

## OKM; E-kirje komission tiedonannosta kyberturvallisuusakatemiaista

### Kokous

**Komission tiedonanto** Kyberturvallisuuteen liittyvän osaamisvajeen pienentäminen EU:n kilpailukyvyyn, kasvun ja häiriönsietokyvyn parantamiseksi ("Kyberturvallisuusakatemia") COM(2023) 207 final

### Eduskuntatunnus

### Käsittelyvaihe ja jatkokäsittelyn aikataulu

Komission julkaisi 18.4.2023 tiedonannon Kyberturvallisuuteen liittyvän osaamisvajeen pienentäminen EU:n kilpailukyvyyn, kasvun ja häiriönsietokyvyn parantamiseksi ("Kyberturvallisuusakatemia") (COM(2023) 207 final) osana ns. kyberpakettia. Paketti sisälsi ehdotuksen kybersolidaarisuussäädökseksi, muutosehdotukset kyberturvallisuusasetukseen sekä tiedonannon Kybertaitoakatemiasta (Cyber Skills Academy). Valtioneuvosto on antanut U-kirjelmän kybersolidaarisuussäännöksestä ja kyberturvallisuusasetuksen muuttamisesta eduskunnalle 6.7.2023.

Tiedonanto on esitelty neuvoston horisontaalisessa Kyber-työryhmässä osana kyberturvallisuuspakettia. EU-puheenjohtajamaa Espanja tavoittelee neuvoston yleisnäkemyksen hyväksymistä lainsäädäntöehdotuksista vuoden 2023 loppuun mennessä. Puheenjohtaja ei ole ilmoittanut tiedonannon mahdollisesta jatkokäsittelystä tai aikataulusta.

### Suomen kanta

Hallitusohjelman mukaisesti Suomi tukee toimia EU:n kriisivarautumisen vahvistamiseksi. Suomi pitää tärkeänä, että kyberturvallisuusosaaminen ja -koulutus nostetaan osaksi unionin kriisivarautumista ja kokonaisturvallisuutta. Alan osaamispuulan ratkaisemiseksi esitetty koordinoitu lähestymistapa on kannatettava. Suomi katsoo, että eri toimijoiden, koulutustarjonnan ja rahoitusmahdollisuuksien yhteen tuominen yhteiselle di-

gitaaliselle alustalle voi lisätä läpinäkyvyyttä, saavutettavuutta ja uudenlaisia yhteistyömuotoja. On kuitenkin tarpeen huomioida, että kyberosaamisen osaajapulaan vastataan koko ajan jäsenmaiden koulutusjärjestelmien tutkimukseen perustuvalla koulutustarjonnalla. Suomi korostaa yhteistyötä olemassa olevien toimijoiden kanssa. Suomi katsoo, että digitaalisten palveluiden tulee olla yhteentoimivia ja hyödyntää mahdollisimman paljon jo olemassa olevia ratkaisuja.

Suomelle jää epäselväksi, mitä ehdotuksessa tarkoitetaan koulutuksen kehittämisellä EU-tasolla, ja painottaa jäsenmaiden koulutusjärjestelmien kehittämisen sekä jäsenmaiden strategisen yhteistyön merkitystä. Suomi pitää tärkeänä, että pidempien koulutusten rinnalla on käytettävissä dynaamisia välineitä vastaamaan nopeasti työmarkkinoiden osaa- mistarvemuutoksiin. Samalla Suomi muistuttaa, että jäsenvaltiot päättävät tutkintojen vii- tekehysten sisällöstä sekä osaamisen tunnustamisesta.

Suomi katsoo, että kyberturvallisuuden koulutuksessa tulee huomioida myös soveltavat kyberturvallisuuden osaajat sekä kiinnittää huomiota osaajien monimuotoisuuteen. Suomi korostaa tarvetta kyberturvallisuustaitojen opettamiseen kaikilla koulutustasoilla. Työelämän osaamistarpeiden lisäksi huomiota tulee kiinnittää kansalaisten valmiuksiin vastata esimerkiksi tietoturvaloukkauksiin, informaatiovaikuttamiseen, opettajien valmiuksiin kasvattaa oppilaita kriittiseen medialukutaitoon sekä yleiseen kyberriskitietoi- suuteen yhteiskunnallisen resilienssin lujittamiseksi. Suomi korostaa koulutuksen ja tut- kimuksen välistä yhteyttä tarvittavan osaamisen turvaamiseksi. Suomi katsoo, että kybe- rosaamisen rinnalla huomiota tulee kiinnittää myös informaatioturvallisuusosaamiseen. Suomi katsoo, että Euroopan unionin kyberturvallisuusviraston ENISA:n toiminnassa tu- lisi välttää päällekkäisyyksiä kansallisten viranomaisten toiminnan kanssa. Valtioneu- vosto pitää tärkeänä, että kyberturvallisuuden viranomaisille esitettyjä lisätehtäviä tarkas- teltaessa pyritään hillitsemään ehdotuksesta syntyvä hallinnollinen lisätaakka.

