Informaatioteknologian tiedekunnan julkaisuja
No. 93/2022

Lehto, Martti (toim.)

Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimus – hankkeen loppuraportti

JYVÄSKYLÄN YLIOPISTO

Informaatioteknologian tiedekunnan julkaisuja
No. 93/2022

Editor: Martti Lehto
Covers: Teemu Rahikka

ISBN 978-951-39-9336-8 (verkkoj.)
ISSN 2323-5004

Jyväskylä 2022

Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimus – hankkeen loppuraportti

Martti Lehto (toim.)

2022

SISÄLLYS

Johdanto

Kyberturvallisuuteen tähtäävän tutkimuksen, kehittämisen ja koulutuksen toteuttaminen eri tasoilla vahvistaa kansallista osaamista ja Suomea tietoyhteiskuntana. EU-tasolla ja kansallisesti on julkaistu useita strategioita, joiden tavoitteena on parantaa kyberturvallisuuden osaamista sekä luoda edellytyksiä alan tutkimukselle, koulutukselle ja innovaatiotoiminnalle.

Tällä tutkimushankkeella edistettiin ja siinä otettiin huomioon niitä tavoitteita, joita on esitetty EU:n kyberturvallisuusstrategiassa 2020, EU:n digitaalista kehitystä edistävissä ohjelmissa, Suomen kyberturvallisuusstrategiassa (2019) ja sen kehittämisohjelmassa (2021) sekä EU:n ja Suomen osaamisen kehittämisen ohjelmissa.

Tällä Liikenne- ja viestintäministeriön Jyväskylän yliopistolta tilaamalla kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimuksella selvitettiin laaja-alaisesti kyberturvallisuuteen liittyvän osaamisen määrällinen ja laadullinen kehittäminen.

Hankkeen päätutkimuskysymykseksi määriteltiin, ”Millaisia toimenpiteitä tarvitaan Suomen kyberturvallisuusosaamisen määrällisen ja laadullisen tilanteen parantamiseksi?” Tutkimuksessa laadittiin selkeä tilannekuva kyberturvallisuuden opetuksesta eri koulutusasteilla sekä tarvittavat toimenpiteet määrällisen ja laadullisen kyberturvallisuusosaamistarpeen tyydyttämiseksi opetusohjelmissa.

Hankkeen toteuttaneet organisaatiot olivat Jyväskylän yliopisto, Jyväskylän ammattikorkeakoulu, Turun ammattikorkeakoulu ja Linkitin Oy. Toteutettavia työpaketteja oli seitsemän ja tehty tutkimustyö jakaantui osallistuneiden organisaatioiden osalta seuraavasti:

Organisaatio	**Tehtävät**	**Osallistujat**
Jyväskylän yliopisto	Kyberopetuskartoitus yliopistoissa Kyberopetuskartoitus lukioissa Kyberopetuskartoitus perusopetuksessa Muiden toimijoiden antaman kyberkoulutuksen kartoitus	Martti Lehto Jussi Simola Annika Nykänen Jussi Aaltonen Marianne Lindroth Matias Holmström
Jyväskylän ammattikorkeakoulu	Kyberopetuskartoitus ammattikorkeakouluissa	Karo Saharinen Tuomo Sipola Tero Kokkonen
Turun ammattikorkeakoulu	Kyberopetuskartoitus ammatillisessa koulutuksessa	Mika Koivunen Poppy Skarli Jani Ekqvist Jarkko Paavola
Linkitin Oy	Kyberosaamisen määrällisen tarpeen kartoitus	Antti Sillanpää

Yhteenveto

Kyberturvallisuusalalla osaajapula on valtava. Tässä tutkimuksessa on kartoitettu, kuinka tähän ongelmaan vastataan. Kysely- ja haastattelututkimuksen sekä asiakirjojen sisällönanalyysin avulla on käyty läpi perusopetuksessa, lukioissa, ammattikouluissa, ammattikorkeakouluissa ja yliopistoissa sekä kolmannen sektorin piirissä annettavaa kyberturvallisuuden/tietoturvallisuuden/digiturvallisuuden opetusta. Selkeä tulos on, etteivät nykyresurssit riitä kattamaan kaikkia rekrytointitarpeita, vaan siihen tarvitaan merkittäviä julkisia panostuksia suuruusluokaltaan 8–9 miljoonaan euroa vuodessa.

Tutkimuksen yhteydessä esiin on tullut käsitteistön ja termistön kirjavuus. Käsitteitä kyberturvallisuus, digitaalinen turvallisuus ja tietoturvallisuus käytetään usein rinnakkaisina käsitteinä. Niille ei ole kansallisesti tai kansainvälisesti yhteisesti hyväksyttyä määrittelyä. Valtiovarainministeriön raportissa ”Julkisen hallinnon digitaalinen turvallisuus” (Valtiovarainministeriön julkaisuja 2020:23) määritellään digitaalinen turvallisuus laajaksi käsitteeksi, jonka viitekehykseen sisältyy riskienhallintaan, toiminnan jatkuvuudenhallintaan ja varautumiseen sekä kyberturvallisuuteen, tietoturvallisuuteen ja tietosuojaan liittyviä asioita.

Linjauksia osaamisen uudistamiseen

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.

Opetus- ja kulttuuriministeriö säätelee koulutusvastuiden kautta sitä, mitä tutkintoja ja millä tutkintotasoilla kussakin korkeakoulussa voidaan suorittaa ja mitä tutkintoon johtavaa koulutusta niitä velvoitetaan järjestämään. Säätelyllä pyritään turvaamaan koulutustarjonta yhteiskunnan ja työelämän tarpeiden mukaisesti ja tekemään valtakunnallista työnjakoa korkeakoulujen välillä. Opiskelijavalinnan perusteista päättäminen eli se, millaista osaamista opiskelijoilta eri aloilla edellytetään, kuuluu korkeakoulujen autonomiaan.

Valtioneuvoston koulutuspoliittisen selonteon (Valtioneuvoston julkaisuja 2021:24) mukaan ”Suomen yhteiskunnan ja hyvinvoinnin kehittyminen edellyttää, että osaamistaso nousee ja erityisesti huippuosaaminen vahvistuu”. Tavoitteena on, että vuonna 2030 vähintään puolet nuorista aikuisista suorittaa korkeakoulututkinnon. Tavoitteen saavuttamiseksi tarvitaan vuoteen 2030 mennessä yhteensä 100 000 uutta korkeakoulututkintoa enemmän kuin nykyisillä koulutusmäärillä saavutetaan. *Korkeakoulutuksen ja tutkimuksen visio 2030* -työssä linjattiin, että Suomi tarvitsee nykyistä enemmän osaajia, korkealaatuista korkeakoulutusta sekä tutkimus- ja innovaatiotoimintaa, ja myös vahvaa kytkeytymistä muualla tuotettuun uuteen tietoon. Korkeakoulut ovat lisänneet aloituspaikkoja, minkä lisäksi hallituksen päätöksellä korkeakoulujen aloituspaikkoja on lisätty reilulla 10 000:lla vuosina 2020–2022.

Selonteon mukaan asetetun tavoitteen saavuttamiseksi lisäaloituspaikat suunnattaisiin painotetusti niille aloille ja alueille, joilla on koulutuskysyntää ja joilta työllistytään

hyvin, kuitenkin huomioiden joustavuus suhteessa kysynnän ja työmarkkinoiden muutoksiin. Keskeistä on vahvistaa muunto- ja täydennyskoulutusta, jossa jatkuvalla oppimisella on tärkeä rooli.

Jatkuvan oppimisen ja työllisyyden palvelukeskus (JOTPA) edistää työikäisten osaamisen kehittämistä ja osaavan työvoiman saatavuutta. Se analysoi työelämän osaamis- ja työvoimatarpeita, rahoittaa työikäisille tarkoitettuja koulutuksia, kehittää tieto-, neuvonta- ja ohjauspalveluja, tukee alueellista ja muuta yhteistyötä sekä osallistuu jatkuvan oppimisen digitaalisen palvelukokonaisuuden kehittämiseen. JOTPAn käytössä on yli 40 miljoonaa euroa, ja se aloittaa verkostomaisen ennakoinnin kehittämistyön oppilaitosten ja korkeakoulujen kanssa niiden strategisen ja operatiivisen toiminnan suunnittelun tueksi. Lisäksi palvelukeskus käynnistää tunnistamiensa koulutus- ja osaamistarpeiden perusteella valtionavustushakuja ja hankintamenettelyjä.

Kyberturvallisuuden kansalaistaidot ovat yhä tärkeämmässä roolissa digitalisoituvissa yhteiskunnissa. Kyberturvallisuuden kansalaistaitojen vahvistamiseksi Aalto-yliopisto ja liikenne- ja viestintäministeriö toteuttavat vuosina 2022–2024 hankkeen, jossa luodaan EU-jäsenmaihin yhteinen kyberturvallisuuden kansalaistaitojen koulutuspaketti. Projektin tärkein tavoite on tuottaa kyberkansalaistaitoja opettavan, kaikille avoimen verkkosivun avaaminen. Verkkosivun sisältö tulee olemaan saatavissa kaikilla Euroopan unionin virallisilla kielillä.

Digitaalisen turvallisuuden opetus perusopetuksessa

Digitaalisen turvallisuuden koulutustarve ja sen tärkeys tunnistetaan perusopetuksessa. Tuoreet hankkeet kuten *Kyberturvallisuuden kehittämisohjelma*, *Uudet lukutaidot -kehittämisohjelma* ja Opetushallituksen ohjeistus kouluille koskien tietoturvaa osoittavat, että peruskoulutasolla halutaan tehdä toimenpiteitä, jotta digitaalinen turvallisuus nousisivat tärkeäksi osa-alueeksi koulutusta ja opetusta suunniteltaessa. Valittavana on kolme mallia, miten digitaalisen turvallisuuden opetusta voidaan kehittää ja lisätä peruskouluopetuksessa. Mallit eivät sulje toisiaan pois.

A. Digitaalinen turvallisuus laaja-alaisen osaamisen osa-alueeksi

Tässä mallissa kehitettäisiin laaja-alaisen osaamisen käsitettä. Tällä hetkellä laaja-alainen osaaminen sisältää seitsemää osa-aluetta, jotka muodostavat kaikkien peruskoulun oppiaineiden yhteiset tavoitteet. Lisäämällä digitaalisen turvallisuus yhdeksi omaksi osa-alueeksi (**Digitaalinen turvallisuus, L8**) se tulisi näkyväksi ja konkreettiseksi osa-alueeksi peruskoulussa.

B. Digitaalinen turvallisuus osaksi TVT-osaamisaluetta

Pienempi rakenteellinen muutos, jolla digitaalinen turvallisuus tulisi näkyvämmin esille peruskoulun kaikille osa-alueille, olisi sisällyttää digitaalinen turvallisuus nykyiseen tieto- ja viestintäteknologian osa-alueeseen (5).

C. Digitaalinen turvallisuus osaksi tieto- ja viestintäteknologian (TVT) opetusta

Tämä tavoite voitaisiin toteuttaa vahvistamalla tieto- ja viestintäteknologia pakollisuutta Suomen peruskouluissa. Nyt tämän valinnaisaineen esiintyminen tarjonnassa on

riippuvainen koulun omista painotussuunnista tai halusta tarjota TVT-opintoja valinnaisainetarjonnassaan. TVT-opetukseen sisällytettäisiin digitaalisen turvallisuuden osa-alue.

Digitaalisen turvallisuuden opetus lukioissa

Valittavana on kolme mallia, miten digitaalisen turvallisuuden opetusta voidaan kehittää ja lisätä lukio-opetuksessa. Tutkimuksessa nousi esille kolme, osin päällekkäistä mallia, jotka eivät sulje toisiaan pois.

A. Digitaalinen turvallisuus laaja-alaisen osaamisen osa-alueeksi

Tämä ratkaisu voitaisiin toteuttaa nykyisen opetussuunnitelman perusteella kehittämällä laaja-alaisen osaamisen käsitettä. Tällä hetkellä laaja-alainen osaaminen muodostuu kuudesta osa-alueesta ja sen osa-alueet muodostavat kaikkien oppiaineiden yhteiset tavoitteet. Lisäämällä **digitaalinen turvallisuus** yhdeksi omaksi osa-alueekseen, tulisi se näkyväksi lukion koulutuksessa.

B. Digitaalinen turvallisuus osaksi nykyisten laaja-alaisen osaamisen osa-alueita

Pienempi rakenteellinen muutos, jolla digitaalinen turvallisuus tulisi näkyvämmin esille lukion kaikille osa-alueille olisi sisällyttää digitaalinen turvallisuus johonkin nykyistä osa-alueista.

C. Digitaalinen turvallisuus osaksi tieto- ja viestintäteknologian (TVT) opetusta

Tämä kehityssuunta voitaisiin toteuttaa parantamalla tieto- ja viestintäteknologian opetuksen saatavuutta lukioissa. Tieto- ja viestintäteknologian opetukseen lisättäisiin digitaalinen turvallisuus yhdeksi sen osa-alueeksi.

Digitaalisen turvallisuuden opetuksen vahvistaminen vaatii lukio-opetukseen lisäresursseja. Yhden kokonaisen osa-alueen lisääminen laaja-alaiseen osaamiseen käsitteeseen vaatisi muutoksia opetussuunnitelmaan. Lisäksi opettajille tulisi varmistaa mahdollisuus täydennyskoulutukseen sitä halutessaan, jotta osa-alueen toteuttaminen oppiaineen opetuksessa olisi kaikille tasapuolisesti mahdollista.

Lisäksi yksi kehityssuunta on selvittää mahdollisuutta lisätä **ICT-alan erityislukioita** Suomeen tai vaihtoehtoisesti mahdollisuutta lisätä ICT-alan linjoja jo olemassa oleviin lukioihin. Näihin ICT-opintoihin sisällytettäisiin digitaalisen turvallisuuden opetusta.

Kyberturvallisuuden koulutus ammatillisessa koulutuksessa

Kyberturvallisuuskoulutusta annetaan nykyisin lähinnä IT-tuen, IT-asentajan ja tietoverkkoasentajan koulutuksissa. Kyberturvallisuuteen liittyviä tutkinnon perusteita pidetään hyvänä lähtökohtana opetukselle. Perusteita pidettiin kuitenkin niin vaativina, että osaamisen osoittamiseen näyttöinä työpaikoilla ei juurikaan ole mahdollisuuksia, vaan näytöt suoritetaan oppilaitoksessa.

Kyberturvallisuuden osaamisalueita sisältyy ainoastaan tieto- ja viestintätekniikan perus-, ammatti- ja erikoisammattitutkintoihin, kaikkiin näihin valinnaisena osaamisalu-

eena. Kansallisen kyberturvallisuusosaamisen kasvattamiseksi suositamme, että **kyberturvallisuuden koulutuksesta tulee pakollinen osa ICT-koulutusta.** Lisäksi opetusta tulisi jatkossa integroida osaksi kaikkea muuta ammatillista opetusta systemaattisesti.

Opettajien kiinnostus oman osaamisensa kehittämiseen on välttämätöntä ja sitä tulee tukea. Korkeakouluille tulee myöntää resurssia järjestää jatkuvan oppimisen mahdollisuuksia ammatillisille opettajille. Opettajien tutustumista työelämään tulee edistää.

Eri oppilaitosten **yhteistyötä** opettajalta opettajalle on **kehitettävä** ja sille on **luotava alusta ja foorumi.** Yhteistyöllä on nähtävissä monia hyötyjä. Tutkintojen perusteiden ollessa samat, on samoja koulutusmateriaaleja mahdollista hyödyntää. Koulutusympäristöjen kehittämistä voidaan tehdä yhteistyönä. Ajantasaista tietoa teknologian kehittymisestä on helppo jakaa. Yhteistyössä koottujen valmiiden mallien myötä madaltuu myös koulutuksen aloittamisen kynnys muissa oppilaitoksissa.

Työelämäyhteistyötä tulee kehittää jakamalla yrityssektorille tietoisuutta perus-, ammatti- ja erikoisammattitutkinnoista ja niihin sisältyvistä harjoitteluista.

Kyberturvallisuuden koulutus ammattikorkeakouluissa

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

Ammattikorkeakouluissa annettava kyberturvallisuusopetus (AMK- ja YAMK-korkeakoulututkinto, sekä erikoistumis- täydennys- ja muuntokoulutus) on sisällöllisesti kattavaa ja kykenee modulaarisen rakenteen perusteella muuntautumaan teollisuuden tarpeisiin. Tällä hetkellä ammattikorkeakoulujen kyberturvallisuuteen painottuvassa koulutuksessa sisäänotto on noin 555 (A-malliset ja B-malliset tutkinto-ohjelmat). A-luokituksen mukaisen koulutuksen sisäänotto noin 165 ja B-tason 390. **Koulutuksen resursseihin pitää panostaa**, jotta pystytään vastaamaan jatkuvasti laajenevan digitalisaation mukanaan tuomiin vaatimuksiin**.**

Koulutuksen resursseja mietittäessä on myös huomioitava se, että ammattikorkeakoulut antavat pääsääntöisesti teknistä kyberturvallisuuskoulutusta, joka kouluttaa tekniseen osaamiseen. Tällainen insinööritieteiden **opetus vaatii laajat ja monimutkaiset oppimisympäristöt**, jotka ovat kalliita hankkia ja ylläpitää. Jotta riittävä tekninen osaaminen voidaan taata, on tarvittavien oppimis- ja koulutusympäristöjen hankinta, kehitys- ja ylläpitokulut huomioitava resursoinnissa.

Opettajien määrän lisääminen on välttämätöntä, jos kyberturvallisuusalan opettamista halutaan lisätä. Haasteena opettajien määrän lisäämisessä on opetustyön houkuttelevuus tarpeeksi osaavien asiantuntijoiden rekrytoimiseksi. Nopeasti kehittyvän alan aiheiden täytyy tukea työelämää, ja tämän vuoksi aiheiden täytyy myös osaltaan tulla työelämän tarpeista.

Kyberturvallisuuden **opetusta tulee kohdentaa** myös eri työelämän aloille. Näin tarvittavaa osaamista olisi käytettävissä yhteiskunnassa yleisellä tasolla. Tutkintoja päivittävä täydennyskoulutus vaatii myös opetusresursseja.

Kyberturvallisuuden koulutus yliopistoissa

Kyberturvallisuuden ja turvallisuuden tutkinto-ohjelmien sisäänottomäärän voidaan arvioida olevan noin 250 vuonna 2022. Arvioiden mukaan tutkinto-ohjelmista valmistuu 60–70 % aloittaneista normaalissa tutkintoajassa. Kokonaisuudessaan tutkinto-ohjelmista valmistuu noin 80 %. Ilman tutkintoa työelämään siirtyneillä on tietysti varsin hyvät kyberturvallisuuden osaamisvalmiudet. Kokonaisuudessaan yliopistojen tuottama osaajamäärä on melko vähäinen suhteessa tunnistettuun osaajapulaan.

Hakijamäärät keskeisiin alan tutkinto-ohjelmiin kuten Jyväskylän yliopiston kyberturvallisuuden maisteriohjelmaan, Aalto-yliopiston Security and Cloud Computing (Security) ja Turun yliopiston Cyber Security -pääaineeseen osoittavat, että kyberturvallisuus koulutusalana kiinnostaa ihmisiä merkittävissä määrin.

Yliopistot tarjosivat tarkasteluhetkellä vähäisissä määrin kyberturvallisuuden täydennys- ja erikoistumiskoulutusta. Poikkeuksena oli Aalto-yliopisto, jossa alaan liittyvää täydennyskoulutusta oli enemmän tarjolla. Sen sijaan FITech verkostoyliopiston kautta on mahdollista opiskella useita kyberturvallisuuden kursseja lukuvuotena 2021–2022. Toisaalta sen valikoima koostuu yksittäisistä kursseista, eikä sen kautta ole mahdollista opiskella erillisiä kokonaisuuksia kyberturvallisuudesta.

Kyberturvallisuuden opetuksessa ei ole yliopistojen välistä yhteistyötä ja sen kehittämisen hyödyt nähtiin kuitenkin merkittävinä. Lisäresurssit kehittäisivät opetusta ja se näkyisi esimerkiksi kyberturvallisuuden **käytännön taitojen kehittävien harjoitusten lisäämisenä** opetukseen nykyistä enemmän. Yhtenä resurssihaasteena on kyberturvallisuuden osaajien rekrytointi.

Kyberturvallisuuden osaajien määrää yhteiskunnassa voidaan lisätä vaikuttamalla useaan eri tekijään. Yksi keino on **lisätä alan tutkinto-ohjelmia** ja **kasvattaa tutkinto-ohjelmien sisäänottomääriä**. Tämän toteuttaminen **vaatii henkilöresurssien kasvattamisen**. Lisäksi kyberturvallisuuden osaajien määrää voidaan lisätä **kehittämällä yliopistojen täydennyskoulutusta** ja FITech verkostoyliopiston kurssitarjontaa esimerkiksi kyberturvallisuuden opintokokonaisuuden muodossa. Lisäksi **opetusyhteistyön syventäminen yliopistojen välillä** mahdollistaisi opiskelijoita erikoistumaan monipuolisemmin eri kyberturvallisuuden osa-alueisiin.

Käynnissä oleva **Digivisio 2030** –hanke mahdollistaisi kyberturvallisuuden koulutuspilotin toteuttamisen. Digivisio-hankkeessa kaikki suomalaiset korkeakoulut rakentavat yhdessä oppimiselle tulevaisuutta. Tavoitteena on oppimisen uusi aikakausi, jonka ytimessä on digipedagogiikan jatkuva kehittäminen ja jossa jokainen meistä voi helpommin oppia ja kerryttää osaamistaan muuttuvassa maailmassa.

