

Hallintovaliokunta

Valtioneuvoston kirjelmä eduskunnalle ehdotuksista Euroopan parlamentin ja neuvoston kyberturvallisuusasetukseksi (CSA2) ja NIS 2-muutosdirektiiviksi

Suurelle valiokunnalle

JOHDANTO

Vireilletulo

Valtioneuvoston kirjelmä eduskunnalle ehdotuksista Euroopan parlamentin ja neuvoston kyberturvallisuusasetukseksi (CSA2) ja NIS 2-muutosdirektiiviksi (U 17/2026 vp): Asia on saapunut hallintovaliokuntaan mahdollisia toimenpiteitä varten.

Asiantuntijat

Valiokunta on kuullut:

- neuvotteleva virkamies Katariina Simonen, sisäministeriö
- neuvotteleva virkamies Emma Hokkanen, liikenne- ja viestintäministeriö
- neuvotteleva virkamies Marième Korhonen-Cara, liikenne- ja viestintäministeriö
- ylitarkastaja Eevi Vuorinen, liikenne- ja viestintäministeriö

Valiokunta on saanut kirjallisen lausunnon:

- suojelupoliisi
- Liikenne- ja viestintävirasto

VALTIONEUVOSTON KIRJELMÄ

Ehdotus

Valtioneuvoston kirjelmä koskee Euroopan komission 20.1.2026 antamaa ehdotusta (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) sekä komission samana päivänä antamaa ehdotusta (COM(2026) 13 final) Euroopan parlamentin ja neuvoston direktiiviksi direktiivin (EU) 2022/2055 (NIS2) muuttamisesta sen yksinkertaistamiseksi ja yhdenmukaistamiseksi CSA2-ehdotuksen kanssa.

Valiokunnan lausunto HaVL 10/2026 vp

Asetusehdotuksen mukaan ENISA:n tehtäviä selkeytetään ja päivitetään kyberturvallisuuden uhkaympäristöön sopiviksi. Komission ehdottamalla uudella EU:n laajuisella kyberturvallisuussertifikaatilla voisi osoittaa, että sertifiointin kohde täyttää soveltuvassa sertifiointijärjestelmässä määritellyt tekniset kyberturvallisuusvaatimukset. NIS2-direktiivin toimijoille ehdotetaan velvoitteita ICT-toimitusketjujen ei-teknisten riskien hallitsemiseksi.

Direktiiviehdotuksen mukaan NIS 2-direktiivin soveltamisalaa laajennetaan merenalaisen tiedonsiirtoinfrastruktuurin tarjoajiin, energia- ja kemianteollisuuden toimijoihin sekä eurooppalaisten digitaalisten identiteetti- ja yrityslompakoiden tarjoajiin.

Valtioneuvoston kanta

Kyberturvallisuusasetus (CSA2)

Valtioneuvosto katsoo kyberturvallisuuden olevan olennainen osa EU:n sisämarkkinoiden häiriöttömän toiminnan ja yhteiskuntavakauden sekä kansalaisten yksityisyyden turvaamista. Valtioneuvosto kannattaa EU:n lainsäädännön tavoitetta vahvistaa kyberturvallisuuden hallinnointia sekä sitä, että asiaankuuluvilla toimielimillä, viranomaisilla ja muilla sidosryhmillä olisivat paremmat edellytykset estää, havaita ja torjua kyberturvallisuusuhkia koordinoitulla ja tehokkaalla tavalla.

Valtioneuvosto suhtautuu myönteisesti Euroopan kyberturvallisuusvirasto ENISA:n mandaatin kokonaisvaltaiseen uudelleentarkasteluun muuttunut uhkaympäristö sekä unionin kyberturvallisuuslainsäädäntö huomioiden. Valtioneuvosto katsoo, että ENISA:n toiminnan tulee olla tehokasta, priorisoitua ja läpinäkyvää. ENISA:n toiminnan ja tehtävien tulisi ensisijaisesti täydentää jäsenmaiden viranomaisten kyberturvallisuustehtäviä.

