate (autonoomsete) 5G tuumikvõrkude kasutuselevõttu ja vahetades välja 4G-seadmed muudes võrkude osades (näiteks raadio juurdepääsuvõrkudes) kooskõlas 5G tegevuskava eesmärkidega¹⁹.

Lisaks sellele võivad telekommunikatsioonivõrkude operaatorid 5G tarkvaral põhinevate võrkude keerukuse tõttu üha enam jätta kolmandatest isikutest üksuste hooldes lisaks võrguseadmete tarnimisele ka sellised ülesanded nagu 5G-võrkude hooldamine ja uuendamine, samuti muud allhangitavad teenused. Vastavalt ELi koordineeritud riskihindamisele kujutab see enesest tõsise turvariski allikat. Seda aspekti tuleks niisiis eriti tähelepanelikult jälgida. Samuti tuleb ilmtingimata põhjalikult hinnata selliste tarnijate riskiprofiili turvalisust, kellele on ülesandeks tehtud nende teenuste osutamine, ennekõike juhul, kui nimetatud ülesandeid ei täideta ELis. Selleks et säilitada pikas perspektiivis 5G taristu terviklus, tuleks võtta asjakohased meetmed, sealhulgas ennekõike kohaldada piiranguid seoses 5G-võrkude tundlike osadega või vajalikke erandeid kõrge riskitasemega üksuste puhul vastavalt meetmepaketi riskileevendamismeetmetele.

punktides 2.28 ja 2.29 aga on kindlaks tehtud hulk muud liiki tundlikke varasid ja piirkondi (nt konkreetsed üksused või geograafilised piirkonnad).

¹⁹ 14. septembri 2016. aasta dokument (COM (2016) 588) „5G Euroopa jaoks: tegevuskava.“

5.2. Komisjoni roll meetmepaketi rakendamise toetamisel

Komisjon toetab jätkuvalt 5G küberturvalisust puudutava ELi lähenemisviisi rakendamist üldiselt ja lisaks sellele korraldab ka konkreetseid algatusi seoses nende meetmepaketi meetmete ja eesmärkidega, kus ta saab anda lisaväärtust. Vastavalt vajadusele kasutab komisjon täiel määral oma volitusi ja asjaomaseid vahendeid kindlakstehtud turvakaalutlustega tegelemiseks. Sel moel ning tegutsedes koos liikmesriikide ja erasektoriga tahab komisjon toetada strateegilisi meetmeid, mis aitavad tagada ELi tehnoloogilise sõltumatus ja juhirolli võrgutehnoloogia tulevases arengus, küberturvalisuse tehnoloogias ja kõigis neis elementides, millest meie majandus ja turvalisus sõltuvad.

Konkreetselt võtab komisjon järgmised meetmed, et tagada meetmepaketi vastavate riskileevendamismeetmete rakendamine tema pädevusse kuuluvates valdkondades.

5G-võrkude küberturvalisuse ja 5G väärtusahela mitmekesisuse tagamine

- **Küberturvalisuse alane koostöö:** jätkab liikmesriikide toetamist, et tagada riiklike meetmete tulemuslik, koordineeritud ja õigeaegne rakendamine võrgu- ja infoturbe koostöörühma vahendusel.
- **Telekommunikatsiooni ja küberturvalisust puudutavad normid:** toetab meetmepaketi selliste meetmete rakendamist, mis puudutavad turvanõudeid, eriti seoses elektroonilist sidet käsitlevate Euroopa õigusnormide vastavate sätetega, ning vaeb lisandväärtust, mis võib olla tehnilisi ja korralduslikke turvameetmeid täpsustavatel rakendusaktidel riiklike normide täiendamise ning operaatorite suhtes kehtestatud turvameetmete tulemuslikkuse ja järjekindluse suurendamise seisukohast.
- **Standardimine:** võtab Euroopa turvalisus- ja koostalitluseesmärkide saavutamiseks meetmeid, et säilitada Euroopa osalus vastavates standardiorganisatsioonides ja vajaduse korral seda suurendada. Ennekõike hindab ja edendab komisjon koos liikmesriikidega tehnilisi kirjeldusi ja standardeid, mis võimaldavad 5G tarnijate seadmete koostalitlust võrgu eri osades, sealhulgas pärandvõrkudes, et luua tõeline müüjate paljusus, näiteks avatud ja koostalitlusvõimeliste liideste abil.
- **Sertifitseerimine:** toetab 5G-võrkude vajadusi rahuldavaid 5G sertifitseerimiskavu vastavalt ELi küberturvalisuse alase sertifitseerimise raamistikule.
- **Välismaiste otseinvesteeringute taustauuringud:** toetab investeeringute taustauuringute ELi raamistiku rakendamist, kaardistades 5G väärtusahela, sealhulgas tundlikud võrguvarad, ja tehes korrapäraselt järelevalvet välismaiste otseinvesteeringute suhtes kogu väärtusahela ulatuses. Koosõlas välismaiste otseinvesteeringute taustauuringute ajakavaga (alates 2020. aasta oktoobrist) hakkab komisjon 5G valdkonda tehtud välisinvesteeringuid kontrollima vastavalt määruses EL 2019/452 esitatud suunistele, võttes arvesse ELi koordineeritud riskihindamist ja ELi meetmepaketti.
- **Kaubanduse kaitsemeetmed:** jälgib igasugust asjaomast arengut ELi ja kolmandate riikide turul ning kaitseb ELi ettevõtteid Euroopa 5G-turul kaubanduse kaitsemeetmeid kasutades võimalike kaubandust moonutavate tavade (dumping või subsideerimine) eest, muu hulgas algatades vajaduse korral esialgse uurimise.

