EUROOPAN
KOMISSIO

Bryssel 29.1.2020
COM(2020) 50 final

KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE, NEUVOSTOLLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE JA ALUEIDEN KOMITEALLE

5G:n turvallinen käyttöönotto EU:ssa – EU:n välineistön täytäntöönpano

1. Johdanto

Viidennen sukupolven (5G) televiestintäverkoilla tulee olemaan keskeinen merkitys eurooppalaisen yhteiskunnan ja talouden kehityksen kannalta. Niiden odotetaan tarjoavan valtavia taloudellisia mahdollisuuksia ja muodostavan tärkeän perustan digitalisaatiolle ja vihreälle muutokselle sellaisilla aloilla kuin liikenne, energia, valmistusteollisuus, terveydenhuolto, maatalous ja media.

5G-verkot voivat vaikuttaa lähestulkoon kaikkiin EU:n kansalaisten elämänalueisiin. 5G-verkkojen kyberturvallisuus on sen vuoksi olennaisen tärkeää, jotta voidaan suojella talouksiamme, yhteiskuntiamme ja demokraattisia järjestelmiämme ja lisäksi taata yhteiskunnan luotettava digitaalinen muutos kaikkien EU:n kansalaisten hyödyksi.

Monien kriittisten palvelujen riippuvuus 5G-verkoista merkitsee sitä, että systeemisten ja laajojen häiriöiden seuraukset olisivat erityisen vakavia. Koska digitaaliset ekosysteemit ovat luonteeltaan yhteenliitettyjä, tällaisilla häiriöillä voisi olla merkittäviä vaikutuksia yli kansallisten rajojen. Tämän vuoksi 5G-verkkojen kyberturvallisuus on unionille strategisesti tärkeä kysymys aikana, jolloin kyberhyökkäysten määrä on kasvussa, ne ovat entistä sofistikoituneempia ja niiden takana on hyvin monia eri uhkatoimijoita, myös EU:n ulkopuolisia valtioita tai valtion tukemia toimijoita. 5G-verkkojen kaltaisten kriittisten infrastruktuureiden turvallisuuden takaamiseksi tarkoituksena on nyt määritellä ensimmäistä kertaa yhteiset eurooppalaiset toimintaperiaatteet. Tämä lähestymistapa ei millään tavoin rajoita EU:n sisämarkkinoiden avoimuutta, kunhan riskiperusteisia EU:n turvallisuusvaatimuksia noudatetaan.

Eurooppa-neuvosto kehotti 22. maaliskuuta 2019 omaksumaan yhteisen lähestymistavan 5G-verkkojen turvallisuuteen. Komissio antoi 26. maaliskuuta 2019 suosituksen (EU) 2019/534 5G-verkkojen kyberturvallisuudesta[1]. Suosituksessa jäsenvaltioita kehotettiin laatimaan kansalliset riskinarvioinnit ja tarkistamaan kansallisia vaatimuksia ja menetelmiä sekä tekemään EU:n tasolla yhteistyötä koordinoitua riskinarviointia varten ja valmistelemaan mahdollisista riskienhallintatoimenpiteistä koostuva välineistö. Tämä tiedonanto on osa kattavaa eurooppalaista digitaalistrategiaa, jonka Eurooppa-neuvosto on pyytänyt komissiota laatimaan.

2. 5G:n käyttöönotto EU:ssa

5G-verkkoinfrastruktuurin käyttöönotto Euroopassa on keskeinen tekijä Euroopan teollisuusstrategian ja kilpailukyvyn kannalta. Komissio katsoo, että 5G-verkkoteknologioiden käyttöönotto on merkittävä tulevien digitaalisten palvelujen mahdollistaja. Komissio hyväksyi vuonna 2016 5G-toimintasuunnitelman varmistaakseen, että unionilla on digitaalisen muutoksen edellyttämä verkkoinfrastruktuuri vuodesta 2020 eteenpäin ja jotta se voidaan ottaa kattavasti käyttöön kaupunkialueilla ja tärkeimmillä liikenneväylillä vuoteen 2025 mennessä[2]. Gigabittiyhteiskuntaa koskevassa tiedonannossa

[1] Suositus (EU) 2019/534 5G-verkkojen kyberturvallisuudesta, EUVL L 88, 29.3.2019, s. 42–47.
[2] COM(2016) 588, 14.6.2016, ”5G-Eurooppa: toimintasuunnitelma”.

asetetaan tavoitteeksi mobiilidatayhteyksien saatavuus kaikkialla[3], myös maaseudulla ja syrjäisillä alueilla.

Taajuuksien jakamiseen liittyen jäsenvaltiot ovat jakaneet 16 prosenttia 5G:n pioneeritaajuuksista[4]. Moniin jakomenettelyihin liittyviä julkisia kuulemisia odotetaan lähikuukausina, koska jäsenvaltioilla on oikeudellinen velvoite sallia kaikkien 5G:n pioneeritaajuusalueiden käyttö vuoden loppuun mennessä.

Eurooppa on maailmanlaajuisesti eturintamassa 5G-palvelujen kaupallisessa käynnistämisessä[5]. Tällä hetkellä ennakoidaan, että ensimmäiset 5G-palvelut ovat käytössä 138 Euroopan kaupungissa vuoden 2020 loppuun mennessä. Varhaisvaiheessa 5G-verkot perustuvat nykyiseen neljännen sukupolven (4G) verkkoteknologiaan, ja 5G-palveluja tarjotaan suurelle yleisölle pääasiassa joko kapasiteetti- ja nopeusparannuksena 4G:hen nähden tai kustannustehokkaana langattomana vaihtoehtona kiinteille verkoille[6].

Uudet yritystenväliset palvelut esimerkiksi energian, elintarvikkeiden ja maatalouden, terveydenhuollon, valmistusteollisuuden tai liikenteen aloilla tarjoavat mahdollisuuksia, joita Eurooppa on vienyt eteenpäin 1 miljardin euron luokkaa olevilla investoinneilla. Tähän sisältyy 300 miljoonan euron EU-rahoitus Horisontti 2020 -ohjelmasta erityisen julkisen ja yksityisen sektorin 5G-kumppanuuden yhteydessä. Investointikohteisiin kuuluu yli 160 laajamittaista 5G-kokeilua Euroopassa, kuten kymmenen rajat ylittävää valtaväylää verkottuneen ja automatisoidun liikkuvuuden 5G-pohjaisten palvelujen laajamittaista testaamista varten. Kokeilut käsittävät 5G:n mahdollistamia sovelluksia eri aloilla ulottuen kestävästä terveydenhuollosta ja automatisoidusta liikkuvuudesta aina resurssitehokkaaseen maatalouteen, älykkäisiin sähköverkkoihin ja Industry 4.0 -teknologiaan. Lisäksi EIP on Euroopan strategisten investointien rahaston tuella myöntänyt lainoja 5G-teknologian tutkimuksen ja kehittämisen nopeuttamiseksi.