Valtioneuvosto suhtautuu myönteisesti ENISA:n toiminnan laajentamiseen operatiivisen yhteistyön tukeen sekä tilannekuvan tuottamiseen huomioiden kuitenkin, että ensisijainen vastuu kyberturvan tasoa varmistavissa ja yhteiskunnan toimijoita tukevissa viranomaistehtävissä on jäsenmailla ja sen viranomaisilla. Tiedonvaihtoon, jolla voisi olla negatiivisia vaikutuksia kansalliseen turvallisuuteen, suhtaudutaan varauksellisesti. Valtioneuvosto suhtautuu kuitenkin myönteisesti ENISA:n yhteistyön tiivistämiseen kumppanimaiden ja kansainvälisten organisaatioiden, kuten NATO:n kanssa.

Valtioneuvosto pitää ENISA:n tehtävien laajentamista tietojärjestelmähaavoittuvuuksien hallintaan liittyviin palveluihin erityisen tärkeänä. Unionin omien kyvykkyyksien vahvistaminen tietojärjestelmähaavoittuvuuksien hallinnassa vahvistaa unionin strategista autonomiaa.

Valtioneuvosto pitää tärkeänä, että jäsenmaat ja komissio ovat jatkossakin tasa-arvoisessa asemassa ENISA:n toimintaan liittyvässä päätöksenteossa. Jäsenmaiden tulee itse voida päättää viraston toimielimiin nimitettävistä edustajista sekä virastoon lähetettävistä asiantuntijoista.

Valtioneuvosto pitää tärkeänä, että tällä asetuksella ei ennakoita tulevan rahoituskehityksen (2028–2034) rahoitusta. Tulevan kauden rahoituksen mitoitukseen otetaan kantaa erikseen osana rahoituskehitysneuvottelujen kokonaisuutta.

Valiokunnan lausunto HaVL 10/2026 vp

Valtioneuvosto korostaa, että EU:n toimielinten ja virastojen hallintomenojen taso sekä henkilöstömäärä on pidettävä maltillisena. Valtioneuvosto pyytää jatkovalmistelussa tarkennuksia ENISA:n keräämiin maksuihin ja toiminnan rahoittamiseen liittyen.

Valtioneuvosto suhtautuu kyberturvallisuuden osaamiseen liittyvän tarkemman sääntelyn kehittämiseen varauksellisesti. Valtioneuvosto pitää tärkeänä varmistaa, että osaamisen liittyvät toimenpiteet ovat jäsenvaltioille vapaaehtoisia ja resurssineutraaleja.

Valtioneuvosto tukee yleisesti eurooppalaisen kyberturvallisuuden sertifiointikehyksen uudistamista, tehostamista ja selkeyttämistä. Valtioneuvosto suhtautuu lähtökohtaisesti myönteisesti kybertason ja EU:n lainsäädännön vaatimustenmukaisuusolettaman sisällyttämistä sertifiointijärjestelmien soveltamisalaan. Lisäksi valtioneuvosto kannattaa eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien ylläpitostrategian ja -toimien lisäämistä osaksi sertifiointikehystä. Valtioneuvosto pitää tärkeänä, että jäsenvaltioilla on mahdollisuus osallistua eurooppalaisen kyberturvallisuuden sertifiointikehyksen prosesseihin. Lisäksi valtioneuvosto katsoo, että sertifiointien tulee säilyä lähtökohtaisesti vapaaehtoisina.

Valtioneuvosto pitää kannatettavana, että EU:ssa haetaan ehdotuksen pohjalta yhteisiä ICT-toimitusketjuja koskevia ratkaisuja, jotka vahvistavat näiden turvallisuutta, edistävät sisämarkkinoiden toimintaa ja EU:n teknologista suvereniteettia. Toimenpiteiden tulee olla ennakoitavia ja hallittuja sekä perustua asianmukaiseen kuulemiseen ja vaikutusarviointiin. Valtioneuvosto katsoo, että ehdotuksessa esitettyjen toimenpiteiden tulee olla myös oikeasuhtaisia ja riskiperustaisia. Valtioneuvosto pitää tärkeänä, että jäsenvaltiot voivat jatkossakin asettaa asetusehdotusta pidemmälle meneviä kansallisia velvoitteita ja toimenpiteitä, erityisesti viestintäverkkojen turvallisuuden varmistamiseksi. Valtioneuvosto tukee ehdotuksen tavoitetta ja pitää samalla tärkeänä, että unionin ja jäsenvaltioiden toimivallan rajat säilyvät selkein erityisesti kansallista turvallisuutta koskevissa asioissa. Valtioneuvosto myös korostaa jäsenvaltioiden keskeistä roolia ICT-toimitusketjujen riskien arvioinnissa.

