KYBERTURVALLISUUDEN AMMATTILAISTEN KOULUTUS

// Martti Lehto

Kyberturvallisuusalalla osaajapula on valtava. Tutkimustulokset osoittavat selvästi, että nykyinen kyberammattilaisten määrä ei riitä kattamaan kaikkia kyberturvallisuuden rekrytointitarpeita. Kyberturvallisuuskoulutukseen tarvitaan korkeakoulujen välistä yhteistyötä, kolmannen sektorin tukea ja julkisen tahon panostuksia.

JOHDANTO

Suomi on maailman johtava digitalisaation hyödyntäjä korkeakoulutuksessa ja siihen perustuvassa jatkuvassa oppimisessa. Tavoitteena on, että opetussisällöt avataan mahdollisimman laajasti käyttöön. Osaamisen uudistamisen kasvavien tarpeiden vuoksi tulisi jatkuvan oppimisen painottua yhä enemmän korkeakoulujen koulutustehtävässä.

Maailmanlaajuisesti on tunnistettu pula osaavista kyberturvallisuusasiantuntijoista. Osaajapulan kannalta on otettava huomioon erilaiset osaamistarpeet eri tehtävissä. Kyberturvallisuuden tietojen, taitojen ja kykyjen osalta osaamiskenttä on melko laaja ja osaajan pitää erikoistua johonkin tiettyyn kokonaisuuteen. Tämä on otettava huomioon koulutuksessa, eli mihin tehtävään valmistuvan osaajan oletetaan työllistyvän. Toki on selvää, että koulutuksen kautta saavutetaan tietty perusosaaminen ja myöhemmin työtehtävien, erikoistumisen ja mahdollisten erikoiskoulutusten kautta saavutetaan syvempi erikoisasiantuntijuus kyseiseen aihealueeseen.

KYBERTURVALLISUUSKOULUTUS AMMATTIKORKEAKOULUISSA

Ammattikorkeakouluissa annettava kyberturvallisuusopetus (AMK- ja YAMK-korkeakoulututkinto, sekä erikoistumis- täydennys- ja muuntokoulutus) on sisällöllisesti kattavaa ja kykenee modulaarisen rakenteen perusteella muuntautumaan teollisuuden tarpeisiin. Tieto- ja viestintätekniikan sekä tietojenkäsittelyn tutkinto-ohjelmien sisällä tarjotaan kyberturvallisuuden koulutusta.

Opetussuunnitelmarakenteet ovat eri luokkia sen suhteen, onko kyberturvallisuus sijoitettu pakollisiin, erikoistumis- (tai ammatillisiin opintoihin) vai vapaasti valittaviin opintoihin. Tärkeimpiä ovat kyberturvallisuuteen tähtäävät koulutusohjelmat ja koulutusohjelmat, joiden sisällä tarjotaan kyberturvallisuuden erikoistumisopintoja. Tämän luokituksen perusteella YAMK-tason neljä koulutusohjelmaa löytyy kolmessa ammattikorkeakoulussa:

- JAMK, Master's Degree in Information Technology, Cyber Security, Insinööri
- TurkuAMK, Ohjelmistotekniikka ja ICT
- Insinööri
- Tradenomi
- XAMK, Kyberturvallisuus, Insinööri

AMK-ohjelmat koostuivat monimutkaisista opetussuunnitelmarakenteista. Joissakin ammattikorkeakouluissa opetussuunnitelmat on laadittu siten, että opiskelijoille on tarjolla paljon kursseja valittavaksi. Vaihtoehtoisesti erikoistuminen on rakennettu yhdeksi opetussuunnitelmaksi, josta opiskelijat voivat tehdä modulaarisia valintoja. Neljä ammattikorkeakoulua tarjoaa AMK-tason kyberturvallisuuden koulutusohjelman:

- JAMK, tieto- ja viestintätekniikka, insinööri
- Laurea, tietojenkäsittely, kyberturvallisuus, tradenomi
- TurkuAMK
- Tieto- ja viestintätekniikka, insinööri
- Tietojenkäsittely, tradenomi
- XAMK, kyberturvallisuus, insinööri

Tällä hetkellä ammattikorkeakoulujen kyberturvallisuuteen painottuvassa koulutuksessa sisäänotto on noin 555 (165 tutkinto-opiskelijaa ja 390 sivuaineopiskelijaa). Lisää kyberturvallisuuden asiantuntijoita tarvitaan vastaamaan jatkuvasti laajenevan digitalisaation vaatimuksiin. Tämän seurauksena kyberturvallisuusosaamista tarvitaan yhä enemmän eri digitalisoituvilla toimialoilla.
Koulutuksen resursseja pohdittaessa tulee myös muistaa, että ammattikorkeakoulut tarjoavat pääsääntöisesti teknistä kyberturvallisuuskoulutusta, joka tähtää tekniseen osaamiseen. Tällainen insinööriopetus vaatii laajoja ja monimutkaisia oppimisympäristöjä, joiden hankkiminen ja ylläpito on kallista. Riittävän teknisen osaamisen takaamiseksi resurssien allokoinnissa tulee huomioida tarvittavien oppimis- ja koulutusympäristöjen hankinta-, kehitys- ja ylläpitokustannukset.

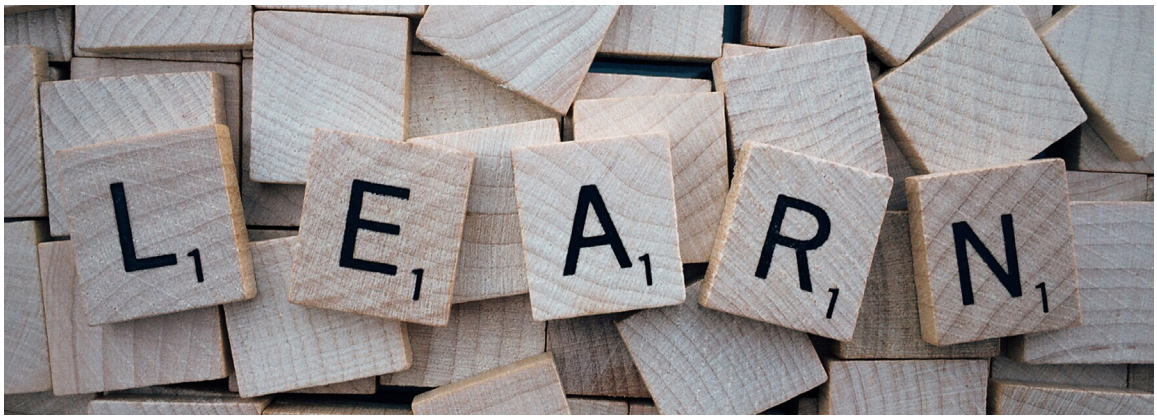
KYBERTURVALLISUUSKOULUTUS YLIOPISTOISSA

Kyberturvallisuuteen keskittyneiden koulutusohjelmien määrä on pieni ja opetus on keskittynyt maisteritasolle. Yliopistot tuottavat suhteellisen vähän kyberturvallisuuden asiantuntijoita suhteessa havaittuun osaamispulaan. Suuri osa koulutusohjelmista on integroinut kyberturvallisuuden tutkintorakenteeseen valinnaisina tai pakollisina opintoina 1-15 opintopisteen suuruisina Yliopistot tarjoavat vähän täydennyskoulutusta kyberalalla. Seuraavassa taulukossa on esitetty kyberturvallisuuskoulutuksen (pää- ja sivuaine) sisältävät koulutusohjelmat:

Yliopisto	Koulutusohjelmat/Kurssimoduulit	Sisäänotto 2022
Aalto yliopisto	Security and Cloud Computing (Security)	11
Aalto yliopisto	Security and Cloud Computing (SECCLO)	76
Helsingin yliopisto	Tietojenkäsittelytieteen maisteriohjelma	45
Tampereen yliopisto	Suuntaus: Advanced Studies in Information Security	1-30
Tampereen yliopisto	Master's Programme in Security and Safety Management: Safety Management and Engineering	8
Tampereen yliopisto	Master's Programme in Security and Safety Management: Security Governance	8
Jyväskylän yliopisto	Kyberturvallisuuden maisteriohjelma	45
Jyväskylän yliopisto	Turvallisuuden ja Strategisen analyysin maisteriohjelma	25
Turun yliopisto	Cyber Security -pääaine + EIT Digital Master School kaksoistutkinto-ohjelma	35
Turun yliopisto	Cryptography -pääaine	5
Turun yliopisto	Tietoliikenne- ja kybertuvallisuusteknologia -pääaine	6-8
Oulun yliopisto	Tietotekniikka TkK + DI	100
Åbo Akademi	Temaattinen moduuli: Safety-Critical and Autonomous Systems	n/a
Itä-Suomen yliopisto	Tietojenkäsittelytiede LuK + FM	68
Vaasan yliopisto	Automaatio ja tietotekniikka TkK + DI	52
LUT yliopisto	Tietotekniikka TkK + DI	82

Listauksesta nähdään, että kyberturvallisuuteen keskittyviä tutkinto-ohjelmia on suhteellisen vähän. Yliopistojen tarjoamat kyberturvallisuuden tutkinto-ohjelmat tai läheisesti alaan liittyvät tutkinto-ohjelmat eroavat sisällöllisesti toisistaan. Yliopistoilla on toisin sanoen omat erikoistumisalansa kyberturvallisuudesta. Lisäksi huomionarvoista on se, että opetus on keskittynyt ylempiin korkeakoulututkintoihin. Yksittäisiä kyberturvallisuuden opintoja on yleisesti tarjolla lukuisissa tutkinto-ohjelmissa pakollisina- tai valinnaisina opintoina.

Kyberturvallisuuden ja turvallisuuden koulutusohjelmien arvioitu kokonaissisäänotto on noin 250 (110 pääaineena, 140 sivuaineena) vuonna 2023. Yllä mainittu luku sisältää vain kyberturvallisuuden ja turvallisuuden koulutusohjelmien aloitushaun, eikä siten sisällä niihin liittyvien alojen tutkintoja, esim. tietojärjestelmätiede. Yliopistojen tuottamien asiantuntijoiden määrä on kaiken kaikkiaan suhteellisen pieni, kun otetaan huomioon havaittu osaamispula.



MUIDEN KOULUTUSTARJOAJIEN KYBERTURVALLISUUSKOULUTUS

Ei-tutkintoon tähtäävää kyberturvallisuuskoulutusta on Suomessa saatavilla, mutta tällä hetkellä vallitsee eräänlainen kohtaanto-ongelma. Ne, jotka koulutusta eniten tarvitsisivat, eivät löydä sitä, eivätkä hakeudu siihen. Esimerkiksi senioreille suunnattua koulutusta on vähän tarjolla.

Kolmannella sektorilla laajinta kyberturvallisuuteen liittyvää koulutusta järjestää Maanpuolustuskoulutusyhdistys (MPK). Lisäksi jotkin aikuiskoulutuskeskukset tarjoavat kyberturvallisuuteen liittyvää koulutusta.

Lapset ja nuoret saavat tällä hetkellä kyberturvallisuuskoulutusta osana koulutuspolkuaan sekä perus- ja toisen asteen koulutuksessa että myöhemmissä opinnoissa. Kuitenkin ne, jotka ovat suorittaneet opintonsa aikana, jolloin kyberturvallisuus ei kuulunut peruskoulutukseen tai jatko-opintoja, voivat tällä hetkellä jäädä kokonaan kyberturvallisuuskoulutuksen ulkopuolelle, jos he eivät saa sitä työpaikallaan.