Suomi huomioi komission ehdotuksen kyberturvallisuuden osaamisakatemian perustami- sesta eurooppalaisen digitaali-infrastruktuurikonsortion (EDIC) muodossa ja seuraa sen kehitystä. Suomi pitää hyvänä uusien pysyvien rakenteiden sijaan sellaisia vapaaehtoi- suuteen perustuvia eurooppalaisen tason ratkaisuja, jotka kehittävät yhteistyötä ja hyö- dyntävät olemassa olevia verkostoja ja välineitä nykyistä paremmin.

## **Pääasiallinen sisältö**

Komission tiedonannon mukaan kyberturvallisuus ei ole vain osa eri tahojen turvalli- suutta, vaan myös tarpeellista EU:n poliittiselle tasapainolle, demokratialle sekä elinkei- noelämän kasvulle. Kyberturvallisuushat ovat viime vuosina kasvaneet yhteiskunnan eri sektoreilla.

Komissio näkee, että EU:n turvallisuutta ei voida taata ilman EU:n kriittistä infrastruk- tuuria turvaavia ja osaavia ammattilaisia. EU:n kyberturvallisuuspolitiikan merkittävä kehittyminen viime vuosina on johtanut useisiin aloitteisiin. Osaava työvoima on välttä- mätöntä sekä julkisella että yksityisellä sektorilla, kansallisella ja EU-tasolla, jotta kyber- turvallisuuden lailliset ja poliittikkavaatimukset voidaan toteuttaa.

Komission tiedonannon mukaan EU:ssa on kyberosaajien ja työmarkkinoiden tarpeen välillä on n. 350 000-650 000 osaajan kuilu. Erityisesti naisia osaajissa on vähän. Samoin

kybertaitoja puuttuu iäkkäämmistä ICT-osaajilta. Työmarkkinat etsivät valmiita osaajia ja epäröivät kouluttaa työntekijöitään, mikä edelleen haastaa työmarkkinoita. Komissio näkee, että työnantajilla, koulutuksen järjestäjillä ja poliitikoilla ei ole viestintätyökaluja keskinäiseen keskusteluun eikä täten mahdollisuuksia mitata ja arvioida kyberosaamisen puutetta työmarkkinoilla. Työvoiman kysyntäpuolella haasteena on sellaisten yhteisten foorumien puute, joissa työnantajat voisivat pohtia taitojen arviointia. Työnantajat kaipaavat yhä enemmän kyberturvallisuuden substanssiosaamisen lisäksi myös monialaisia taitoja kuten kriittisen ajattelun, ongelmanratkaisun ja itseohjautuvuuden taitoja.

Vastatakseen kyberturvallisuuden osaamishaasteeseen komissio ehdottaa kyberturvallisuuden osaamisakatemia perustamista. Osaamisakatemia toimisi yhtenä sisäänpääsynä kyberturvallisuusalan koulutustarjontaan, rahoitusmahdollisuuksiin ja erityistoimiin kyberturvallisuuden taitojen kehittämisessä. Osaamisakatemia tähtää kyberturvallisuuden ammattilaisten osaamisen kehittämiseen, ja sen toiminta täydentää komission kahta digitaalisen koulutuksen aloitetta, jotka on annettu samaan aikaan tämän tiedonannon kanssa. Osaamisakatemia toiminta nojaa neljään pilariin:

- (1) rakentaa yhteistä viitekehystä kyberturvallisuusroolien profiileille ja niihin liittyvälle osaamiselle, edistää Euroopan koulutustarjonnan vastaamista tarpeisiin, rakentaa urapolkuja ja tarjota läpinäkyvyyttä kyberturvallisuuden koulutuksiin ja sertifikaatteihin edistäen näin työvoiman tarjontaa;
- (2) varmistaa erilaisten koulutustoimien rahoituksen kanavoitinta ja näkyvyyttä;
- (3) kannustaa sidosryhmiä toimimaan; ja
- (4) määrittelee indikaattoreita työmarkkinoiden kehityksen valvomiseksi ja arvioida toimia.

Osaamisakatemia toimeenpanoa tuetaan Digitaalinen Eurooppa- ohjelmasta 10M€:lla. Komission ehdottaa tiedonannossaan, että osaamisakatemia hallinnollinen muoto olisi eurooppalainen digitaalinfrastruktuurikonsortio (EDIC). EDIC:ien perustamisesta on päätetty Digitaalisen vuosikymmenen politiikkaohjelmassa. Tämä instrumentti tukisi jäsenmaiden yhteistä työskentelyä, sekä yhteistyötä komission, Euroopan unionin kyberturvallisuusviraston (ENISA) ja Eurooppalaisen kyberturvallisuuden osaamiskeskuksen (ECCC) kanssa kansallisten kyberturvallisuuden koordinoitikeskusten tuella. Jäsenmaita kannustetaan vapaaehtoisesti ilmoittamaan 30.5.2023 mennessä kiinnostuksensa mahdollisen EDIC-hakemuksen jättämisestä komissiolle alustavia kommentteja varten. Komissio antaa päätöksen EDIC:n perustamisesta Digitaalisen vuosikymmenen ohjelma-komitean hyväksynnän jälkeen.