Valtioneuvosto edellyttää, että komissiolle delegoitavat toimivaltuudet ovat tarkkarajaisia, oikeasuhtaisia, tarkoituksenmukaisia ja perusteltuja.

Suomen kantoja komission ja korkean edustajan tiedonantoon unionin taloudellisen turvallisuuden vahvistamiseksi on muodostettu selvityksessä E 3/2026 vp. Selvitys sisältää nyt kyseessä olevan ehdotuksen näkökulmasta olennaisen kirjauksen kansainvälisestä yhteistyöstä haitallisten riippuvuuksien vähentämiseksi:

Haitallisten riippuvuuksien vähentämiseksi EU:n tulee edetä nopeasti kauppaneuvotteluissa sekä kumppanuuksissa esimerkiksi kriittisten raaka-aineiden, teollisuuden, energian ja kriittisten teknologioiden toimitus- ja arvoketjuissa. EU:n tulisi kartoittaa standardipohjaisten markkinoiden luomisen edut ja mahdollisuudet ja panostaa sääntely-yhteistyöhön kolmasmaakumppaneiden kanssa. EU:n tulee hyödyntää unionin olemassa olevia välineitä laajasti myös kolmasmaayhteistyössä haitallisten riippuvuuksien purkamiseksi.

Lisäksi Suomen kantoja komission tiedonantoon osaamisunionista on muodostettu selvityksessä E 56/2025 vp, jonka osalta huomioidaan nyt kyseessä olevan ehdotuksen osalta seuraava kirjaus:

Valiokunnan lausunto HaVL 10/2026 vp

Suomi pitää tärkeänä, että komission ehdotukset perustuvat riittävän kattaviin vaikutusarviointeihin. Suomi korostaa, että EU-tason toimenpiteet on tärkeää suunnitella siten, että ne ovat kustannustehokkaita, eivät lisää hallinnollista taakkaa, huomioivat jäsenmaiden erilaiset koulutusjärjestelmät sekä työvoimapolitiittiset painotukset ja hyödyntävät mahdollisimman paljon olemassa olevia rakenteita.

NIS 2 -muutosdirektiivi

Valtioneuvosto kannattaa muutosehdotuksien tavoitteita sääntelyn yksinkertaistamiseksi, sujuvoittamiseksi ja sääntelystä aiheutuvien hallinnollisten kustannuksien alentamiseksi. Valtioneuvosto suhtautuu myönteisesti muutosehdotuksiin, jotka edistävät näitä tavoitteita ja turvaavat samalla kyberturvallisuuden korkeaa tasoa.

Valtioneuvosto pitää tarpeellisena, että osana neuvotteluita arvioidaan tarkemmin ehdotuksen vaikutuksia sääntelystä toimijoille aiheutuviin kustannuksiin ja ehdotuksen tavoitteisiin.

Valtioneuvosto suhtautuu myönteisesti direktiivin soveltamisalaa koskeviin muutosehdotuksiin sekä ehdotukseen keskeisen toimijan kokorajan korottamisesta. Valtioneuvosto pitää tarpeellisena soveltamisalan tarkentamista erityisesti tuotantomäärältään vähäisten sähköntuottajien sekä kemianteollisuuden osalta. Valtioneuvosto pitää tarpeellisena, että neuvotteluissa arvioidaan yksityiskohtaisemmin komission ehdotusta strategisen kaksikäyttöinfrastruktuurin omistajien ja operaattoreiden sisällyttämisestä direktiivin soveltamisalaa erityisesti maanpuolustuksen ja kansallisen turvallisuuden kannalta.

