

**Vabariigi Valitsuse 22. juuni 2006. aasta määruse nr 140
„Nõuded sideteenuse osutamisele ja sidevõrkude tehnilised nõuded“
muutmise määruse eelnõu seletuskiri**

1. Sissejuhatus

Määrus kehtestatakse elektroonilise side seaduse¹ (edaspidi *ESS*) § 87 lõike 2 punkti 4 alusel.

Vabariigi Valitsuse 22. juuni 2006. a määruse nr 140 „Nõuded sideteenuse osutamisele ja sidevõrkude tehnilised nõuded“ (edaspidi *VV määrus nr 140*) muutmise eesmärgiks on kehtestada meetmed üldkasutatava elektroonilise side võrgu (edaspidi *sidevõrk*) turvalisuse ja riigi julgeoleku huvidele vastavuse tagamiseks.

1.1 Sisukokkuvõte

Info- ja kommunikatsioonitehnoloogia (edaspidi *IKT*) on viimaste aastakümnetega arenenud kiiresti ning muutnud arenenud ühiskonnad (kaasa arvatud Eesti) sõltuvaks tehnoloogilistest lahendustest. Eestis on 99% avalikest teenustest saadaval Interneti kaudu e-teenustena ning võrreldes paljude riikidega on Eesti sõltuvus IKT-st erakordselt suur.

Sidesektor on selles kontekstis baastaristu pakkuja, mis võimaldab digiühiskonnal toimida ja areneda. Sidevõrgu tehnoloogiad on samuti aluseks suurt töökindlust ja usaldusväärsust nõudvates kriitilise tähtsusega valdkondades nagu meditsiinis, transpordis, panganduses, energeetikas ning tõusva trendina robotikas ja tehisintellekti lahendustes. Kuna kõik andmed liiguvad läbi sidevõrkude, omavad sidevõrgud järjest olulisemat rolli riigi julgeoleku kontekstis.

Sidevõrgu tehnoloogiad on digiühiskonnas integreeritud peaaegu kõikidesse süsteemidesse (kaasa arvatud elutähtsatesse teenustesse) ja seetõttu tuleb IKT taristut käsitleda fundamentaalselt kriitilise infrastruktuurina. Uute sidevõrkude kasutuselevõtuga kaasneva kiire internetiühenduse kättesaadavuse tõus annab põhjust prognoosida, et tõenäoliselt suureneb internetiühendusega seadmete hulk nii kodanike kodudes kui ka era- ja avalikus sektoris lähiaastatel plahvatuslikult. Rahvusvaheline mobiilsideettevõtjate ühendus GSMA prognoosib, et 2025. a kasvab internetiga ühendatud seadmete arv tänasega võrreldes kolmekordseks ning jõuab ülemaailmselt 25 miljardi seadmeni.²

On paratamatu, et tulenevalt sidevõrkude ning neisse ühendatud seadmete arvu ja olulisuse kasvust muutuvad keerulisemaks ka süsteemid tervikuna. Samuti muutub keerukamaks IKT süsteemide kaitsmine manipulatsioonide ja rünnete eest. Kaasaegsed seadmed pannakse kokku lugematute spetsialiseerunud ettevõtete komponentidest üle maailma, muutes tarneahela kontrollimise ülikalliks ning praktikas võimatuks. Keerukad kiibisüsteemid sisaldavad miljardeid transistoreid ja tarkvara miljoneid ridu koodi, mida pole võimalik adekvaatselt

¹ Elektroonilise side seadus. RT I, 13.03.2019, 47.

² Global System for Mobile Communications. New GSMA Study: 5G to Account for 15% of Global Mobile Industry by 2025 as 5G Network Launches Accelerate. Pressiteade, 25.02.2019. Kättesaadav: <https://www.gsma.com/newsroom/press-release/new-gsma-study-5g-to-account-for-15-of-global-mobile-industry-by-2025/>.

inspekteerida. Kui näiteks Windowsi operatsioonisüsteemi ca 45 miljonit koodirida välja printida, saame umbes 800 000 lehekülge teksti.