Muualla annettava 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.

Lapset ja nuoret saavat osin kyberturvallisuuteen liittyvää koulutusta osana omaa koulutuspolkuaan sekä peruskoulutuksessa että myöhemmissä opiskeluvaiheissa. Kuitenkin ne, jotka ovat opiskelleet aikana, jolloin kyberturvallisuus ei ollut osa peruskoulutusta tai myöhempiä opintoja, voivat tällä hetkellä jäädä täysin ilman kyberturvallisuuskoulutusta, elleivät sitä työpaikkansa kautta saa.

Yrityksille ja muille organisaatioille koulutusta tarjoavia tahoja Suomessa on melko paljon. Suurten yritysten ja julkisten organisaatioiden työntekijät saavat työhönsä liittyen yleensä koulutusta, mutta pk-yritysten työntekijät, itsensä työllistäjät ja yrittäjät voivat jäädä sitä ilman. Tässä voi olla ongelmana myös se, että pk-yritysten johto tai yrittäjät eivät tunnista tarvetta koulutukselle tai esteenä voi olla myös koulutuksen hinta. Koulutustarjonta on hajallaan, ja kaikilla ei ole ymmärrystä siitä, millaista koulutusta he itse tarvitsisivat.

Kansalaisopistot kouluttavat eri ikäryhmiä, mutta edes koulutusorganisaatioilla itsellään ei välttämättä ole käsitystä siitä, millaista koulutusta kannattaisi järjestää.

Suurten yritysten ja julkisten organisaatioiden osalta tilanne on hyvä. Suurilla yrityksillä on kyvykkyyttä ostaa henkilöstölleen kyberturvallisuuskoulutusta, ja sitä tarjoavat yritykset myös mielellään räätälöivät koulutuksen yrityksen henkilöstölle sopivaksi. Julkisella sektorilla HAUS tarjoaa laajan valikoiman kyberturvallisuuteen liittyvää koulutusta, jolla saadaan varmistettua henkilöstön perusosaaminen.

Keskeisiä kehittämiskohteita

Kriittisiksi kohderyhmiksi on tunnistettu erityisesti seniorit, lapset sekä pienten lasten vanhemmat ja maahanmuuttajat, joille ei ole tarjolla koulutusta omalla kielellään. Riskiryhmille tulisi järjestää koulutusta esimerkiksi yhteistyössä heidän kanssaan jo muutenkin työskentelevien tahojen, kuten esimerkiksi lasten osalta Lastensuojelun keskusliiton kanssa. Lisäksi kyberturvallisuusasioiden tärkeydestä tulisi viestiä erityisesti senioreille ja heidän kanssaan työskenteleville.

Pk-yritysten henkilöstö, itsensä työllistäjät ja yrittäjät jäävät helposti vaille riittävää kyberturvallisuuskoulutusta. Näiden tahojen ymmärrystä kyberturvallisuuden merkityksestä tulisi lisätä ja heitä tulisi tukea kyberkoulutuksen hankinnassa. Esimerkiksi palvelusetelit näiden koulutuspalveluiden hankintaan voisivat olla yksi vaihtoehto. Näitä toimijoita helpottaisi, jos tarjolla oleva kyberturvallisuuskoulutus olisi kerättynä esimerkiksi yhden verkkosivuston alle.

Kansalaisopistot ovat suuri senioreiden kouluttaja, mutta kaikilla kansalaisopistoilla tai opettajilla ei ole riittäviä tietoja kyberturvallisuuden kouluttamisesta. Kansalaisopistojen opettajille ja koulutussuunnittelijoille tarvitaan täydennyskoulutusta kyberturvallisuuteen liittyen. Myös subventioita osallistujille tarvitaan.

Muissa EU-maissa on luotu toimivia yhteistyöverkostoja yritysten, kyberturvallisuuskoulutusta koordinoivien valtiollisten tahojen sekä kolmannen sektorin toimijoiden

kanssa. Suomessa tarvittaisiin **kansalaisten kouluttamisesta ja siihen liittyvän yhteistyön koordinoinnista vastaava taho**, jolla olisi riittävät taloudelliset ja henkilöresurssit tämän tehtävän hoitamiseen. Yhteistyöverkostoa voisi hyödyntää kyberkoulutukset kokoavan verkkosivuston suunnittelussa ja kansalaisen kyberturvallisuuden kehittämisen konseptin jatkojalostuksessa. Verkostoon tulisi kutsua mukaan suurimmat koulutustarjoajat kaikilta sektoreilta sekä myös riskiryhmien ja pk-yritysten ja yrittäjien kanssa toimivien tahojen edustajat.

Määrälliset tarpeet ja niiden kehittäminen

Osaajapula on todellisuutta, vaikka sen tasoa on vaikea tarkasti ennustaa. Lähtötietojen perusteella on arvioitu, että tarvitsemme 5 000–8 000 kyberturvallisuuden ammattilaista lähivuosina. Tämän lisäksi 1 000–5 000 uutta ammattilaista tulee tekemään vastaavia töitä muiden töidensä ohessa. Nämä kaikki tarvitsevat vastaavan koulutuksen. Turvalliseen tuotantoon tarvitaan eniten uusia osaajia. Tarkemmin 6 000–13 000 uuden kyberammattilaisen ryhmä voidaan jakaa pääkoulutuksensa mukaan seuraavasti:

1. Turvallinen tuotanto 1 100–2 400 henkilöä,
2. Operointi ja ylläpito 900–1 900 henkilöä,
3. Kokonaisuuden valvonta ja johtaminen 1 000–2 200 henkilöä,
4. Suojaaminen ja puolustus 1 000–2 300 henkilöä,
5. Analysointi 800–1 700 henkilöä,
6. Tiedonkeruu ja operointi 600–1 300 henkilöä,
7. Tutkinta 600–1 300 henkilöä.

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

Ammattikorkeakoulujen lisäaloituspaikkojen kustannus riippuu tutkintotasosta ja tutkinnon alasta. AMK-tasolla lisärahoitus on noin 6 000 €/vuosi/opiskelija. YAMK-tasolla noin 9 000 €/vuosi/opiskelija.

Yliopistotasolla kustannusvaikutus syntyy, kun sisäänotto kasvaa kymmenillä opiskelijoilla. Kandidaattitasolla tarve on noin 6 000 €/vuosi/opiskelija ja maisteritasolla 9 000 €/vuosi/opiskelija.

Nykyisen yliopistojen ja ammattikorkeakoulujen tutkintoon johtavaan koulutukseen tulevien opiskelijoiden sisäänoton lisääminen (yliopistot +250, ammattikorkeakoulut +555) edellyttää noin 6 miljoonan euron vuotuista lisäpanostusta.

Tämän lisäksi tarvitaan resurssien lisäämistä ammatilliseen koulutukseen, muunto- ja täydennyskoulutukseen sekä kolmannen sektorin ja muiden kyberkoulutusta antavien toimijoiden tukemiseen noin 2–3 miljoonaa euroa vuodessa. Keskeistä on rahoituksen pitkäjänteisyyden turvaaminen, jotta kouluttavat laitokset voivat tehdä pitkäjänteisiä koulutusinvestointeja.

1 Perusteita ja lähtökohtia

1.1 Kyberturvallisuusalan koulutuksen tutkimus

Kyberalan koulutusta ja erityisesti sen vaatimuksia on tutkittu maailman laajuisesti runsaasti. Huomionarvoista on, että maailmalla on indikoitu puute kyberalan osaajista. Tämä luonnostaan tuo laadullisia ja määrällisiä vaatimuksia kyberalan koulutukselle. European Cyber Security Organisation (ECSO) on jo vuonna 2017 tutkinut tätä ongelmaa Euroopassa ja summaa tuloksia seuraavasti: osaajista on puutetta, kyberturvallisuuskoulutus vaatii erityisiä adaptiivisia koulutusympäristöjä, koulutus pitää aloittaa ajoissa ja koulutuksessa pitää huomioida molemmat sukupuolet (teknisillä aloilla on tunnetusti enemmän mies- kuin naisopiskelijoita) (ECSO, 2017). Tämän jatkoksi ECSO on esittänyt raportin kyberturvallisuuden osaajilta vaadittavista taidoista (ECSO, 2021). Aiheesta on myös tehty akateemista tutkimusta Euroopassa, ja tulokset ovat hyvin samanlaisia kuin ECSO:n raportissa (Blažič, 2021).

ECSO:n lisäksi kyberturvallisuudesta vaadittavista taidoista on julkaissut U.S National Institute of Standards and Technology (NIST). NIST:in dokumentit *National Initiative for Cybersecurity Education* (NICE) ja *Cybersecurity Workforce Framework* (NICE Framework), tarjoavat referenssirakenteen kyberturvallisuustehtävissä tarvittavista tiedoista, taidoista ja kyvyistä (engl. Knowledge, Skills, and Abilities, KSA). (Newhouse et al., 2017) Aiheen pohjalta muita opetussuunnitelmareferenssejä on myös julkaistu:

- Computing Curricula 2020 (CC, 2020), tarjoaa perusteet tietojenkäsittelyn akateemisille koulutusohjelmille.
- Cybersecurity Curricula 2017 (CSEC, 2017), tarjoaa standardinomaiset perusteet kyberturvallisuuden koulutusohjelmille.

Kyberturvallisuusosaamisen ja -koulutuksen perusteita ja linjauksia tarjoavat mm. seuraavat organisaatiot:

- Association for Computing Machinery (ACM),
- IEEE Computer Society (IEEE-CS),
- Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC),
- International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8).

On otettava huomioon, että em. dokumentit ovat jo joitain vuosia vanhoja ja ala sekä sen osaamisvaatimukset kehittyvät kiihtyvällä vauhdilla.

Euroopan unionin verkko- ja tietoturvavirasto (European Union Agency for Cybersecurity, ENISA) on julkaissut raportin osaajapulan korjaamiseen korkea- asteen koulutuksen avulla (ENISA, 2021). Raportti tarjoaa yleiskatsauksen kyberturvallisuuden koulutustarjonnasta Euroopassa analysoimalla äskettäin perustetun kyberturvallisuuskorkeakoulutietokannan (CyberHEAD) keräämiä ja tuottamia tietoja. Lisäksi raportti kuvaa EU:n jäsenvaltioiden omaksumia lähestymistapoja pyrkimyksessä lisätä ja ylläpitää kyberturvallisuusosaamisen työvoimaa. Raportissa em. lähestymistavat on luokiteltu ja analysoitu ENISAn National Capabilities Assessment Frameworkin (NCAF) määrittelemien tavoitteiden perusteella. Nämä tavoitteet ovat: kyberturvallisuustietoisuus, koulutus, haasteet ja harjoitukset. Raportti (ENISA, 2021) esittää myös viisi korjaussuositusta EU:n kyberturvallisuuden osaamisvajeeseen:

1. Lisätään sisäänottoja/ilmoittautumisia ja sitä kautta valmistumisia kyberturvallisuuskoulutusohjelmiin,
2. Tuetaan yhtenäistä lähestymistapaa hallituksen, teollisuuden ja korkeakoulujen välillä,
3. Yhteistyön lisääminen jäsenvaltioiden välillä,
4. Kyberturvallisuusmarkkinoiden tarpeiden ja trendien analysointi,
5. CyberHEADin käytön ja edistämisen tukeminen.

International Information Systems Security Certification Consortium (ISC)[2] on julkaissut tutkimuksen kyberturvallisuustyövoimasta. Tutkimuksen mukaan kyberturvallisuusammattilaisia työskentelee maailmanlaajuisesti 4,19 miljoonaa henkilöä. Siitä huolimatta, että ammattilaisia on globaalisti noinkin suuri määrä, puute kyberturvallisuusammattilaisista on 2,72 miljoonan henkilön luokkaa. Tämä antaa mielikuvan myös kansallisesta osaajavajeesta ja koulutusvaatimuksesta. (ISC2, 2021)

1.2 Näkökulmia kyberosaamisen kehittämiseen

Kyberturvallisuuden kehittämisohjelman periaatepäätöksessä 10.6.2021 määritetään keskeiset toimenpiteet kyberturvallisuuden parantamiseksi koko yhteiskunnassa. Periaatepäätöksen mukaan vahva kansallinen kyberturvallisuus edellyttää tarvittavaa osaamista ja laajaa osallistumista yhteiskunnan kaikilla eri tasoilla, tiivistä yhteistyötä erityisesti julkishallinnon ja elinkeinoelämän välillä, vahvaa kotimaista kyberturvallisuusteollisuutta, joka luo kyvykkyyksiä digitaalisen yhteiskunnan palveluiden turvaamiselle ja viranomaisten kyberturvallisuuskyvykkyyksiä, jotka luovat pohjaa koko yhteiskunnan turvalliselle toiminnalle.

Periaatepäätökseen annettiin laajasti lausuntoja, joista tähän on koottu niistä keskeisimmät. Lausunnoissa kannettiin huolta siitä, että emme pysty riittävästi huolehtimaan yritystemme ja julkisen hallinnon tuottamien palveluiden ja tietojen turvallisuudesta, ellei meille saada lisää lähivuosina merkittävässä määrin uusia alan ammattilaisia. Kyberturvallisuuden ja siihen liittyvien turvallisuuden eri osa-alueiden muodostuessa entistä kompleksisimmiksi toimintaympäristöiksi, tämä edellyttää myös uudenlaista kansallista koulutusta; koulutuksen tulee kehittyä vastaamaan digitaalisessa toimintaympäristössä tapahtuvaa muutosta. Tärkeintä on nostaa huippuluokan osaaminen tärkeäksi painopistealueeksi.

Huippuluokan osaamisen kehittäminen on tärkeä osa tulevaisuuden kyberturvallisuustarpeisiin vastaamista. Tästä syystä osaamista tulee kehittää ja koulutusmahdollisuuksia laajentaa nykyisestä. Huippuosaajien lisäksi tarvitaan myös käytännönläheistä kansalaisten kouluttamista. Lasten ja nuorten kouluttamisessa on syytä kiinnittää huomiota kansalaisten perustaitojen kehittämiseen tietoturvallisuuden, medialukutaidon sekä yksityisyyden suhteen. Näillä perustaidoilla parannetaan myös kansakunnan resilienssiä.

Osaamisen kehittämisessä koulutusjärjestelmän lisäksi merkittävässä roolissa ovat järjestöt ja heidän panoksensa kansalaisten kyberturvallisuusosaamisen kehittämisessä. Siksi on tärkeää tukea yhteistyötä sellaisten järjestöjen kanssa, jotka kehittävät ja auttavat kansalaisten ja tulevien huippuosaajien ruohonjuuritason osaamista ja tekemistä. Ongelmaksi tässä muodostuu se, että ei ole oikein olemassa sellaista foorumia, jolla tätä yhteistyötä voitaisiin suunnitella ja tehdä. Sellainen olisi syytä perustaa.

Kyberturvallisuuden opetuksen pitäisi olla sisällytettynä laajasti teknologia-alan tutkinto-ohjelmiin. Lisäksi peruskyberturvallisuusosaamisen pitäisi sisältyä kaikkiin korkeakoulututkintoihin. Tämä tukisi myös tavoitetta arjen kyberturvallisuusosaamisen lisäämisestä. Tämän osalta voisi harkita jopa asetustason muutosta niin, että tutkintoasetuksiin kirjattaisiin osaamistavoitteeksi modernin tietoyhteiskunnan vaatima perusosaaminen.

Osaamisen määrätietoisen vahvistamisen avulla eri ikäluokat ja kansanosat luovat vankan perustan kyberturvallisuudelle. Lisäksi osaaminen mahdollistaa tarvittavien teknologisten kyberkyvykkyyksien rakentamisen niin viranomaisten kuin yritystenkin tarpeisiin. On syytä varmistaa, että tutkimuksen, kyberturvallisuutta valmistavan teollisuuden ja kyberturvallisuuden käyttäjäorganisaatioiden osaamistarpeet huomioidaan kaikilla osa-alueilla. Jatkuva vuoropuhelu työelämän kanssa osaamistarpeista on keino viestiä sisältötarpeista.

Tutkintoon johtava koulutus ei tuota riittävää osaamista alalla ja siksi on turvauduttava työssä oppimiseen ja täydennyskoulutukseen työvoiman osaamisen turvaamiseksi. On aivan selvää, että työelämässä on opittava uutta aiempaa nopeammin, eikä kaikkia työelämätarpeita voida toteuttaa osana tutkintoon johtavaa koulutusta. Koulutusohjelmien kestot ovat pitkiä ja niiden muutostahti hidas. Jatkuvan oppimisen joustavat toteutusmuodot tulevat joka tapauksessa yleistymään kaikilla aloilla työelämän tarvitseman osaamisen tueksi.

Kansalaisten kybertaitojen parantaminen koulutuksen kautta on tärkeä tavoite, joka vahvistaisi Suomea korkean koulutuksen ja osaamisen maana ja loisi pohjan tulevaisuuden yhteiskunnalle. Elinkeinoelämää ja yhteiskuntaa tukevan tutkintopohjaisen koulutustarjonnan lisäksi tulisi panostaa joustavaan täydennyskoulutukseen ja elinikäistä oppimista tukevaan kurssi- ja koulutustarjontaan.

Kehittämisohjelmassa kuvatut keinot kansalaistaitojen (ml. tietoisuus uhkista, medialukutaito) kehittämisestä ovat hyviä, kuten myös niiden sisällyttäminen peruskoulun opetussuunnitelmaan. Tämän lisäksi tarvitaan myös erityisiä toimia, joilla tavoitetaan myös ne osat väestöstä, jotka eivät välttämättä ole kyberuhkien tai -hyökkäysten ensisijaisia kohteita, mutta joihin laajojen kriisien vaikutukset väistämättä ulottuvat.

Osaamispohjan vahvistaminen ja kyberturvallisuusteollisuuden toimintaedellytysten parantaminen ovat ensiarvoisen tärkeitä paitsi elinkeinopoliittisesti, myös kansallisen turvallisuuden näkökulmasta. Se tarkoittaa, että Suomessa tulee tehdä huomattavia lisäpanostuksia alan koulutuksen lisäämiseen, investointeihin sekä tutkimus- ja tuotekehityshankkeiden käynnistämiseen ja niiden tulosten markkinoille saamiseen. Osaajapula haittaa jo nykyisellään alan kehitystä ja yritysten menestymismahdollisuuksia. Isot teknologiamurrokset ja digitalisaatio tulevat entisestään kasvattamaan kyberturvallisuusalan osaamispulaa. Koulutusmahdollisuuksia tulee lisätä niin työelämässä kuin eri koulutusasteillakin.

Koulutusohjelmien ja -polkujen rinnalle voisi yhdeksi väyläksi nostaa myös oppisopimuskoulutuksen ja harjoitteluohjelmat, joissa voidaan erikoistua ja syventyä kyberturvallisuuteen ja oppimiseen käytännön työn kautta. Ulkomaisten erityisosaajien houkuttelun rinnalle voisi Suomeen houkutella erilaisin kannustimin myös nuorempia kyberturvallisuusalasta kiinnostuneita ja alalla vähemmän aikaa olleita ulkomaisia työntekijöitä. Tiiviiden yhteyksien luominen kansallisiin ja kansainvälisiin huippuosaamiskeskittymiin on tärkeää ja vaatii suunnitelmaa ja panostuksia.

Kyberuhkien ennaltaehkäisy vaatii laaja-alaista yhteistyötä. Päätavoitteena on tunnistaa, estää ja poistaa riskitekijöitä sekä tilanteita, jotka mahdollistavat digitaaliseen mediaan liittyviä riskejä. Kansalaisten osallisuus ennaltaehkäisevässä työssä on merkityksellistä ja se tulee toteuttaa laajassa yhteistyössä yhdessä oppilaitosten, palveluntarjoajien, ohjelmistokehittäjien, sosiaalisen median, tutkijoiden, juristien, poliisin, sosiaalipalveluiden sekä muiden lasten kanssa työskentelevien ammattilaisten kanssa.

Jokaisella kansalaisella mutta erityisesti lapsilla on oikeus saada ikä- ja kehitystason mukaista tietoa, turvataitoja ja opastusta. Lapsia, nuoria ja aikuisia tulisi kouluttaa internetin vaaroista. Kyberturvallisuuden kehittämiseksi onkin tärkeää, että kaikenikäisille kehitetään opetusmateriaalia, jota hyödyntämällä voidaan paremmin havainnollistaa Internetin vaaroja ja kyberrikollisuuden eri muotoja ja ilmiöitä.

On tarvetta varmistaa kyberturvallisuusalalle riittävä professorien ja tutkijakoulutettavien määrä. Nykyisessä tilanteessa alan tutkimusta tehdään useassa yliopistossa, mutta resursseja on myönnetty liian vähän. Kansalliseen koulutukseen tulisi kiinnittää huomioita pitkäjänteisesti. Lisäksi kansallisten osaajien hyödyntämisessä, samoin kuin kansallisessa ja kansainvälisessä yhteistyössä, tulee jatkossakin toimia aktiivisesti viranomaisten ja yksityisten toimijoiden kesken (toiminnallisen kyberturvallisuuden ekosysteemin luominen ja kyberteollisuuden hyödyntäminen viranomaistoiminnassa).

Kyberturvallisuusosaaminen on jatkossa osa koulusivistystä. Kansalaisten kyberturvallisuusosaamiseen liittyviä asioita tulee viestiä monikanavaisesti ja niitä tulee kohdentaa myös erilaisista toiminnallisista rajoitteista kärsiville ryhmille.