Eurooppalainen sähköisen viestinnän säännöstö, jäljempänä ’säännöstö’[7], jota sovelletaan 21. joulukuuta 2020 lähtien, on tärkeä perusta luotaessa investointiystävällistä ympäristöä 5G-verkoille ja muulle tulevalle teknologialle. Myös julkiset rahoitusohjelmat, kuten Verkkojen Eurooppa -välineen digitaaliosio[8] tai Euroopan rakenne- ja investointirahastot, ovat olennainen keino tukea 5G-verkkojen tulevaa käyttöönottoa, erityisesti kun on kyse yhteisöjen yhteyksistä 5G-pohjaisiin palveluihin esimerkiksi kouluissa, sairaaloissa, kaupungeissa ja paikallishallinnossa.

---

[3] COM(2016) 587 ”Verkkoyhteydet kilpailukykyisillä digitaalisilla sisämarkkinoilla – Kohti eurooppalaista gigabittiyhteiskuntaa”.

[4] http://www.5GObservatory.eu

[5] http://www.5GObservatory.eu

[6] Osa 5G-verkkojen uusista toiminnoista otetaan käyttöön vaiheittain. Ensimmäisessä vaiheessa (hyvin lyhyellä tai lyhyellä aikavälillä) 5G:n käyttöönotto koostuu ensisijaisesti ns. NSA-verkoista (non stand-alone), joissa pelkästään radioliityntäverkko on päivitetty 5G-teknologiaan ja jotka muutoin ovat edelleen riippuvaisia tällä hetkellä käytössä olevista 4G-runkoverkoista, jotka tulevat tarjoamaan loppukäyttäjille parempaa mobiililaajakaistapalvelua. Seuraavissa vaiheissa (lyhyellä ja keskipitkällä tai pitkällä aikavälillä) SA-verkkojen (stand-alone -verkkojen) ja niihin sisältyvien 5G-runkoverkkotoimintojen käyttöönotto johtaa ajan myötä 5G:n edellyttämään huomattavasti laajempaan verkkoarkkitehtuurin muutokseen.

[7] Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/1972 eurooppalaisesta sähköisen viestinnän säännöstöstä (uudelleenlaadittu).

[8] Ehdotus asetukseksi Verkkojen Eurooppa -välineestä ja asetusten (EU) N:o 1316/2013 ja (EU) N:o 283/2014 kumoamisesta, 6.6.2018, COM(2018) 438.

Ottaen huomioon Euroopan strategiset mahdollisuudet 5G-palveluissa eri aloilla on ensiarvoisen tärkeää, että operaattorit ja palveluntarjoajat investoivat kehittyneisiin 5G-verkko- ja -palveluratkaisuihin. Nämä edellyttävät paitsi uusia 5G-radioverkkoja myös uusia stand alone -tyyppisiä 5G-runkoverkkoja, jotta voidaan tarjota kehittyneitä 5G-toimintoja, kuten verkon viipalointia[9] ja reunalaskentaa[10].

Komissio tukee jatkossakin täysipainoisesti 5G:n onnistunutta käyttöönottoa EU:ssa muun muassa toimimalla yhdessä jäsenvaltioiden ja sidosryhmien kanssa 5G:n mahdollisuuksien hyödyntämiseksi. Relevantteihin terveysnäkökohtiin kiinnitetään asianmukaista huomiota ennalta varautumisen periaatteen[11] pohjalta yhteistyössä asianomaisten kansainvälisten järjestöjen ja tiedeyhteisön kanssa.

3. 5G-verkkojen kyberturvallisuutta koskeva koordinoitu EU-tason riskinarviointi

Työskentelemällä kollektiivisesti verkko- ja tietoturva-alan yhteistyöryhmässä[12] kukin jäsenvaltio sai valmiiksi oman 5G-verkkoinfrastruktuurejaan koskevan kansallisen riskinarviointinsa ja toimitti tulokset komissiolle ja Euroopan unionin kyberturvallisuusvirastolle ENISAlle heinäkuun 2019 alkuun mennessä.

Kansallisten riskinarviointien perusteella jäsenvaltioiden, komission ja ENISAn edustajista koostuva verkko- ja tietoturva-alan yhteistyöryhmä julkaisi 9. lokakuuta 2019 raportin 5G-verkkojen kyberturvallisuutta koskevasta koordinoidusta EU-tason riskinarvioinnista[13]. Raportissa määritellään 5G-verkkojen tärkeimmät uhat ja uhkatoimijat, herkimmät kohteet ja suurimmat (tekniset ja muun tyyppiset) haavoittuvuudet. Tältä pohjalta raportissa yksilöitiin joukko EU:n kannalta strategisesti merkittäviä riskikategorioita. Niitä havainnollistetaan konkreettisilla riskiskenaarioilla, joissa otetaan huomioon eri parametrien (haavoittuvuuksien, uhkien ja uhkatoimijoiden) merkitykselliset yhdistelmät eri kohteiden osalta (ks. lisäys).

Täydentääkseen raporttia ja lisäpanoksena välineistöön ENISA teki uhkaympäristöstä kohdennetun kartoituksen[14], joka sisälsi yksityiskohtaisen analyysin tietyistä teknisistä näkökohdista, erityisesti verkkokohteiden ja niihin vaikuttavien uhkien määrittelystä.

Koordinoidussa EU-tason riskinarvioinnissa tuodaan esiin useita 5G-verkkojen kannalta tärkeitä näkökohtia :

a) 5G:n mukanaan tuomat teknologiset muutokset lisäävät yleistä hyökkäyspintaa ja hyökkääjien mahdollisten sisääntuloväylien määrää.

[9] 5G-verkon viipalointi (slicing) mahdollistaa eri palvelukerrosten pitkälle menevän eriyttämisen samassa fyysisessä verkossa, mikä lisää mahdollisuuksia tarjota eriytettyjä palveluja koko verkossa.

[10] Reunalaskenta on hajautetun laskennan paradigma, joka tuo laskennan ja datan säilytyksen lähemmäksi paikkaa, jossa sitä tarvitaan. Näin voidaan parantaa vasteaikoja ja säästää kaistanleveyttä.

