SUOSITUKSET

KOMISSION SUOSITUS (EU) 2019/534,
annettu 26 päivänä maaliskuuta 2019,
5G-verkkojen kyberturvallisuudesta

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen ja erityisesti sen 292 artiklan,

sekä katsoo seuraavaa:

(1) Komissio on katsonut, että viidennen sukupolven (5G) verkkoteknologian käyttöönotto on merkittävä tulevaisuuden digitaalipalvelujen mahdollistaja ja digitaalisten sisämarkkinoiden strategian painopiste. Komissio hyväksyi 5G-toimintasuunnitelman varmistaakseen, että unionilla on vuodesta 2020 käytettävissään digitalisaation edellyttämä yhteenliitettävyysinfrastruktuuri ([1]).

(2) 5G-verkoilla kehitetään nykyistä neljännen sukupolven (4G) verkkoteknologiaa tarjoamalla uutta palvelukapasiteettia, jolloin verkoista tulee monilta osin unionin talouden keskeinen infrastruktuuri ja mahdollistaja. Kun 5G-verkot on otettu käyttöön, ne muodostavat selkärangan monenlaisille palveluille, jotka ovat olennaisia sisämarkkinoiden toiminnan kannalta. Ne ovat tarpeen myös, jotta voidaan ylläpitää yhteiskunnan ja talouden keskeisiä toimintoja, jotka liittyvät esimerkiksi energiaan, liikenteeseen, pankkialaan, terveyteen ja teollisuuden hallintajärjestelmiin. Demokraattisten prosessien, kuten vaalien, järjestäminen tulee myös nojautumaan yhä enemmän digitaaliseen infrastruktuuriin ja 5G-verkkoihin.

(3) Monet kriittiset palvelut ovat riippuvaisia 5G-verkoista, minkä vuoksi laajan järjestelmähäiriön seuraukset olisivat erityisen vakavia. Sen vuoksi 5G-verkkojen kyberturvallisuus on unionille strategisesti tärkeä kysymys aikana, jona kyberhyökkäysten määrä on kasvussa ja ne ovat kehittyneempiä kuin koskaan.

(4) Digitaalista ekosysteemiä tukevat infrastruktuurit ovat kytköksissä toisiinsa ja luonteeltaan ylikansallisia, ja niitä koskevat uhat ovat luonteeltaan rajatylittäviä. Sen vuoksi kaikki yhdessä jäsenvaltiossa ilmenevät 5G-verkkoja koskevat merkittävät heikkoudet ja/tai kyberhäiriötilanteet vaikuttaisivat koko unioniin. Tästä syystä olisi säädettävä toimenpiteistä, joilla tuetaan 5G-verkkojen yhteistä korkeatasoista kyberturvallisuutta.

(5) Jäsenvaltiot ovat vahvistaneet, että tarvitaan unionin tason toimia. Eurooppa-neuvosto ilmoitti 21. maaliskuuta 2019 antamissaan päätelmissä odottavansa komissiolta suositusta 5G-verkkojen turvallisuutta koskeviksi yhteisiksi toimintalinjoiksi ([2]).

(6) Euroopan suvereeniuden varmistamisen olisi oltava keskeinen tavoite, kuitenkin täysin avoimuutta ja suvaitsevaisuutta koskevia EU:n arvoja kunnioittaen ([3]). Ulkomaiset sijoitukset strategisilla aloilla, EU:ssa sijaitsevien kriittisten omaisuuserien, teknologioiden ja infrastruktuurin hankinnat ja kriittisten laitteiden toimitukset voivat aiheuttaa riskejä EU:n turvallisuudelle.

(7) 5G-verkkojen kyberturvallisuus on keskeistä unionin strategisen riippumattomuuden varmistamisessa, kuten yhteisessä tiedonannossa ”Strateginen katsaus EU:n ja Kiinan suhteisiin” ([4]) todetaan.