– **Konkurentsieeskirjad:** jälgib 5G riist- ja tarkvara tarnete turgude toimimist, et tagada nende tegutsemise konkurentsi tingimustes, muu hulgas seoses võimaliku nn lõksujäämisega ühe tarnija kätte lepingulistel või tehnilistel põhjustel.

– **ELi rahastamisprogrammid:** tagab, et vastavaid tehnoloogiavaldkondi puudutavates ELi rahastamisprogrammides osalemise tingimus on turvanõuete täitmine, kasutades turvalisust puudutavaid nõudmisi täielikult ära ja rakendades neid teadusuuringute ja innovatsiooni programmides, eriti programmis „Euroopa horisont“, digitaalse Euroopa programmis, Euroopa ühendamise rahastu 2-s, Euroopa struktuuri- ja investeerimisfondides ja muudes asjaomastes programmides. Samasugust lähenemisviisi tuleks rakendada ka ELi väljapoole suunatud rahastamisprogrammide ja -vahendite puhul, muu hulgas rahvusvaheliste finantseerimisasutuste kaudu antava rahastuse puhul.

– **Riigihanked:** kasutab 5G-võrkude vallas korraldatud riigihankeid, et toetada 5G-võrkude puhul määratletud turvalisuse, tarnijate mitmekesisuse ja pikaajalise kestlikkusega seotud eesmärgi. Ennekõike püüab ta tagada, et 5G-võrkude valdkonnas riigihankelepingute sõlmimisel võetakse asjakohaselt arvesse turvalisusega seotud aspekte, nagu on ette nähtud ELi riigihanke-eeskirjadega.

– **Intsidentidele reageerimine ja kriisiohje (tegevuskava) ning küberturvalisuse õppused:** kasutab täielikult ära ulatuslikele küberturvalisuse intsidentidele koordineeritud reageerimist käsitleva ELi tegevuskava²⁰ väljatöötamist. Lisaks sellele kaalub ta koos ENISAgaga võimalust korraldada 5G küberturvalisuse õppused niipea, kui turg on selleks küps.

Lisaks sellele tehakse liidu välisasjade ja julgeolekupoliitika kõrge esindaja ja komisjoni asepresidendi ning nõukogu vastutusel järgmist.

– **Pahatahtlikule kübertegevusele ELi ühise diplomaatilise reageerimise raamistik (küberdiplomaatia meetmete kogum)²¹:** ELi puutumatust ja julgeolekut ohustava pahatahtliku kübertegevuse korral kutsutakse liikmesriike üles kasutama ELi küberdiplomaatia meetmete kogumisse kuuluvaid ühise välis- ja julgeolekupoliitika meetmeid, sealhulgas vajaduse korral piiravaid meetmeid, et soodustada koostööd, hõlbustada ohtude leevendamist ja mõjutada võimalike ründajate käitumist.

Lisaks sellele aitab mitu programmi kaasa selliste eesmärkide saavutamisele nagu pikaajalise sõltuvuse vältimine või sellesse sattumise ohu piiramine, propageerides mitmekesist ja kestlikku 5G-turgu, muu hulgas säilitades ELi võimekuse 5G väärtusahelas ning investeerides innovatsiooni, järgides seejuures ELi rahvusvahelisi kohustusi.

Küberturvalisuse ja võrgutaristehnoloogia alase innovatsiooni ja investeerimise propageerimine

– **ELi rahastamisprogrammid:** suurendada investeringuid võrgutehnoloogia ja selle aluseks olevate elementide alastes teadusuuringutesse ja innovatsiooni ning nende kasutuselevõttu. Komisjon on teinud ettepaneku investeerida ELi järgmises eelarves (2021–2027) küberturvalisustehnoloogiasse ligi 3 miljardit eurot. See hõlmab teadustegevust ja

²⁰ Komisjoni soovitus (EL) 2017/1584 koordineeritud reageerimise kohta ulatuslike küberturvalisuse intsidentide ja kriiside korral.

²¹ Nõukogu 20. novembri 2017. aasta järeldused 9916/17.

innovatsiooni programmi „Euroopa horisont“ raames ning toetust küberturvalisuse alasele suutlikkusele digitaalse Euroopa programmi raames. InvestEU programm saab samuti anda rahalist toetust 5G valdkonna teadus- ja arendustegevusele ning toetada selle kasutuselevõttu.