[11] Neuvoston suositus 1999/519/EY, annettu 12 päivänä heinäkuuta 1999, väestön sähkömagneettisille kentille (0 Hz – 300 GHz) altistumisen rajoittamisesta.

[12] Perustettu Euroopan parlamentin ja neuvoston direktiivillä (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa. Verkko- ja tietoturva-alan yhteistyöryhmä perustettiin verkko- ja tietoturvadirektiivillä varmistamaan EU:n jäsenvaltioiden keskinäinen strateginen yhteistyö ja tiedonvaihto kyberturvallisuuden alalla.

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

[14] ENISA Threat landscape for 5G networks: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

– Parempi toiminnallisuus verkon reunassa ja vähemmän keskitetty arkkitehtuuri kuin aiemmissa mobiiliverkkojen sukupolvissa merkitsee sitä, että osa runkoverkkojen toiminnoista voidaan integroida verkkojen muihin osiin, mikä vastaavasti tekee laitteista haavoittuvampia (esim. tukiasemat tai verkkoresurssien hallinnan kehysympäristön (MANO) toiminnot).

– Ohjelmiston kasvava osuus 5G-laitteissa lisää ohjelmiston kehittämiseen ja päivittämiseen liittyviä riskejä, luo uusia konfigurointivirheiden riskejä ja antaa turvallisuusanalyysissä tärkeämmän aseman valinnoille, joita kukin matkaviestinoperaattori tekee verkon käyttöönottovaiheessa.

b) Nämä uudet tekniset ominaisuudet merkitsevät sitä, että matkaviestinoperaattoreiden riippuvuudella ulkopuolisista toimittajista ja niiden roolilla 5G-toimitusketjussa on aiempaa suurempi merkitys.

Tämä puolestaan lisää hyökkäysreittien määrää, joita uhkatoimijat, muun muassa EU:n ulkopuoliset valtiot tai valtion tukemat toimijat, voivat hyödyntää, koska niillä on valmiudet (aikomus ja resurssit) tehdä hyökkäyksiä EU:n jäsenvaltioiden televiestintäverkkoja vastaan, ja se potentiaalisesti lisää myös tällaisten hyökkäysten vaikutusten vakavuutta.

Tässä ympäristössä, jossa altistumien hyökkäyksille kasvaa ulkopuolisten laitetoimittajien myötävaikutuksella, yksittäisten toimittajien riskiprofiilista tulee erityisen tärkeä, erityisesti tilanteissa, joissa toimittajalla on merkittävä läsnäolo verkoissa tai alueilla.

c) Suuri riippuvuus yhdestä ainoasta toimittajasta lisää altistumista tälle toimittajalle ja tämän toimittajan mahdollisen epäonnistumisen seurauksille. Se myös pahentaa heikkouksien tai haavoittuvuuksien mahdollisia vaikutuksia ja kasvattaa todennäköisyyttä, että uhkatoimijat hyödyntävät niitä, etenkin silloin, kun riippuvaisuus koskee toimittajaa, johon liittyy suuri riski.

d) Jos jotkin 5G:lle kaavailluista uusista sovelluskohteista toteutuvat, 5G-verkoista tulee tärkeä osa monien kriittisten IT-sovellusten toimitusketjua, mikä vaikuttaa paitsi luottamuksellisuutta ja yksityisyyttä koskeviin vaatimuksiin myös siten, että näiden verkkojen eheydestä ja saatavuudesta tulee keskeinen turvallisuushaaste sekä kansallisesta että EU:n näkökulmasta.

Lähde: Koordinoitu EU-tason riskinarviointi

Koordinoidussa EU-tason riskinarvioinnissa todetaan, että nämä haasteet luovat uuden turvallisuusparadigman, minkä vuoksi 5G-sektoriin ja sen ekosysteemiin sovellettavaa nykyistä strategia- ja turvallisuuskehystä on arvioitava uudelleen ja jäsenvaltioiden on toteutettava tarvittavat toimenpiteet riskien vähentämiseksi.

Jotta tunnistettuihin riskeihin voidaan puuttua tehokkaasti ja lujittaa 5G-verkkojen turvallisuutta ja häiriönsietokykyä, tarvitaan kokonaisvaltaista lähestymistapaa, mikä edellyttää, että otetaan käyttöön keskeiset toimenpiteet ja niihin liittyvät tukitoimet, joiden avulla riskeihin voidaan puuttua samanaikaisesti. Koordinoitu EU-tason riskinarviointi tarjoaa pohjan kansallisella ja EU:n tasolla sovellettavien riskinhallintatoimenpiteiden määrittämiselle.

Neuvosto tuki 3. joulukuuta 2019 antamissaan päätelmissä koordinoidun riskinarvioinnin tuloksia ja korosti ”koordinoidun toimintatavan ja suosituksen tehokkaan täytäntöönpanon merkitystä sisämarkkinoiden pirstoutumisen välttämiseksi”[15]. Se kehotti jäsenvaltioita, komissiota ja ENISAa ”toteuttamaan kaikki niiden toimivaltaan kuuluvat tarvittavat toimenpiteet sähköisten viestintäverkkojen, erityisesti 5G-verkkojen, turvallisuuden ja eheyden varmistamiseksi ja jatkamaan koordinoidun toimintatavan vakiinnuttamista, jotta 5G-teknologioihin liittyviin turvallisuushaasteisiin voidaan vastata.”

4. 5G-kyberturvallisuutta koskeva EU:n välineistö

Verkko- ja tietoturva-alan yhteistyöryhmä julkaisi 29. tammikuuta 2020 EU:n riskinhallintatoimenpiteiden välineistön[16]. Siinä käsitellään kaikkia koordinoidussa riskinarviointiraportissa yksilöityjä riskejä.