(8) Myös Euroopan parlamentin päätöslauselmassa turvallisuusuhkista, jotka liittyvät kiinalaisen teknologian lisääntymiseen EU:ssa ([5]), kehotetaan komissiota ja jäsenvaltioita toteuttamaan unionin tason toimia.

(9) Tässä suosituksessa käsitellään 5G-verkkojen kyberturvallisuusriskejä ja annetaan ohjausta, joka koskee asianmukaista riskianalyysia ja kansallisen tason riskienhallintatoimia, koordinoidun Euroopan tason riskianalyysin kehittämistä sekä sellaisen prosessin laatimista, jolla kehitetään parhaista riskienhallintatoimenpiteistä koostuva yhteinen välineistö.

(10) Sähköisten viestintäverkkojen suojaamiseksi on jo olemassa vahva unionin lainsäädäntökehys.

([1]) COM(2016) 588 final.
([2]) Maaliskuun 21. ja 22 päivänä 2019 kokoontuneen Eurooppa-neuvoston päätelmät.
([3]) Unionin tila 2018: Suvereeni Eurooppa – On aika toimia, 12. syyskuuta 2018.
([4]) JOIN(2019) 5 final.
([5]) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0156+0+DOC+PDF+V0//FI

(11) Sähköistä viestintää koskeva unionin järjestelmä ([6]) edistää kilpailua, kehittää sisämarkkinoita ja suojelee loppukäyttäjän etuja. Lisäksi sillä on eurooppalaisen sähköisen viestinnän säännöstöön ([7]) liittyvä verkkoyhteyksiä koskeva lisätavoite, joka ilmaistaan tuotoksina: sekä kiinteiden että liikkuvien erittäin suuren kapasiteetin yhteyksien laaja saatavuus ja käyttöönotto kaikkien unionin kansalaisten ja yritysten keskuudessa. Direktiivissä 2002/21/EY edellytetään, että jäsenvaltiot varmistavat yleisten viestinnän verkkojen eheyden ja turvallisuuden. Lisäksi ne velvoitetaan varmistamaan, että yleisiä viestintäverkkoja tai yleisesti saatavilla olevia sähköisiä viestintäpalveluja tarjoavat yritykset toteuttavat tarvittavat tekniset ja organisatoriset toimenpiteet hallitakseen asianmukaisesti verkkojen tai palvelujen turvallisuuteen kohdistuvia riskejä. Direktiivissä säädetään myös, että toimivaltaisilla kansallisilla sääntelyviranomaisilla on valtuuksia, myös valtuudet antaa sitovia ohjeita, tällaisten velvoitteiden noudattamisen varmistamiseksi.

(12) Euroopan parlamentin ja neuvoston direktiivi 2002/20/EY ([8]) mahdollistaa myös sen, että jäsenvaltiot voivat viestinnän luottamuksellisuuden suojaamiseksi Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY ([9]) mukaisesti liittää yleisvaltuutukseen ehtoja, jotka koskevat julkisten verkkojen turvaamista luvatonta käyttöä vastaan.

(13) Unioni on perustanut useita yhteistyöelimiä näiden velvoitteiden noudattamisen tukemiseksi. Euroopan unionin verkko- ja tietoturvavirasto (ENISA), komissio, jäsenvaltiot ja kansalliset sääntelyviranomaiset ovat kehittäneet kansallisille sääntelyviranomaisille tekniset suuntaviivat, jotka koskevat poikkeamista ilmoittamista, turvatoimia sekä uhkia ja omaisuutta ([10]). Euroopan parlamentin ja neuvoston direktiivillä (EU) 2016/1148 ([11]) perustettu, toimivaltaisista viranomaisista koostuva yhteistyöryhmä tukee ja helpottaa yhteistyötä erityisesti antamalla strategista ohjausta tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden verkoston toimia varten. Verkosto helpottaa operatiivista yhteistyötä teknisellä tasolla.