Valtioneuvosto pitää tärkeänä, että NIS 2 -direktiivin vaatimukset ovat oikeasuhtaisia ja riskiperusteisia. Valtioneuvosto suhtautuu alustavan varauksellisesti ehdotukseen komission toimivallasta täysharmonisoida riskienhallintatoimenpiteitä täytäntöönpanosäädöksillä. Valtioneuvosto pitää tarkoituksenmukaisena, että jäsenvaltioilla on riittävä kansallinen liikkumavara riskienhallintaa koskevien vaatimusten asettamisessa.

Valtioneuvosto pitää lähtökohtaisesti hyvänä, että eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisia sertifiointeja voitaisiin hyödyntää NIS 2 -direktiivin vaatimustenmukaisuuden osoittamisessa.

Valtioneuvosto suhtautuu myönteisesti ehdotukseen ENISA:n tehtävästä laatia rajat ylittäviä kyberturvallisuusriskien arviointeja. Valtioneuvosto pitää kuitenkin tärkeänä, että ENISA:n toimivaltaisuus valvovien viranomaisten tukemisessa ja sitä koskevien tietojen saamisessa perustuu jäsenvaltion viranomaisen suostumukseen.

Valtioneuvosto suhtautuu alustavan varauksellisesti ehdotukseen kiristyshaittaohjelmätietojen ilmoittamiseen liittyviin uusiin velvollisuuksiin sekä ehdotukseen komissiolle siirrettyyn säädösvallan laajennuksesta kiristyshaittaohjelmätietojen ilmoittamista koskien. Valtioneuvosto pitää tältä osin tarpeellisena, että neuvotteluissa arvioidaan tarkemmin, miten ehdotus vaikuttaa sääntelystä toimijoille aiheutuviin kustannuksiin ja hallinnolliseen taakkaan.

Valiokunnan lausunto HaVL 10/2026 vp

VALIOKUNNAN PERUSTELUT

Komission ehdotuksessa uudeksi kyberturvallisuusasetukseksi (CSA2) ehdotetaan Euroopan unionin kyberturvallisuusvirasto ENISA:n mandaattia uudistettavaksi huomioiden kyberturvallisuuden uhkaympäristön jatkuva muuttuminen. Ehdotuksen mukaan ENISA:n tehtävänä olisi tukea jäsenvaltioita ja EU-toimielimiä kyberturvallisuuteen liittyvän EU-lainsäädännön ja politiikkojen kehittämisessä ja toimeenpanossa, vahvistaa kyberturvallisuusvalmiuksia ja resilienssiä koko EU:ssa, edistää operatiivista yhteistyötä ja tiedonvaihtoa, osallistua EU:n kyberturvallisuussertifiointijärjestelmän kehittämiseen ja ylläpitoon sekä edistää kyberturvallisuusosaamista ja -koulutusta. Asetuksessa säädettäisiin myös EU:n laajuudesta kyberturvallisuussertifikaatista, jolla voitaisiin osoittaa, että sertifiointin kohde täyttää soveltuvassa sertifiointijärjestelmässä määritellyt tekniset kyberturvallisuusvaatimukset. Lisäksi NIS2-direktiivin toimijoille ehdotetaan velvoitteita ICT-toimitusketjujen ei-teknisten riskien hallitsemiseksi. Komission ehdottamalla NIS2-direktiivin muutoksella laajennetaan direktiivin soveltamisalaa merenalaisen tiedonsiirtoinfrastruktuurin tarjoajiin, energia- ja kemianteollisuuden toimijoihin sekä eurooppalaisten digitaalisten identiteetti- ja yrityslompakoiden tarjoajiin.

