KAITSEMINISTEERIUM

Teie: 13.02.2026 nr 17.1.1/26-0036/-2T

Justiits- ja Digiministeerium
Suur-Ameerika 1, 15006 Tallinn
info@justdigi.ee

Meie: 17.03.2026 nr 5-8/26/10-3

COM(2026) 16 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital networks, amending Regulation (EU) 2015/2120, Directive 2002/58/EC and Decision No 676/2002/EC and repealing Regulation (EU) 2018/1971, Directive (EU) 2018/1972 and Decision No 243/2012/EU (Digital Networks Act)

Riigikantselei esitas Kaitseministeeriumile arvamuse esitamiseks COM(2026) 16 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital networks, amending Regulation (EU) 2015/2120, Directive 2002/58/EC and Decision No 676/2002/EC and repealing Regulation (EU) 2018/1971, Directive (EU) 2018/1972 and Decision No 243/2012/EU (Digital Networks Act) ehk EL küberturvalisuse määruse eelnõu. Esitame järgmised tähelepanekud:

I. Kaitseministeerium toetab muudatusi, mis lisanduvad NIS2 alla:

1. Allveekaablite andmeside taristu (kaablid ja nendega seotud rajatised) kui eraldi määratletud objekt. Siinkohal vajab täpsustamist allveekaabli andmeside taristu „operaatori" määratlus juhtudeks, kus kaablit omab konsortsium, opereerimist teeb üks osapool ja maismaajaamad/„landing station" teenused on allhankes.
2. Strateegilise kahese kasutusega taristu omanikud/haldajad/ettevõtjad (seotult sõjalise mobiilsuse loogikaga). Need muudatused suurendavad teenuste järjepidevuse kaitset just nendes valdkondades, kus rikke mõju oleks Eestis ja piirkonnas kiiresti piiriülene.
3. Mikro- ja väike-DNS teenusepakkujate automaatselt väljaviimist kohaldamisalast, kuid soovime, et süsteem jätaks võimaluse (riikliku kriitilisuse hindamise kaudu) hõlmata väikseid DNS-teenuseid, kui nende töökindlus on kriitiline (nt oluliste avalike teenuste sõltuvused). Eesti praktikas on näha, et ründajad on DDoS-kampaaniates sihtinud üha enam nimeservereid, sest neid on keerulisem kaitsta kui hästi „turvatud" veebiservereid.
4. ENISA rolli suurendamist piiriüleste teenusepakkujate järelevalve ja vastastikuse abi koordineerimisel ning registri kasutamist ühtsema pildi loomiseks. See vähendab dubleerivaid kontrolle ja toetab ühtlasemat turutasandit. Samas rõhutame ranget konfidentsiaalsus- ja ligipääsuhalduse tarvilikkust. Registriandmete osas peab olema detailne kirjeldus, kuidas tagatakse IP-vahemike ja digiaadresside kaitse ning millised asutused saavad ligipääsu andmetele. Ligipääs registrile peab olema rollipõhine ja logitav ja eriti tundliku taristu (sh kahese kasutusega) andmeid käsitletaks minimaalsuse ja vajaduspõhisuse põhimõttel.
5. Postkvant-krüptograafiale ülemineku poliitika nõue riiklikes küberstrateegiates. Eesti riiklik küberturvalisuse strateegia 2024–2030 käsitleb kvantohte ja seab sihte kvantkindlate sideturbelahenduste kasutamiseks ning krüptograafilise kompetentsi tugevdamiseks. EL nõue tugevdab vajalikku ajastust ja koordineerimist.

II. Art 21 lg 5 maksimaalse harmoniseerimise teema jääb ebaselgeks, mistõttu on vaja lahti mõtestada:

1. millal loetakse riiklik nõue „täiendavaks" (näiteks, kas riiklik infoturbestandard E-ITS kui „rakendusraamistik" on täiendav nõue või üks võimalik vastavusviis);
2. kuidas käsitleda kiiresti muutuvat ohtu, kui EL rakendusakt ei kata konkreetset riskimeedet piisavalt (näiteks uued ründetehnikad).

III. Soovitame lisada selgituse, et riik võib sätestada täiendavaid nõudeid üksnes (i) erandlikel, põhjendatud

juhtudel ja (ii) mitte vastuolus EL rakendusaktidega ning, et E-ITS tüüpi raamistikud tuleb käsitleda eelkõige „vastavuse saavutamise meetodina" mitte automaatselt keelatud „lisanõudena". „Küberhoiaku" sertifitseerimise puhul vajame selgust sertifikaadi ulatuse ja kontrollitavuse osas:

1. mida täpselt sertifitseeritakse (protsessid, juhtimine, tehnilised kontrollid);
2. kuidas arvestatakse allhanke ja pilveteenuste kasutust;
3. milline on sertifikaadi kehtivuse tühistamise/peatamise mõju.

IV. Soovitame täpsustada, et pädev asutus võib teha sihitud järelevalvetoiminguid ka sertifikaadi olemasolul, kui (a) sertifikaat ei kata kõiki Art 21 kohustusi, (b) esineb oluline intsident või (c) on mõistlik kahtlus sertifikaadi aluseks oleva praktika olulisest muutumisest.

Lugupidamisega

(allkirjastatud digitaalselt)

Hanno Pevkur
minister

Jarmo Maasing
jarmo.maasing@kaitseministeerium.ee