(14) Euroopan uuden kyberturvallisuussertifiointikehyksen ([12]) pitäisi olla olennainen tukiväline johdonmukaisen turvallisuustason edistämiseksi. Sen pitäisi mahdollistaa sellaisten kyberturvallisuussertifiointijärjestelmien kehittäminen, joilla vastataan 5G:tä hyödyntävien laitteiden ja ohjelmistojen käyttäjien tarpeisiin. Tämä infrastruktuuri on kriittisen tärkeää, minkä vuoksi ensisijaisena tavoitteena pitäisi olla asiaa koskevien eurooppalaisten kyberturvallisuussertifiointijärjestelmien kehittäminen 5G-verkoissa käytettäville tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille. Jäsenvaltioiden ja markkinatoimijoiden olisi osallistuttava aktiivisesti tällaisten sertifiointijärjestelmien kehittämiseen, myös tukemalla erityisten suojausprofiilien kehittämistä 5G-verkoille.

(15) Koska lainsäädäntöä ei ole yhdenmukaistettu unionin tasolla, jäsenvaltiot voivat määritellä unionin lainsäädännön mukaisesti annetuilla kansallisilla teknisillä määräyksillä, että eurooppalaisen kyberturvallisuussertifiointijärjestelmän pitäisi olla pakollinen. Jäsenvaltiot voivat käyttää eurooppalaisia kyberturvallisuussertifiointijärjestelmiä myös julkisten hankintojen ja Euroopan parlamentin ja neuvoston direktiivin 2014/24/EU ([13]) soveltamisen yhteydessä. Lisäksi ne voisivat tukea tukimekanismien – kuten neuvontakeskuksen – perustamista sellaisten julkisen sektorin ostajien avuksi, jotka ostavat kyberturvallisuuden alan ratkaisuja.

(16) Tietosuojan ja yksityisyyden korkealla tasolla on tärkeä asema 5G-verkkojen turvallisuuden varmistamisessa. Unionin tasolla on lisäksi määritelty sääntöjä, joilla varmistetaan henkilötietojen käsittelyn turvallisuus, myös sähköisen viestinnän yhteydessä. Yleisessä tietosuoja-asetuksessa ([14]) asetetaan velvoite käsitellä henkilötietoja tavalla, jolla varmistetaan niiden turvallisuus, myös estämällä luvaton pääsy henkilötietoihin ja niiden käsittelyyn käytettyihin laitteisiin sekä näiden tietojen ja laitteiden luvaton käyttö. Sähköisen viestinnän tietosuojadirektiivissä

([6]) Euroopan parlamentin ja neuvoston direktiivi 2002/21/EY, annettu 7 päivänä maaliskuuta 2002, sähköisten viestintäverkkojen ja -palvelujen yhteisestä sääntelyjärjestelmästä (puitedirektiivi) (EUVL L 108, 24.4.2002, s. 33), sekä erityisdirektiivit.

([7]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/1972, annettu 11 päivänä joulukuuta 2018, eurooppalaisesta sähköisen viestinnän säännöstöstä (EUVL L 321, 17.12.2018, s. 36).

([8]) Euroopan parlamentin ja neuvoston direktiivi 2002/20/EY, annettu 7 päivänä maaliskuuta 2002, sähköisiä viestintäverkkoja ja -palveluja koskevista valtuutuksista (valtuutusdirektiivi) (EYVL L 108, 24.4.2002, s. 21).

([9]) Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi) (EYVL L 201, 31.7.2002, s. 37).

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

([11]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa (EUVL L 194, 19.7.2016, s. 1).

([12]) Ehdotus: Euroopan parlamentin ja neuvoston asetus EU:n kyberturvallisuusvirastosta ENISAsta ja asetuksen (EU) 526/2013 kumoamisesta sekä tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (”kyberturvallisuusasetus”), COM/2017/ 477 final – 2017/0225 (COD).

([13]) Euroopan parlamentin ja neuvoston direktiivi 2014/24/EU, annettu 26 päivänä helmikuuta 2014, julkisista hankinnoista ja direktiivin 2004/18/EY kumoamisesta (EUVL L 94, 28.3.2014, s. 65).

