PÄÄESIKUNTA
Oikeudellinen osasto
Sotilaslakimies Katriina Härmä
Helsinki

20.4.2026

Eduskunnan puolustusvaliokunnalle

U 17/2026 ehdotus Euroopan parlamentin ja neuvoston kyberturvallisuusasetukseksi (CSA2) ja NIS 2 -muutosdirektiiviksi

1. Yleistä

Euroopan komissio on antanut 20.1.2026 ehdotuksen (COM(2026) 11 final) Euroopan parlamentin ja neuvoston asetukseksi Euroopan unionin kyberturvallisuusvirasto ENISA:sta, Euroopan kyberturvallisuuden sertifiointikehyksestä ja ICT-toimitusketjujen turvallisuudesta sekä asetuksen (EU) 2019/881 kumoamisesta (CSA2-ehdotus). Komissio antoi CSA2-ehdotuksen kanssa samanaikaisesti ehdotuksen (COM(2026) 13 final) Euroopan parlamentin ja neuvoston direktiiviksi direktiivin (EU) 2022/2055 (NIS 2) muuttamisesta sen yksinkertaistamiseksi ja yhdenmukaistamiseksi CSA2-ehdotuksen kanssa (NIS2-muutosehdotus).

Pääesikunta pitää esitettyjä ehdotuksia kannatettavina, vaikka niillä ei tunnisteta olevan suoraa vaikutusta Puolustusvoimien toimintaan kansallisen turvallisuuden ja puolustuksen kuuluessa jäsenvaltioiden toimivaltaan ja siten sääntelyn soveltamisalan ulkopuolelle. Välillinen vaikutus on kuitenkin merkittävä, sääntelyn vaikuttaessa Puolustusvoimien yhteistyökumppaneihin ja huoltovarmuuskriittisiin yrityksiin. Pääesikunta katsoo, että ehdotukset tukevat puolustusvoimien toimintaa ja puolustusjärjestelmään vaikuttavien järjestelmien, palveluiden ja palveluntuottajien kybersuojaa mm. tilaus-toimitusketjuhyökkäyksiä vastaan sekä mahdollistamalla riskiyritysten tuotteiden käytön rajoittamista.

2. Kyberturvallisuusasetusehdotus (CSA2)

Pääesikunta pitää tärkeänä sitä, että ehdotuksessa on tunnistettu kybertoimintaympäristön jatkuva muutos (mukaan lukien kasvavat uhkat sekä digitalisoituvat dataperusteiset kriittiset palvelut), joka on ollut yksi syy CSA:n uudelleentarkastelulle.

Pääesikunta suhtautuu myönteisesti ENISA:n roolin kasvattamiseen sikäli, kun sillä tähdätään toiminnan tehostamiseen Naton suuntaan.

Pääesikunta pitää kannatettavana eurooppalaisen kyberturvallisuuden sertifiointikehyksen uudistamista, tehostamista ja selkeyttämistä. Sikäli kun edeltävät sertifiointikehykset eivät ole olleet toimivia on syytä kokemuksiin perustuen tarkastella asiaa uudelleen ja löytää parempia ratkaisuja. Sertifiointia voidaan hyödyntää ja edellyttää Puolustusvoimien kumppaneilta osoittamaan kyberturvallisuuden tasoa.

3. NIS 2 -muutosdirektiivi

NIS 2 -direktiivin velvoitteet eivät koske Puolustusvoimien toimintaa sen jäädessä soveltamisalan ulkopuolelle. Pääesikunta suhtautuu kuitenkin myönteisesti muutosehdotuksiin, jotka edistävät sääntelyn tavoitteita ja turvaavat kyberturvallisuuden korkeaa tasoa.

Nykyisen NIS 2 -direktiivin 5 artiklan mukaan se ei esitä jäsenvaltioita antamasta säännöksiä, joilla tavoitellaan kyberturvallisuuden korkeampaa tasoa tai säännöksiä, joita sovelletaan direktiivin soveltamisalaa laajemmalti. Pääesikunta pitääkin tärkeänä, että mikäli NIS 2 -muutosdirektiivien vaatimusten toimeenpano edellyttäisi jatkossa muutoksia kansalliseen lainsäädäntöön, esimerkiksi kyberturvallisuuslakiin (124/2025), niin tässä yhteydessä selvitettäisiin myös tarkemmin mahdollisuutta laajentaa soveltamisalaa kansallisesti soveltuvin osin myös Puolustusvoimiin ja puolustuskyvyn kannalta kriittisiin järjestelmiin.