Keerukust lisavad sagedased tarkvara uuendused ja kriitilised turvapaigad, mille paigaldamisega pole aega oodata. Limiteeritud kontrollvõimaluse tõttu on seadmete/tehnoloogia tootja usaldamine muutunud kriitiliseks faktoriks. Tehnoloogia tootja pole enam pelgalt seadmete ja tarkvara tarnija, vaid laiemalt tehnoloogilise teenuse pakkuja, kellega ehitatakse üles aastatepikkune koostöösuhe. Sellest lähtuvalt on vaja riskianalüüsides tegemisel kasutusele võtta kriteeriumid, mis mõõdavad tehnoloogia tootja usaldusväärsust, lisaks tootja seadmete tehnilise turvaseme hindamisele.

Eesti IKT taristu puhul tuleb samuti arvestada riigikaitse aspektiga. Eesti riigikaitse tugineb laia riigikaitse käsitusel ning NATO (Põhja-Atlandi Lepingu Organisatsioon) kollektiivkaitsel. See tähendab, et riigi kaitsmine ei hõlma üksnes sõjalist riigikaitset, vaid et riigi kaitses peavad valmis olema kõik riigiasutused ja kogu ühiskond.³ Riigi tõhus kaitse tagatakse nii sõjaliste kui ka mittedõjaliste võimete, ressursside ja tegevustega nii avalikust, era- kui ka kolmandast sektorist. IKT taristu on selles kontekstis oluline riigi ja ühiskonna toimepidevuse tagamiseks ning riigikaitse korraldamiseks. Riskianalüüsides koostamisel tuleb seetõttu arvesse võtta Eesti iseseisva kaitsevõime vajadusi ning samuti meie liitlaste hinnanguid ja piiranguid tehnoloogia kasutamise osas. Eesmärgiks on tagada olukord, kus meie IKT taristu on turvaline ja usaldusväärne nii meie endi kui ka NATO liitlaste silmis.

Võrkude kvaliteedi kindlustamiseks, küberrünnete mõju minimeerimiseks ja poliitiliste manipulatsioonide vältimiseks tuleb tagada, et sidevõrkude rajamine ning nende vahendusel sideteenuste osutamine toimuks turvalise tehnoloogia abil ning usaldusväärse partneri poolt. Euroopa Komisjon ütleb oma 26.03.2019. a soovitusel (EL) 2019/534 5G sidevõrkude turvalisus⁴, et liikmesriigid peaksid riskide hindamisel kaaluma nii tehnilisi, kui ka muid faktoreid. Tehnilisteks faktoriteks on näiteks turvanõrkused (haavatavused, tagauksed), mida võidakse kasutada küberluureks ning andmete ja süsteemide häirimiseks / hävitamiseks. Muudeks (usaldusväärsuse) faktoriteks on muu hulgas kolmandate riikide mõju tehnoloogia tootjale, mõjujõuga riigi valitsemisvorm ning julgeolekualaste koostöölepingute ja teiste küberturvalisust ja privaatsust puudutavate lepingute olemasolu või nende puudumine.

Samuti soovitab Euroopa Komisjon pöörata riskianalüüsides tegemisel tähelepanu kõikidele sidevõrgu seadmetele ja komponentidel terve elutsükli jooksul. See puudutab kogu riist- ja tarkvara nende disaini, arendamise, hankimise, rakendamise, opereerimise ja hooldamise faasides.

9. oktoobril 2019. a avalikustas Euroopa Liidu võrgu- ja infoturbe koostöögrupp liikmesriikide poolt välja töötatud 5G sidevõrkude riskianalüüsi.⁵ Selles öeldakse, et tuleviku sidevõrgud (5G) mängivad kesksel rollil Euroopa Liidu ühiskonna ja majanduse digitaalses transformatsioonis ning seetõttu on 5G sidevõrkude turvalisus kriitilise tähtsusega. Kõige suurema ja tõenäolisema ohuna nähakse Euroopa Liidu väliseid riike, kellel on huvi ja ressursse läbi viia kõrgelt arenenud küberrünnakuid. Eriti ohtlikud on riigid, kellele omistatud küberrünnete ajalugu näitab agressiivse küberprogrammi olemasolu.

³ Kättesaadav: <https://www.riigikantselei.ee/et/julgeoleku-ja-riigikaitse-koordineerimine>.