([14]) Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EUVL L 119, 4.5.2016, s. 1).

määritellään erityiset säännöt, jotka koskevat viestinnän ja loppukäyttäjille tarkoitettujen päätelaitteiden luottamuksellisuuden suojaamista. Lisäksi siinä asetetaan palveluntuottajille velvoite toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet palvelujensa turvallisuuden varmistamiseksi.

(17) Unioni on lisäksi hyväksynyt säädöksen, jolla suojellaan kriittisiä, esimerkiksi viestinnässä käytettäviä, infrastruktuureja ja teknologioita sallimalla jäsenvaltioiden seurata ulkomaisia suoria sijoituksia turvallisuuteen ja yleiseen järjestykseen liittyvistä syistä ja perustamalla yhteistyömekanismi, jonka puitteissa jäsenvaltiot ja komissio voivat vaihtaa tietoja ja ottaa esiin huolenaiheita, jotka liittyvät tiettyihin sijoituksiin ([15]).

(18) Jäsenvaltiot ja operaattorit toteuttavat tällä hetkellä tärkeitä toimia 5G-verkkojen laajamittaisen käyttöönoton mahdollistamiseksi. Useat jäsenvaltiot ovat ilmaisseet huolensa 5G-verkkoihin liittyvistä mahdollisista turvallisuusriskeistä, kun on kyse 5G-verkoille suunniteltujen radiotaajuusalueiden käyttöoikeuksien myöntämismenettelyistä, ja harkinneet toimenpiteitä näiden riskien varalta ([16]).

(19) 5G-verkkojen kyberturvallisuusriskejä vähennettäessä olisi otettava huomioon sekä teknisiä että muita tekijöitä. Teknisiä tekijöitä voivat olla esimerkiksi kyberhaavoittuvuudet, joita voidaan hyödyntää luvattoman pääsyn saamiseksi tietoihin (kybervakoilu taloudellisiin tai poliittisiin tarkoituksiin) taikka muihin haitantekotarkoituksiin (kyberhyökkäykset, joilla pyritään häiritsemään tai tuhoamaan järjestelmiä ja tietoja). Tärkeitä näkökohtia, joita olisi pohdittava, ovat tarve suojella verkostoja niiden koko elinkaaren ajan sekä tarve kattaa kaikki asiaan liittyvät laitteet, mukaan lukien 5G-verkkojen suunnittelu-, kehitys-, hankinta-, käyttöönotto-, toiminta- ja ylläpitovaiheissa.

(20) Muut tekijät voivat olla esimerkiksi sääntelyllisiä tai muita vaatimuksia, jotka koskevat tieto- ja viestintäteknologialaitteiden toimittajia. Tällaisten tekijöiden merkityksen arvioinnissa olisi otettava huomioon muun muassa kolmannen maan vaikutuksen kokonaisriski, erityisesti sen hallintomalliin liittyen, turvallisuutta koskevien yhteistyösopimusten tai muiden vastaavien tietosuojaan liittyvien järjestelyjen, kuten tietosuojan riittävyyttä koskevien päätösten, puute unionin ja kyseisen kolmannen maan välillä sekä se, onko kyseinen maa osapuolena monenvälisissä, kansainvälisissä tai kahdenvälisissä sopimuksissa, jotka koskevat kyberturvallisuutta, kyberrikollisuuden torjuntaa tai tietosuojaa.

(21) Tärkeä vaihe 5G-verkkojen kyberturvallisuutta koskevan unionin toimintatavan kehittämisessä olisi riskinarvioinnin toteuttaminen kansallisella tasolla. Tämä auttaisi jäsenvaltioita mukauttamaan turvavaatimuksia ja riskienhallintaa koskevia kansallisia toimenpiteitään arvioinnin tulosten perusteella.

(22) Koordinointia olisi kehitettävä, jotta voitaisiin varmistaa kyberturvallisuusuhkien lieventämiseen tarkoitettujen toimenpiteiden tehokkuus. Nämä toimenpiteet ovat olennaisia sisämarkkinoiden moitteettoman toiminnan ja henkilötietojen ja yksityisyyden suojan kannalta.