Kansalaisten kyberturvallisuusosaamisen arviointi tulisi ottaa osaksi kansallista kyberturvallisuusmittaristoa. Kansallinen kyberturvallisuuskyvykkyys on avainasemassa ja luo pohjan koko yhteiskunnan kyberturvallisuudelle. Osana kansallista kyberturvakyvykkyyttä tulee huolehtia ja mahdollistaa kuntien edellytykset keskeisinä yhteiskunnan toimijoina saavuttaa haluttu kyvykkyystaso. Toimialasta riippumattoman kyberturvallisuuskoulutuksen kehittäminen perusopetuksesta yliopistotasolle saakka luo vahvan perustan osaamisen kehittämiselle. Uusien liiketoimintamahdollisuuksien tukeminen koulutuksen rinnalla vahvistaa alan kehittymistä.

Koulutukseen tehtävät muutokset ovat erittäin tärkeitä. Tarvetta on kyberturvallisuuden ammateissa toimiville, mutta ehkä tätäkin tärkeämpää on varhaiskasvatuksesta lähtevän koulutuksen kautta varmistua siitä, että kaikki kansalaiset ymmärtävät kyberturvallisuuden perusteet ja työelämään siirtyvät tai työelämässä olevat kykenevät ymmärtämään kyberturvallisuuden vaatimukset oman työnsä kannalta - esim. palveluja tuotekehitystehtävissä toimivan on tiedettävä, miten kyberturvallisuus tulee huomioida näissä kehitystehtävissä.

Kansallisen kyberturvallisuuden huippuosaamisen kehittäminen edellyttää riittävän osaamiskeskittymän muodostumista. Tällaisen osaamiskeskittymän luominen edellyttää esitettyä laajaa kansallista ja kansainvälistä yhteistyötä. Kansainvälisen kilpailukyvyn saavuttaminen edellyttää, että saamme Suomeen korkeatasoisia opiskelijoita, tutkijoita ja alan asiantuntijoita. Kyberturvallisuuden kehittämisen kannalta on välttämätöntä, että Suomi on houkutteleva kohde kansainvälisille asiantuntijoille.

Kotimaisen koulutuksen kehittämistä ja työperäisen maahanmuuton esteiden purkamista tarvitaan, mutta lyhyellä aikavälillä on tarve purkaa kansainvälisten huippuosaajien maahantulon esteitä ja hidasteita, joka on nopeavaikutteisempi toimi kuin koulutusjärjestelmän kokonaisvaltainen kehittäminen.

Huippuosaamiselle on tarvetta kaikissa kyberturvallisuuden osa-alueissa. Kuitenkaan ei ole tarpeen tavoitella tilannetta, jossa kaikki osa-alueet ovat pelkkää huippuosaamista. Onnistuakseen huiput tarvitsevat tuekseen tasavahvoja osaajia. Tasavahvasta joukosta on myös edellytyksiä nousta useampia huippuosaajia. Huippuosaaminen voi syntyä muutakin kautta kuin perus- ja jatkotutkinto-opinnoissa. Täydennys- tai muuntokoulutettu saattaa olla tarvittava erityis- tai huippuosaaja, koska hänessä yhdistyy kyberturvallisuuden ja jonkin muun alan osaaminen. Toiminnan ja tietoteknisen osaamisen yhdistyminen on keskeinen kyberturvallisuuden menestystekijä. Tarvitaan kolmenlaista osaamista:

1. Kansalaistaito
   - mitä jokaisen pitää osata kyberturvallisuudesta eläkseen ja toimiakseen tietoyhteiskunnassa?
2. Alakohtainen perusosaaminen
   - mitä eri aloilla ja ammateissa pitää osata kyberturvallisuudesta?
3. Erityisasiantuntijataidot
   - mitkä ovat kyberammattilaisten yleiset ja alakohtaiset erityisosaamisvaatimukset?

Korkeasti koulutettuja kyberturvallisuusasiantuntijoita ei ole riittävästi tarjolla vastaamaan suomalaisen yhteiskunnan ja yrityskentän tarpeisiin. Tässä avainasemassa on lahjakkaimpien huippuosaajien kouluttaminen sekä kotimaisista että kansainvälisistä opiskelijoista, ja heidän integrointinsa yhteiskunnan ja elinkeinoelämän palvelukseen. Erityisesti ulkomailta tulleiden asiantuntijoiksi valmistuneiden opiskelijoiden integroitumista Suomeen tulisi tukea voimakkaasti.

ICT-alan huippuosaaminen nousee tulevaisuuden kriittiseksi menestystekijäksi, ja osaamisen varmistamiseksi tarvitaan voimakasta panostusta koulutukseen, tutkimukseen ja tuotekehitykseen. Koulutuksen kaikilla asteilla tulee opettaa nykyistä laajemmin paitsi tietotekniikan turvallista käyttöä myös sen hyödyntämistä ja kehittämistä. Monipuolinen panostaminen tieto- ja viestintätekniikan koulutukseen jo perusopetuksesta lähtien on koko Suomen digiyhteiskunnan tulevaisuuden välttämätön edellytys.

Useiden vuosien koulutus ei kuitenkaan ratkaise akuuttia osaajapulaa. Aiemman osaamisen päivittäminen vastaamaan työelämän nykytarpeita on varmistettava joustavilla koulutusratkaisuilla. Työelämässä jo olevilla tulee olla mahdollisuus erilaisten muuntokoulutusten avulla siirtyä aloille, joilla osaajia tarvitaan.

Kyberturvallisuuden opetuksen pitäisi olla sisällytettynä yleisesti teknologia-alojen koulutuksessa mm. sivuainevaihtoehtoina ja koulutuksen suunnittelussa otetaan huomioon myös elinkeinoelämän tarpeet. Erillisten koulutusohjelmien, sivuainekokonaisuuksien ja muiden laajempien opintojen lisäksi kyberturvallisuuden perusasiat tulee sisällyttää kaikkeen teknologia-alan koulutukseen. On tärkeää, että kyberturvallisuusosaaminen ei keskity liiaksi yksinomaan erillisiin kyberturvallisuuden koulutusohjelmiin. Vastaavasti on tärkeää, että myös esimerkiksi liiketoimintajohdolla on riittävästi kyberturvallisuusosaamista, ja koulutusta tulisi olla tarjolla sekä täydennyskoulutuksena että muiden alojen koulutuksen yhteydessä.

Kansalaisten kyberturvataitojen kehittämisen kannalta on tärkeää, että kyberturvallisuus sisällytetään jo varhaiskasvatuksen ja peruskoulun opetussuunnitelmaan ja että kyberturvallisuustaidot on tässä yhdistetty muihin digitaaliseen toimintaympäristöön liittyviin taitoihin.

Vahva kyberturvallisuus edellyttää kansalaisten kykyä tunnistaa kyberuhkia, ymmärtää oman toiminnan merkitys ja suojautua niiltä sekä kykyä raportoida havainnoista tarvittaessa viranomaisille. Järjestöt ovat keskeisessä roolissa tunnistaessaan kansalaisten toimintavalmiuksia käyttää digitaalisia palveluita ja laitteita sekä tunnistaessa niihin liittyviä riskejä ja menettelytapoja ongelmatilanteisiin jouduttaessa. Kansallisella tasolla ajantasainen kyberturvallisuuskoulutus ei ole yhdenmukaista eikä tavoita kaikkia, jolloin meillä on suuri joukko omaehtoisen kouluttautumisen sekä tiedonhaun varassa ja saatavilla olevan koulutuksen tavoittamattomissa.

Maanpuolustuksen kuuluessa kaikille, myös kyberpuolustus kuuluu kaikille. Yleinen kybertaitojen kasvattaminen sekä kyberturvallisuuden koulutusjärjestelmän kehittäminen ovat kokonaisuuksia, joiden kautta myös kyberpuolustus saa osaamista ja kykyä niin päivittäiseen etulinjaan kansalaisten parantuneen osaamisen kautta kuin kyberpuolustuksen huippuammattilaisiksi palkattuna henkilökuntana tai asevelvollisina. Kyberosaamisen kehittäminen sekä siviili- että maanpuolustustehtävässä tukevat siten vahvasti toisiaan.

Suomessa on syytä kehittää uusia kotimaisia kyberturvatuotteita, -palveluita ja tätä kautta osaamista. Tätä mitataan suoraan alan patenttien ja liikevaihdon määrällä. Toimittaessa pelkästään ulkomaisilla tieto- ja tietoturvajärjestelmillä osaaminen on siirtynyt Suomesta pois eikä siirry kotimaiseksi osaamiseksi. Lisäksi tänne ei hakeudu osaajia, koska täällä ei kehitetä merkittävästi uutta.

Kehittämisohjelmassa on erinomaisesti nostettu huippuluokan osaamisen kehittämistarve esiin ja esitetty hyviä toimenpiteitä. Pelkästään kyberturvallisuuden opetuksen sisällyttäminen teknologia-alojen koulutukseen ei riitä tavoitteisiin pääsemisessä, mikäli henkilötietojen käsittelyn suunnittelua ei ole laajemmin huomioitu. Omien tietojensa käsittelyä ja niihin liittyviä oikeuksia olisi hyvä saada turvallisten käytäntöjen lisäksi entistä selkeämmin osaksi opetusta, jotta tietosuojasta ja tietoturvasta saataisiin aito kansalaistaito.

2 Kyberturvallisuuden opetus peruskoulussa

2.1 Peruskoulun tietoturvallisuusosaamisen aikaisempi tutkimus

Tietoturvaosaamisen tarve kouluissa on tiedossa. Tieto- ja viestintäteknologiataidot sisältyvät opetussuunnitelmiin ja Opetushallitus onkin todennut, että lisääntyvä tietotekniikan käyttö tuo esille uusia huomioon otettavia riskejä (Opetushallitus, 2021). Tutkimusta ja keinoja pyritään kehittämään niin, että ne olisivat lasten näkökulmasta kiinnostavia ja opittavia.

Opetushenkilöstön tietotaitoa opettaa digiturvallisuutta ovat tutkineet Koivula Ja Mustola (2017) varhaiskasvatuksen ympäristössä. Heidän tutkimuksensa mukaan opetushenkilöstön valmiudet opettaa digiturvallisuutta ovat heikot. Lapset osaavat käyttää laitteita monesti aikuisia paremmin, eikä varsinaista pedagogista kasvatusta aiheeseen synny lainkaan. Myös Tekerekin ja Tekerekin (2019) tutkimus puoltaa ajatusta siitä, että lapset ovat aikuisia taitavampia laitteiden käyttäjiä.

Kososen (2019) tutkimus viides- ja kuudesluokkalaisten tietotekniikkaosaamisesta Lahdessa osoitti, että lapsilla on puutteita tietoturvan hallinnassa. Tutkimuksen mukaan lapset jakavat yhteystietoja ja tunnuksia toisilleen. Toisaalta oppilaiden itsearviointien perusteella salasanat koetaan turvallisiksi, eikä niitä jaeta muille. Tutkimuksen mukaan myös materiaalin jakamisessa on parannettavaa ja lapset eivät ymmärrä, millaiset kuvat ovat soveliaita jaettavaksi internetissä.

Turkkilainen tutkimus alakouluikäisten tietoturvallisuusosaamisesta osoitti, että alakouluikäisten ymmärrys tietoturvan perusasioista oli matala (Tekerek & Tekerek, 2017). Tutkimuksen mukaan tämä näkyy muun muassa salasanojen heikkoutena, turvallisen kommunikaation puutteena, asiakirjojen suojaamattomuutena ja tutustumisena ihmisiin netin kautta ilman kriittistä tarkastelua. Tutkimuksen mukaan koulutusta digiturvallisuudesta tarvitaan lisää.

Bocharovin, Mozharovin ja Simonovan (2019) Venäjällä tehdyssä tutkimuksessa on tutkittu esikouluikäisten tietoturvan ymmärrystä. Tutkimuksessa todetaan, että opettajien tulisi järjestää simuloituja tilanteita kyberturvallisuusuhkista ja käsitellä tilanteita jälkikäteen oppilaiden kanssa. Tutkimuksessa reagointi erilaisiin uhkiin oli huomattavasti oikeampaa harjoittelun jälkeen. Bocharovin ym. (2019) tutkimuksessa todetaan myös, että kouluikään päästessä vanhempien mahdollisuudet vaikuttaa vähenevät itsenäisyyden lisääntyessä. Ilmiö on havaittavissa selvästi käytännön elämässä Suomessa, kun lapset alkavat kulkea omatoimisesti sen sijaan, että vanhemmat kuljettaisivat lapsia päivähoitoon tai esikouluun.

Bocharovin ym. (2019) mukaan tarvittaisiin systemaattista tietoturvallisuuskoulutusta jo alakouluikäisille lapsille ja lasten tulisi oppia kriittistä ajattelua tiedonhankinnassa, tietoturvauhkien tunnistamista ja päätöksentekoa riskitilanteissa. Opetuksen tavoitteena on myös kasvattaa oppilaiden motivaatiota ottaa tietoturva huomioon toimiessaan erilaisissa digitaalisissa ympäristöissä.

Madetoja (2021) on tehnyt tutkimuksen suomalaisen peruskoulun oppilaiden todentamismenetelmistä ja pohtinut lasten asemaa digitaalisten ympäristöjen käyttäjinä. Tutkimuksen tulokset vastaavat Tekerekin ja Tekerekin (2017) havaintoja. Lapsilla ei ole

käsitystä siitä, miten he voisivat suojella yksityisyyttään digitaalisessa maailmassa ja esimerkiksi salasanat valitaan niin, että ne liittyvät lapsen elämään ja ovat sen vuoksi helposti pääteltävissä.

Yhteenvetona tutkimuksista voi todeta, että monien tutkimuksen mukaan lasten digiturvallisuuden ymmärrys on vielä heikolla tasolla. Haaste on tiedossa ja siihen yritetään kehittää ratkaisuja, joista yksi olisi systemaattisen kyberturvallisuuden/tietoturvallisuuden opetuksen lisääminen.

2.2 Nykytila peruskouluissa

Tukeakseen varhaiskasvatussuunnitelman ja esi- ja perusopetuksen opetussuunnitelmien toimeenpanoa opetus- ja kulttuuriministeriö käynnisti vuonna 2020 *Uudet lukutaidot* -kehittämisohjelman. Ohjelman tavoitteena on kehittää tieto- ja viestintäteknologisten taitojen, medialukutaidon sekä ohjelmointiosaamisen opettamista. Ensimmäisen vuoden aikana kehittämisohjelmassa valmisteltiin perusopetukseen vuosiluokkakokonaisuuskohtaiset TVT-taitojen, medialukutaidon ja ohjelmointiosaamisen osoittamisen kuvaukset. Vastaavasti varhaiskasvatukseen ja esiopetukseen on valmisteltu hyvän pedagogisen toiminnan kuvaukset näille taidoille. Kuvaukset julkaistiin 16.2.2021 uudetlukutaidot.fi-sivustolla. Kuvaukset pohjautuvat perusteasiakirjoihin ja niihin sisältyy myös tietoturvaosaaminen. Ohjelman tavoitteina vuosille 2021–2022 on tukea kuvausten hyödyntämistä varhaiskasvatuksessa ja opetustilanteissa sekä tuottaa ja koota sisältöjen opettamista ja oppimista tukevaa aineistoa ja digitaalisia sisältöjä. *Uudet lukutaidot* -kehittämisohjelma on osa *Oikeus Oppia* -ohjelmaa.

Kyberturvallisuus tai tietoturvallisuus eivät ole omana oppiainekokonaisuutenaan opetussuunnitelmassa. Sen sijaan opetussuunnitelmassa on yhtenä laaja-alaisena osaalueena tieto- ja viestintäteknologia (TVT). Tämä tarkoittaa, että laaja-alaisia osaamistavoitteita sisällytetään eri oppiaineiden vuosiluokkakohtaisiin tavoitteisiin. Opetussuunnitelmassa linjataan, että ”*tieto- ja viestintäteknologiaa hyödynnetään suunnitelmallisesti perusopetuksen kaikilla vuosiluokilla, eri oppiaineissa ja monialaisissa oppimiskokonaisuuksissa sekä muussa koulutyössä*.” Opetuksen sisällön suunnittelusta vastaa opetuksen järjestäjä opetussuunnitelmaa noudattaen.

Opetussuunnitelmassa laaja-alaisella osaamisella tarkoitetaan tietojen, taitojen, arvojen, asenteiden ja tahdon muodostamaa kokonaisuutta. Osaaminen tarkoittaa myös kykyä̈ käyttää tietoja ja taitoja tilanteen edellyttämällä tavalla. Siihen, miten oppilaat käyttävät tietojaan ja taitojaan, vaikuttavat oppilaiden omaksumat arvot ja asenteet sekä tahto toimia. Laaja-alaisen osaamisen lisääntynyt tarve nousee ympäröivän maailman muutoksista. Ihmisenä kasvaminen, opiskelu, työnteko sekä kansalaisena toimiminen nyt ja tulevaisuudessa edellyttävät tiedon- ja taidonalat ylittävää ja yhdistävää osaamista. (Opetushallitus, 2014)

Arvot, oppimiskäsitys ja toimintakulttuuri luovat perustan osaamisen kehittymiselle. Kukin oppiaine rakentaa osaamista oman tiedon- ja taidonalansa sisältöjä ja menetelmiä hyödyntäen. Osaamisen kehittymiseen vaikuttavat sekä ne sisällöt, joiden parissa työskennellään, että erityisesti se, miten työskennellään ja miten oppijan ja ympäristön vuorovaikutus toimii. Oppilaille annettava palaute sekä oppimisen ohjaus ja tuki vaikuttavat etenkin asenteisiin, motivaatioon ja tahtoon toimia.

Oppimiskokonaisuuksilla on useita liittymäkohtia toisiinsa. Niiden yhteisenä tavoitteena on perusopetuksen tehtävän mukaisesti ja oppilaiden ikäkauden huomioon ottaen tukea ihmisenä kasvamista sekä edistä demokraattisen yhteiskunnan jäsenyyden ja kestävän elämäntavan edellyttämää osaamista. Erityisen tärkeätä on rohkaista oppilaita tunnistamaan oma erityislaatunsa, omat vahvuutensa ja kehittymismahdollisuutensa sekä arvostamaan itseään.

Laaja-alaisen osaamisen osa-alueet on esitetty seuraavassa:

Ajattelu ja oppimaan oppiminen (L1)

Ajattelun ja oppimisen taidot luovat perustaa muun osaamisen kehittymiselle ja elinikäiselle oppimiselle. Ajatteluun ja oppimiseen vaikuttaa se, miten oppilaat hahmottavat itsensä oppijoina ja ovat vuorovaikutuksessa ympäristönsä kanssa. Olennaista on myös, miten he oppivat tekemään havaintoja ja hakemaan, arvioimaan, muokkaamaan, tuottamaan sekä jakamaan tietoa ja ideoita. Oppilaita ohjataan huomaamaan, että tieto voi rakentua monella tavalla, esimerkiksi tietoisesti päättelemällä tai intuitiivisesti, omaan kokemukseen perustuen. Tutkiva ja luova työskentelyote, yhdessä tekeminen sekä mahdollisuus syventymiseen ja keskittymiseen edistävät ajattelun ja oppimaan oppimisen kehittymistä. Oppilaita tuetaan rakentamaan perusopetuksen aikana hyvä tiedollinen ja taidollinen perusta sekä kestävä motivaatio jatko-opinnoille ja elinikäiselle oppimiselle.

Kulttuurinen osaaminen, vuorovaikutus ja ilmaisu (L2)

Perusopetuksessa oppilaita ohjataan ympäristön kulttuuristen merkitysten tunnistamiseen ja arvostamiseen sekä oman kulttuuri-identiteetin ja myönteisen ympäristösuhteen rakentamiseen. Oppilaat oppivat tuntemaan ja arvostamaan elinympäristöään ja sen kulttuuriperintöä sekä omia sosiaalisia, kulttuurisia, uskonnollisia, katsomuksellisia ja kielellisiä juuriaan. Heitä kannustetaan pohtimaan oman taustansa merkitystä ja paikkaansa sukupolvien ketjussa. Oppilaita ohjataan näkemään kulttuurinen moninaisuus lähtökohtaisesti myönteisenä voimavarana. Samalla heitä ohjataan tunnistamaan, miten kulttuurit, uskonnot ja katsomukset vaikuttavat yhteiskunnassa ja arjessa, miten media muokkaa kulttuuria sekä pohtimaan myös, millaisia asioita ei voida ihmisoikeuksien vastaisena hyväksyä.

Itsestä huolehtiminen ja arjen taidot (L3)

Oppilaita kannustetaan huolehtimaan itsestä ja toisista, harjoittelemaan oman elämän ja arjen kannalta tärkeitä taitoja sekä lisäämään ympäristönsä hyvinvointia. Oppilaat oppivat perusopetuksen aikana tuntemaan ja ymmärtämään hyvinvointia ja terveyttä edistävien ja sitä haittaavien tekijöiden sekä turvallisuuden merkityksen ja hakemaan niihin liittyvää tietoa. He oppivat myös ajanhallintaa, joka on tärkeä osa arjenhallintaa ja itsesäätelyä. Opetuksessa tarkastellaan teknologian monimuotoisuutta ja ohjataan ymmärtämään sen toimintaperiaatteita ja kustannusten muodostumista. Perusopetuksessa oppilaita ohjataan teknologian vastuulliseen käyttöön ja pohditaan siihen liittyviä eettisiä kysymyksiä.