⁴ ELT L 88, 29.3.2019, lk 42–47. Kättesaadav:

<https://eur-lex.europa.eu/legal-content/ET/TXT/?qid=1569311905525&uri=CELEX:32019H0534>.

⁵ Kättesaadav: https://eu2019.fi/en/article/-/asset_publisher/member-states-publish-a-report-on-eu-coordinated-risk-assessment-of-5g-networks-security.

Samuti tuuakse Euroopa Liidu raportis välja, et oluline on hinnata iga tehnoloogia tootja riskiprofiili. Muu hulgas tuleb analüüsida ettevõtete sõltumatust Euroopa Liidu välistest riikidest, et välistada poliitiliste huvide realiseerimist tehnoloogia kaudu. Selleks on vaja arvesse võtta ettevõtte ja valitsuse seoseid, ettevõttele kohaldatavaid õigusakte (kas õigusaktid lähtuvad demokraatlikest printsiipidest ning andmekaitse põhimõtetest), ettevõtte juhtimise läbipaistvust ning kolmandate riikide võimet rakendada ettevõtte üle sunnimehhanisme. Raporti olulisim sõnum on see, et IKT kasutamise puhul peab riskide hindamine olema kõikehõlmav, mitte ainult tehniliste aspektide keskne.

Pidades silmas digiühiskonna arengut ning muutunud julgeolekuolukorda, on vajalik, et enne sidevõrkude jaoks vajaliku riist- ja tarkvara kasutusele võtmist sidevõrgus, tagatakse nende kooskõla riigi julgeoleku huvidega.

Eelnõu koostamisel kaaluti erinevaid võimalusi sidevõrkude riigi julgeoleku huvidele vastavuse tagamiseks. Valitud lahendus aitab tagada, et sideettevõtja saab riigilt lubava või keelava otsuse enne, kui võrgu rajamiseks planeeritav investeering on sooritatud.

1.2 Eelnõu ettevalmistaja

Määruse eelnõu on välja töötanud IKT seadmete usaldamise poliitika töörühm, mis moodustati väliskaubandus- ja infotehnoloogiainistri 26.06.2019. a käskkirjaga nr 1.1-1/19-100. Nimetatud töörühma juhtis Majandus- ja Kommunikatsiooniministeeriumi riigi küberturvalisuse poliitika juht Raul Rikk (tel: 625 6338, e-post: raul.rikk@mkm.ee).

Töörühma koosseisu kuulusid: Majandus- ja Kommunikatsiooniministeeriumi, Justiitsministeeriumi, Kaitseministeeriumi, Kaitsepolitseiameti, Kaitseväge, Politsei- ja Piirivalveameti, Registrate ja Infosüsteemide Keskuse, Riigi Infosüsteemi Ameti, Riigi Infokommunikatsiooni SA, Riigikantselei, Siseministeeriumi, Tarbijakaitse- ja Tehnilise Järelevalve Ameti (edaspidi *TTJA*), Välisministeeriumi ja Välisluureameti esindajad.

Määruse eelnõu ja seletuskirja on vormistanud Majandus- ja Kommunikatsiooniministeeriumi sideosakonna juhataja asetäitja Mart Laas (tel: 625 6441, e-post: mart.laas@mkm.ee) ja peaspetsialist Liisi Moks (tel: 639 7665; e-post: liisi.moks@mkm.ee).

1.3. Märkused

Eelnõu ei ole seotud muu menetluses oleva eelnõu ega Vabariigi Valitsuse tegevusprogrammiga.

2. Eelnõu sisu ja võrdlev analüüs

Määruse eelnõu koosneb kahest paragrahvist.

Eelnõu § 1.

Eelnõu punktiga 1 täiendatakse VV määruse nr 140 § 3 lõiget 1 punktiga 1¹, millega sätestatakse üldine norm, et sideettevõtja peab planeerima, projekteerima, ehitama, hooldama ja kasutama sideteenuse osutamiseks kasutatavat sidevõrku selliselt, et see oleks kooskõlas riigi julgeoleku huvidega.