EU:n välineistössä määritetään ja kuvataan joukko strategisia ja teknisiä toimenpiteitä ja niiden tehokkuutta parantavat tukitoimet, jotka voidaan ottaa käyttöön havaittujen riskien lieventämiseksi. **Strategisia toimenpiteitä** ovat toimenpiteet, jotka koskevat viranomaisten sääntelyvaltuuksien lisäämistä verkkojen hankintojen ja käyttöönoton valvomiseksi, erityistoimenpiteet muista kuin teknisistä heikkouksista johtuviin riskeihin puuttumiseksi sekä mahdolliset aloitteet, joilla edistetään kestävää ja monipuolista 5G-toimitus- ja arvoketjua systeemisten pitkän aikavälin riippuvuusriskien välttämiseksi. **Teknisillä toimenpiteillä** vahvistetaan 5G-verkkojen ja -laitteiden turvallisuutta puuttumalla teknologioista, prosesseista ja inhimillisistä ja fyysisistä tekijöistä aiheutuviin riskeihin. Lisäksi kullekin koordinoidussa EU-tason riskinarvioinnissa määritellylle riskialueelle esitetään **riskinhallintasuunnitelmat**, jotka perustuvat vaikuttavuudeltaan parhaiden toimenpiteiden valikoimaan.

Verkko- ja tietoturva-alan yhteistyöryhmän hyväksymissä EU:n välineistöä koskevissa päätelmissä suositellaan, että kaikki jäsenvaltiot ja komissio toteuttavat tietyt **keskeiset toimenpiteet**:

EU:n välineistöä koskevat päätelmät

EU:n välineistössä esitetään joukko toimenpiteitä ja toimia, jotka – tarkoituksenmukaisesti yhdisteltyinä ja tehokkaasti täytäntöön pantuina – muodostavat perustan koordinoidulle lähestymistavalle tällä alalla. Koska koordinoidussa EU-tason riskinarvioinnissa määriteltyjä riskialueita on laaja kirjo ja ne ovat luonteeltaan erilaisia, mikään yksittäinen toimenpidetyyppi ei riitä, vaan kaikkien keskeisten riskialueiden kattamiseksi tarvitaan useampia toimenpiteitä tarkoitustaan vastaavina yhdistelminä.

Mahdollisten riskinhallintasuunnitelmien arvioinnin ja vaikuttavuudeltaan parhaiden toimenpiteiden määrittämisen pohjalta tässä välineistössä suositellaan seuraavaa:

1. Kaikkien jäsenvaltioiden olisi varmistettava, että niillä on käytössä toimenpiteitä (ml. kansallisten viranomaisten valtuudet), jotta voidaan reagoida asianmukaisesti ja oikeasuhteisesti jo tunnistettuihin ja tuleviin riskeihin, ja erityisesti varmistettava, että ne voivat riskiperusteista lähestymistapaa

[15] Neuvoston päätelmät 5G-verkon merkityksestä Euroopan taloudelle ja 5G-verkkoon liittyvien turvallisuusriskien lieventämisestä. 3.12.2019, 14517/19 https://www.consilium.europa.eu/media/41595/st14517-en19.pdf.

[16] 5G-verkkojen kyberturvallisuus – EU:n riskinhallintatoimenpiteiden välineistö, 29.1.2020. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

noudattaen asettaa rajoituksia, kieltoja ja/tai erityisiä vaatimuksia ja ehtoja 5G-verkkolaitteiden toimitukselle, käyttöönotolle ja käytölle turvallisuuteen liittyvistä eri syistä.

Jäsenvaltioiden olisi erityisesti

- ***tiukennettava matkaviestinoperaattoreiden turvallisuusvaatimuksia** (esim. tiukka pääsyn valvonta, turvallista toimintaa ja seurantaa koskevat säännöt ja tiettyjen toimintojen ulkoistamisen rajoitukset);*

- *arvioitava toimittajien riskiprofiilit ja tältä pohjalta **sovellettava asianmukaisia rajoituksia suuririskisiksi katsottuihin toimittajiin, mukaan lukien tarvittavat toimittajien poissulkemiset, jotta voidaan vähentää tehokkaasti riskejä, jotka kohdistuvat EU:n laajuisessa koordinoidussa riskinarvioinnissa kriittisiksi ja arkaluonteisiksi määriteltyihin keskeisiin kohteisiin** (esim. ydinverkkotoiminnot, verkkoresurssien hallinnan kehysympäristön (MANO) toiminnot ja liityntäverkkojen toiminnot);*

- *varmistettava, että kullakin toimijalla on asianmukainen toimitusten monipuolistamiseen tähtäävä strategia, jolla **vältetään tai rajoitetaan merkittävää riippuvuutta** yhdestä ainoasta toimittajasta (tai toimittajista, joilla on samankaltainen riskiprofiili), sekä varmistettava toimittajien asianmukainen tasapaino kansallisella tasolla ja **vältettävä riippuvuutta toimittajista, joita pidetään suuririskisinä**. Tämä edellyttää myös sitä, että vältetään lukkiutuminen yhteen ainoaan toimittajaan, myös edistämällä laitteiden parempaa yhteentoimivuutta.*

2. Euroopan komission olisi yhdessä jäsenvaltioiden kanssa edistettävä

- ***monipuolisen ja kestävän 5G-toimitusketjun** ylläpitämistä pitkän aikavälin riippuvuuden välttämiseksi muun muassa*

  *o hyödyntämällä täysimääräisesti EU:n nykyisiä välineitä ja erityisesti seuraamalla mahdollisia **ulkomaisia suoria sijoituksia**, jotka vaikuttavat 5G:n keskeisiin omaisuuseriin, ja välttämällä mahdollisesta polkumyynnistä tai tuista johtuvia **vääristymiä** 5G:n toimitusmarkkinoilla ja*

  *o lujittamalla jatkossakin **EU:n valmiuksia 5G-verkoissa ja niiden jälkeisissä teknologioissa** hyödyntäen kyseeseen tulevia EU:n ohjelmia ja rahoitusta;*

- *jäsenvaltioiden välistä koordinointia **standardointiin** liittyvissä kysymyksissä erityisten turvallisuustavoitteiden saavuttamiseksi ja **tarvittavan EU:n laajuisen sertifiointijärjestelmän tai -järjestelmien** kehittämistä tuotteiden ja prosessien turvallisuuden parantamiseksi.*

3. Jotta tämä koordinoitu lähestymistapa pysyisi jatkuvasti ajan tasalla, verkko- ja tietoturva-alan yhteistyöryhmän tehtävänantoa olisi tältä osin laajennettava samoin kuin yhteistyötä muiden asiaankuuluvien elinten ja yksikköjen kanssa, jotta voidaan erityisesti

- *tarkistaa määräajoin – komission ja ENISAn tuella – 5G-verkkojen ja 5G:n jälkeisten verkkojen turvallisuutta koskevat **kansalliset ja EU:n riskinarvioinnit** ja tältä pohjalta kehittää edelleen ja yhdenmukaistaa käytettyjä arviointimenetelmiä ja mukautua kehittyvän 5G-teknologian vaatimuksiin;*

- ***seurata ja arvioida** yksityiskohtaisesti ja säännöllisesti välineistön **täytäntöönpanoa** jäsenvaltioiden järjestelmällisen raportoinnin pohjalta;*

- *huolehtia koordinoinnista ja tuesta EU-tason yhteistyötä edellyttävien **tukitoimien** täytäntöönpanossa ja erityisesti eri toimenpiteisiin liittyvän ohjeistuksen laadinnassa ja parhaiden käytäntöjen vaihdossa;*

- *tukea tarvittaessa mahdollista pidemmälle menevää koordinointia EU:n tasolla erityisesti **verkko-operaattoreita koskevien teknisten ja organisatoristen turvallisuusvaatimusten** lähentämiseksi edelleen.*

Lähde: EU:n välineistö.