(23) Kansallisen riskinarvioinnin pitäisi muodostaa perusta unionin koordinoidulle riskinarvioinnille, joka muodostuu uhkaympäristön kartoittamisesta sekä yhteisestä arvioinnista, jonka jäsenvaltiot toteuttavat komission tuella yhdessä Euroopan unionin kyberturvallisuusviraston (ENISA) kanssa.

(24) Yhteistyöryhmän olisi kansalliset ja unionin riskinarvioinnit huomioon ottaen laadittava välineistö, jossa yksilöidään kyberturvallisuusuhkien ja niiden lieventämiseen tähtäävien mahdollisten toimenpiteiden tyypit esimerkiksi sertifioinnin, testauksen ja pääsynvalvonnan aloilla. Lisäksi sen olisi yksilöitävä mahdollisia erityistoimenpiteitä, jotka soveltuvat yhden tai useamman jäsenvaltion havaitsemien riskien lieventämiseen. Yhteistyöryhmän olisi hyödynnettävä Euroopan unionin kyberturvallisuusviraston (ENISA), Europolin, Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelimen (BEREC) ja EU:n tiedusteluanalyysikeskuksen tukea. Komission pitäisi hyödyntää välineistöä kehittäessään yhteisiä vähimmäisvaatimuksia, jotta 5G-verkkojen kyberturvallisuuden korkeaa tasoa voitaisiin parantaa entisestään kaikkialla unionissa.

(25) Toteutettaessa toimenpiteitä kyberturvallisuusriskien lieventämiseksi olisi otettava huomioon kyberturvallisuuden pitäminen esillä erilaisten palveluntuottajien kautta kutakin yksittäistä verkkoa rakennettaessa.

([15]) Euroopan parlamentin ja neuvoston asetus (EU) 2019/452, annettu 19 päivänä maaliskuuta 2019, unioniin tulevien ulkomaisten suorien sijoitusten seurantaan tarkoitettujen puitteiden perustamisesta (EUVL L 79I, 21.3.2019, s. 1).

([16]) Vuonna 2019 on tarkoitus järjestää ainakin yhtä taajuusaluetta koskeva huutokauppamenettely seuraavissa 11 jäsenvaltiossa: Alankomaat, Belgia, Irlanti, Itävalta, Kreikka, Liettua, Portugali, Ranska, Saksa, Tšekki, Unkari. Vuonna 2020 on tarkoitus järjestää kuusi muuta huutokauppaa seuraavissa kuudessa maassa: Espanja, Liettua (useita taajuuksia), Malta, Puola, Slovakia, Yhdistynyt kuningaskunta. Lähde: http://5gobservatory.eu/observatory-overview/observatory-reports/

(26) Tämä suositus ei saisi rajoittaa jäsenvaltioiden toimivaltaa sellaisten toimien osalta, jotka koskevat yleistä turvallisuutta, puolustusta, kansallista turvallisuutta tai yksittäisen valtion toimia rikosoikeuden alalla, mukaan lukien jäsenvaltioiden oikeus sulkea palveluntuottajia ja toimittajia markkinoiltaan kansalliseen turvallisuuteen liittyvistä syistä,

ON ANTANUT TÄMÄN SUOSITUKSEN:

I **TAVOITTEET**

1) Tässä suosituksessa yksilöidään toimia, jotka olisi toteutettava 5G-verkkojen kyberturvallisuuden varmistamiseen tähtäävän unionin lähestymistavan kehittämisen tueksi ja seuraavien toimien mahdollistamiseksi:

   a) Jäsenvaltiot arvioivat 5G-verkkoon kansallisella tasolla vaikuttavia kyberturvallisuusriskejä ja toteuttavat tarvittavat turvatoimet.

   b) Jäsenvaltiot ja unionin asiaan liittyvät toimielimet, virastot ja muut elimet kehittävät yhdessä unionin koordinoidun riskinarvioinnin, joka perustuu kansallisiin riskinarviointeihin.

   c) Direktiivillä (EU) 2016/1148 perustettu yhteistyöryhmä yksilöi mahdolliset yhteiset toimenpiteet niiden kyberturvallisuusriskien lieventämiseksi, jotka liittyvät digitaalista ekosysteemiä, erityisesti 5G-verkkoja, tukevaan infrastruktuuriin.