Monilukutaito (L4)

Monilukutaidolla tarkoitetaan erilaisten tekstien tulkitsemisen, tuottamisen ja arvottamisen taitoja, jotka auttavat oppilaita ymmärtämään monimuotoisia kulttuurisia viestinnän muotoja sekä rakentamaan omaa identiteettiään. Oppilaat tarvitsevat monilukutaitoa osatakseen tulkita maailmaa ympärillään ja hahmottaa sen kulttuurista monimuotoisuutta. Monilukutaito merkitsee taitoa hankkia, yhdistää, muokata, tuottaa, esittää ja arvioida tietoa eri muodoissa, eri ympäristöissä ja tilanteissa sekä erilaisten välineiden avulla. Monilukutaito tukee kriittisen ajattelun ja oppimisen taitojen kehittymistä. Oppilaiden tulee voida harjoittaa taitojaan sekä perinteisissä että monimediaisissa, teknologiaa eri tavoin hyödyntävissä oppimisympäristöissä.

Tieto- ja viestintäteknologinen osaaminen (L5)

Tieto- ja viestintäteknologinen (TVT) osaaminen on tärkeä kansalaistaito sekä itsessään että osana monilukutaitoa. Se on oppimisen kohde ja väline. Perusopetuksessa huolehditaan siitä, että kaikilla oppilailla on mahdollisuudet tieto- ja viestintäteknologisen osaamisen kehittämiseen. Tieto- ja viestintäteknologiaa hyödynnetään suunnitelmallisesti perusopetuksen kaikilla vuosiluokilla, eri oppiaineissa ja monialaisissa oppimiskokonaisuuksissa sekä muussa koulutyössä.

Työelämätaidot ja yrittäjyys (L6)

Työelämä, ammatit ja työn luonne muuttuvat mm. teknologisen kehityksen ja talouden globalisoitumisen seurauksena. Työn vaatimusten ennakointi on vaikeampaa kuin ennen. Oppilaiden tulee perusopetuksessa saada yleisiä valmiuksia, jotka edistävät kiinnostusta ja myönteistä asennetta työtä ja työelämää kohtaan. Oppilaiden on tärkeä saada kokemuksia, jotka auttavat oivaltamaan työn ja yritteliäisyyden merkityksen, yrittäjyyden mahdollisuudet sekä oman vastuun yhteisön ja yhteiskunnan jäsenenä. Koulutyössä opitaan ryhmätoimintaa, projektityöskentelyä ja verkostoitumista.

Osallistuminen, vaikuttaminen ja kestävän tulevaisuuden rakentaminen (L7)

Yhteiskunnalliseen toimintaan osallistuminen on demokratian toimivuuden perusedellytys. Perusopetuksessa luodaan edellytykset oppilaiden kiinnostukselle kouluyhteisön ja yhteiskunnan asioita kohtaan. Oppilaat osallistuvat oman opiskelunsa, yhteisen koulutyön ja oppimisympäristön suunnitteluun, toteuttamiseen ja arviointiin. He saavat tietoja ja kokemuksia kansalaisyhteiskunnan osallistumis- ja vaikuttamisjärjestelmistä ja keinoista sekä yhteisöllisestä työskentelystä koulun ulkopuolella. Heitä ohjataan ymmärtämään omien valintojen, elämäntapojen ja tekojen merkitys paitsi itselle, myös lähiyhteisöille, yhteiskunnalle ja luonnolle.

2.3 Laaja-alaisen osaamisen sisältö koskien tieto- ja viestintäteknologiaa (L5)

Yksi laaja-alaisista osaamistavoitteista on tieto- ja viestintäteknologinen osaaminen, joka on tärkeä kansalaistaito sekä itsessään että osana monilukutaitoa. Oppilaita opas-

tetaan tuntemaan TVT:n erilaisia sovelluksia ja käyttötarkoituksia sekä huomaamaan niiden merkitys arjessa. Tavoitteena on, että he oppisivat hahmottamaan myös sen riskejä globaalissa maailmassa. Tieto- ja viestintäteknologista osaamista kehitetään neljällä pääalueella:

1. Oppilaita ohjataan ymmärtämään tieto- ja viestintäteknologian käyttö- ja toimintaperiaatteita ja keskeisiä käsitteitä sekä kehittämään käytännön TVT-taitojaan omien tuotosten laadinnassa.
2. Oppilaita opastetaan käyttämään tieto- ja viestintäteknologiaa vastuullisesti, turvallisesti ja ergonomisesti.
3. Oppilaita opetetaan käyttämään tieto- ja viestintäteknologiaa tiedonhallinnassa sekä tutkivassa ja luovassa työskentelyssä.
4. Oppilaat saavat kokemuksia ja harjoittelevat TVT:n käyttämistä vuorovaikutuksessa ja verkostoitumisessa.

Seuraavassa on esitetty vuosiluokkakohtaisesti 2. pääalue, jossa keskitytään tieto- ja viestintäteknologian turvalliseen ja vastuulliseen käyttöön:

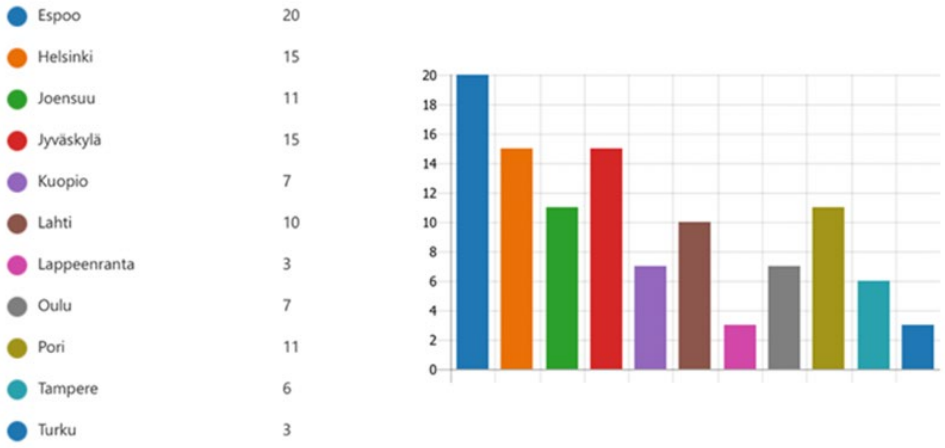
- 1. ja 2. vuosiluokilla tavoitteena on, että oppilaiden kanssa keskustellaan ja luodaan yhdessä TVT:n turvallisia käyttötapoja ja hyviä käytöstapoja.
- 3.–6. vuosiluokilla oppilaita ohjataan TVT:n vastuulliseen ja turvalliseen käyttöön, hyviin käytöstapoihin sekä tekijänoikeuksien perusperiaatteiden tuntemiseen. Koulutyössä harjoitellaan eri viestintäjärjestelmien sekä opetuskäytössä olevien yhteisöllisten palvelujen käyttöä.
- Kun siirrytään yläkoulu 7.–9. vuosiluokille otetaan esille tietoturva ja siihen liittyvät riskit konkreettisemmin: oppilaita ohjataan turvalliseen ja eettisesti kestävään tieto- ja viestintäteknologian käyttöön. He oppivat, miten suojaudutaan mahdollisilta tietoturvariskeiltä ja vältytään tiedon häviämiseltä. Vastuulliseen toimintaan ohjataan pohtimalla, mitä esimerkiksi käsitteet tietosuoja ja tekijänoikeus tarkoittavat, ja mitä seurauksia vastuuttomasta ja lainvastaisesta toiminnasta voi olla. (Opetushallitus, 2014)

Liitteessä 1 on esitetty esimerkkejä valinnaisten aineiden opetussuunnitelmista perusopetuksessa.

2.4 Kouluille tehdyn kyselyn analyysi

Tutkimukseen valittiin 11 kaupunkia ympäri Suomen, ja kysely lähetettiin yhteensä 448 koulun rehtorille. Koulut ovat ala-, ylä- tai yhteiskouluja, jotka noudattavat Suomen perusopetuksen Opetussuunnitelmaa. Saatekirjeessä pyydettiin välittämään kyselylinkki kyseisen koulun opettajille, jotka opettavat tietotekniikkaa tai ovat työssään tietoturvallisuuden kanssa tekemisissä. Vastauksia saatiin yhteensä 108 kappaletta (kts. kuva 1).

Kysymykseen siitä, millä vuosiluokilla kukin opetti, vastauksia tuli eniten opettajilta, jotka opettavat vuosiluokkia 7.–9., toiseksi eniten opettajilta, jotka opettavat vuosiluokkia 3.–6., ja vähiten opettajilta, jotka opettavat vuosiluokkia 1.–2. Huomioitavaa on, että vain neljä opettajaa valitsi ainoastaan vuosiluokat 1.–2., eli suurin osa opettaa myös vanhempia vuosiluokkia alkuopetuksen lisäksi. Jakauma on esitetty kuvassa 2.



KUVA 1. Kyselyyn vastanneiden määrä kaupungeittain

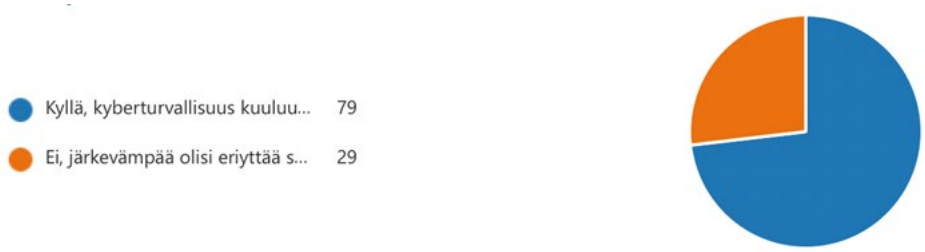
KUVA 2. Vuosiluokkakohtainen jakauma

KUVA 3. Opettajana toimimisen työvuodet

Opettajana toimimiseen eniten vastauksia (48 kpl) tuli opettajilta, jotka ovat toimineet opettajana yli 20 vuotta ja vähiten vastauksia (10 kpl) tuli opettajilta, jotka ovat toimineet opettajana alle 5 vuotta (kts. kuva 3).

Opettajia pyydettiin arvioimaan asteikolla 1–5 (täysin eri mieltä – täysin samaa mieltä) sisällyttävätkö he kyberturvallisuuden opetusta oppiaineen sallimissa raameissa. Keskiarvoksi muodostui 3,45. Opettajat, jotka vastasivat väliltä 4–5 edustavat hyvin tasapuolisesti sekä alakoulun että yläkoulun opettajia. Kuitenkin opettajat, jotka vastasivat väliltä 1–2 edustavat enimmäkseen vuosiluokkien 7.–9. opettajia. Voidaan todeta, että alakoulussa kyberturvallisuus/tietoturvallisuus tulee laajemmin eri oppiaineissa esille kuin yläkoulussa. Tulos esitetty kuvassa 4.

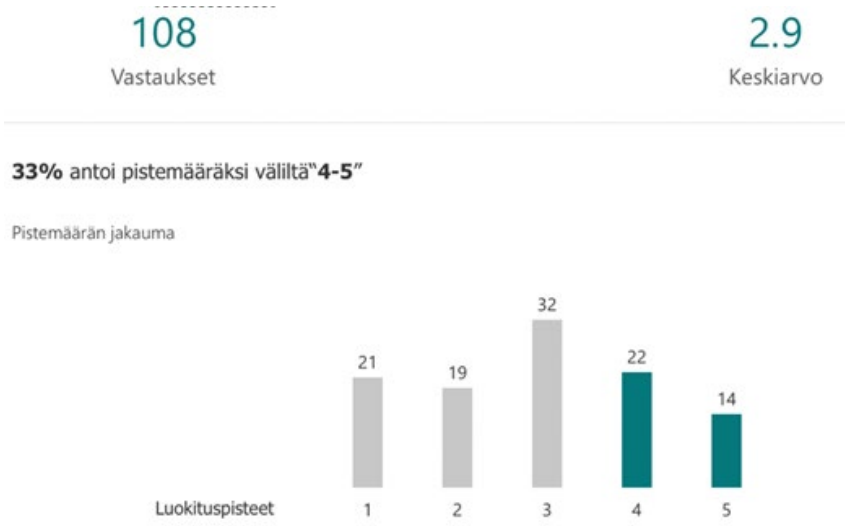
KUVA 4. Kyberturvallisuuden opetuksen sisällytys omaan oppiaineeseen



KUVA 5. Kyberturvallisuuden eriyttäminen omaksi oppiaineeksi

Opettajilta kysyttiin, tulisiko kyberturvallisuuden opetus sisällyttää jollakin tavoin kaikkiin oppiaineisiin vai eriyttää se esimerkiksi osaksi tietotekniikan opetusta. Tämä jakoi opettajien mielipiteitä: 27 % vastanneista kokee, että olisi järkevämpää eriyttää kyberturvallisuuden opetus osaksi tietotekniikan opetusta. 73 % vastanneista kokee, että kyberturvallisuus kuuluu kaikille peruskoulun osa-alueille (kts. kuva 5). Eriyttämisen kannalla olevista opettajista enemmistö opettaa vuosiluokkia 7.–9., mikä on linjassa edellisen kysymyksen vastausten kanssa, kun kysyttiin kyberturvallisuuden sisällyttämistä omaan oppiaineeseen. Yläkoulun opettaja voi kokea vaikeammaksi kyberturvallisuuden sisällyttämisen tiettyyn oppiaineeseen, kun taas alakoulussa lähtökohtaisesti saman opettajan opettaessa useampaa eri ainetta samalle luokalle kyberturvallisuus voi olla helpompi sisällyttää omaan opetukseen.

Kyselyssä selvitettiin, onko peruskouluissa tietoturvasta vastaava henkilö, jonka tehtävänä on huolehtia koulun henkilöstön ja oppilaiden tietoturvallisesta osaamisesta ja käyttäytymisestä. Opettajia pyydettiin arvioimaan vastaus asteikolla 1–5 (täysin eri mieltä – täysin samaa mieltä). Vastausten keskiarvoksi muodostui 2,9, ja vastaukset jakautuivat hyvin tasaisesti koko asteikolla. Voidaan todeta, että selkeää tietoturvasta vastaavaa henkilöä on vaikea nimetä/asia ei ole yhden henkilön vastuulla (kts. kuva 6).



KUVA 6. Koulun tietotekniikasta ja -turvasta vastaava henkilö

KUVA 7. Laitteiston ja palveluiden tietoturvallinen käyttö

Kyselyssä pyydettiin opettajia arvioimaan oppilaiden ja henkilöstön tietämystä laitteistojen ja opiskeluun liittyvien palvelujen tietoturvallisesta käytöstä. Arviointi tapahtui asteikolla 1–5 (täysin eri mieltä – täysin samaa mieltä). Keskiarvoksi muodostui 3,26. Eniten vastauksia tuli välillä 3–4, josta voidaan päätellä, että opettajat kokevat sekä omansa että oppilaiden tietämyksen laitteistojen ja opiskeluun liittyvien palvelujen tietoturvallisesta käytöstä melko vahvaksi (kts. kuva 7).

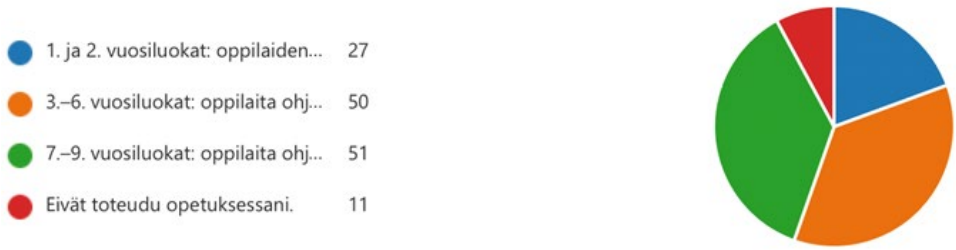
Opettajia pyydettiin arvioimaan, toteutuvatko opetussuunnitelman eri vuosiluokkakohtaiset tavoitteet koskien tieto- ja viestintäteknologian turvallista käyttöä omassa opetuksessaan. Vastausvaihtoehdot olivat:

- 1. ja 2. vuosiluokat: oppilaiden kanssa keskustellaan ja luodaan yhdessä TVT:n turvallisia käyttötapoja ja hyviä käytöstapoja.
- 3.–6. vuosiluokat: oppilaita ohjataan TVT:n vastuulliseen ja turvalliseen käyttöön, hyviin käytöstapoihin sekä tekijänoikeuksien perusperiaatteiden tuntemiseen.

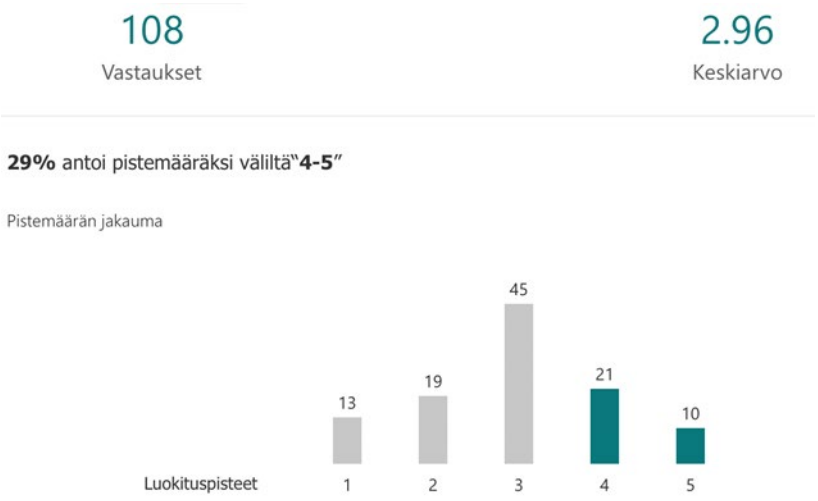
- 7.–9. vuosiluokat: oppilaita ohjataan turvalliseen ja eettisesti kestävään TVT:n käyttöön. Opetellaan suojautumaan mahdollisilta tietoturvariskeiltä ja vältytään tiedon häviämiseltä. Opitaan, mitä esimerkiksi käsitteet tietosuoja ja tekijänoikeus tarkoittavat, ja mitä seurauksia vastuuttomasta ja lainvastaisesta toiminnasta voi olla.

Valtaosa opettajista koki, että tavoitteet toteutuvat opetuksessa. Yksitoista opettajaa arvioi, että vuosiluokkakohtaiset tavoitteet eivät toteudu omassa opetuksessa. Näistä opettajista kaikki opettavat vuosiluokkia 7.–9 (kts. kuva 8).

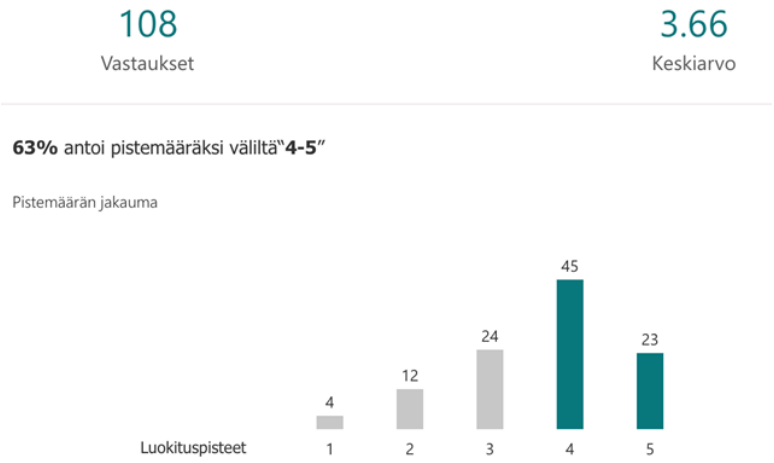
Opettajia pyydettiin arvioimaan asteikolla 1–5 (täysin eri mieltä – täysin samaa mieltä), kuinka selkeät ohjeet nykyinen opetussuunnitelma sisältää kyber- ja tietoturvallisuuden opettamisen tueksi. Keskiarvoksi muodostui 2.96 (kts kuva 9). Eniten vastauksia kertyi asteikolla 3, joka osoittaa, että vastanneet opettajat saavat jonkinlaisen tuen opetussuunnitelmasta, mutta eivät pidä opetussuunnitelman ohjeita kuitenkaan riittävän selkeinä koskien kyberturvallisuuden/tietoturvallisuuden opettamista.