Välineistöä koskevat päätelmät osoittavat, että jäsenvaltiot ovat vakaasti päättäneet yhdessä vastata 5G-verkkojen turvallisuushaasteisiin. Tällä on olennainen merkitys turvallisuuteen sekä jäsenvaltioiden sisällä että EU:n laajuisesti – niin kansantalouksien kuin EU:n sisämarkkinoidenkin ja Euroopan teknologisen suvereniteetin kannalta. Sekä koordinoitu EU-tason riskinarviointi että EU:n välineistö osoittavat sen kollektiivisen työn suuren arvon, jota verkko- ja tietoturva-alan yhteistyöryhmässä on tehty kaikkien jäsenvaltioiden, komission ja ENISAn edustajien intensiivisenä yhteistyönä.

Välineistö mahdollistaa EU:n yhteisen lähestymistavan 5G-verkkojen kyberturvallisuuteen ja tukee yhdenmukaista toimintaa sisämarkkinoilla EU:n strategioiden ja koordinoinnin kautta samoin kuin jäsenvaltioiden toimivallan käyttöä erityisesti kansalliseen turvallisuuteen liittyen. Sen sisältämien riskinhallintatoimenpiteiden ja -suunnitelmien pohjalta EU voi vastata yhteisiin 5G-kyberturvallisuushaasteisiin tarkoituksenmukaisesti, tehokkaasti ja oikeasuhteisesti.

Komissio on tyytyväinen 5G-kyberturvallisuutta koskevan EU:n välineistön julkaisemiseen ja antaa täyden tukensa kaikille edellä mainituille välineistöä koskeville päätelmille.

Komissio kehottaa jäsenvaltioita ja asianomaisia unionin toimielimiä, virastoja ja muita elimiä

i) varmistamaan tehokkaiden ja tarkoituksenmukaisten riskinhallintastrategioiden pikainen täytäntöönpano koko EU:ssa EU:n välineistön mukaisesti ja

ii) huolehtimaan tarvittavin lisätoimin koordinoinnista unionin tasolla, muun muassa jatkamalla työtä verkko- ja tietoturva-alan yhteistyöryhmässä ja perustamalla luotettava mekanismi EU:n välineistön täytäntöönpanon seuraamiseksi, jotta voidaan varmistaa toimenpiteiden tehokkuus ja sisämarkkinoiden moitteeton toiminta.

5. Välineistön käyttöönotto

Jäsenvaltioiden on sitouduttava soveltamaan välineistöä päättäväisesti, jotta 5G-turvallisuutta koskeva eurooppalainen lähestymistapa olisi uskottava ja menestyksekäs. Vaikka jäsenvaltiot päättävät yksittäisen toimenpiteen soveltuvuudesta kansallisten olosuhteiden mukaan, on ehdottoman tärkeää, että **verkko- ja tietoturva-alan yhteistyöryhmän suosittelemat keskeiset toimenpiteet (ks. edellä esitetyt välineistöä koskevat päätelmät) otetaan käyttöön kaikissa jäsenvaltioissa ja joidenkin toimenpiteiden osalta EU:n tasolla**, jotta havaittujen riskeihin voitaisiin puuttua.

Komissio on valmis antamaan täyden tukensa seuraavissa vaiheissa ja kehottaa jäsenvaltioita

– toteuttamaan **30. huhtikuuta 2020** mennessä konkreettisia ja mitattavissa olevia toimia EU:n välineistöä koskevissa päätelmissä suositeltujen keskeisten toimenpiteiden täytäntöönpanemiseksi;

– laatimaan komission ja ENISAn tuella **30. kesäkuuta 2020 mennessä** verkko- ja tietoturva-alan yhteistyöryhmän raportin näiden keskeisten toimenpiteiden täytäntöönpanon tilanteesta kussakin jäsenvaltiossa hyödyntäen erityisesti verkko- ja tietoturva-alan yhteistyöryhmän puitteissa tehtävää säännöllistä raportointia ja seurantaa.

5.1. Riskiperusteinen yhteinen lähestymistapa 5G-toimittajiin

Koska perimmäisenä tavoitteena on varmistaa 5G-verkkojen turvallisuus ja häiriönsietokyky ja näiden verkkojen kestävyys, jäsenvaltiot olivat yhtä mieltä siitä, että on tarpeen arvioida yksittäisten toimittajien riskiprofiilia ja tämän pohjalta soveltaa asiaankuuluvia rajoituksia suuririskisiksi katsottuihin toimittajiin, mukaan lukien tarvittavat toimittajien poissulkemiset, jotta voidaan vähentää tehokkaasti keskeisiin kohteisiin kohdistuvia riskejä siten kuin välineistössä esitetään. Komissio on valmis tukemaan jäsenvaltioita näiden toimenpiteiden täytäntöönpanossa.

Koordinoidussa EU-tason riskinarvioinnissa ja EU:n välineistössä annetaan toimenpiteiden EU:n laajuisen täytäntöönpanon tueksi ohjeita, jotka koskevat 1) toimittajien riskiprofiilin arviointia[17] ja 2) verkkoelementtien ja -toimintojen[18] sekä muiden kohteiden haavoittuvuutta. Sekä koordinoitu EU-tason riskinarviointi että välineistön toimenpiteet kattavat 5G-verkkolaitteiden ja verkkopalvelujen toimittajiin liittyvät riskit. Ne eivät kata muita tuotteita tai palveluja, joita nämä tai muut toimittajat voivat tarjota.

Kuten koordinoidun EU-tason riskinarvioinnin kohdassa 2.37 määritetään, yksittäisten toimittajien riskiprofiileja voidaan arvioida useiden tekijöiden perusteella.