#### *Viitekehys*

ENISA on jo tehnyt työtä kyberosaamisen ammattilaisten profiilien määrittelemiseksi Eurooppalaisen kyberosaamisen viitekehysten alla. Tätä viitekehystä tulisi komission mukaan käyttää Kyberturvallisuuden osaamisakatemia pohjana.

Viitekehykseen liitettävät työprofiilit tulevat myös osaksi ESCO ammattiluokitusjärjestelmää.

#### *Yhteistyö koulutuksen kehittämiseksi*

Kyberturvallisuuden osaamisakatemia EDICin käynnistettyä toimintansa sen tulisi saada jäsenmailta tukea tullakseen kyberturvallisuuskoulutuksen suunnittelun ja tarjonnan eurooppalaiseksi vertailupaikaksi käsitellen taitoja, joista on eniten kysyntää. Sen olisi tar-

jottava aloittaville yrityksille, pk-yrityksille sekä sekä julkishallinnolle työpaikkakoulutus- ja harjoittelumahdollisuuksia kyberturvallisuusalan innovatiivisissa yrityksissä ja kyberturvallisuuden osaamiskeskuksissa.

Osaamisakatemia houkuttelee nuoria sukupolvia kyberturvallisuusurille. Jäsenmaiden tulisi – kuten komission esityksessä digitaalisten taitojen kehittämiseksi koulutuksessa – mahdollistaa alaan erikoistuneiden opettajien rekrytointi ja heidän kyberosaamisensa kehittäminen.

Komissio jatkaa yhteisten EU-tason koulutusohjelmien ja tutkinto-ohjelmien sekä pienten osaamiskokonaisuuksien kehittämisen tukemista Erasmus+ rahoituksella myös kyberturvallisuuden alalle. Myös Eurooppalaiset yliopistot –verkostoa ja ammatillisen huippuosaamisen keskusta tuetaan lisähauilla. Lisäksi Digitaalinen Eurooppa- ohjelman rahoitus sekä muut EU-rahoitusohjelmat tukevat yhteistyön päämääriä esimerkiksi henkilökoh- taisten oppimistilien kautta.

Kansallisia kyberturvallisuuden koordinaatiokeskuksia kannustetaan perustamaan Kyber Kampuksia jäsenmaissa kyberturvallisuuden osaamiskeskittymiksi.

#### *Synergia ja kyberturvallisuuskoulutuksen läpinäkyvyys*

Komission tiedonannon mukaan kyberturvallisuuden osaamisakatemia toimii yhtenä luokkuna niille jotka ovat kiinnostuneita kyberturvallisuusurasta. Lyhyellä aikavälillä tämä tapahtuu tiedonannon mukaan komission Digitaaliset taidot ja työpaikat – alustalla ja mukaan liitettäisiin muun muassa ENISAn tarjontaa. Lisäksi ENISA kehittää ja vakiinuttaa tiedonannon mukaan kaksi tietovarantoa olemassa olevista julkisen ja yksityisen sektorin koulutuksista sekä kyberturvallisuussertifioinneista yhdessä muun muassa serti- fikaatteja myöntävien tahojen kanssa. Tiedonannon mukaan tämä työ hyödyttää myös kansallisia kyberturvallisuuden koordinoitikeskuksia, joiden tehtävänä on edistää ja le- vittää kyberturvallisuuden koulutusohjelmia. Ammattilaisten koulutuksen laadun takaa- miseksi ENISA kehittää pilotin tutkimaan mahdollisuuksia Eurooppalaisen kyberturvalli- suuden todistusjärjestelmän luomiseksi.

Komissio pitää tiedonannon mukaan tärkeänä, että kyberturvallisuuden palveluita tarjoaa osaava ja kokenut henkilöstö. Tämän vuoksi komissio esittää lisäystä Kyberturvallisuus- asetukseen, jolla mahdollistetaan sertifiointijärjestelmät hallittuihin turvallisuuspalvelui- hin EU:n tasolla.