Yrityksille ja muille organisaatioille kouluttajia on Suomessa melko paljon. Suuryritysten ja julkisten organisaatioiden työntekijät saavat yleensä työnsä yhteydessä koulutusta, mutta pk-yritysten työntekijät, itsensä työllistäjät ja yrittäjät voivat jäädä sitä ilman. Toinen ongelma voi olla se, että pk-yritysten johto tai yrittäjät eivät tunnista koulutuksen tarvetta.

KYBERTURVALLISUUDEN ASIANTUNTIJOIDEN MÄÄRÄLLINEN TARVE

Elinkeinoelämä, viranomaiset ja kolmas sektori tarvitsevat uusia kyberammattilaisia. Liikenne- ja viestintäministeriön kyberosaamistarpeita kartoittavassa kyselyssä 73 % vastaajista näkee organisaatioissaan merkittävää osaajapulaa. Lähes kaikki vastaajat ottaisivat uusia ammattilaisia, jos heitä vain saisi. Kyselyn perusteella tarpeet vaihtelevat voimakkaasti. Osaamistarve-esiselvityksessä pienelle ryhmälle (16 %) vastaajista osaamisvaje vaaransi toiminnan turvallisuuden tai kannattavuuden. Kyse ei ole enää kasvun heikkenemisestä vaan peräti elinkelpoisuudesta.

Kysyntä on kova myös kyberturvallisuusalan sisällä. Kyberalan (FISC) kyselyn mukaan alan yrityksistä 87 % aikoi palkata kyberturvallisuusalan henkilökuntaa. Kyberalan jäsenkyselyn perusteella noin 35 % vastaajista ilmoitti osaavan työvoiman puutteen olevan merkittävin alan kasvua rajoittava tekijä.

Ammattitaitopula on todellisuutta, vaikka sen tasoa on vaikea ennustaa tarkasti. Nykyisten tietojen perusteella arvioidaan, että Suomi tarvitsee lähivuosina 5 000–8 000 kyberturvallisuuden ammattilaista. Lisäksi 1 000–5 000 uutta ammattilaista tarvitaan työskentelemään kyberturvallisuuden parissa muun työnsä ohella. Kaikki nämä ihmiset tarvitsevat koulutusta.

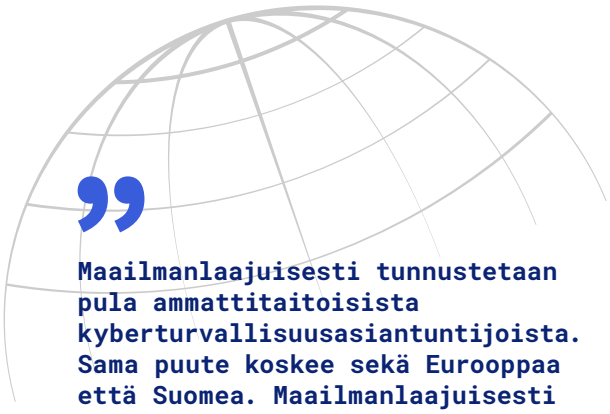
Yrityksillä on monenlaisia osaamistarpeita. Osaamisprofiili voidaan määritellä yleisesti käytetyn NCWF-luokituksen perusteella. Tätä yhdysvaltalaista viitekehystä on käytetty laajasti kuvaamaan kyberturvallisuuteen liittyviä osaamisen pääluokkia ja osaamiskategorioita sekä näiden alla olevia erityisosaamisaloja. Tutkimuksen mukaan yritysten määrälliset tarpeet vaihtelevat eri osaamisalueilla. Turvalliseen tuotantoon tarvitaan eniten uusia osaajia. Tämä 6 000–13 000 uuden kyberammattilaisen tarve jakautuu pääkoulutusalan mukaan seuraavasti:

1. Turvallinen tuotanto 900–1 500 uutta henkilöä,
2. Operointi ja ylläpito 700–1 100 henkilöä,
3. Kokonaisuuden valvonta ja johtaminen 800–1 300 henkilöä,
4. Suojaaminen ja puolustus 900–1 400 henkilöä,
5. Analysointi 600–1 000 henkilöä,
6. Tiedonkeruu ja operointi 500–800 henkilöä,
7. Tutkinta 500–800 henkilöä.