Toimittajien riskiprofiilit olisi arvioitava yksinomaan turvallisuusnäkökohtien pohjalta ja objektiivisin perustein. Jotta toimenpiteet olisi helpompi panna täytäntöön koordinoidulla tavalla, välineistössä suositellaan, että jäsenvaltiot vaihtavat tietoja kansallisista toimintamalleista ja parhaista käytännöistä. Komissio katsoo, että tämän toimenpiteen pitäisi olla seuraavan vaiheen ykkösprioriteetteja työssä, jota verkko- ja tietoturva-alan yhteistyöryhmässä tehdään yhdessä komission ja ENISAn kanssa.

On tärkeää päättää jo hyvissä ajoin suuririskisiksi katsottuihin toimittajiin sovellettavista rajoituksista, myös tarvittavista toimittajien poissulkemisista, jotta voidaan vähentää tehokkaasti riskejä, sekä toimenpiteistä, joilla vältetään riippuvuus näistä toimittajista. Toimimalla näin mahdollisimman varhaisessa vaiheessa, mahdollisuuksien mukaan 5G-taajuuksien toimilupaprosessien yhteydessä, voidaan myös lisätä ennustettavuutta markkinatoimijoiden kannalta ja näin edistää 5G-verkkojen nopeaa käyttöönottoa samoin kuin varmistaa 5G-verkkojen pitkän aikavälin turvallisuus ja 5G-toimitusketjun häiriönsietokyky.

Samalla toimenpiteiden kansalliselle täytäntöönpanolle voidaan tarvittaessa ja perustelluissa tapauksissa määritellä erilaisia aikakehyksiä, erityisesti silloin, kun vallitsee suuri riippuvuus suuririskisiksi arvioitujen toimittajien laitteista tai palveluista (esim. ottamalla huomioon laitteiden päivityssyklit ja etenkin siirtyminen NSA-verkoista (non stand-alone) varsinaisiin 5G-verkkoihin (stand-alone)). Jäsenvaltiot voisivat harkita sopivien siirtymäaikojen

[17] Koordinoidun EU-tason riskinarvioinnin kohta 2.37.

[18] Koordinoidun EU-tason riskinarvioinnin kohdassa 2.21 esitetään elementtien ja toimintojen pääkategoriat ja niiden yleinen haavoittuvuustaso ja luetellaan keskeiset tekijät, jotka jäsenvaltiot ovat yksilöineet kunkin kategorian osalta, ja sen kohdissa 2.28 ja 2.29 määritetään muuntyyppisiä herkkiä kohteita tai alueita (esim. erityisiä yksiköitä tai maantieteellisiä alueita).

sisällyttämistä täytäntöönpanosuunnitelmiinsa kyseeseen tulevia verkko-operaattoreita varten. Tässä yhteydessä siirtymäkaudet olisi määriteltävä siten, että säilytetään kannustimet investoida nykyaikaisiin verkkolaitteisiin tai jopa vahvistetaan niitä, mihin sisältyy kehittyneiden (stand-alone) 5G-runkoverkkojen käyttöönoton nopeuttaminen ja nykyisten 4G-laitteiden korvaaminen verkkojen muissa osissa (esim. radioliityntäverkossa) 5G-toimintasuunnitelman[19] tavoitteiden mukaisesti.

Lisäksi ohjelmistopohjaisten 5G-verkkojen monimutkaisuuden vuoksi teleoperaattorit saattavat yhä useammin tukeutua kolmansiin osapuoliin tietyissä tehtävissä, kuten 5G-verkkojen ja -ohjelmistojen ylläpidossa ja päivityksessä, sekä käyttää verkkolaitteiden toimittamisen lisäksi myös muita ulkoistetusti hallinnoituja palveluja. Kuten koordinoidussa EU-tason riskinarvioinnissa kuvataan, tämä on vakavan turvallisuusriskin lähde. Tähän näkökohtaan olisi sen vuoksi kiinnitettävä erityistä huomiota. Myös näistä palveluista vastaavien toimittajien riskiprofiilista on olennaisen tärkeää tehdä perusteellinen turvallisuusarviointi erityisesti silloin, kun kyseisiä tehtäviä ei suoriteta EU:ssa. Vastaavasti olisi huolehdittava asianmukaisista toimenpiteistä muun muassa soveltamalla rajoituksia varsinkin 5G-verkkojen herkissä osissa tai sulkemalla pois suuririskiset tahot välineistöön kuuluvien riskinhallintatoimenpiteiden mukaisesti, jotta 5G-infrastruktuurin pitkän aikavälin eheys voidaan säilyttää.

5.2. Komission rooli välineistön täytäntöönpanon tukemisessa

Komissio tukee 5G-kyberturvallisuuteen sovellettavan EU:n lähestymistavan täytäntöönpanoa yleisesti ja tekee myös välineistön toimenpiteisiin ja tavoitteisiin liittyviä erityisaloitteita silloin, kun ne voivat tuoda lisäarvoa. Komissio hyödyntää täysimääräisesti toimivaltaansa ja kyseeseen tulevia välineitään siinä määrin kuin se on tarpeen yksilöityjen turvallisuusnäkökohtien huomioon ottamiseksi. Tällä tavoin ja toimimalla kollektiivisesti yhdessä jäsenvaltioiden ja yksityisen sektorin kanssa komissio pyrkii tukemaan strategisia toimenpiteitä, joilla varmistetaan EU:n teknologinen riippumattomuus ja johtajuus verkkoteknologioiden tulevassa kehittämisessä, kyberturvallisuusteknologioissa ja kaikissa olennaisissa rakenneosissa, joista koko taloutemme ja turvallisuutemme ovat riippuvaisia.

Komissio toteuttaa erityisesti seuraavat toimet varmistaakseen vastaavien välineistöön kuuluvien riskinhallintatoimenpiteiden täytäntöönpanon toimivaltaansa kuuluvilla aloilla:

5G-verkkojen kyberturvallisuuden ja monimuotoisen 5G-arvoketjun turvaaminen:

– **Kyberturvallisuusyhteistyö**: Jatketaan jäsenvaltioiden tukemista kansallisten toimenpiteiden tehokkaassa, koordinoidussa ja viivyttelemättömässä täytäntöönpanossa verkko- ja tietoturva-alan yhteistyöryhmän kautta.