II **MÄÄRITELMÄT**

2) Tässä suosituksessa tarkoitetaan

   a) ’5G-verkoilla’ kaikkia olennaisia infrastruktuurin osatekijöitä, jotka liittyvät matkaviestinnän ja langattoman viestinnän teknologiaan, jota käytetään sellaisissa yhteenliitettävyys- ja lisäarvopalveluissa, joihin liittyy edistyneitä suorituskykyominaisuuksia – kuten hyvin suuret datanopeudet ja kapasiteetti, lyhyen vasteajan viestintä ja erittäin korkea luotettavuusaste – taikka tukemaan suurta määrää verkkoon liitettyjä laitteita. Näihin voivat kuulua aikaisemmat verkkoelementit, jotka perustuvat matkaviestinnän ja langattoman viestinnän edellisiin sukupolviin, kuten 4G:hen ja 3G:hen. 5G-verkkojen tulisi katsoa sisältävän kaikki verkon olennaiset osat;

   b) ’digitaalista ekosysteemiä tukevalla infrastruktuurilla’ infrastruktuuria, jolla mahdollistetaan digitaalinen muutos monissa talous- ja yhteiskuntaelämän kriittisissä sovelluksissa.

III **TOIMET KANSALLISELLA TASOLLA**

3) Jäsenvaltioiden olisi 30. kesäkuuta 2019 mennessä toteutettava 5G-verkkoinfrastruktuurin riskinarviointi, jossa olisi muun muassa yksilöitävä kaikkein arimmat osatekijät, joihin kohdistuvilla tietoturvaloukkauksilla olisi huomattava kielteinen vaikutus. Lisäksi jäsenvaltioiden olisi samaan päivään mennessä tarkistettava kansallisella tasolla sovellettavia turvavaatimuksia ja riskienhallintamenetelmiä ottaakseen huomioon kyberturvallisuusuhkat, jotka voivat johtua i) teknisistä tekijöistä, kuten 5G-verkkojen erityisistä teknisistä ominaisuuksista, ja ii) muista tekijöistä, kuten oikeudellisesta ja poliittisesta kehyksestä, joita kolmansissa maissa saatetaan soveltaa tieto- ja viestintäteknisten laitteiden toimittajiin.

4) Jäsenvaltioiden olisi kansallisen riskinarvioinnin ja tarkistuksen perusteella sekä unionin tason koordinoidut toimet huomioon ottaen

   a) päivitettävä 5G-verkkojen yhteydessä sovellettavia turvavaatimuksia ja riskienhallintamenetelmiä;

   b) päivitettävä velvoitteet, jotka direktiivin 2002/21/EY 13 a ja 13 b artiklan nojalla koskevat yleisiä viestintäverkkoja tai yleisesti saatavilla olevia sähköisiä viestintäpalveluja tarjoavia yrityksiä;

   c) liitettävä yleisvaltuutukseen ehtoja, jotka koskevat julkisten verkkojen turvaamista luvatonta käyttöä vastaan, ja pyydettävä direktiivin 2002/20/EY nojalla yrityksiä, jotka osallistuvat tuleviin 5G-kaistojen radiotaajuusalueiden käyttöoikeuksien myöntämismenettelyihin, sitoutumaan verkkoihin liittyvien turvavaatimusten noudattamiseen.

   d) sovellettava muita ehkäiseviä toimenpiteitä, joilla on tarkoitus lieventää mahdollisia kyberturvallisuusriskejä.