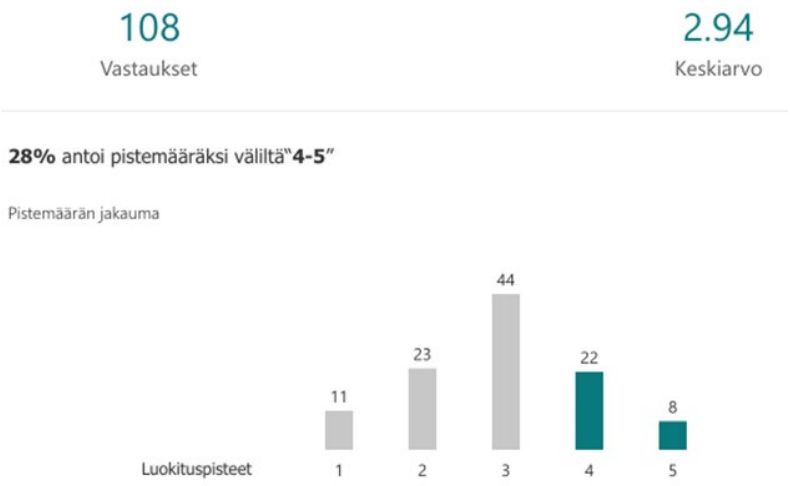
KUVA 8. Opetussuunnitelman tietoturvallisen käytön tavoitteet vuosiluokittain



KUVA 9. Opetussuunnitelman ohjeistus kyberturvallisuuden opetukseen



KUVA 10. Osaamisen taso opettajan omasta näkökulmasta



KUVA 11. Täydennyskoulutuksen saatavuus

Opettajat suhtautuivat melko positiivisesti omaan tietämykseensä ja osaamiseensa sisällyttää kyberturvallisuutta osaksi opetustaan. Kysymyksen arviointi tapahtui asteikolla 1–5 (täysin eri mieltä – täysin samaa mieltä). Keskiarvoksi muodostui 3.66. Opettajat, jotka vastasivat asteikolla 4–5 (68 kpl), jakautuvat melko tasan sekä vuosiluokkien 3.–6. että vuosiluokkien 7.–9. opettajiin. Asteikolla 1–3 (40 kpl) vastanneista opettajista selkeä enemmistö (27 kpl) opettaa vuosiluokkia 7.–9. Tämä on linjassa aiempien kysymysten vastausten kanssa, joissa yläkoulun opettajat näkevät kyberturvallisuuden/tieturvallisuuden mieluummin omana oppiaineenaan kuin sisällytettynä kaikkiin oppiaineisiin. Kuvassa 10 on esitetty opettajien näkemys kyberturvallisuuden opettamisen kyvykkyydestään.

Kyberturvallisuuteen liittyvän täydennyskoulutuksen saatavuuteen suhtauduttiin melko neutraalisti. Arviointi tapahtui asteikolla 1–5 (täysin eri mieltä – täysin samaa mieltä) ja keskiarvoksi muodostui 2,94. Asteikolla 1–2 vastanneista opettajista (34 kpl) – jotka kokevat täydennyskoulutuksen saatavuuden heikoksi – n. 60 % opettaa vuosiluokkia 7–9 (kts. kuva 11). Vastauksia tarkastellessa asteikon eri vaihtoehtojen välillä esiin ei

nouse tiettyä ikäryhmää, joka kokisi täydennyskoulutuksen saatavuuden erityisen heikoksi tai vastaavasti erityisen hyväksi – eroavaisuudet tulevat eri vuosiluokkien opettamisen välillä.

2.5 Digitaalisen turvallisuuden opetuksen kehittäminen perusopetuksessa

2.5.1 Yleiset kehittämistarpeet

Digitaalisen turvallisuuden koulutustarve ja sen tärkeys tunnistetaan eri tahoilla, joten halukkuutta koulutuksen kehittämiseen on. Tuoreet hankkeet kuten *Kyberturvallisuuden kehittämisohjelma*, *Uudet lukutaidot -kehittämisohjelma* ja Opetushallituksen ohjeistus kouluille koskien tietoturvaa osoittavat, että peruskoulutasolla halutaan tehdä toimenpiteitä, jotta digitaalinen turvallisuus nousisivat tärkeäksi osa-alueeksi koulutusta ja opetusta suunniteltaessa.

Tällä hetkellä kuitenkin materiaalit ja työkalut toimivat enemmänkin ohjenuorina ja tukena kuin velvoitteina, jolloin vastuu materiaalien käytöstä ja sen käyttämättä jättämisestä on opetuksen järjestäjällä. Tämän lisäksi opetussuunnitelmassa mainitut tieto- ja viestintäteknologian käytön tavoitteet eri oppiaineiden sisällä jäävät laveiksi, joten toteutustavat voivat vaihdella suuresti esimerkiksi eri kaupunkien välillä, puhumattakaan kaupungin sisällä eri kouluissa. Tieto- ja viestintäteknologia esiintyy useilla kaupungeilla yhtenä valinnaisaineena, mutta digitaalista turvallisuutta näissä käydään läpi hyvin niukasti. Tavoitteet ovat usein hyvin samanlaiset vuosiluokasta riippumatta.

Huomioitavaa on, että *Kyberturvallisuuden kehittämissuunnitelman* yhtenä tavoitteena on, että digitaalinen turvallisuus sisällytettäisiin opetussuunnitelmaan omana aiheenaan. Tämä tavoite olisi erityisen tärkeä toteutuessaan. Sen lisäksi, että peruskoulutason oppilaiden digiturvallisuusosaamisesta pidetään huolta, täytyy samalla huolehtia riittävästä koulutustarjonnasta ja -tasosta myös opettajille. Näin saadaan katettua koko peruskoulun tarpeet koskien digitaalista turvallisuutta.

Jotta Suomen kyberturvallisuusstrategian tavoite täyttyisi ja kaikilla on mahdollisuus toimia turvallisesti digitaalisessa maailmassa, tulee tutkimuksia peruskouluikäisten digiturvallisuuden opetustarpeesta tehdä lisää.

Koskisen tutkimus vuonna 2009 osoitti, että muun muassa lasten kyvyssä tunnistaa jaettavaksi sisällöksi kelpaava materiaali on puutteita. Samat haasteet ovat edelleen läsnä. Yhteydenpitokanavat lisääntyvät koko ajan ja riski kasvaa, siksi on erittäin tärkeää, että haasteeseen vastataan tehokkaasti koko lasten elämän osalta.

2.5.2 Kyselystä tehdyt johtopäätökset

Digitaalisen turvallisuuden opetuksen kehittämistä peruskouluopetuksessa voidaan lähestyä kahdella tavalla, sillä tutkimuksessa kartoitettiin opettajien näkemystä siitä, tulisiko digiturvallisuus olla osana jokaista oppiainetta vai tulisiko se eriyttää osaksi esimerkiksi tietotekniikan opetusta. Peruskoulun opetussuunnitelmassa määritellään useiden oppiaineiden osalta taitoja, joita tarvitaan myös turvalliseen toimintaan digitaalisessa maailmassa kuten lähdekritiikki ja medialukutaito, mutta suoraan digitaaliseen turvallisuuteen/kyberturvallisuuteen/tietoturvallisuuteen ei oteta selkeästi kantaa.

Kyselyn tulokset osoittavat, että peruskouluissa digitaalisen turvallisuuden opettamisen sisällyttäminen oppiaineen sallimissa rajoissa vaihtelee opettajien välillä – osa ei sisällytä digitaalista turvallisuutta opetukseensa lainkaan. Lisäksi digitaalisen turvallisuuden opetuksen kehittämisen suuntaviivat jakavat mielipiteitä opettajien keskuudessa.

Tutkimuksessa nousi esille kolme mallia siitä, miten digitaalisen turvallisuuden opetusta voidaan kehittää ja lisätä peruskouluopetuksessa (mallit eivät sulje toisiaan pois):

Malli 1: Digitaalinen turvallisuus laaja-alaisen osaamisen käsitteeksi

Tämä kehityssuunta voitaisiin toteuttaa nykyisen opetussuunnitelman perusteella vaikuttamalla laaja-alaisen osaamisen käsitteeseen tieto- ja viestintäteknologian osaamisen osalta. Tällä hetkellä laaja-alainen osaaminen muodostuu seitsemästä osa-alueesta ja nämä laaja-alaisen osaamisen osa-alueet muodostavat kaikkien peruskoulun oppiaineiden yhteiset tavoitteet. Lisäämällä yhdeksi omaksi osa-alueekseen digitaalinen turvallisuus, se tulisi näkyväksi ja konkreettiseksi osa-alueeksi peruskoulun kaikille osa-alueille. Laaja-alaisen osaamisen osa-alueita olisi tässä ratkaisussa:

- Ajattelu ja oppimaan oppiminen (L1)
- Kulttuurinen osaaminen, vuorovaikutus ja ilmaisu (L2)
- Itsestä huolehtiminen ja arjen taidot (L3)
- Monilukutaito (L4)
- Tieto- ja viestintäteknologinen osaaminen (L5)
- Työelämätaidot ja yrittäjyys (L6)
- Osallistuminen, vaikuttaminen ja kestävän tulevaisuuden rakentaminen (L7)
- **Digitaalinen turvallisuus (L8)**

Tätä lisäystä voidaan hyvin perustella sillä, että digitaalinen turvallisuus ja sen merkitys on kasvanut yhteiskunnan kaikilla sektoreilla viimeisten vuosien aikana varsin nopeassakin tahdissa. Lisäksi se on läsnä kaikkialla myös koulumaailmassa, se käy ilmi myös kyselylomakkeen avoimissa vastauksissa – suurinta osaa vastauksista ei voitu määrittää liittyvän vain yhteen opetettavaan aineeseen, vaan kyberturvallisuus näkyy kaikissa oppiaineissa.

Digitaalisen turvallisuuden opetuksen sisällyttäminen jollakin tavoin jokaiseen oppiaineeseen vaatisi peruskouluihin lisäresursseja. Erityisesti yhden kokonaisen osa-alueen lisääminen laaja-alaiseen osaamiseen käsitteeseen vaatisi laajoja muutoksia opetussuunnitelmaan ja tämän seurauksena myös oppiaineiden opetussisältöihin. Tätä varten opettajille niin ala- kuin yläkouluissakin tulisi varmistaa mahdollisuus täydennyskoulutukseen, jotta osa-alueen toteuttaminen oppiaineen opetuksessa olisi mahdollista.

Malli 2: Digitaalinen turvallisuus osaksi TVT-osaamisaluetta

Pienempi rakenteellinen muutos, jolla digitaalinen turvallisuus tulisi näkyvämmin esille peruskoulun kaikille osa-alueille, olisi sisällyttää digitaalinen turvallisuus nykyiseen tieto- ja viestintäteknologian osa-alueeseen (5).

Malli 3: Digitaalinen turvallisuus osaksi laajennettua TVT-opetusta

Tämä tavoite voitaisiin toteuttaa vahvistamalla tieto- ja viestintäteknologia pakollisuutta Suomen peruskouluissa. Nyt tämän valinnaisaineen esiintyminen tarjonnassa on riippuvainen koulun omista painotussuunnista tai halusta tarjota TVT-opintoja valinnaisainetarjonnassaan. TVT-opetukseen sisällytettäisiin digitaalisen turvallisuuden osa-alue.

Suurin osa kyselyyn vastanneista opettajista ilmoitti sisällyttävänsä kyberturvallisuutta osana opetustaan. Mikäli digitaalinen turvallisuus olisi osa TVT-opetusta, on huomioitavaa, että tämä kehityssuunta vaatii myös lisäresursseja ajatellen opettajien koulutuksen sisältöä, mutta myös henkilöstön määrää. Tässä kehityssuunnitelmassa olisi tärkeää kiinnittää huomiota seuraaviin asioihin:

- Peruskoulussa olisi mahdollista/pakollista opiskella tieto- ja viestintäteknologiaa tietty tuntimäärä viikossa ja osana sen opetusta käsiteltäisiin myös digitaalista turvallisuutta aiempaa laajempana kokonaisuutena.
- Opettajille täytyy olla entistä parempi mahdollisuus kouluttautua tieto- ja viestintäteknologian opettajaksi – tämä vaatii myös koulutuksen järjestäjältä koulutussisältöjen uudistusta.
- Täydennyskoulutuksessa tulisi käsitellä myös digitaalista turvallisuutta ja sen opettamista.
- Lisäksi yksi kehityssuunta on selvittää mahdollisuutta lisätä tieto- ja viestintäteknologian painotuslinjoja Suomen peruskouluihin.

Lähteet

Bocharov, M. I., Mozharov, M. S. & Simonova, I. V. (2019). Systematic information security training in elementary school. *Advances in Economics, Business and Management Research*, 500, 600-605.

Eu, Z., Lim, S., Chong, K., Ting, T. & Tan, L. (2021). Information Security Awareness. Haettu osoitteesta: https://www.researchgate.net/publication/355663812 .

Jyväskylän kaupunki, (2016). Jyväskylän perusopetuksen opetussuunnitelma: Tieto- ja viestintäteknologia. *https://peda.net/opetussuunnitelma/ksops/jyvaskyla/luku12/12-22/tjv*

Kaikkien kaupunkien opsit

Koivula, M. & Mustola, M. (2017). Digiloikka ja ei-kenenkään-alue varhaiskasvatuksessa. Haettu osoitteesta: https://jyx.jyu.fi/bitstream/handle/123456789/53753/koivulamustoladigiloikka.pdf?sequence=1&isAllowed=y .

Lahden kaupunki, (2016). Lahden kaupungin perusopetuksen opetussuunnitelma. *https://eperusteet.opintopolku.fi/ - /fi/ops/54589/perusopetus/valinnaisetoppiaineet/11020123*

Lappeenrannan kaupunki, (2016). Kesämäen koulu: Valinnaisaineet luokilla 7-9. https://www.kesamaenkoulu.fi/opiskelu/valinnaisaineet/valinnaisaineet-luokilla-7-9/

Madetoja, A. (2021). Tapaustutkimus perusopetusoppilaiden todentamismenetelmistä. Pro gradu -tutkielma, Jyväskylän yliopisto. Haettu osoitteesta: https://jyx.jyu.fi/handle/123456789/76525

Opetushallitus, (2014). Perusopetuksen opetussuunnitelman perusteet 2014. *https://www.oph.fi/sites/default/files/documents/perusopetuksen_opetussuunnitelman_perusteet_2014.pdf*

Opetushallitus (2021). Opetustoimen ja varhaiskasvatuksen turvallisuus. Haettu osoitteesta: https://www.oph.fi/fi/koulutus-ja-tutkinnot/opetustoimen-ja-varhaiskasvatuksen-turvallisuus

Opetushallitus, (2021). Tieto- ja viestintäteknologinen osaaminen. *https://uudetlukutaidot.fi/wp-content/uploads/2021/03/Versio-1-Tieto-ja-viestintateknologinen-osaaminen-suomi.pdf*

Opetushallitus (2021). Tietoturva ja -suoja koulussa. Haettu osoitteesta: https://www.oph.fi/fi/koulutus-ja-tutkinnot/tietoturva-ja-suoja-koulussa

Oulun kaupunki (2015). Oulun kaupungin perusopetuksen opetussuunnitelman perusteet 2014 ja Oulun kaupungin paikalliset linjaukset. *https://eperusteet.opintopolku.fi/ - /fi/ops/20650/perusopetus/valinnaisetoppiaineet/10612244*

Paananen, R., (2021). Kyberturvallisuuden kehittämisohjelma. Liikenne- ja viestintäministeriö, Helsinki. *https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163219/LVM_2021_7.pdf?sequence=1&isAllowed=y*

Tekeret, M. & Tekerek, A. (2017). A research on students' information security awareness. *Turkish Journal of Education,* 2(3), 61-70.

Turvallisuuskomitea (2019). Suomen kyberturvallisuusstrategia 2019. Haettu osoitteesta: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf

Welling, A. (2020). Mietityttääkö lastesi tietoturva? Alakoululaisille tarkoitettu mobiilipeli opettaa, miten vastata häirikölle netissä. Haettu osoitteesta: https://yle.fi/uutiset/3-11179317

3 Kyberturvallisuuden opetus lukiossa

3.1 Lukion opetussuunnitelma

Opetussuunnitelma otettiin paikallisesti käyttöön 01.08.2021 alkaen. Uusi lukiolaki astui vuomaan 01.08.2019, mutta kaikki paikallisessa opetussuunnitelmassa tarkemmin kuvattavat eli opetukseen, oppimisen tukeen, ohjaukseen sekä yhteistyöhön liittyvät asiat velvoittavat koulutuksen järjestäjiä elokuusta 2021 alkaen. (Opetushallitus, 2019, 9)

Lukiouudistuksen tavoitteena on kehittää kansakunnan koulutustasoa, jotta Suomi menestyisi mahdollisimman hyvin tulevina vuosikymmeninä. Tavoitteena on nostaa korkeakoulutettujen osuus 25–34-vuotiaiden ikäluokasta 50 prosenttiin lain luomishetken 41 prosentista. Uudistuksella halutaan lisätä lukiokoulutuksen vetovoimaa yleissivistävänä, korkeakouluihin jatko-opintokelpoisuuden antavana koulutusmuotona, vahvistaa koulutuksen laatua ja oppimistuloksia sekä sujuvoittaa siirtymistä toisen asteen opinnoista korkea-asteelle. Joustavammat ja yksilöllisemmät opintopolut, niiden vaatima ohjaus ja tuki, oppiainerajat ylittävät opinnot sekä korkeakouluyhteistyö ovat keskeisiä keinoja tavoitteiden saavuttamiseksi. (Opetushallitus, 2019, 9)

Lukiokoulutuksessa edistetään sekä oppiaineiden tavoitteiden ja keskeisten sisältöjen hallintaa myös kehitetään laaja-alaista osaamista. Sen osa-alueet muodostavat kaikkien oppiaineiden yhteiset tavoitteet:

1. Hyvinvointiosaaminen
2. Vuorovaikutusosaaminen
3. Monitieteiden ja luova osaaminen
4. Yhteiskunnallinen osaaminen
5. Eettisyys ja ympäristöosaaminen
6. Globaali- ja kulttuuriosaaminen

Laaja-alainen osaaminen auttaa suuntaamaan oppiaineissa opittuja tietoja ja taitoja käytännön elämään. Laaja-alainen osaaminen viittaa oppimisen ja osaamisen perustana oleviin kognitiivisiin taitoihin, metataitoihin sekä ominaisuuksiin, joita tarvitaan opiskelussa, työssä, harrastuksessa ja arjessa. Lisäksi se luo edellytykset tiedoille ja taidoille, joiden avulla voidaan hallita muutosta digitalisoituvassa ja monimutkaistuvassa maailmassa. (Opetushallitus, 2019, 9–10)

Uuden opetussuunnitelman mukaisesti pakolliset ja valtakunnalliset valinnaiset opinnot on jäsennelty lukion opetussuunnitelman perusteisiin 1–3 opintopisteen moduuleiksi, joista paikallisesti rakennetaan joko oppiaineiden omia tai yhteisiä opintojaksoja. Nämä entisten kurssien sijaan laadittavat opintojaksot voivat olla laajuudeltaan ja muodoltaan erilaisia. (Opetushallitus, 2019, 10)

3.2 Lukiokoulutuksen tavoitteita

Tavoitteena on edistää opiskelijoiden hyvinvointia ja tukea heitä opinnoissaan yhä paremmin. Lukioiden toimintakulttuurissa painotetaan vahvemmin opiskelijoiden osallisuutta, yhteistyötä, yhteisöllisyyttä ja monimuotoisuutta yksilölliset tarpeet samalla huomioon ottaen. Lukio-opintojen opiskelijalähtöisyys ja opintojen henkilökohtaistaminen vahvistuvat, jolloin opiskelumotivaatio ja opintojen mielekkyys kasvavat. (Opetushallitus, 2019, 10)

Kaikki nuorten lukiokoulutuksen järjestäjät laativat paikallisen opetussuunnitelman näiden lukion opetussuunnitelman perusteiden mukaan, jollei opetus- ja kulttuuriministeriön myöntämästä järjestämisluvasta muuta johdu. Lisäksi, jos lukiokoulutuksen järjestämislupaan liittyy erityinen koulutustehtävä, siihen liittyvät määräykset otetaan huomioon opetussuunnitelmaa laadittaessa. Paikallisessa opetussuunnitelmassa päätetään lukion opetus- ja kasvatustyöstä. Koulutuksen järjestäjä laatii vuosittain hyväksymäänsä opetussuunnitelmaan perustuvan suunnitelman opetuksen käytännön järjestämisestä. Paikallista opetussuunnitelmaa laadittaessa tulee ottaa huomioon muiden oppilaitosten opetustarjonta sekä lukion toimintaympäristö, paikalliset osaamisvahvuudet ja erityisresurssit. Lukiopaikkakunnan tai -alueen luonto ja ympäristö, historia, kieliolosuhteet sekä elinkeino- ja kulttuurielämä tuovat opetussuunnitelmaan paikallisuutta. Lisäksi käytännön yhteistyö eri alojen asiantuntijoiden kanssa lisää opiskelun elämänläheisyyttä ja syvällisyyttä. Opetussuunnitelmassa laadittaessa myös ajankohtaistetaan lukion opetussuunnitelman perusteissa määrättyjä asioita. Koulutuksen järjestäjä päättää, miten paikallinen opetussuunnitelma laaditaan lukion opetussuunnitelman perusteiden pohjalta. Paikallinen opetussuunnitelma laaditaan yhdessä lukion henkilöstön, opiskelijoiden, opiskelijoiden huoltajien sekä säännösten edellyttämiltä osin lisäksi kunnan sosiaali- ja terveydenhuollon toimeenpanoon kuuluvia tehtäviä hoitavien viranomaisten kanssa. Lisäksi yhteistyötä opetussuunnitelman laatimisessa voidaan tehdä myös muiden koulutuksen järjestäjien ja eri sidosryhmien kanssa. Yhteistyön tarkoituksena on pyrkiä varmistamaan lukiokoulutuksen korkeatasoisuus, yhteiskunnallinen merkittävyys sekä koko yhteisön sitoutuminen yhdessä määriteltyihin tavoitteisiin ja toimintatapoihin. (Opetushallitus, 2019, 13–14)

Lukion opetussuunnitelmassa määritellään, että lukiokoulutuksella on useita tehtäviä. Yhtenä tehtävänä on laaja-alaisen yleissivistyksen vahvistaminen. Yleissivistys koostuu tässä kontekstissa arvoista, tiedoista, taidoista, asenteista ja tahdosta, joiden avulla kriittiseen ja itsenäiseen ajatteluun pystyvät yksilöt osaavat toimia myötätuntoisesti, vastuullisesti, yhteisöllisesti ja itseään kehittäen. Lisäksi lukiokoulutuksen aikana, opiskelija kartuttaa ihmistä, kulttuureja, yhteiskuntaa ja ympäristöä koskevaa olennaista tietoa, toimijuutta ja osaamista. Opetuksen tavoitteena on myös valmistaa opiskelijaa ymmärtämään elämässä ja maailmassa vallitsevia monitahoisia keskinäisriippuvuuksia sekä jäsentämään laaja-alaisia ilmiöitä. (Opetushallitus, 2019, 16)