– **Televiestintäsäännöt ja kyberturvallisuussäännöt**: Tuetaan välineistöön kuuluvien, turvallisuusvaatimuksiin liittyvien toimenpiteiden täytäntöönpanoa, etenkin sähköisen viestinnän eurooppalaisen säännöstön asianomaisten säännösten osalta, ja tarkastellaan, saataisiinko lisäarvoa mahdollisista täytäntöönpanosäädöksistä, joissa esitetään yksityiskohtaisesti tekniset ja organisatoriset turvatoimet, jotta voidaan täydentää kansallisia sääntöjä ja tehostaa ja yhdenmukaistaa operaattoreille määrättyjä turvatoimia.

[19] COM(2016) 588, 14.9.2016, ”5G-Eurooppa: toimintasuunnitelma”.

– **Standardointi**: Autetaan erityisin toimin ylläpitämään ja tarvittaessa lisäämään Euroopan osallistumista standardointielinten työhön turvallisuutta ja yhteentoimivuutta koskevien Euroopan tavoitteiden saavuttamiseksi. Komissio aikoo yhdessä jäsenvaltioiden kanssa arvioida ja edistää teknisiä eritelmiä ja standardeja, jotka mahdollistavat yhteentoimivuuden 5G-laitteiden toimittajien välillä verkon eri osissa, myös vanhoissa verkoissa, jotta voidaan luoda todellinen monitoimittajaympäristö esimerkiksi avointen ja yhteentoimivien rajapintojen avulla.

– **Sertifiointi**: Tuetaan 5G-verkkojen tarpeita vastaavien 5G-sertifiointijärjestelmien kehittämistä EU:n kyberturvallisuuden sertifiointikehyksen puitteissa.

– **Suorien ulkomaisten sijoitusten seuranta**: Tuetaan EU:n seurantakehyksen täytäntöönpanoa kartoittamalla koko 5G-arvoketju, muun muassa herkät verkkokohteet, ja seuraamalla säännöllisesti ulkomaisia suoria sijoituksia arvoketjun laajuudelta. Ulkomaisten suorien sijoitusten seurantaan sovellettavan aikataulun mukaisesti (tilanne lokakuussa 2020) komissio aikoo tarkastella 5G-verkkojen alalla tehtäviä ulkomaisia investointeja asetuksessa (EU) 2019/452 annetuin suuntaviivoin ottaen huomioon koordinoidun EU-tason riskinarvioinnin ja EU:n välineistön.

– **Kaupan suojatoimet**: Seurataan kaikkea merkityksellistä markkinakehitystä EU:ssa ja kolmansissa maissa ja suojataan EU:n toimijoita Euroopan 5G-markkinoilla kaupan suojatoimenpiteillä, joilla voidaan puuttua mahdollisiin kauppaa vääristäviin käytäntöihin (polkumyyntiin tai tukiin), ja tarvittaessa myös käynnistämällä alustavia tutkimuksia.

– Kilpailusäännöt: Seurataan 5G-laitteistojen ja -ohjelmistojen toimitusmarkkinoita toimivan kilpailun varmistamiseksi ja myös liittyen tilanteisiin, joissa sopimusperusteisista tai teknisistä syistä voidaan jäädä riippuvaiseksi yksittäisestä toimittajasta.

– **EU:n rahoitusohjelmat**: Varmistetaan, että osallistuminen EU:n rahoitusohjelmiin kyseeseen tulevilla teknologian aloilla edellyttää turvallisuusvaatimusten noudattamista, ja hyödynnetään tässä täysimääräisesti turvallisuusehtoja ja tehostetaan niiden täytäntöönpanoa T&I-ohjelmissa, kuten Horisontti Eurooppa -ohjelmassa, Digitaalinen Eurooppa -ohjelmassa ja Verkkojen Eurooppa 2 -välineessä, samoin kuin Euroopan rakenne- ja investointirahastoissa ja muissa asiaankuuluvissa ohjelmissa. Vastaavaa lähestymistapaa olisi noudatettava myös EU:n ulkoisissa rahoitusohjelmissa ja -välineissä, myös kansainvälisten rahoituslaitosten kautta tarjottavassa rahoituksessa.

– Julkiset hankinnat: Tehdään julkiset hankinnat 5G-verkkojen alalla tavalla, jolla voidaan tukea 5G-verkkojen turvallisuudelle, toimittajien monimuotoisuudelle ja pitkän aikavälin kestävyydelle määriteltyjä tavoitteita. Pyritään erityisesti varmistamaan, että turvallisuusnäkökohdat otetaan asianmukaisesti huomioon myönnettäessä 5G-verkkoihin liittyviä hankintasopimuksia julkisia hankintoja koskevien EU:n sääntöjen mukaisesti.

– **Tietoturvaloukkauksiin reagointi ja kriisinhallinta (EU:n suunnitelma) ja kyberharjoitukset**: Hyödynnetään täysimääräisesti EU:n suunnitelmaa[20] koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja sen kehitystä. Harkitaan lisäksi

[20] Komission suositus koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin (EU 2017/1584).

yhdessä ENISAn kanssa mahdollisuutta toteuttaa 5G-kyberharjoitus heti, kun markkinoiden kypsyys sen sallii.

Ja unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan ja komission varapuheenjohtajan sekä neuvoston vastuulla:

– **EU:n yhteistä diplomaattista vastausta haitallisiin kybertoimiin koskevat puitteet (kyberdiplomatian välineistö)**[21]: EU:n koskemattomuutta ja turvallisuutta uhkaavien haitallisten kybertoimien tapauksessa jäsenvaltioita kannustetaan käyttämään soveltuvia yhteisen ulko- ja turvallisuuspolitiikan toimenpiteitä, jotka ovat osa EU:n kyberdiplomatian välineistöä (mukaan lukien tarvittaessa rajoittavat toimenpiteet), jotta voidaan edistää yhteistyötä, helpottaa uhkien lieventämistä ja vaikuttaa potentiaalisten hyökkääjien käyttäytymiseen.

Lisäksi useilla ohjelmilla tuetaan tavoitteita välttää ja rajoittaa pitkän aikavälin riippuvuusriskiä edistämällä monipuolisia ja kestäviä markkinoita 5G-verkkoja varten, muun muassa pitämällä yllä EU:n valmiuksia 5G:n arvoketjussa ja investoimalla innovointiin, noudattaen samalla EU:n kansainvälisiä velvoitteita.