Mõiste „riigi julgeolek“ on käesoleva eelnõu puhul sisustatud Riigikogu poolt 2017. a kinnitatud julgeolekupoliitika alustes (edaspidi *JPA*)⁶ ja Vabariigi Valitsuse poolt kinnitatud riigikaitse arengukavas 2017–2026 (edaspidi *RKAK*)⁷. JPA sätestab Eesti julgeolekupoliitika eesmärgina kindlustada Eesti riigi iseseisvus ja sõltumatus, rahva ja riigi kestmine, territoriaalne terviklikkus, põhiseaduslik kord ja elanikkonna turvalisus. RKAK määrab ühe olulise riigikaitse tegevussuunana riigi ja ühiskonna toimimise mistahes olukorras. See hõlmab elutähtsate teenuste või muude riigikaitse tähenduses oluliste teenuste toimepidevuse tagamist. Sideteenused kuuluvad elutähtsate teenuste hulka ning sidevõrkude rajamine on nendega vahetult seotud.

Laia riigikaitse seisukohast on seega oluline, et riigi ja ühiskonna harjumuspärasest toimimisest tagavate teenuste kasutatavus ei satuks võrguseadmete tarkvaravigade, võimalike tootja poolt tekitatud tehnoloogiliste „tagauste“ või nende vastu suunatud pahatahtlike rünnakute ja manipulatsioonide tõttu ohtu.

Eelnõu punktiga 2 täiendatakse VV määrust nr 140 §-ga 3¹. Uus paragrahv koosneb viiest lõikest.

Paragrahvi 3¹ lõige 1 seab elutähtsa teenuse osutajast sideettevõtjale kohustuse enne sidevõrgu riist- ja tarkvara kasutusele võtmist esitada TTJA-le elektrooniliselt kooskõlastamiseks sidevõrgu riist- ja tarkvara tehnilise dokumentatsiooni.

See nõue kehtib ainult sideettevõtjast elutähtsa teenuse osutajale, kes ESS § 87 lõike 4 alusel on telefoniteenuse, mobiiltelefoniteenuse ja andmesideteenuse osutaja, kelle teenust tarbib vähemalt 10 000 lõppkasutajat. Eestis on selliseid sideettevõtjaid viis ning nende osakaal sideturust on ca 90–95%.

Hädaolukorra seaduse (edaspidi *HOS*) mõistes peab iga valdkonna elutähtsa teenuse osutaja (side mõistes – sideettevõtja, kelle teenust tarbib vähemalt 10 000 lõppkasutajat) tagama oma valdkonna elutähtsa teenuse (side mõistes HOS § 36 lõike 1 punktid 5–7 ehk telefoni-, mobiiltelefoni- ja andmesideteenuse) toimepidevuse. Elutähtsa teenuse toimepidevus on teenuse osutaja järjepideva toimimise suutlikkus ja järjepideva toimimise taastamise võime pärast katkestust. Täpsemini, elutähtsa teenuse toimepidevuse tagamine on suunatud sellele, et elutähtis teenus oleks kättesaadav tarbijatele igal ajahetkel, ka hädaolukorra ajal. Selleks peab elutähtsa teenuse osutaja olema võimeline osutama teenust katkematult olenemata olukorrast ehk omama vastavaid vahendeid, tehnilist ettevalmistust jne ning olema suuteline võimalikult kiiresti taastama teenuse katkematu osutamise.⁸

Sideettevõtja poolt TTJA-le kooskõlastamiseks esitatav sidevõrgu riist- ja tarkvara tehniline dokumentatsioon sisaldab vähemalt järgmisi andmeid:

- 1) Riist- ja tarkvara nimetus – millise riist- või tarkvaraga on tegemist;
- 2) Riist- ja tarkvara tootnud ettevõtja (tootja);
- 3) Riist- ja tarkvara funktsionaalsus sidevõrgus – millist funktsiooni riist- ja tarkvara täidab;
- 4) Riist- ja tarkvara kasutuskoht sidevõrgus – loogiline asetsemine võrgus ja füüsiline asukoht;
- 5) Riist- ja tarkvara kasutamise alguse ja lõpu kuupäev – mis kuupäevast, mis kuupäevani.

⁶ Eesti julgeolekupoliitika alused. Kättesaadav: https://www.riigikantselei.ee/sites/default/files/content-editors/Failid/2017.05.31_jpa_riigikogu.pdf.

⁷ Riigikaitse arengukava 2017–2026. Kättesaadav: https://www.riigikantselei.ee/sites/default/files/content-editors/Failid/rkak_2017_2026_avalik_osa.pdf.