Opetus- ja kasvatustehtävät ovat olennainen osa lukiokoulutusta. Opintojen aikana, yksilö rakentaa ihmiskäsitystään, identiteettiään, maailmankuvaansa ja -katsomustaan sekä paikkaansa maailmassa. Saman aikaisesti yksilö kehittää suhdettaan menneisyyteen ja suuntautuu tulevaisuuteen. Lisäksi lukiokoulutus kehittää valmiuksia elämänhallintaan ja työelämään sekä syventää opiskelijan kiinnostusta tieteiden ja taiteiden maailmasta. Lukiokoulutus ohjaa opiskelijaa tulevaisuuden suunnitelmien laadintaan, maailmankansalaisuuteen kasvamiseen ja jatkuvaan oppimiseen. (Opetushallitus, 2019, 16)

3.3 Lukio-opetuksen yleiset tavoitteet

Valtakunnallisessa lukion opetussuunnitelmassa todetaan, että ”Lukion opetus ja muu toiminta järjestetään lukiokoulutusta koskevassa valtioneuvoston asetuksessa

(810/2018) määriteltyjen lukiokoulutuksen yleisten valtakunnallisten tavoitteiden mukaan". (Opetushallitus, 2019, 58)

Tavoitteena on, että opiskelijalla on mahdollisuus kasvaa sivistyneeksi yhteiskunnan jäseneksi, hankkia muuttuvan toimintaympäristön edellyttämiä tietoja ja taitoja sekä kerryttää jatkuvan oppimisen taitoja. Erityisesti korostetaan laaja-alaisen yleissivistyksen ja kokonaisuuksien ymmärtämisen merkitystä sekä kannustetaan eettisesti vastuulliseen ja aktiiviseen toimijuuteen osana paikallista, kansallista, eurooppalaista ja globaalia yleisöä. (Opetushallitus, 2019, 58)

Opintojen aikana yksilö saa monenlaisia kokemuksia uuden tiedon ja osaamisen rakentamisesta laaja-alaisesti ja oppiainerajat ylittäen. Opiskelija kehittää tiedonhankinta- soveltamistaitojaan sekä ongelmanratkaisutaitojaan. Opiskelija saa kokemuksia tutkivasta oppimisesta ja osallisuudesta tieteen ja tutkimuksen tekoon. Opetuksen tavoitteena on vahvistaa myös opiskelijan monilukutaitoa, niin että hän ymmärtää tieteen- ja taiteenaloille ominaista kieltä sekä motivoituu erilaisten tekstien tutkimisesta, tulkitsemisesta ja tuottamisesta. Opiskelija oppii arvioimaan tekstien ja tiedon luotettavuutta. Lisäksi opetus ohjaa opiskelijaa syventämään ymmärrystään tieto- ja viestintäteknologiasta sekä käyttämään sitä tarkoituksenmukaisesti, vastuullisesti ja turvallisesti niin itsenäisessä kuin yhteisöllisessä työskentelyssä. (Opetushallitus, 2019, 58)

3.4 Laaja-alainen osaaminen

Laaja-alaisella osaamisella on lukiokoulutusta eheyttävä tehtävä. Laaja-alaisen osaamisen osa-alueet muodostavat lukion oppiaineiden yhteiset tavoitteet. (Opetushallitus, 2019, 60) Laaja-alaisen osaamisen tavoitteet ovat:

- Hyvä yleissivistys
- Kestävän tulevaisuuden rakentaminen
- Vahvat jatko-opinto, työelämä- ja kansainvälisyysvalmiudet

Laaja-alaisen osaamisen keskiössä on hyvä, tasapainoinen ja sivistynyt ihminen. Laaja-alainen osaaminen rakentuu kuudesta osa-alueesta. Opetussuunnitelmassa todetaan, että: "Lukiokoulutuksen arvoperusta, oppimiskäsitys ja toimintakulttuuri luovat perustan laaja-alaisen osaamisen kehittymiselle. Laaja-alaisen osaamisen osa-alueiden tavoitteisiin pyritään kaikissa lukio-opinnoissa. Kukin oppiaine lähestyy laaja-alaista osaamista oman tiedon- ja tieteenalansa lähtökohdista. Laaja-alainen osaaminen on keskeinen osa sekä oppiainekohtaisia että oppiaineita yhdistäviä opintoja". (Opetushallitus, 2019, 61)

Paikallisissa opetussuunnitelmissa täydennetään ja konkretisoidaan laaja-alaista osaamista jokaisen oppiaineen kohdalla sekä opintojakson kuvauksessa. Laaja-alaisessa osaamisessa huomioidaan lukion toimintakulttuuri. Lisäksi sen toteutusta täydennetään opetussuunnitelmaan sisällytettävissä korkeakouluopintoihin ja työelämän tutustumisen sekä kansainvälisen osaamisen järjestelyjen kuvauksissa. Temaattisten opintojen sisältöjä voidaan valita laaja-alaisen osaamisen osa-alueista. (Opetushallitus, 2019, 61–62):

- Globaali- ja kulttuuriosaaminen
  - Kansainvälisyysvalmiudet ja maailmankansalaisen asenne
  - Suomalaisen, eurooppalaisen ja globaalin kulttuuriperinnön tuntemus sekä kulttuurisen moninaisuuden ymmärtäminen

  - Eettinen toimijuus globaalissa media- ja teknologia maailmassa
- Hyvinvointiosaaminen
  - Huolenpito itsestä ja muista
  - Omien vahvuuksien tunnistaminen ja käyttäminen sekä identiteetin rakentaminen
  - Sinnikkyys muutosten ja yllätysten maailmassa
- Vuorovaikutusosaaminen
  - Tunne- ja empatiataidot
  - Sosiaaliset taidot, yhteistyökyky ja yhdessä oppimisen taidot
  - Kielitaitoisuus ja rakentavan viestinnän taito
- Monitieteinen ja luova osaaminen
  - Uteliaisuus ja motivaatio oppia sekä etsiä merkityksiä ja yhdistellä asioita uudenlaisilla tavoilla
  - Oppimisen säätely, lähdekriittisyys ja jatkuva oppimistaitojen kehittäminen
  - Monilukutaito digiajassa
- Yhteiskunnallinen osaaminen
  - Demokratiataidot, vaikuttaminen turvallisen oikeudenmukaisen ja kestävän tulevaisuuden puolesta
  - Osaamisen käyttäminen sekä omaksi että yhteiskunnan hyväksi
  - Uudistumiskyky, työelämävalmiudet ja yrittäjämainen asenne
- Eettisyys ja ympäristöosaaminen
  - Arvolähtöinen ja eettinen toiminta yhteiseksi hyväksi
  - Luonnon monimuotoisuuden arvostaminen ja tutkimustietoon perustuva ilmasto-osaaminen
  - Kiertotalouden ymmärtäminen ja kestävä kuluttajuus

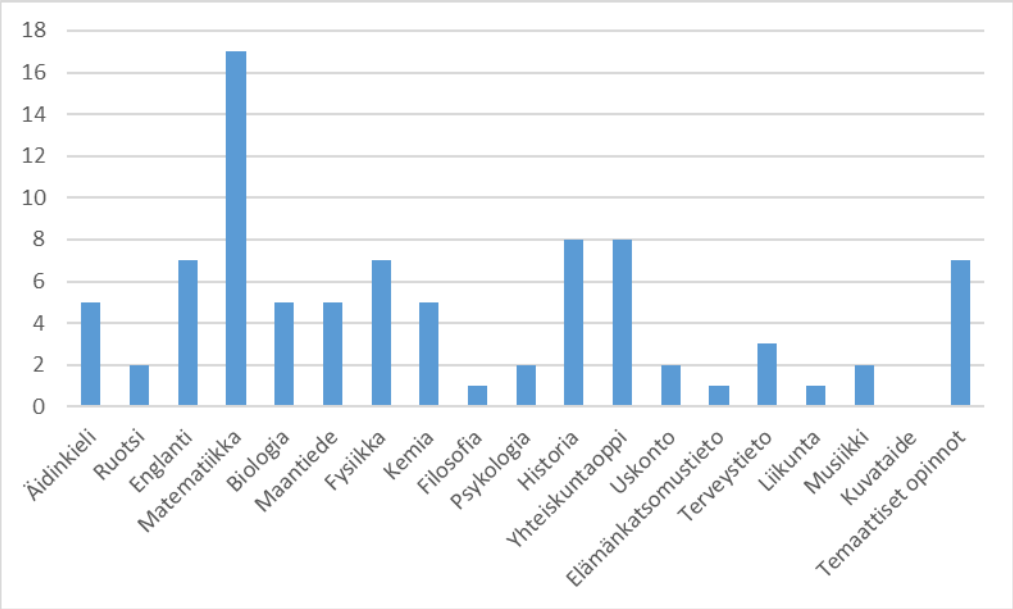
3.5 Kyselyn tulokset

Kysely kohdistettiin 103 lukioon ja se lähetettiin lukioiden rehtoreille. Kyselyyn saatiin vastauksia 54 kappaletta 16 kaupungista. Tutkimuksen vastaajiksi etsittiin opettajia, jotka opetuksessaan käsittelevät kyberturvallisuutta/tietoturvallisuutta/digitaalista turvallisuutta. Yhdestä lukiosta on voinut vastata useampi kuin yksi opettaja.

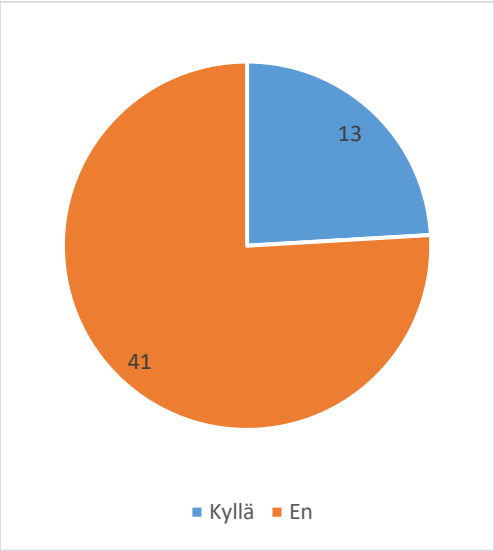
Eniten vastauksia tuli matematiikan opettajilta (17 kpl) ja vähiten liikunnan (1kpl), filosofian (1 kpl), elämänkatsomustiedon (1kpl) ja kuvataiteen (0 kpl) opettajilta. Useat opettajat ilmoittivat opettavansa useampaa kuin yhtä oppiainetta. Kuvassa 12 on esitetty opettajien oppiaineet.

Kyselyssä kartoitettiin opettaako vastaaja tieto- ja viestintäteknologiaa lukiossaan. Kyselyyn vastanneista opettajista 13 ilmoitti opettavansa tieto- ja viestintäteknologiaa (kts. kuva 13).

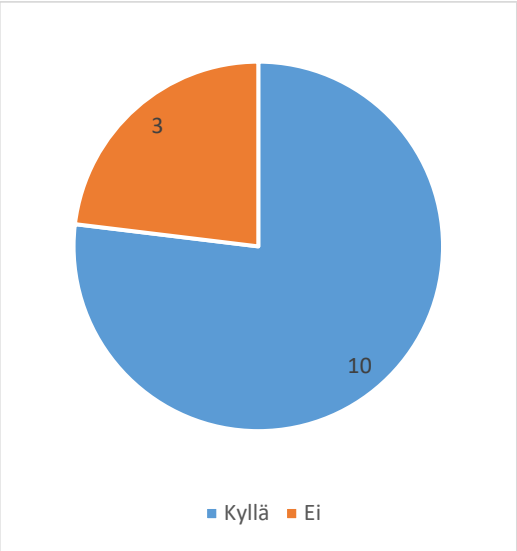
Tieto- ja viestintäteknologian opettajista 10 sisällyttää opetukseensa kyber- ja tietoturvallisuutta käsitteleviä opintoja. Puolestaan kolme opettajaa ilmoitti, että ei sisällytä kyberturvallisuuden opetusta tieto- ja viestintäteknologian opetukseensa (kts. kuva 14).



KUVA 12. Opettajien oppiaineet



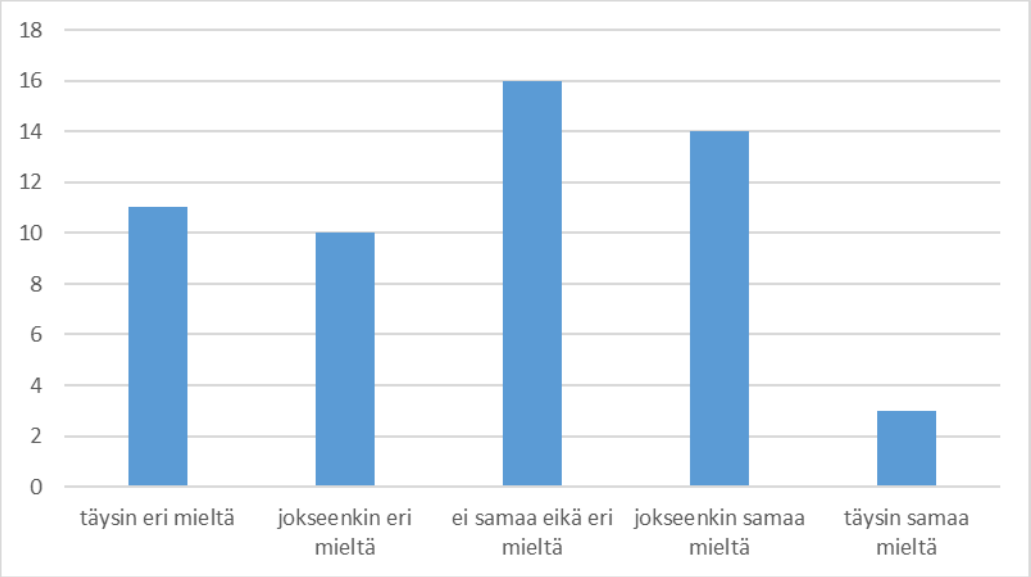
KUVA 13. Tieto- ja viestintäteknologian opettajien määrä otoksessa



KUVA 14. Kyberturvallisuuden opetus tieto- ja viestintäteknologian opetuksessa

Opettajia pyydettiin arvioimaan asteikolla 1–5 (täysin eri mieltä – täysin samaa mieltä) sisällyttävätkö he kyberturvallisuuden opetusta oppiaineen sallimissa raameissa. Keskiarvoksi muodostui 2,77. Vastausten välillä oli merkittävää hajontaa. Opettajat, jotka vastasivat kysymykseen väliltä 4–5 edustavat useita eri oppiaineita. Lukuun ottamatta tieto- ja viestintäteknologiaa, aineiston pohjalta ei voida tehdä johtopäätöstä,

että tietyn oppiaineen edustajat sisällyttäisivät kyberturvallisuuden opetusta merkittävästi enemmän kuin toiset. Myös opettajat, jotka vastasivat väliltä 1–2 edustavat useita eri oppiaineita (kts. kuva 15).

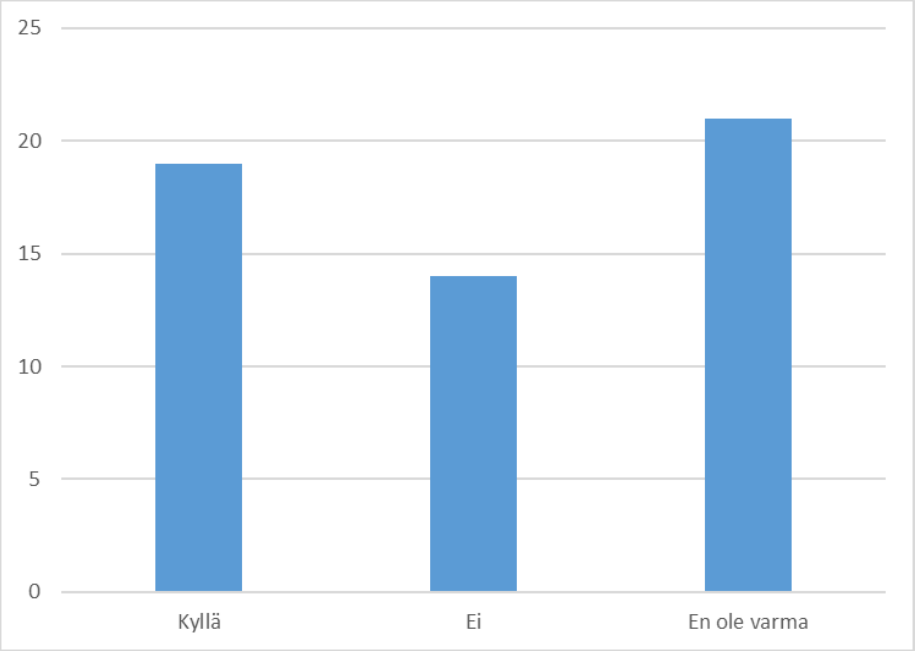


KUVA 15. Kyberturvallisuuden opetuksen sisällyttäminen oppiaineen opetukseen

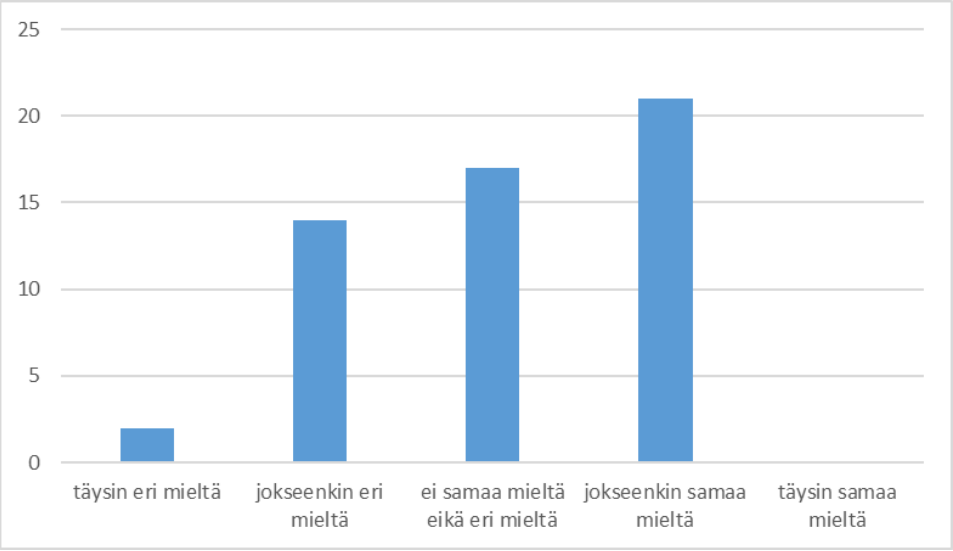
KUVA 16. Kyberturvallisuuden opetuksen sisällyttämisestä jokaisen oppiaineen opetukseen

Opettajilta kysyttiin tulisiko kyberturvallisuuden opetus sisällyttää jollakin tavoin kaikkiin oppiaineisiin vai tulisiko se eriyttää esimerkiksi osaksi tietotekniikan opetusta. Tämä jakoi opettajien mielipiteitä ja näkyi myös tieto- ja viestintäteknologian opettajien keskuudessa. Viisi tieto- ja viestintäteknologian opettajaa oli sitä mieltä, että kyberturvallisuuden opetus pitäisi jollakin tavoin sisällyttää jokaiseen oppiaineeseen ja puolestaan seitsemän oli sitä mieltä, että kyberturvallisuuden opetus olisi järkevämpää eriyttää esimerkiksi osaksi tietotekniikan opetusta. Kun huomioidaan kaikki vastaukset, niin

enemmistö oli sitä mieltä, että kyberturvallisuus kuuluu lukion kaikille osa-alueille. Kuvassa 16 on esitetty opettajien arvio kyberturvallisuuden opetuksen sisällyttämisestä jokaiseen oppiaineeseen.