Hallintovaliokunta toteaa, että kyberturvallisuus on keskeinen osa kokonaisturvallisuutta, ja kyberturvallisuuden merkitys on korostunut entisestään nykyisessä turvallisuusympäristössä. Valiokunta kannattaa valtioneuvoston tavoin EU:n lainsäädännön tavoitetta vahvistaa kyberturvallisuuden hallinnointia sekä sitä, että asiaankuuluvilla toimielimillä, viranomaisilla ja muilla sidosryhmillä olisi paremmat edellytykset estää, havaita ja torjua kyberturvallisuusuhkia koordinoitulla ja tehokkaalla tavalla. Myös esimerkiksi Euroopan varautumisunionin strategiassa ja sisäisen turvallisuuden strategiassa (ProtectEU) kyberturvallisuus asetetaan EU:n resilienssin ytimeen. Valiokunta viittaa lisäksi juuri valmistuneeseen mietintöönsä sisäisen turvallisuuden selonteosta, jossa valiokunta käsittelee muun muassa teknologisen kehityksen vaikutuksia turvallisuuteen sekä suunnitelmallista uuden teknologian ja uudenlaisten toimintatapojen hyödyntämistä turvallisuuden parantamiseksi. Nykyisessä turvallisuusympäristössä hybridi- ja kyberuhkien suorituskykyjen kehittäminen yhteisesti eri viranomaisten kesken on välttämätöntä (HaVM 5/2026 vp — VNS 6/2025 vp, s. 22—23 ja 39).

Hallintovaliokunta kiinnittää huomiota siihen, että komission toteuttamassa vaikutustenarvioinnissa ei selvityksen mukaan ole juurikaan arvioitu lainsäädäntöpakettin vaikutuksia lainvalvontaviranomaisten toimintaan tai otettu huomioon komissiossa tehtävää työtä salauksen teknologiatiekartan osalta samalla kun esitykseen sisältyy kuitenkin kvanttialauksen kehittämiseen liittyviä ehdotuksia. Myöskään ehdotetun kyberturvallisuusasetuksen johdantokappaleista ei käy ilmi, että asetuksessa olisi huomioitu lainvalvontaviranomaisten digitaaliseen tietoon pääsyn tarpeet tai viimeaikaisen teknologisen kehityksen vaikutus viranomaisten pääsyssä tietoon. Valiokunta katsoo, että näihin seikkoihin tulee kiinnittää jatkoneuvotteluissa huomiota. Valiokunta pitää tärkeänä lainvalvontaviranomaisten näkökulman huomioimista myös esimerkiksi sertifiointia koskevien toimien yhteydessä.

Hallintovaliokunta pitää perusteltuna, että ENISA:n mandaattia tarkastellaan muuttunut uhkaympäristö ja unionin kyberturvallisuuslainsäädäntö huomioiden. Valiokunta katsoo, että

Valiokunnan lausunto HaVL 10/2026 vp

ENISA:n tehtävien ja toiminnan tulee tuottaa konkreettista lisäarvoa jäsenmaille ja EU:n muille toimielimille ja virastoille, ja toimintojen päällekkäisyyksiä tulee välttää. Valiokunta tähdentää, että ensisijainen vastuu kyberturvan tasoa varmistavissa ja yhteiskunnan toimijoita tukevissa viranomaistehtävissä on kuitenkin jäsenmailla ja sen viranomaisilla.

Hallintovaliokunta korostaa kansallisen turvallisuuden kuuluvan jäsenvaltioiden toimivaltaan. Tämä on selvästi todettu myös ehdotetun kyberturvallisuusasetuksen 2 artiklan 4 kohdassa, jossa yhtenevästi Euroopan unionista tehdyn sopimuksen (SEU) 4(2) artiklan kanssa on kirjattu, että kansallinen turvallisuus pysyy yksinomaan kunkin jäsenvaltion vastuulla. Valiokunta toteaa, että kansalliset tiedustelu- ja turvallisuuspalvelut toimivat kukin oman maansa kansallisen lainsäädännön perusteella suojatessaan kansallista turvallisuutta. Tiedustelutiedon hankkiminen on tarkasti säänneltyä ja turvallisuus- ja tiedustelupalveluihin tyypillisesti kohdistetaan ulkoista valvontaa, joka on myös tarkemmin kansallisesti lailla säädetty ja toteutettu.