Tutkimus osoittaa, että erityisiä tarpeita oli (a) valvonnassa ja hallinnassa (erityisaloilla, kuten järjestelmäarkkitehtuuri, kyberturvallisuuden hallinta, strategiat ja strategioiden parissa työskentelevät kyber- tai tietoturvapäälliköt) sekä (b) operatiivisessa osaamisessa, jossa painottuu järjestelmien suojaus sekä sitä tukeva analyysi. Julkinen sektori hakee suhteellisesti enemmän laaja-alaisen osaamisen johtajia ja riskinhallintaosaajia, kun taas elinkeinoelämä hakee enemmän hallinto- ja arkkitehtuuriosaajia.

Osaamistarve on jakautunut melko tasaisesti kaikille kyberturvallisuuden osaamisalueille. Tämä tarkoittaa kokonaisvaltaisen koulutuksen tarvetta. Korkeakoulujen tutkinto-opintojen sekä muunto- ja täydennyskoulutuksen tulee kattaa kaikki nämä osa-alueet vastatakseen osaamistarpeisiin.

Elinkeinoelämä, viranomaiset ja kolmas sektori tarvitsevat uusia kyberammattilaisia. Liikenne- ja viestintäministeriön kyberosaamistarpeita kartoittavassa kyselyssä 73 % vastaajista näkee organisaatioissaan merkittävää osaajapulaa. Lähes kaikki vastaajat ottaisivat uusia ammattilaisia, jos heitä vain saisi.



Maailmanlaajuisesti tunnustetaan pula ammattitaitoisista kyberturvallisuusasiantuntijoista. Sama puute koskee sekä Eurooppaa että Suomea. Maailmanlaajuisesti ammattitaitoisen työvoiman tarve on miljoonia; Suomen osalta voidaan sanoa, että se on useita tuhansia.

JOHTOPÄÄTÖKSIÄ

Kyberturvallisuudessa yksi tärkeimmistä ja arvokkaimmista asioista on ammattitaitoinen henkilöstö. Riippumatta teknisistä ratkaisuista ja prosesseista organisaatiossa, sillä ei ole kybersietokykyä ilman ammattitaitoista henkilöstöä. Tämä koskee kaikkia työtehtäviä, koska henkilöstön epäpätevyys tai tiedon puute voi altistaa organisaation haavoittuvuuksille kybertoimintaympäristössä.

Maailmanlaajuisesti tunnustetaan pula ammattitaitoisista kyberturvallisuusasiantuntijoista. Sama puute koskee sekä Eurooppaa että Suomea. Maailmanlaajuisesti ammattitaitoisen työvoiman tarve on miljoonia; Suomen osalta voidaan sanoa, että se on useita tuhansia.

Tähän osaamispulaan liittyen on tärkeää ottaa huomioon eri työtehtävissä tarvittavat erilaiset taidot. Kyberhyökkäysten tunnistaminen ja tapausten hallinta edellyttää erilaista kyberturvaosaamista kuten kyberturvallisuuden hallinta tai uusien järjestelmien hankinta. Tämä on otettava huomioon koulutuksessa, eli mihin työtehtäviin valmistuvien opiskelijoiden odotetaan työllistyvän. Tietenkin tulee muistaa, että koulutus antaa tiettyjä perusosaamisen, jota voidaan myöhemmin kehittää syvemmäksi osaamiseksi työtehtävien, erikoistumisen ja mahdollisen alan erikoiskoulutuksen kautta.