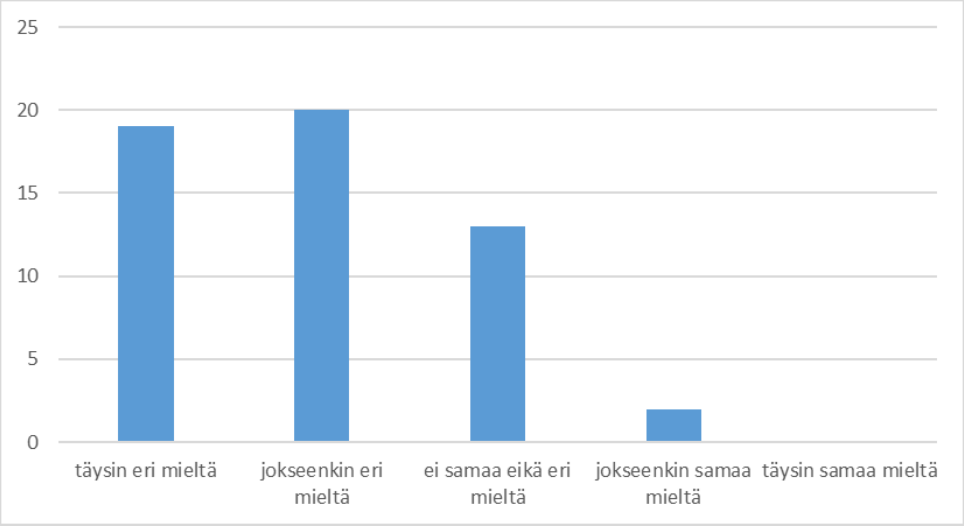
KUVA 17. Lukion tietoturvasta vastaava henkilö



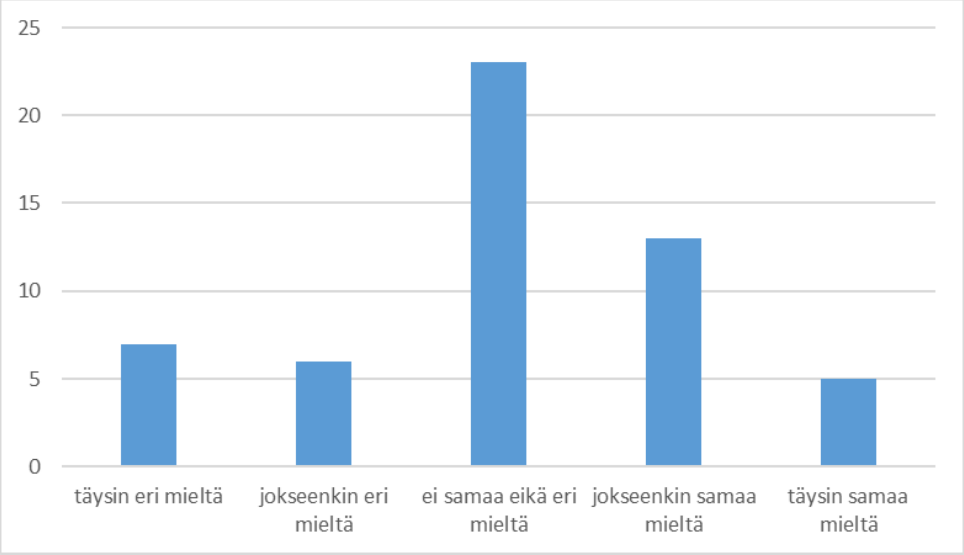
KUVA 18. Oppilaiden ja opettajien kyberturvallisuusosaaminen

Osana kyselyä myös selvitettiin, onko lukiossa tietoturvasta vastaava henkilö, jonka tehtävänä on huolehtia koulun henkilöstön ja oppilaiden tietoturvallisesta osaamisesta ja käyttäytymisestä. Tulokset osoittavat, että tässä on merkittäviä lukiokohtaisia eroja (kts. kuva 17).

Opettajia pyydettiin arvioimaan oppilaiden ja henkilöstön tietämystä laitteistojen ja opiskeluun liittyvien palvelujen tietoturvallisesta käytöstä. Arviointi tapahtui asteikolla 1–5. Keskiarvoksi muodostui 3,05 (kts. kuva 18). Tulokset osoittavat, että vastanneet opettajat suhtautuvat keskimääräisesti melko neutraalisti opettajien ja oppilaiden tietämykseen laitteistojen ja opiskeluun liittyvien palvelujen tietoturvallisesta käytöstä.



KUVA 19. Opetussuunnitelman ohjeiden selkeys kyberturvallisuuden opettamisen osalta

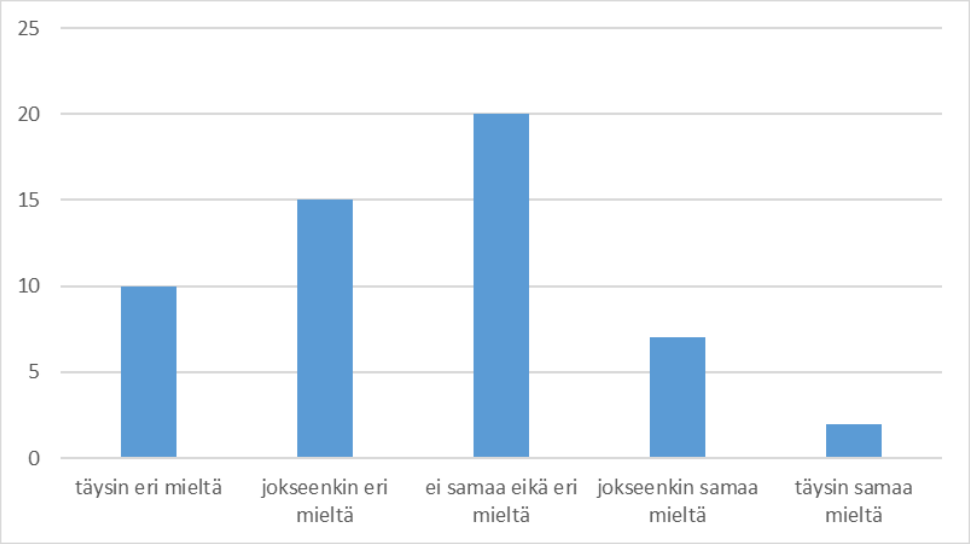


KUVA 20. Opettajien tietämyksen ja osaamisen taso kyberturvallisuuden opettamisessa

Opettajia pyydettiin arvioimaan asteikolla 1–5, miten selkeästi nykyinen opetussuunnitelma sisältää ohjeita kyber- ja tietoturvallisuuden opettamiseksi. Keskiarvoksi muodostui 1,96 (kts. kuva 19). Alhainen keskiarvo osoittaa, että vastanneet opettajat eivät pidä opetussuunnitelman ohjeita selkeinä kyber- ja tietoturvallisuuden opettamisen osalta.

Opettajat suhtautuivat keskimäärin melko neutraalisti omiin valmiuksiinsa sisällyttää kyberturvallisuutta osana opetustaan. Arviointi tapahtui asteikolla 1–5. Keskiarvoksi muodostui 3,06. Opettajiin, jotka vastasivat asteikolla 4–5 (18 kpl) lukeutuu kahdeksan

opettajaa, jotka opettavat muun muassa tieto- ja viestintäteknologiaa. Lisäksi opettajat, jotka vastasivat väliltä 4–5 edustavat useita eri kaupunkeja ja oppiaineita. Yleisimmät oppiaineet näiden opettajien keskuudessa ovat matematiikka, historia, yhteiskuntaoppi ja fysiikka. Muitakin oppiaineen edustajia on kuten biologia, maantiede, musiikki ja terveystieto. Myös opettajat, jotka vastasivat väliltä 1–2 edustavat useaa eri kaupunkia ja oppiainetta (kts. kuva 20).



KUVA 21. Täydennyskoulutuksen saatavuus

Kyberturvallisuuteen liittyvän täydennyskoulutuksen saatavuuteen suhtauduttiin varauksellisesti. Arviointi tapahtui asteikolla 1–5. Keskiarvoksi muodostui 2,55. Yhdeksän opettajaa, jotka antoivat vastauksen väliltä 4–5 edustavat kuutta eri kaupunkia ja useaa eri oppiainetta. Näistä yhdeksästä neljä opettaa muun muassa tieto- ja viestintäteknologiaa. Aineistosta ei käy ilmi, että tietyn kaupungin opettajat kokisivat, että täydennyskoulutusta olisi saatavilla keskimääräistä paremmin. Lisäksi opettajat, jotka antoivat arvosanan väliltä 1–2 edustavat useita eri kaupunkeja ja oppiaineita (kts. kuva 21).

3.6 Oppiainekohtaisia esimerkkejä

Opettajat saivat halutessaan kertoa tarkemmin, miten kyberturvallisuus näkyy heidän opetuksessaan. Tulokset osoittavat, että kyberturvallisuuden opetusta sisällytetään useissa eri oppiaineissa ja kursseissa, vaikka suoraan kyberturvallisuuteen/tietoturvallisuuteen/digitaaliseen turvallisuuteen ja sen opettamiseen opetussuunnitelma ei ota oppiainekohtaisesti merkittävästi kantaa. Osa vastauksista myös osoittaa, että kyberturvallisuus ja sen opettaminen eivät näyttäydy kaikille läheiseltä asialta eikä välttämättä tarpeelliseltakaan.

Tässä on listattu lainauksina opettajien kertomat esimerkit:

Historia ja yhteiskuntaoppi

”Osana yhteiskuntaoppia puhutaan kyberuhkakuvista, kyberturvallisuudesta, hybridisodasta jne. Tiedonvälitys, media- ja lähdekriittisyys, tekijänoikeudet jne.”

”Käsittelen aihetta modernin maailman ongelmien käsittelyssä historialliselta kannalta ja puhuessani kylmän sodan ajan vakoilusta, jota vertaan opiskelijoille nykyajan tilaan. Pyrin pitämään opetussisältöni ajankohtaisena ja antamaan esimerkkejä ajan tasalla olevien artikkeleiden ja materiaalien avulla. Ohjeistan myös opiskelijoita netin käytössä tietolähteenä ja esimerkiksi tekijänoikeus/plagiointikysymyksissä/lähdekriittisessä tiedonhaussa, tämä osuus sisältää myös huomattavan osan tietoturva-aiheiden pohdintaa”.

”Yhteiskuntaopin opettajana käsittelen YH3-kurssilla osana turvallisuuspolitiikan teemakokonaisuutta kyberturvallisuutta sekä institutionaalisella tasolla että yksilötasolla. Näytän usein esimerkiksi kotimaisen Team Whack-sarjan lyhyitä jaksoja arkisina esimerkkeinä. Historian opinnoissa HI2-kurssin loppuosassa käsitellään puolestaan keskinäisriippuvuuden maailmaa ja nykyhetken uhkakuvia, ja näihin kyberturvallisuus kytkeytyy erityisen luontaisesti. Tässä liikutaan lähtökohtaisesti valtiollisella tasolla”.

Maantiede

”Maantieteessä opetetaan riskien maantieteessä kyberriskeistä. Myös GPS-paikannuksen yhteydessä puhutaan näistä riskeistä”.

Biologia

”Biologiassa tästä puhutaan mm. DNA-testien ja yksilöntunnistuksen yhteydessä”.

Terveystieto

”Tehdessämme tehtäviä/projekteja jne. otan puheeksi mitä itsestään kannattaa julkaista, miten salasanojaan kannattaa käyttää jne.”

”Terveystiedossa puhutaan kyberturvallisuudesta mm. terveyteen liittyvissä tietokannoissa ja potilastietojärjestelmissä, tutkimustulosten säilömisessä ja seksuaalisen häirinnän käsittelyn yhteydessä.”

”Terveystiedon tunnilla kerron, että eivät laittaisi mitään sellaisia kuvia nettiin, joita ei haluaisi siellä olevan (esim. seksuaalisuuteen ja alastomuuteen liittyen), kerron myös, että ei voi levittää muista kuvia netissä. Kerron mistä saa apua, jos joutuu rikoksen uhriksi. Joskus poliisi vierailee kertomassa turvallisesta nettikäyttäytymisestä ja olemme myös joku kerta katsottu poliisin videon nettiturvallisuuteen liittyen ja katsomme riku.fi videoita, millaisia tilanteita/rikoksia voi tapahtua esim. seksuaaliterveyteen tai kiusaamiseen liittyvissä tapauksissa. Pyydän keksimään monipuolisia salasanoja, kun kirjaudumme esim. oppikirjoihin ja merkitsemään ne itselle muistiin.”

Tieto- ja viestintäteknologia

”Opetan myös tietotekniikkaa, siellä käsitellään salasanojen, omien tietojen antamisen ym. näkökulmasta.”

”Opetan koulussani lukion 1. luokkalaisille tietokoneen käyttötaitoja, otamme uudet koneet haltuun. Kurssi on osaltani vain puolet yhden opintopisteen yhteismäärästä ja kurssi sijoittuu heti ensimmäiseen periodiin. Kyberturvallisuutta ehtii sivuta vain hyvin pienen määrän ohessa. Samalla tavalla opetan peruskoulussa 7-luokan TVT-tunnit, siellä

ehdimme hieman paremmin sivuta asiaa. Resurssit ovat niin minimaaliset ja asiaa on paljon, jota pitää ehtiä käydä kurssin aikana. Erittäin tärkeä asia, johon pitäisi panostaa enemmän.”

Matematiikka ja fysiikka

”Silloin tällöin jutellaan salasanoista ja joskus tulee eteen tilanteita, joissa opiskelijan tili on kaapattu. Näissä yleensä kaappausyritys on kuopattu ennen kuin ehdimme edes reagoimaan tilanteeseen.”

Opinto-ohjaus

”Olen lukion opinto-ohjaaja. Opo joutuu tekemään runsaasti työtä sähköisten asiakirjojen parissa ja mm. siksi kyberturvallisuus olisi tärkeää myös opinto-ohjauksessa.”

Psykologia

”Kurssilla pyrin myös nostamaan tietoisuutta median toiminnasta ja keinoista, jotta median käyttöturvallisuus kasvaisi. Muuten pyrin toimimaan esimerkkinä + huomioimaan turvallisuusnäkökulmia esim. medioissa (evästeiden käyttö, asioiden kyseenalaistaminen jne.).”

3.7 Kyberturvallisuuden opetuksen kehittäminen lukio-opetuksessa

Kyberturvallisuuden opetuksen kehittämistä lukio-opetuksessa voidaan lähestyä usealla tavalla. Tässä raportissa kartoitettiin opettajien näkemystä siitä tulisiko kyberturvallisuuden opetus jollakin tavoin sisällyttää jokaiseen oppiaineeseen vai tulisiko se eriyttää osaksi esimerkiksi tietotekniikan opetusta. Tutkimuksessa esille nousi kolme mallia, jotka eivät ole toistensa poissulkevia:

Malli 1: Digitaalinen turvallisuus lukion kaikille osa-alueille

Tämä kehityssuunta voitaisiin toteuttaa nykyisen opetussuunnitelman perusteella vaikuttamalla laaja-alaisen osaamisen käsitteeseen. Tällä hetkellä laaja-alainen osaaminen muodostuu kuudesta osa-alueesta ja sen osa-alueet muodostavat kaikkien oppiaineiden yhteiset tavoitteet. Lisäämällä yhdeksi omaksi osa-alueeksi **digitaalinen turvallisuus**, tulisi kyberturvallisuus näkyväksi lukion kaikille osa-alueille. Tätä näkökulmaa voidaan perustella sillä, että digitaalinen turvallisuus ja sen merkitys on kasvanut yhteiskunnan kaikilla sektoreilla. Lisäksi se on koulutusalana poikkitieteellinen ja se käy ilmi myös kyselyn vastauksissa. Opettajat kertoivat useiden oppiaineiden puolesta esimerkkejä siitä, miten kyberturvallisuus näkyy osana heidän opetustaan. Tämän lisäksi yksi vastaaja nosti esille kyberturvallisuuden merkityksen opinto-ohjaajan työssä.

Malli 2: Digitaalinen turvallisuus osaksi nykyisten laaja-alaisen osaamisen osa-alueita

Pienempi rakenteellinen muutos, jolla digitaalinen turvallisuus tulisi näkyvämmin esille lukion kaikille osa-alueille olisi sisällyttää digitaalinen turvallisuus johonkin nykyistä osa-alueista.

Malli 3: Digitaalinen turvallisuus osana tieto- ja viestintäteknologian opetusta

Tämä kehityssuunta voitaisiin toteuttaa lisäämällä tieto- ja viestintäteknologian opetuksen määrää lukioissa. Tieto- ja viestintäteknologian opetukseen sisällytettäisiin yhtenä osa-alueena digitaalinen turvallisuus. Suurin osa vastanneista tieto- ja viestintäteknologian opettajista ilmoitti sisällyttävänsä digiturvallisuutta osana opetustaan. Tämä kehityssuunta vaatii lisäresursseja. Seuraaviin seikkoihin tulee kiinnittää huomiota:

1. Tieto- ja viestintäteknologian opetuksen saatavuutta parannetaan lukioissa ja osana sen opetusta käsiteltäisiin myös digitaalista turvallisuutta
2. Opettajille täytyy varmistaa mahdollisuus täydennys kouluttautua tieto- ja viestintäteknologian opettajaksi
3. Täydennyskoulutuksessa tulisi käsitellä myös digitaalista turvallisuutta ja sen opettamista

Lisäksi yksi kehityssuunta on selvittää mahdollisuutta lisätä ICT-alan erityislukioita Suomeen tai vaihtoehtoisesti mahdollisuutta lisätä ICT-alan linjoja jo olemassa oleviin lukioihin.

Digitaalisen turvallisuuden opetuksen sisällyttäminen jollakin tavoin jokaiseen oppiaineeseen vaatii lukio-opetukseen lisäresursseja. Erityisesti yhden kokonaisen osa-alueen lisääminen laaja-alaiseen osaamiseen käsitteeseen vaatisi merkittäviä muutoksia opetussuunnitelmaan. Lisäksi opettajille tulisi varmistaa mahdollisuus täydennyskoulutukseen sitä halutessaan, jotta osa-alueen toteuttaminen oppiaineen opetuksessa olisi kaikille tasapuolisesti mahdollista.

3.8 Johtopäätökset

Lukion opetussuunnitelmassa on määritelty laaja-alainen osaaminen ja siihen liittyvät osa-alueet. Nämä osa-alueet muodostavat lukion oppiaineiden yhteiset tavoitteet. Laaja-alainen osaaminen luo muun muassa edellytykset tiedoille ja taidoille, joiden avulla voidaan hallita muutosta digitalisoituvassa ja yhä kompleksisemmassa maailmassa. Lukion opetukselle on määritelty useita yleisiä tavoitteita. Yhtenä tavoitteena on ohjata yksilöä harjaannuttamaan ymmärrystään tieto- ja viestintäteknologiasta sekä hyödyntämään sitä tarkoituksenmukaisesti, vastuullisesti ja turvallisesti niin itsenäisessä kuin yhteisöllisessä työskentelyssä.

Havainnot opetussuunnitelmasta kyberturvallisuuden/tietoturvallisuuden/digitaalisen turvallisuuden osalta voidaan jakaa kolmeen kategoriaan:

1. tieto- ja viestintäteknologiaa ja digitaalisia toimintaympäristöjä hyödynnetään oppiaineiden opetuksessa
2. Parissa oppiaineessa huomioidaan suoraa kyberturvallisuuteen/tietoturvallisuuteen/digitaaliseen turvallisuuteen linkittyviä asioita
3. Oppiaineissa harjoitellaan taitoja, joita tarvitaan myös turvalliseen toimintaan digitaalisessa ympäristössä kuten lähdekritiikki ja medialukutaito

Tutkimuksen tulokset osoittavat, että vastanneet opettajat eivät koe opetussuunnitelman sisältävän selkeitä ohjeita kyberturvallisuuden opettamisen osalta. Opettajat suhtautuivat keskimäärin melko neutraalisti omiin valmiuksiinsa sisällyttää kyberturvallisuutta osana opetustaan. Opettajien mielipiteet jakaantuivat sen osalta tulisiko kyberturvallisuuden opetus sisällyttää jollakin tavoin lukion kaikille osa-alueille vai tulisiko kyberturvallisuuden opetus eriyttää osaksi esimerkiksi tietotekniikan opetusta. Suurin osa

vastanneista tieto- ja viestintäteknologian opettajista sisällyttää opetukseensa kyberturvallisuuden opetusta. Vastaukset hajaantuivat selkeästi, kun kysyttiin sisällyttääkö opettaja kyberturvallisuuden opetusta oppiaineen sallimissa raameissa. Lisäksi kyberturvallisuuden täydennyskoulutuksen saatavuuteen suhtauduttiin varauksellisesti.

Opettajien havainnollistamat esimerkit kyberturvallisuuden sisällyttämisestä oppiaineen opetukseen osoittaa, että se on yksi osa-alue useissa eri oppiaineissa ja kursseissa. Toisaalta kuten aikaisemmin on todettu, niin opettajien vastaukset hajaantuivat selkeästi sen osalta, että sisällyttävätkö he kyberturvallisuuden opetusta oppiaineen sallimissa raameissa. Tällä hetkellä vaikuttaa siis siltä, että kyberturvallisuutta on sisällytetty useassa tapauksessa monipuolisesti oppiaineen opetukseen, mutta tilanteessa on selkeää vaihtelua opettajien välillä.

Kyberturvallisuuden opetuksen lisäämistä ja kehittämistä voidaan lähestyä useasta eri näkökulmasta. Tässä raportissa esitettiin kaksi kehityspolkua, jotka eivät ole toistensa poissulkevia. Ensimmäisessä kehityspolussa kyberturvallisuuden opetusta integroidaan osaksi kaikkia oppiaineita vaikuttamalla laaja-alaiseen osaamiseen ja sen sisältöön. Toisessa vaihtoehdossa kyberturvallisuuden opetusta lisätään ja kehitetään parantamalla tieto- ja viestintäteknologian opetuksen saatavuutta ja huomioidaan kyberturvallisuus osana sen opetusta.

Lähteet

Opetushallitus (2019). Lukion opetussuunnitelman perusteet 2019. https://www.oph.fi/sites/default/files/documents/lukion_opetussuunnitelman_perusteet_2019.pdf

4 Kyberturvallisuuden opetus ammatillisessa koulutuksessa

4.1 Ammatillinen koulutusjärjestelmä Suomessa

Suomessa ammatillista koulutusta ohjaa laki ammatillisesta koulutuksesta (Finlex, 2017a), jota täsmennetään asetuksella 673/2017 (Finlex, 2017c), sekä muut lakiin liittyvät asetukset, erityisesti opetus- ja kulttuuriministeriön asetus ammatillisen koulutuksen tutkintorakenteesta (Finlex, 2017b), jota on viimeksi päivitetty asetuksella 596/2021. Lain mukaan ammatillisia tutkintoja ovat perustutkinnot (PT), ammattitutkinnot (AT) ja erikoisammattitutkinnot (ET). Asetus ammatillisen koulutuksen tutkintorakenteesta määrittelee edelleen, mitkä tutkintonimikkeet ovat käytössä millekin ammatilliselle tutkinnolle. Opetushallitus puolestaan määrää lain 531/2017 15 § perusteella tutkinnon perusteet, jotka sisältävät muun muassa, mitkä osaamisalueet sisältyvät pakollisina ja valinnaisina kuhunkin tutkintonimikkeeseen.