Hallintovaliokunta toteaa, että tiedustelutietoa, jota kansallisen lain sallimia menetelmiä käyttämällä hankitaan ja joka on pääasiassa salaiseksi luokiteltua tietoa siihen liittyvine käyttörajoituksineen, voidaan luovuttaa vain lain sallimiin tarkoituksiin ja sellaisille tahoille, jotka ovat asianmukaisesti turvallisuusselvitettyjä ja joiden tilat ovat auditoituja ja sallivat turvallisuusluokitellun tiedon käsittelyn. Tämä huomioiden hallintovaliokunta suhtautuu varauksellisesti asetusehdotuksessa ENISA:lle esitettyyn mahdollisuuteen saada tiedustelutietoja.

Valiokunta toteaa, että EU:ssa keskitettynä tiedustelutiedon vastaanottajana ja analysoijana toimii jo nykyisin EU:n tiedusteluanalyysikeskus INTCEN, jonka henkilöstö koostuu pääosin tiedustelu- ja turvallisuuspalvelujen paikalle lähettämistä henkilöistä. Kyseessä on siten EU-virasto, jonka työntekijät ovat tiedustelun ammattilaisia. INTCEN on turvallisuus- ja tiedustelupalveluiden luotettu kumppani ja turvallisuus- ja tiedustelupalvelut luovuttavat säännönmukaisesti tietojaan sen käsiteltäväksi EU-tason päätöksentekijöille ja työryhmille jaettavien strategisten analyysien ja uhka-arvioiden laatimista varten. INTCEN:llä on toimintansa luonteen vuoksi myös turvalliset tilat ja tavat viestiä turvallisuus- ja tiedustelupalveluiden kanssa.

Valiokunnan saaman selvityksen perusteella vaikuttaakin siltä, että osa asetusehdotuksessa ENISA:lle ehdotetuista toimivaltuuksista on päällekkäisiä joko tiedustelu- ja turvallisuuspalveluiden tai INTCEN:n tehtävien kanssa (esim. 11 artikla). Valiokunta katsoo, että päällekkäisten rakenteiden luomisen sijasta olemassa olevia rakenteita tulisi pyrkiä hyödyntämään täysimääräisesti ja löytää synergiaetuja eri EU-tason toimijoiden keskinäisestä yhteistyöstä.

Varovaista suhtautumista ja tarkempaa analyysiä näyttäisivät vaativan myös esimerkiksi ehdotukset kyberuhkatiedustelun tietovaraston kehittamisestä ja kolmannen maan nimeämisestä kyberturvallisuushaasteita aiheuttavaksi maaksi. Jatkoneuvotteluissa tulisi myös varmistua sääntelyssä käytettävien käsitteiden yksiselitteisyydestä, esimerkkinä operatiivinen yhteistyö, jonka osalta olisi hyvä selvittää, mihin kansallisiin viranomaisiin ja minkälaiseen operatiiviseen yhteistyöhön sillä viitataan.

Valiokunnan lausunto HaVL 10/2026 vp

VALIOKUNNAN LAUSUNTO

Hallintovaliokunta ilmoittaa,

että se yhtyy asiassa valtioneuvoston kantaan korostaen edellä esitettyjä näkökohtia.

Helsingissä 24.4.2026

Asian ratkaisevaan käsittelyyn valiokunnassa ovat ottaneet osaa

puheenjohtaja Mauri Peltokangas ps
varapuheenjohtaja Pihla Keto-Huovinen kok
jäsen Alviina Alametsä vihr
jäsen Petri Honkonen kesk
jäsen Juha Hänninen kok
jäsen Christoffer Ingo r
jäsen Mari Kaunistola kok
jäsen Rami Lehtinen ps
jäsen Mira Nieminen ps
jäsen Saku Nikkanen sd
jäsen Hanna Räsänen kesk
jäsen Joakim Vigelius ps
jäsen Juha Viitala sd
jäsen Paula Werning sd
jäsen Ben Zyskowitz kok

Valiokunnan sihteerinä on toiminut

valiokuntaneuvos Minna-Liisa Rinne