⁸ HOS seletuskiri. Kättesaadav: <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/6e396188-c9c2-4673-9fb6-ad324ec9a36c/Hädaolukorra%20seadus>

Kuna sideettevõtja suhtleb juba praegu sideturu reguleerimise ja sageduslubade teemal TTJA-ga, siis on igati loogiline, et ka sel teemal suhtleb sideettevõtja TTJA-ga, mitte kolme erineva ameti ja Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukoguga.

Paragrahvi 3¹ lõige 2 sätestab, et kuna TTJA-l puudub nii riigi julgeoleku kui ka küberturvalisuse hindamise pädevus, esitab TTJA sideettevõtja sidevõrgu riist- ja tarkvara tehnilise dokumentatsiooni riigi julgeoleku huvidele vastamise kontrollimiseks riigi julgeolekuasutustele (julgeolekuasutuste seaduse mõistes Kaitsepolitseiamet ja Välisluureamet) ja Riigi Infosüsteemi Ametile. Nimetatud asutustel on sidevõrgu riist- ja tarkvara kasutuselevõtu kohta arvamuse avaldamiseks aega 30 tööpäeva, arvamuse küsimisest arvates. Ametid lähtuvad arvamuse andmisel oma sisemistest dokumentidest ja nende valdkonna enda või NATO ja Euroopa Liidu partnerite teostatud riskihinnangutest jt samaväärsetest dokumentidest. Nimetatud asutused peavad oma arvamust põhjendama.

Paragrahvi 3¹ lõige 3 sätestab TTJA-le võimaluse küsida eelnõu lõikes 4 tehtava otsuse tegemisel seisukohta Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogult. Nimetatud nõukogu kaalutleb olukordi, kus riigi julgeoleku huvid, majanduslikud huvid, sideteenuse toimepidevuse tagamine ning muud võimalikud huvid on vastuolulised. Näiteks võib tekkida olukord, kus teatud riist- ja tarkvara kasutamine ei ole julgeolekuasutuste poolt koostatud riskihinnangu järgi turvaline, kuid mida ei ole võimalik sideteenuse toimepidevuse seisukohalt kiiresti välja vahetada. Selline olukord nõuab kaalutlemist ning parima võimaliku lahenduse väljatöötamist.

TTJA pöördub Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu poole kaalutletud ja tasakaalustatud seisukoha küsimiseks. Nimetatud nõukogu esitab oma põhjendatud ettepaneku TTJA-le 60 tööpäeva jooksul ettepaneku küsimisest arvates.

Paragrahvi 3¹ lõige 4 sätestab tähtaja, mille jooksul peab TTJA otsustama sideettevõtja kooskõlastamisele esitatud riist- ja tarkvara kasutamise lubamise. TTJA peab 30 tööpäeva jooksul pärast julgeolekuasutuste ja Riigi Infosüsteemi Ametilt arvamuse või Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu ettepaneku saamist otsustama, kas ta annab käesoleva paragrahvi lõikes 1 esitatud sideettevõtja sidevõrgu riist- ja tarkvara tehnilisele dokumentatsioonile kooskõlastuse või jätab selle kooskõlastamata.

Lähtuvalt ESS §-ist 147 vormistab TTJA kooskõlastuse ja kooskõlastamata jätmise otsusena ehk annab haldusakti, mida on võimalik vaidlustada halduskohtus.

Juhul kui TTJA jätab sideettevõtja esitatud sidevõrgu riist- ja tarkvara tehnilise dokumentatsiooni kooskõlastamata, peab ta tulenevalt haldusmenetluse seaduse §-ist 56 lisama otsusesse kooskõlastamata jätmise põhjuse.

Alles seejärel, kui TTJA-lt on laekunud kooskõlastav otsus, võib sideettevõtja võtta kasutusele sidevõrgu riist- ja tarkvara, mille kooskõlastust küsiti.