5) Edellä 4 kohdassa tarkoitettuihin toimenpiteisiin pitäisi sisältyä toimittajille ja operaattoreille asetettuja vahvistettuja velvoitteita huolehtia verkkojen arkojen osien turvallisuudesta sekä tarvittaessa velvoitteita toimittaa toimivaltaisille kansallisille viranomaisille tietoa sähköisiin viestintäverkkoihin suunnitelluista muutoksista, sekä vaatimuksia testauttaa erityisten tietotekniikkakomponenttien ja -järjestelmien turvallisuus ja eheys etukäteen kansallisissa tarkastus-/sertifiointilaboratorioissa.

6) Kahden tai useamman jäsenvaltion olisi toteutettava yhteisiä tietoturvatarkastuksia käyttäen ja jakaen asianmukaista teknistä asiantuntemusta sekä teknisiä tiloja, jotka liittyvät digitaalista ekosysteemiä ja 5G-verkkoja tukevaan infrastruktuuriin, esimerkiksi silloin, kun sama yritys käyttää tai rakentaa verkkoinfrastruktuuria useammassa kuin yhdessä jäsenvaltiossa tai kun verkkorakenteissa on paljon yhtäläisyyksiä. Euroopan unionin kyberturvallisuusviraston (ENISA), Europolin ja Euroopan sähköisen viestinnän sääntelyviranomaisten yhteistyöelimen (BEREC) olisi asetettava etusijalle tähän alaan liittyvät jäsenvaltioiden tukipyynnöt. Näiden arviointien tulokset olisi toimitettava yhteistyöryhmälle ja tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden verkostolle.

IV **KOORDINOIDUT TOIMET UNIONIN TASOLLA**

7) Jotta voitaisiin kehittää yhteinen tapa toimia 5G-verkkoihin liittyvien kyberturvallisuusriskien lieventämiseksi, jäsenvaltioiden olisi alettava noudattaa yhteistyöryhmässä erillistä menettelyä 30. huhtikuuta 2019 mennessä. Jäsenvaltioiden olisi tarvittaessa kutsuttava asiaan liittyviä viranomaisia osallistumaan yhteistyöryhmän työskentelyyn.

Koordinoitu Euroopan tason riskianalyysi

8) Jäsenvaltioiden olisi vaihdettava tietoja keskenään ja asiaan liittyvien unionin elinten kanssa muodostaakseen yleisen tietoisuuden olemassa olevista ja mahdollisista 5G-verkkoihin liittyvistä kyberturvallisuusriskeistä.

9) Jäsenvaltioiden olisi toimitettava kansalliset riskinarviointinsa komissiolle ja Euroopan unionin kyberturvallisuusvirastolle (ENISA) 15. heinäkuuta 2019 mennessä.

10) ENISAn pitäisi laatia erityinen kartoitus 5G-verkkojen uhkaympäristöstä. Direktiivillä (EU) 2016/1148 perustettujen yhteistyöryhmän ja tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden verkoston pitäisi tukea tätä prosessia.

11) Jäsenvaltioiden olisi kaikki nämä tekijät huomioon ottaen laadittava 1. lokakuuta 2019 mennessä komission tuella ja yhdessä Euroopan unionin kyberturvallisuusviraston (ENISA) kanssa yhteinen arviointi unionin laajuisesta altistumisesta riskeille, jotka liittyvät digitaalista ekosysteemiä ja erityisesti 5G-verkkoja tukevaan infrastruktuuriin.

12) Tässä yhteisessä arvioinnissa olisi asetettava etusijalle riskianalyysi, joka keskittyy erityisesti 5G-verkkojen ydinelementteihin kuuluviin arkoihin tai haavoittuviin osatekijöihin, käyttö- ja kunnossapitokeskukseen sekä teollisuussovelluksissa käytettyihin 5G-liityntäverkkoelementteihin.

13) Toisessa vaiheessa yhteinen arviointi olisi laajennettava digitaalisen arvoketjun muihin strategisiin osatekijöihin.