Lisaks sellele on komisjon teinud ettepaneku luua järgmise programmi „Euroopa horisont“²² raames ELi institutsiooniline partnerlus seoses valdkonnaga NGI/6G („Arukad võrgud ja teenused“) koostöös tööstusega ja koordineerides tegevust liikmesriikidega, et viia lõpule 5G kasutuselevõtt ja ennekõike selleks, et valmistuda mobiilsidetehnoloogia järgmise põlvkonna, **6G tulekuks**. Tehtud on ettepanek investeerida ELi eelarvest (2021–2027) enam kui 2,5 miljardit eurot; sellele lisandub käesoleva algatuse jaoks vähemalt 7,5 miljardit eurot erasektori investeeringuid.

– **Tööstuslik arendamine ja kasutuselevõtt:** hindab 5G väärtusahelas esineda võivad turulünki või probleeme, mis õigustaksid suunatud meetmeid järgmise pikaajalise eelarve raames või võimaliku küberturvalisuse teemalise üleeuroopalist huvi pakkuva tähtsa projekti raames vastavalt üleeuroopalist huvi pakkuvate tähtsate projektide kõrgetasemelise foorumi soovitudele. Üleeuroopalist huvi pakkuvate tähtsate projektide kavandamise ja korraldamise üle otsustavad liikmesriigid ja ettevõtted. ELi normid toimivad tugiraamistikuna ning komisjon on valmis vajalikke kontakte soodustama ja suuniseid andma.

²² Rahastamine on võimalik ka Euroopa ühendamise rahastu versioonist 2.0 ja digitaalse Euroopa programmist.

6. Kokkuvõte

5G-võrgud annavad Euroopa kodanikele, ühiskonnale ja majandusele terve hulga võimalusi. Seepärast on 5G-võrkude turvalisuse ja vastupidavuse tagamine äärmiselt oluline. Teisalt on küberohud – sealhulgas ELi mittekuuluvate riikide või riigi toetusel tegutsevate isikute sekkumise risk – pidevalt arenev probleem, mis on üha tõsisem sedamööda, kuidas kasvab sõltuvus tehnoloogiast ja andmetest. Küberturvalisuse hooletusse jätmine õnestsaks usaldust digitaalrajanduse ja -ühiskonna vastu ega laseks EL-il sellest täit kasu saada. Selleks on vaja samamoodi pidevalt arenevat ja jõulist vastulööki.

Koordineeritud ja järjepidev lähenemisviis elutähtsate tehnoloogiavaldkondade ja võrkude küberturvalisusele ELis on ELi jaoks hädavajalik, et tagada oma tehnoloogiline sõltumatus ning säilitada tööstusvõimekus ja seda edendada. Komisjon toetab täielikult 5G-võrkude küberturvalisust käsitleva ELi lähenemisviisi rakendamist, tagades samal ajal, et ELi turud jäävad avatuks toodetele ja teenustele, mis vastavad küberturvalisuse ja usaldusväarsuse üha arenevatele nõuetele.

Selle eesmärgi saavutamiseks on oluline, et kõik 5G turvalisusega seotud sidusrühmad püsiksid ihu ja hingega asja juures ja et liikmesriikide, komisjoni ja ENISA koostöö jätkuks.

Järgmise sammuna kutsub komisjon liikmesriike üles, nagu eespool mainitud, kiiresti tegutsema meetmepaketi raames kokku lepitud meetmete tulemuslikuks ja objektiivseks rakendamiseks ning jätkama komisjoni ja ENISA toetusel koostööd ELi tasandi koordineerimise tagamiseks. Samal ajal teeb komisjon algust kõigi tema pädevusse kuuluvate asjaomaste toimingutega, et toetada meetmepaketi rakendamist liikmesriikides ja võimendada selle mõju.

Liide. Riskikategooriad (allikas: ELi koordineeritud riskihindamine)

	Riskikategooriad
Ebapiisavate turvameetmetega seotud riskistsenaariumid	<i>R1: võrkude väär konfigureerimine</i>
	<i>R2: puudulik juurdepääsukontroll</i>
5G tarneahelaga seotud riskistsenaariumid	<i>R3: toodete halb kvaliteet</i>
	<i>R4: üksikute võrkude sõltuvus ühest tarnijast või riigisisese mitmekesisuse puudumine</i>
Peamiste ohusubjektide tegutsemisviisiga seotud riskistsenaariumid	<i>R5: riigi sekkumine 5G tarneahela kaudu</i>
	<i>R6: Lõppkasutajate vastu sihitud 5G-võrkude ärakasutamine organiseeritud kuritegevuse või kuritegeliku organisatsiooni poolt</i>
5G-võrkude ja muude elutähtsate süsteemide vastastikuse sõltuvusega seotud riskistsenaariumid	<i>R7: elutähtsa taristu või elutähtsate teenuste tõsised häired</i>
	<i>R8: ulatuslikud tõrked võrkude töös elektrivarustuse või muude tugisüsteemide katkestuse tõttu</i>
Lõppkasutajate seadmetega seotud riskistsenaariumid	<i>R9: Asjade interneti kuritarvitamine</i>