Innovoinnin ja investointien edistäminen kyberturvallisuudessa ja verkkoinfrastruktuurien teknologioissa:

– EU:n **rahoitusohjelmat**: Lisätään tutkimukseen, innovointiin ja verkkoteknologioiden ja niiden perustana olevien rakenneosien käyttöönottoon tehtäviä investointeja. Komissio on ehdottanut lähes 3 miljardin euron investointeja kyberturvallisuusteknologioihin EU:n seuraavassa talousarviossa vuosiksi 2021–2027. Tähän sisältyvät Horisontti Eurooppa -ohjelmasta tuleva tutkimus- ja innovaatiorahoitus ja Digitaalinen Eurooppa -ohjelmasta saatava tuki kyberturvallisuusvalmiuksille. Myös InvestEU-ohjelmasta voidaan myöntää taloudellista tukea 5G-alan tutkimukseen ja kehittämiseen ja tukea 5G:n käyttöönottoa.

Lisäksi komissio on ehdottanut tulevan Horisontti Eurooppa -ohjelman[22] yhteydessä EU:n institutionaalista kumppanuutta seuraavan sukupolven internetin ja 6G-verkkojen alalla (NGI/6G – ”Älykkäät verkot ja palvelut”) yhteistyössä teollisuuden kanssa ja koordinoidusti jäsenvaltioiden kanssa, jotta voidaan paitsi huolehtia 5G:n käyttöönotosta myös **valmistautua** seuraavan sukupolven mobiiliteknologiaan eli **6G:hen**. EU:n talousarviosta (2021–2027) ehdotettu EU-rahoitus on yli 2,5 miljardia euroa, minkä lisäksi aloitteeseen on määrä saada vähintään 7,5 miljardin euron yksityiset investoinnit.

– **Teollinen kehittäminen ja käyttöönotto**: Arvioidaan 5G-arvoketjun laajuudelta mahdollisia markkinavajeita tai markkinoiden toimintapuutteita, jotka edellyttäisivät kohdennettuja toimia seuraavassa pitkän aikavälin talousarviossa tai mahdollista Euroopan yhteistä etua koskevaa tärkeää hanketta (IPCEI) kyberturvallisuuden alalla korkean tason IPCEI-foorumin ehdotusten mukaisesti. Päätös IPCEI-hankkeiden suunnittelusta ja perustamisesta kuuluu jäsenvaltioille ja yrityksille. EU:n säännöt tarjoavat mahdollistavan kehyksen, ja komissio on valmis helpottamaan tarvittavia yhteyksiä ja antamaan ohjausta.

[21] Neuvoston päätelmät 20.11.2017, 9916/17.

[22] Rahoitusta voidaan myöntää myös Verkkojen Eurooppa 2.0 -välineestä ja Digitaalinen Eurooppa -ohjelmasta.

6. Päätelmät

5G-verkot tarjoavat monenlaisia mahdollisuuksia Euroopan kansalaisille, yhteiskunnalle ja taloudelle. Siksi on olennaisen tärkeää varmistaa 5G-verkkojen turvallisuus ja häiriönsietokyky. Samaan aikaan kyberturvallisuusuhat (ml. EU:n ulkopuolisista valtioista tai valtion tukemista toimijoista johtuva häiriöriski) ovat jatkuvasti kehittyvä haaste, jonka merkitys kasvaa sitä mukaa kuin riippuvuus teknologiasta ja datasta lisääntyy. Kyberturvallisuuden laiminlyöminen heikentäisi luottamusta digitaalitalouden ja -yhteiskunnan kehitykseen ja estäisi EU:ta saamasta siitä täyttä hyötyä. Tämä vastaavasti edellyttää jatkuvasti kehittyvää ja tehostettua reagointia.

Koordinoitu ja johdonmukainen lähestymistapa kriittisten teknologioiden ja verkkojen kyberturvallisuuteen EU:ssa on olennainen edellytys, jotta EU voi varmistaa teknologisen riippumattomuutensa sekä ylläpitää ja kehittää teollisia valmiuksia. Komissio antaa täyden tukensa 5G-verkkojen kyberturvallisuutta koskevan EU:n lähestymistavan täytäntöönpanolle ja varmistaa samalla, että EU:n markkinat pysyvät avoimina tuotteille ja palveluille, jotka täyttävät viimeisimmät kyberturvallisuus- ja luotettavuusvaatimukset.

Tätä varten on tärkeää, että kaikkien sidosryhmien sitoutuminen 5G-turvallisuuteen säilyy korkealla tasolla. Tämä edellyttää jatkuvaa yhteistyötä jäsenvaltioiden, komission ja ENISAn välillä.

Kuten edellä esitetään, komissio kehottaa jäsenvaltioita ensimmäisessä vaiheessa ryhtymään välittömästi pikaisiin toimiin, jotta välineistössä sovitut toimenpiteet voidaan panna täytäntöön tehokkaasti ja objektiivisesti, ja jatkamaan yhteistyötä komission ja ENISAn tuella koordinoinnin varmistamiseksi EU:n tasolla. Samaan aikaan komissio käynnistää kaikki tarvittavat toimivaltansa piiriin kuuluvat toimet tukeakseen välineistön täytäntöönpanoa jäsenvaltioissa ja vahvistaakseen sen vaikutusta.

Lisäys: Riskikategoriat (lähde: Koordinoitu EU-tason riskinarviointi).

	Riskikategoriat
Riittämättömiin turvatoimiin liittyvät riskiskenaariot	*R1: Verkkojen virheellinen konfigurointi*
	R2: Puutteet pääsyn valvonnassa
5G:n toimitusketjuun liittyvät riskiskenaariot	*R3: Tuotteiden heikko laatu*
	R4: Riippuvuus yhdestä ainoasta toimittajasta yksittäisissä verkoissa tai riittämätön monimuotoisuus koko maassa
Tärkeimpien uhkatoimijoiden toimintatapoihin liittyvät riskiskenaariot	*R5: Valtion puuttuminen 5G-toimitusketjun kautta*
	R6: Loppukäyttäjiin kohdistuva järjestäytyneen rikollisuuden tai rikollisjärjestön harjoittama 5G-verkkojen hyväksikäyttö
5G-verkkojen ja muiden kriittisten järjestelmien keskinäisiin riippuvuussuhteisiin liittyvät riskiskenaariot	*R7: Kriittisten infrastruktuurien tai palvelujen merkittävä häiriö*
	R8: Verkkojen laajamittainen toimintahäiriö, joka johtuu sähköntoimitusten tai muiden tukijärjestelmien keskeytymisestä
Loppukäyttäjien laitteisiin liittyvät riskiskenaariot	*R9: Esineiden internetin hyväksikäyttö*