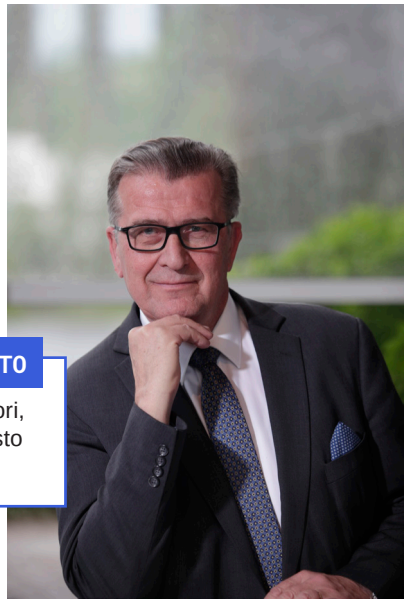
Kyberturvallisuuskoulutus tulee myös kohdistaa työelämän eri osa-alueille. Näin tarvittavat taidot olisivat yleisesti yhteiskunnan saatavilla. Myös tutkintoja päivittävä täydennyskoulutus vaatii opetusresursseja. Koulutuksen tulee tuottaa tarpeeksi asiantuntijoita, jotta yhteiskunta on valmis vastaamaan nykymaailman haasteisiin.

Kyberturvallisuuden asiantuntijoiden määrää yhteiskunnassa voidaan lisätä useisiin tekijöihin vaikuttamalla. Yksi tapa on lisätä alan koulutusohjelmien määrää ja aloittamista. Tämä edellyttää henkilöresurssien lisäämistä. Lisäksi kyberturvallisuuden asiantuntijoiden määrää voidaan lisätä kehittämällä täydennyskoulutusta. Lisäksi korkeakouluorganisaatioiden välisen koulutusyhteistyön parantaminen mahdollistaisi opiskelijoille entistä monipuolisempia erikoistumisaloja kyberturvallisuuden eri osa-alueilla.

Kyberturvallisuuskoulutuksen sisäänottovahvuuksien nostaminen edellyttää resursseja sekä koulutukseen että tutkimukseen. Haasteena on nopealla aikataululla saada rekrytoitua tutkijoita ja opettajia korkeakouluihin.

Muissa EU-maissa on luotu toimivia yhteistyöverkostoja yritysten, kyberturvallisuuskoulutusta koordinoivien valtiollisten tahojen sekä kolmannen sektorin toimijoiden kanssa. Suomi hyötyisi myös kansalaisten kouluttamisesta ja koulutusyhteistyötä koordinoivan toimielimen johdolla toimivasta kansalaisten kyberturvataitojen kehittämisen yhteistyöverkostosta. Yhteistyöverkostoa voisi hyödyntää kyberkoulutukset kokoavan verkkosivuston suunnittelussa ja kansalaisen kyberturvallisuuskonseptin jatkokehityksessä.

Askel oikeaan suuntaan on otettu, kun opetus- ja kulttuuriministeriö on rahoittanut vuonna 2022 alkanutta kyberturvallisuuskoulutuksen kehittämisen ja saatavuuden lisäämisen ohjelmaa. Kyseessä on Jyväskylän yliopiston ja Jyväskylän ammattikorkeakoulun koordinoima laaja yhteistyöhanke. Hanke kokoaa verkoston kehittämään, koordinoimaan ja tarjoamaan kyberturvallisuuden korkeakoulutusta. Siihen osallistuu yhdeksän yliopistoa ja 11 ammattikorkeakoulua sekä verkostoyliopisto FiTECH. ■



MARTTI LEHTO

Työelämäprofessori,
Jyväskylän yliopisto

Artikkeli perustuu Valtion kyberturvallisuusjohtaja Rauli Paanaselle vuonna 2022 tehtyyn raporttiin: Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimushanke, JYU tutkimuspaperi 93/2022