Paragrahvi 3¹ lõige 5 kohaselt seab TTJA käesoleva eelnõu § 3¹ lõikes 1 nimetatud nõude sagedusloa tingimuseks. Sagedusluba on ESS § 11 lõike 2 kohaselt dokument, mis annab õiguse kasutada teatud raadiosagedusi TTJA poolt määratud tingimustel. Sama paragrahvi lõike 4 kohaselt kehtestatakse sagedusloaga asjassepuutuvate raadiosageduste kasutamisele teatud tingimused ja nõuded, mille hulka kuuluvad ka tehnilised tingimused raadiosageduste kasutamiseks.

Käesoleva sätte kohaselt seab TTJA elutähtsat teenust ostutava sideettevõtja sagedusloale kõrvaltingimuse kooskõlastada riist- ja tarkvara enne selle kasutuselevõttu TTJA-ga.

ESS § 18 lõike 1 kohaselt võib TTJA sagedusloa tingimuse rikkumise korral selle alusel raadiosageduste kasutamise õiguse peatada ning sama paragrahvi lõike 3 punktis 4 sätestatud

tingimustel sagedusloa kehtetuks tunnistada. Tulenevalt sellest, et eelnõu § 3¹ lõikes 1 sätestatud nõude täitmine selgub üksnes läbi lõikes 4 sätestatud kooskõlastuse, luuakse kõnealuse sätte abil mehhanism, mille abil on võimalik eelnõu § 3¹ lõikes 1 sätestatud kohustust rikkuvale sideettevõtjale antud sagedusloa kehtivus peatada ning rikkumise jätkumise korral see kehtetuks tunnistada.

3. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõul ei ole puutumust Euroopa Liidu õigusega.

4. Määruse mõjud

4.1. Sotsiaalne, sealhulgas demograafiline mõju

Määruse muudatusega ei kaasne sotsiaalseid ega demograafilisi mõjusid.

4.2. Mõju riigi julgeolekule ja välissuhetele

Määruse muudatusega kaasneb positiivne mõju riigi julgeolekule ja välissuhetele. Eelnõu abil tagatakse, et rajatavad sidevõrgud ei kujutaks ohtu riigi julgeolekule laia riigikaitse põhimõtete tähenduses, hõlmates seejuures ka riigi kriitilist infrastruktuuri ja elutähtsaid teenuseid.

Välisluureameti poolt 2019. a I ja II kvartalis läbi viidud riskianalüüsis leiti, et uute tehnoloogiate tingimusteta lubamine Eesti sidetaristusse võib tuua kaasa negatiivseid tagajärgi, mis puudutavad nii era- kui avalikku sektorit ja riigi majandusruumi toimimist tervikuna. Riigil on kohustus tagada, et sidevõrgud rajataks usaldusväärsele tehnoloogiale, mille kasutamine ei too kaasa olukorda, kus riik ei saa tagada oma kodanikele põhiõiguste- ja vabaduste, sh privaatsuse, sõnumisaladuse ja intellektuaalse omandi kaitset. Ebausaldusväärsest tehnoloogiast tulenevate julgeolekuriskide realiseerumise korral on kõige nõrgemas positsioonis just lõpptarbijad tavalised elanikud, kes ei saa olukorras, kus sidevõrgud on ebausaldusväärsetelt või kergesti haavatavalt rajatud, iseenda küberturvalisuse tagamiseks midagi ette võtta.

Ka riigikaitse perspektiivist on oluline, et kriitilistesse süsteemidesse integreeritavad sidevõrgud oleksid toodetud usaldusväärsete osapoolte poolt, ei oleks lihtsate meetodite abil manipuleeritavad ning ühilduks meie liitlaste poolt kasutatavate süsteemidega Euroopa Liidus ja NATO-s. On oluline, et Eesti sidevõrke ei rajataks ebausaldusväärsele tehnoloogiale, mille kaudu on tõenäoline riigikaitseks kasutatavate süsteemide halvamine või mille kasutamist liitlasriigid ei aktsepteeri ja mis võiks seeläbi kaasa tuua viivitusi või takistusi kriitilise tähtsusega infovahetuses.