Yhteinen unionin välineistö riskien vähentämiseksi

14) Yhteistyöryhmän olisi yksilöitävä parhaat 4 kohdassa tarkoitetut, kansallisella tasolla sovellettava käytännöt. Näiden kansallisten parhaiden käytäntöjen perusteella olisi sovittava 31. joulukuuta 2019 mennessä asianmukaisista, tehokkaista ja oikeasuhtaisista mahdollisista riskienhallintatoimenpiteistä kansallisella ja unionin tasolla havaittujen kyberturvallisuusriskien lieventämiseksi. Komissio hyödyntäisi tätä toimenpiteiden välineistöä kehittäessään yhteisiä vähimmäisvaatimuksia, jotta 5G-verkkojen kyberturvallisuuden korkeaa tasoa voitaisiin parantaa entisestään kaikkialla unionissa.

15) Välineistössä olisi oltava

a) kartoitus niistä turvallisuusriskityypeistä, jotka voivat vaikuttaa 5G-verkkojen kyberturvallisuuteen (esim. toimitusketjun riskit, ohjelmistojen haavoittuvuusriskit, pääsynvalvontaan liittyvät riskit sekä riskit, jotka johtuvat oikeudellisesta ja poliittisesta kehyksestä, joita kolmansissa maissa saatetaan soveltaa tieto- ja viestintäteknisten laitteiden toimittajiin), ja

b) joukko mahdollisia lievennystoimia (esim. kolmannen osapuolen sertifiointi laitteille, ohjelmistoille tai palveluille, muodollinen laitteisto- ja ohjelmistotestaus tai vaatimustenmukaisuuden tarkistaminen, prosessit, joilla varmistetaan pääsynvalvonnan olemassaolo ja käyttö sekä sellaisten tuotteiden, palveluiden tai toimittajien yksilöinti, joiden turvallisuutta ei pidetä varmana). Näillä toimenpiteillä pitäisi voida vastata kaikentyyppisiin turvallisuusriskeihin, joita yksi tai useampi jäsenvaltio on havainnut riskinarvioinnissaan.

16) Kun 5G-verkkoja koskevat eurooppalaiset kyberturvallisuussertifiointijärjestelmät on kehitetty, jäsenvaltioiden olisi annettava unionin lainsäädännön mukaisesti kansallisia teknisiä määräyksiä, joiden mukaan näiden järjestelmien kattamien tieto- ja viestintätekniikan tuotteiden, palvelujen ja järjestelmien sertifiointi on pakollista.

17) Jäsenvaltioiden olisi yhdessä komission kanssa määriteltävä yleisvaltuutukseen liitettävät ehdot, jotka koskevat julkisten verkkojen turvaamista luvatonta käyttöä vastaan, sekä verkkoihin liittyvät turvavaatimukset, jotta ne voisivat direktiivin 2002/20/EY nojalla pyytää sitoumuksia yrityksiltä, jotka osallistuvat 5G-kaistojen radiotaajuuksien käyttöoikeuksien myöntämismenettelyihin. Nämä olisi mahdollisuuksien mukaan otettava huomioon 4 kohdan c alakohdan mukaisissa toimenpiteissä.

18) Jäsenvaltioiden olisi tehtävä komission kanssa yhteistyötä sellaisten erityisten turvavaatimusten kehittämiseksi, joita voitaisiin soveltaa 5G-verkkoihin liittyvien julkisten hankintojen yhteydessä. Niihin tulisi sisältyä velvoittava vaatimus soveltaa julkisissa hankinnoissa kyberturvallisuussertifiointijärjestelmiä, jos tällaiset järjestelmät eivät vielä sido kaikkia toimittajia ja operaattoreita.

V **UUDELLEENTARKASTELU**

19) Jäsenvaltioiden olisi yhdessä komission kanssa arvioitava tämän suosituksen vaikutuksia 1. lokakuuta 2020 mennessä asianmukaisten jatkotoimien määrittämiseksi. Arvioinnissa olisi otettava huomioon unionin koordinoidun riskinarvioinnin tulokset sekä unionin välineistö.

Tehty Strasbourgissa 26 päivänä maaliskuuta 2019.

Komission puolesta

Julian KING

Komission jäsen