Jäsenmaita kannustetaan sisällyttämään kyberturvallisuuden pieniä osaamiskokonaisuuksia kansallisiin tutkintojen viitekehyksiin sekä varmistamaan tuki kyberturvallisuuden oppimiseen tarkoitettujen pienten osaamiskokonaisuuksien kehittämiseksi ja tunnustami- selle neuvoston eurooppalaisesta lähestymistavasta pieniin osaamiskokonaisuuksiin anta- man suosituksen mukaisesti. Myös Eurooppalaiset digitaaliset osaamistodistukset ovat mahdollisia, ja ne voidaan tulevaisuudessa lisätä eID digitaaliseen lompakkoon.

#### *Sidosryhmien sitouttaminen*

Komissio pyytää sidosryhmiä osallistumaan sitoumuksiin kyberturvallisuuden osaamisen lisäämiseksi. Nämä lupaukset tulisi raportoida Digitaalisten taitojen ja työpaikkojen alus- talla. Sitoumusten tekijöitä kannustetaan liittymään myös Digitaalisiin laajoihin kumppa- nuuksiin Osaamissopimuksen (*Pact for Skills*) alla. Jäsenmaita kannustetaan edistämään *Women in Digital* -julkilausumaa ja käyttämään ESR+-rahoitusta työelämän sukupuoli- kuilujen kaventamiseen esimerkiksi tyttöjen ja naisten mentorointiohjelmilla. Jäsenmai-

den olisi osana kansallisia kyberturvallisuusstrategioitaan toteutettava erityisiä toimenpiteitä kyberturvallisuuden osaamisvajeen lieventämiseksi, jotta voidaan varmistaa kyberturvallisuusdirektiivin NIS2 asianmukainen täytäntöönpano. Jotkut jäsenmaat hyödyntävät synergioita siviili-, puolustus- ja lainvalvonta- aloitteita.

#### *Rahoitus*

Kyberturvallisuuden osaamisakatemia selvittää muiden mukana olevien EU-tason toimijoiden kanssa miten EU-rahoitusta käytetään kyberturvallisuustaitojen kehittämiseen ja osaajapulan vähentämiseen. Eurooppalainen kyberturvallisuuden osaamiskeskus tulee rahoittamaan toimia osaajapulaan liittyen. Digitaalisten taitojen ja työpaikkojen alusta tulee toimimaan kyberturvallisuuden rahoituksen yhtenä luukkuna. Rahoitusta on muun muassa Osaamissopimuksen, Digitaalisen koulutuksen toimintaohjelman ja Digitaalinen Eurooppa- ohjelman sekä Euroopan puolustusrahaston kautta. Synergioita tulee hyödyntää myös Erasmus+, ESR+, EAKR, RRF ja InvestEU- rahastojen osalta.

#### *Mittaaminen*

Kyberturvallisuuden osaamisakatemia kehittää metodologian, jonka avulla voidaan arvioida kyberturvallisuuden osaamisen kehittymistä. Uusia indikaattoreita kehitetään yhdemmäksi DESI:n (Digitaalinen talous ja yhteiskunta indeksi) kanssa. ENISA kerää tietoja kansallisten kyberturvallisuuden koordinaatiokeskusten kanssa. ENISA tuottaa vuosittaisen raportin, jota hyödynnetään DESIn kanssa eurooppalaisen ohjausjakson kansallisissa suosituksissa sekä ENISAN kahden vuoden välein tehtävässä raportoinnissa kyberturvallisuuden direktiivin täytäntöönpanosta. ENISA ehdottaa komissiolle avainindikaattoreita.

### **EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely**

Komission tiedonannolla ei ole oikeusvaikutuksia.

### **Käsittely Euroopan parlamentissa**

-

### **Kansallinen valmistelu**

Jaosto EU19 (viestintä)  
Jaosto EU29 (työllisyys)  
Jaosto EU30 (koulutus)

### **Eduskuntakäsittely**

Komission tiedonantoa COM(2023) 207 final ei ole käsitelty eduskunnassa.

### **Kansallinen lainsäädäntö, ml. Ahvenanmaan asema**

Komission tiedonannolla ei ole vaikutusta kansalliseen lainsäädäntöön.

### **Taloudelliset vaikutukset**

Komission tiedonannolla ei ole välittömiä taloudellisia vaikutuksia.

### **Muut asian käsittelyyn vaikuttavat tekijät**

Suomi on ilmaissut komissiolle ottavansa kantaa osallistumisesta EDIC-hakuun hallitusohjelman valmistuttua.

### **Asiakirjat**

COM(2023) 207 final

### **Laatijan ja muiden käsittelijöiden yhteystiedot**

Päivi Bosquet, OKM, [paivi.bosquet@gov.fi](mailto:paivi.bosquet@gov.fi), p. 0295 330 375  
Sarita Friman, VNEUS [sarita.friman@gov.fi](mailto:sarita.friman@gov.fi), p. 0295 160144

### **VAHVA-tunnus**

EU/687/2023

**Liitteet** Napsauta tähän ja kirjoita liitteet

**Viite** Napsauta tähän ja kirjoita viite