Euroopa Liidu liikmesriigid on jõudnud ühiselt seisukohale, et IKT riskide hindamisel tuleb arvesse võtta kõiki aspekte – nii tehnilisi, kui ka mittetehnilisi.⁹ Liikmesriikide ühises riskianalüüsis tõdetakse, et tuleviku sidevõrkude (5G) kontekstis on kõige suuremaks ohuks Euroopa Liidu välised ebademokraatlikud riigid, kellel on huvi ja võimekus ellu viia küberrünnakuid ning kes omavad mõjuvõimu enda jurisdiktsioonis asuvate ettevõtete üle. Seetõttu on oluline rakendada liikmesriikides protseduure, mis võimaldaksid hinnata tehnoloogia tootja riskiprofiili ning vältida ebausaldusväärsete tarnijate mõju.

4.3. Majanduslik mõju

Eelnõuga ei teki riigile, kohalikele omavalitsustele ega ka sideteenuste lõppkasutajatele vältimatuid kulusid.

⁹ Kättesaadav: https://eu2019.fi/en/article/-/asset_publisher/member-states-publish-a-report-on-eu-coordinated-risk-assessment-of-5g-networks-security.

Sideettevõtjate jaoks võivad eelnõuga kaasneda teatavad kulud, kui riist- või tarkvara jäetakse kooskõlastamata ning sobilik riist- või tarkvara ei ühildu olemasoleva sidevõrguga ning sellest tulenevalt on vajalik olemasolevat riist- või tarkvara välja vahetada. Vastava kulu suurust ei ole võimalik ette ennustada, kuna pole teada millist riist- või tarkvara sideettevõtjad plaanivad soetada.

Määruse rakendamisega seotud kuludega seonduvat on detailsemalt kirjeldatud seletuskirja punktis 5.

4.4. Mõju riigiasutuste ja kohaliku omavalitsuse asutuste korraldusele

Määrus omab mõju MKM haldusala eelarvele, kuna määruse rakendamiseks on vaja luua üks uus töökoht. Tegemist on sidevõrgu riist- ja tarkvara hindamisega riigi julgeoleku seisukohast, mille osas täna TTJA-l pädevus puudub. Lisandub töökoormus menetluste näol (dokumentide kontroll, otsuste ettevalmistamine, töö koordineerimine osapoolte vahel jne) ning vajalik on sisuline panustamine Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu töösse.

Julgeolekuasutuste ja Riigi Infosüsteemi Ameti ning Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu töökoormus suureneb, kuid selle mõju suurus on seotud TTJA poolt arvamuse / ettepaneku küsimiseks saadetud riist- ja tarkvara tehnilise dokumentatsioonide hulgast.

5. Määruse rakendamiseks vajalikud kulutused ja määruse rakendamise eeldatavad tulud

Määruse rakendamisega on vaja suurendada MKM haldusala eelarvet ühe inimese palgakulu võrra, milleks hinnanguliselt on kalendriaastas koos kõikide maksudega 32 112,00 eurot.

Sideettevõtjate jaoks võivad eelnõuga kaasneda teatavad kulud, kui riist- või tarkvara jäetakse kooskõlastamata ning sobilik riist- või tarkvara ei ühildu olemasoleva sidevõrguga ning sellest tulenevalt on vajalik olemasolevat riist- või tarkvara välja vahetada. Vastava kulu suurust ei ole võimalik ette ennustada, kuna pole teada millist riist- või tarkvara sideettevõtjad plaanivad soetada.

Küll aga peavad elutähtsat teenust osutavad sideettevõtjad sidevõrkude rajamisel arvestama käesolevast määrusest tulenevate kohustustega. Seetõttu ei ole võimalik välistada olukorda, et lahendused, mida ettevõtja oleks kooskõlastuskohustuse puudumisel majanduslikult kõige soodsamate tingimuste tõttu eelistanud, ei pruugi riigi julgeolekuhuvide seisukohalt sidevõrgu rajamiseks sobida ning valida tuleb mõni muu, konkureeriv pakkuja.

6. Määruse jõustumine

Määrus jõustub kuus kuud pärast määruse avaldamist. sellega antakse sideettevõtjatele üleminekuaeg.

7. Eelnõu kooskõlastamine

Eelnõu esitatakse kooskõlastamisele eelnõude infosüsteemi (EIS) kaudu Justiitsministeeriumile, Siseministeeriumile, Kaitseministeeriumile, Rahandusministeeriumile, Riigikantseleile ja Välisministeeriumile ning arvamuse avaldamiseks Eesti Infotehnoloogia ja Telekommunikatsiooni Liidule.