Tutkintojen mitoituksen peruste on osaamispiste. Osaamispisteen laajuutta ei varsinaisesti ole laissa määritelty, vaan osaamispisteiden määrä määräytyy sen perusteella, mikä on tutkinnon osan kattavuus, vaikeusaste ja merkittävyys suhteessa koko tutkintoon (531/2017 12 §). Koko tutkinnon tulee toisaalta vastata laajuudeltaan lukion oppimäärän laajuutta (531/2017 15 §). Määritelmää tarkennetaan 1.8.2022 voimaan tulevalla valtioneuvoston asetuksella 583/2021 (Finlex, 2021), joka määrittele, että laajuuden arvioinnin lähtökohtana käytetään 12 tuntia opetusta ja ohjausta osaamispistettä kohti, mikäli opiskelijalla ei ole aiemmin hankittua osaamista tutkinnon osan suorittamiseksi.

Ammatillisen perustutkinnon laajuus on 180 osaamispistettä, ammattitutkinnon 120, 150 tai 180 osaamispistettä, ja erikoisammattitutkinnon 160, 180 tai 210 osaamispistettä. Perustutkintoon sisältyy 35 osaamispistettä yhteisiä tutkinnon osia, jotka koostuvat viestintä- ja vuorovaikutusosaamisesta, matemaattis-luonnontieteellisestä osaamisesta sekä yhteiskunta- ja työelämäosaamisesta.

Ammatillinen perustutkinto tuottaa laaja-alaiset ammatilliset perusvalmiudet sekä erikoistuneempaa osaamista vähintään yhdeltä osa-alueelta. Ammattitutkinto sisältää perustutkintoa syvällisempää osaamista tai kohdistuu rajatumpiin työtehtäviin. Erikoisammattitutkinto sisältää edelleen ammattitutkintoa syvällisempää tai monialaista osaamista. (https://www.oph.fi/fi/koulutus-ja-tutkinnot/tutkintorakenne)

Tutkinnon osien suorittaminen perustuu näyttöihin, joissa osaaminen osoitetaan tekemällä käytännön työtehtäviä aidoissa työtilanteissa ja työprosesseissa (537/2017 52 §). Haastatelluissa ammatillisissa oppilaitoksissa perustutkinnon osaamiskokonaisuuksia opetetaan pääasiassa oppilaitoksessa, ammatti- ja erityisesti erikoisammattitutkinto taas suoritetaan pääasiassa työpaikalla tapahtuvina näyttöinä.

Suomessa on yhteensä 156 ammatillista koulutusta antavaa oppilaitosta. Näistä 30 % (43 kpl) järjestää ICT-alan opetusta (taulukko 1).

Taulukko 1. Tieto- ja viestintätekniikan ammatillisen opetuksen järjestäjät

Ael-Amiedu Oy	Optima Samkommun
Ammattiopisto Spesia Oy	Oulun kaupunki
Axxell Utbildning Ab	Oulun seudun koulutuskuntayhtymä
Careeria Oy	Pohjois-Karjalan koulutuskuntayhtymä
Espoon Seudun koulutuskuntayhtymä	Raahen koulutuskuntayhtymä
Etelä-Savon Koulutus Oy	Raision seudun koulutuskuntayhtymä
Helsingin kaupunki	Rovaniemen koulutuskuntayhtymä
Helsinki Business College Oy	Salon seudun koulutuskuntayhtymä
Hyria Koulutus Oy	Sasky koulutuskuntayhtymä
Jokilaaksojen koulutuskuntayhtymä	Satakunnan koulutuskuntayhtymä
Jyväskylän koulutuskuntayhtymä	Savon koulutuskuntayhtymä
Järviseudun koulutuskuntayhtymä	Seinäjoen koulutuskuntayhtymä
Kajaanin kaupunki	Suupohjan koulutuskuntayhtymä
Kemi-Tornionlaakson koulutuskuntayhtymä Lappia	Svenska framtidsskolan i Helsingforsregionen Ab
Keski-Pohjanmaan koulutusyhtymä	Tampereen kaupunki
Keski-Uudenmaan koulutuskuntayhtymä	Turun kaupunki
Kiipulasäätiö	Vaasan kaupunki
Kotkan-Haminan seudun koulutuskuntayhtymä	Valkeakosken seudun koulutuskuntayhtymä
Koulutuskuntayhtymä Tavastia	Vantaan kaupunki
Kouvolan kaupunki	Ylä-Savon koulutuskuntayhtymä
Luksia, Länsi-Uudenmaan koulutuskuntayhtymä	Äänekosken ammatillisen koulutuksen kuntayhtymä
Länsirannikon Koulutus Oy	

4.2 Kyberturvallisuuden opetus ammatillisessa koulutuksessa

Kyberturvallisuuden osaamisalueita sisältyy ainoastaan tieto- ja viestintätekniikan perus-, ammatti- ja erikoisammattitutkintoihin, kaikkiin näihin valinnaisena osaamisalueena. Perustutkinnossa opiskelija voi suorittaa tutkinnon osan Kyberturvallisuuden ylläpitäminen, jonka laajuus on 30 osaamispistettä. Ammattitutkinnon osana on mahdollista suorittaa Kyberturva-asiantuntijana toimiminen, jonka laajuus on 40 osaamispistettä. Erikoisammattitutkinnon osana voi suorittaa Tietoturva-analyytikkona toimimisen, laajuudeltaan 60 osaamispistettä. Tutkinnon osien lisäksi kyberturvallisuusosaamista on haastattelun kohteena olleissa oppilaitoksissa sisällytetty myös muille tieto- ja viestintätekniikan opintojaksoille silloin, kun se on esimerkiksi toimivan ja turvallisen järjestelmän toteuttamisen kannalta tarpeellista. Koska kyberturvallisuus on valinnainen tutkinnon osa, jotkin haastatellut oppilaitokset eivät tarjonneet sitä lainkaan.

ICT-alan perustutkinnon on vuosien 2011–2020 välillä vuosittain suorittanut keskimäärin 2075 opiskelijaa (2082 vuonna 2020), ammattitutkinnon 186 (312 vuonna 2020) ja erikoisammattitutkinnon 12 (27 vuonna 2020) (Vipunen, 2022). Tutkintonimike tieto- ja viestintätekniikka on tullut käyttöön vuonna 2020, aiempi vastaava nimike oli tieto- ja tietoliikennetekniikka. Tarkkaa tietoa siitä, kuinka moni opiskelija suorittaa kyberturvallisuuden osaamisalueita, ei ole saatavissa. Ammatti- ja varsinkin erikoisammattitutkinnon vähäisten suoritusmäärien vuoksi selvityksessä keskitytään perustutkintoon.

4.2.1 Kyberturvallisuus tieto- ja viestintätekniikan tutkintojen perusteissa

Perustutkinto

Tällä hetkellä opiskelun perustana ovat tutkinnon perusteet 2020: Osa 16, Kyberturvallisuuden ylläpitäminen (OPH-2596-2019). Ne sisältävät seuraavat ammattitaitovaatimukset:

- Opiskelija käyttää kyberuhkien hallinta- ja suojautumiskeinoja
  - Suojaa laitteen päivityksillä ja ohjelmistoilla,
  - Hallitsee laitetta hallintatyökaluilla,
  - Vertailee eri salausmenetelmiä ja valitsee tarkoituksenmukaisen salausmenetelmän.
- Opiskelija hallitsee kyberturvariskejä
  - Valvoa tietoverkkoa hyödyntämällä erilaisia analysointityökaluja,
  - Skannata haavoittuvuuksia tarkastelun kohteena olevasta sovitusta verkosta,
  - Varmentaa järjestelmien haavoittuvuuksia,
  - Tekee kehittämisehdotuksia kyberturvan parantamiseksi.
- Opiskelija edistää kyberturvallisuusratkaisuja
  - Tuntee tietoturvaan- ja tietosuojaan liittyvät lait, asetukset sekä muut viranomaismääräykset,
  - Havainnollistaa kyberuhkia ja niitä vastaavia riskejä,
  - Noudattaa työtehtävissään tietoturvaohjeita,
  - Opastaa kyberturva- tai tietosuoja-asioissa.

Tutkinnon perusteet 2022 osa 16, *Kyberturvallisuuden ylläpitäminen* (OPH-4948-2021) astuu voimaan 1.8.2022 alkaen. Kyberturvallisuuden ylläpitäminen ei sisällä muutoksia aiempiin perusteisiin. Osaamisen arvioinnin ja arvosanojen kriteerit on määritelty ainoastaan yleisellä, kaikille tutkinnon osille yhteisellä tasolla.

Haastateltavat pitivät kyberturvallisuuteen liittyviä tutkinnon perusteita hyvänä lähtökohtana opetukselle. Kyberturvallisuuden vaatimusten katsottiin olevan abstraktimpia kuin monet muut tieto- ja viestintätekniikan perusteet. Tätä pidettiin yleisesti hyvänä asiana, koska se mahdollistaa opetuksen sisältöjen sovittamisen myös muuhun opetukseen sekä ajan tasalla pitämisen. Perusteita pidettiin kuitenkin niin vaativina, että osaamisen osoittamiseen näyttöinä työpaikoilla ei juurikaan ole mahdollisuuksia, vaan näytöt suoritetaan oppilaitoksessa. Esimerkkeinä tällaisista osaamisista mainittiin salausmenetelmien valinta, tietoverkon valvonta sekä haavoittuvuuksien skannaus.

4.2.2 Ammattitutkinto

Tutkinnon perusteet 2021: Osa 6, Kyberturva-asiantuntijana toimiminen (OPH-2639-2020) sisältää seuraavat ammattitaitovaatimukset. Opiskelija osaa

- toimia kyberturvatehtävissä,
- testata kyberturvan,
- arvioida ja kehittää kyberturvallisuusratkaisuja.

Tutkinnon perusteet määrittelee lisäksi hyväksytyn suorituksen kriteerit osaamisen arviointia varten. Opiskelija

- huomioi kaikessa toiminnassaan etiikan ja vaitiolovelvollisuuden sekä alan säädökset,

- seuraa kyberuhkien yleistä kehittymistä,
- hyödyntää erilaisia käyttöjärjestelmiä, ohjelmistoja tai muita testausvälineitä,
- konfiguroi testaamisessa käytettäviä ohjelmia,
- tutkii asiakkaan tietojärjestelmän tietoturva-aukot ja haavoittuvuudet,
- suorittaa tutkimuksen uudestaan korjaustoimenpiteiden jälkeen,
- raportoi havaitut haavoittuvuudet ja puutteet,
- laatii priorisoidun toimenpidelistauksen, jolla havaitut haavoittuvuudet ja puutteet voidaan korjata.

Ammattitutkinnon perusteista tehtiin samoja huomioita kuin perustutkinnosta. Perusteita pidettiin sopivan laaja-alaisina ja abstrakteina. Vastaavasti haasteet olivat samanlaisia, näyttöpaikkojen löytäminen työelämässä ei ole suoraviivaista.

4.2.3 Erikoisammattitutkinto

Tutkinnon perusteet 2021: Osa 3, Tietoturva-analyytikkona toimiminen, (OPH-2640-2020) sisältää seuraavat ammattitaitovaatimukset. Opiskelija osaa

- huomioida tiedon- ja riskienhallinnan,
- suunnitella ja hallita organisaation tietojärjestelmien käyttöoikeuksia.

Tutkinnon perusteet määrittelee lisäksi hyväksytyn suorituksen kriteerit osaamisen arviointia varten. Opiskelija

- huomioi kaikessa toiminnassaan etiikan ja vaitiolovelvollisuuden sekä alan säädökset,
- seuraa tietoturvaan liittyvien ratkaisujen kehitystä,
- priorisoi tiedon arvoa ja määrittää toimintakriittisen tiedon saatavuuden ja eheyden,
- hankkii ja testaa erilaisia tiedon suojaamisratkaisuja,
- ottaa huomioon fyysisen turvallisuuden osana tiedon ja riskien hallintaa,
- ylläpitää organisaation tietoturvaan liittyviä ohjeistuksia,
- suunnittelee tietoturvapoikkeamien hallintatapoja ja poikkeamista palautumisen,
- suunnittelee toiminnan jatkuvuuden tietoturvapoikkeamien jälkeisissä tilanteissa,
- osallistuu tietoturvaryhmän toimintaan ja riskienhallinnan suunnitelmien laadintaan,
- suunnittelee ja hallitsee organisaation tietojärjestelmien käyttöoikeuksia,
- suunnittelee ihmisten ja laitteiden tunnistamista ja todentamista,
- suunnittelee järjestelmien ja tietojen näkyvyyksiä ja käyttöoikeuksia,
- suunnittelee käyttöoikeuksien ja käyttöoikeuksien provisioinnin elinkaaren.

Erikoisammattitutkinnon suoritusmäärät olivat haastatelluissa oppilaitoksissa verrattain pieniä, joten niistä ei voi tehdä yleistyksiä tutkinnon osien soveltuvuudesta.

4.3 Tutkimuksen toteutus

4.3.1 Kysely

Selvitys käynnistettiin identifioimalla ammatilliset oppilaitokset, jotka tarjoavat ICT-koulutusta. Prosessi jakaantui kolmeen vaiheeseen.

Selvityksen pohjana käytettiin Opintopolku-palvelua, jossa hakusuodattimina käytettiin termejä “ammatillinen koulutus” ja koulutusala “ICT”. Hakukriteereillä löytyi viisi ammatillista perustutkintoa otsikolla “Elektroniikka-asiantuntija. ICT-asentaja”. Nämä viisi organisaatiota olivat Varia, Vamia, Sedu Lapua, Sedu Seinäjoki, Stadi Ammatti ja Aikuisopisto. Haku toistettiin huhtikuussa 2022, jolloin haku tuotti 54 koulutuksen tarjoajaa. Näistä yksi tarjoajista Sasky näkyy viitenä eri hakukohteena erillisten koulutuslokaatioiden vuoksi. Ero hakutuloksissa johtuu tietojen hakuhetkestä, sillä Opintopolku-palvelussa näkyy vain haettavina olevat koulutukset. Tämä hakumenetelmän tuottama informaatio on riippuvainen hetkestä, jolloin haku tehdään.

Toinen koulutustarjoajien haku toteutettiin palvelusta ammattikoulut.fi (2021). Koulutusalan hakuehtona käytettiin termiä “tietotekniikka/ohjelmointi”. Haulla saatiin 54 tutkintoa, joita tarjoavat 28 eri oppilaitosta. Tämäkään lista ei ole täydellinen, koska esimerkiksi TAI, joka tarjoaa ICT-alan koulutusta ei löytynyt palvelusta. Huomioitavaa on, että palvelusta löytyy koulutuksentarjoajia, jotka eivät löydy Opintopolku-palvelusta. Esimerkkinä tällaisesti toimijasta on Suomen Yrittäjäopisto.

Kolmas haku tehtiin Opetushallinnon tilastopalvelun tietokannasta (Vipunen, 2021). Haku tehtiin v. 2020 tiedoista. Hakuterminä käytetiin Koulutusalaa “Tietojenkäsittely ja Tietoliikenne (ICT). Haun mukaan 59 oppilaitosta tarjoaa ICT-koulutusta, mutta palvelusta ei saa tietoa mitä nämä oppilaitokset ovat. Asian selvittämiseksi tehtiin toinen haku “koulutuksen järjestäjiä”-suodattimella, joka tuotti 156 oppilaitosta. ICT-koulutuksien järjestäjien (59 kpl) löytämiseksi analysoitiin kaikkien 156 oppilaitoksen verkkosivut. Analyysin perusteella löydettiin Suomesta 43 ammatillisen koulutuksen järjestäjää, jotka tarjoavat ICT-koulutusta. Koulutuksen järjestäjien verkkosivuilta kerättiin koulutuspäälliköiden tai tiimivastaavien yhteystiedot kyselyn lähettämistä varten.

Näiden 43 organisaation rehtoreille lähetettiin tutkimuslupapyyntö kyselyn toteuttamiseksi. Tutkimuslupaan saatiin 14 positiivista vastausta. Kysely lähetettiin 18 vastaanottajalle neljässätoista organisaatiossa. Kyselyn sisältö oli seuraava:

- Onko vastauksen antaja mukana toteuttamassa tieto-/kyber-/digitaalisen turvallisuuden koulutusta?
- Missä määrin ko. koulutusta tarjotaan ja milloin sen kouluttaminen on aloitettu eri tutkintotasoilla (PT/AT/EAT)?
- Onko vastaaja halukas osallistumaan teemahaastatteluun?

Vastauksia saatiin seitsemän, joista kaikki ilmoittivat halukkuutensa osallistua haastatteluun. Näistä toteutui lopulta viisi: Oulun Seudun Ammattiopisto, Omnia, Tavastia, Turun ammatti-instituutti, and Business College Helsinki.

4.3.2 Teemahaastattelut

Tutkimuksessa tehtiin viisi teemahaastattelua oppilaitoksille, jotka olivat kyselyssä ilmoittaneet halukkuutensa haastatteluun. Tässä tutkimuksessa teemat valittiin vastaamaan tutkimuksen tavoitteita ryhmän keskustelujen ja tehdyn ennakkohaastattelun perusteella. Teemoiksi valikoitui

1. kyberopetuksen toteutus oppilaitoksessa eri tasoilla (PT/AT/EAT), koulutuksen jakautuminen ja toteutus teoriaan ja käytäntöön sekä koulutuksen painottuminen teknologioihin tai esimerkiksi yksityisyyteen

2. tutkinnon perusteiden kattavuus kyberturvallisuuden osalta, eli millaisia asioita tulisi opettaa ja mitä alueita tulisi kattaa
3. opettajien koulutustarpeet kyberturvallisuuden osalta, millainen on nykytila, miten opettajia tuetaan, millaiset resurssit ovat, miten voitaisiin tukea opettajien osaamisen kehittämistä.

Teemahaastattelujen perusteella saatiin seuraavia havaintoja:

Opetuksen toteutus

Uudistetut tutkinnon perusteet ovat tulleet voimaan vuonna 2018, joten tällä hetkellä opetus on vielä siirtymässä uuden mallin mukaiseksi. Osa haastateltavista on antanut opetusta jo vanhojen perusteiden mukaisesti 15 osp:n ”Tietoturvan ylläpitäminen”-osana. Osa haastateltavista taas aloittaa koulutuksen vasta syksyllä 2022.

Perustutkinnot tehdään koulussa, tutkinnon harjoittelut mahdollisuuksien mukaan työelämässä. Ammatti- ja erikoisammattitutkinnot perustuvat enemmälti työelämässä tehtäviin näyttöihin kuitenkin niin, että niiden osana varmistetaan alemmat tutkinnon sisällön osaaminen. Uusien perusteiden mukaisia AT/EAT-tutkinnon suorittajia ei ole vielä luonnollisesti ollut paljoa, erityisesti AT-koulutuksia ollaan käynnistämässä. Yksittäisille opiskelijoille AT/EAT-koulutuksia ei ole mahdollista järjestää.

Kyberkoulutusta annetaan lähinnä IT-tuen, IT-asentajan ja tietoverkkoasentajan koulutuksissa. Koulutus annetaan joissakin oppilaitoksissa kahdessa 15 osp:n kokonaisuudessa, vaativampien ja enemmän teoriaa sisältävien osuuksien ollessa jälkimmäisessä osassa.

Perusteita käydään läpi useammassakin koulutuksissa, joissain oppilaitoksissa kaikki opiskelijat saavat pienen peruspaketin yhteisten opintojen osana. Haastatteluissa nousi esiin ajatus, että opetusta tulisi jatkossa integroida osaksi muuta opetusta. Esimerkiksi hyvinvointiteknologiassa tietoturvan koulutusta tulisi olla mukana.

Opetuksen sisältö ja tutkinnon perusteet

Tutkinnon perusteiden mukaiset vaatimukset ovat hyvin eritasoisia, osa on hyvinkin haastavia. Opettajien vapaus on melko laaja, etenkin vuoden 2018 perusteiden tuomaa väljyyttä pidettiin hyvänä asiana. Toisaalta se antaa mahdollisuuden sille, että syntyy koulukohtaisia eroja, kuinka syvällisesti asioita opetetaan. Perusteet eivät määrittele mitä käytännön osaamista opinnoissa tulee käsitellä. Alue on laaja ja erityisesti perustutkinnon suorittajat ovat vasta tulossa alalle. Perustutkinnon tavoitteena on antaa vahva pohja.

Työelämän vaatimukset elävät koko ajan, joten ajantasainen kommunikaatio siihen suuntaan on välttämätöntä. Suorien kontaktien myötä on mahdollista selvittää mitä tulisi opettaa. Opiskelijoista tulee tulevaisuuden ammattilaisia, joten koulutuksen ajantasaisuus on tärkeää, vaikka tietyt perusteet ovat muotoutuneet jo kauan sitten. Uhkien ja ongelmien ymmärtäminen on tärkeä osa osaamista. Kielitaitovaatimuksena on suomen lisäksi englanti, esimerkiksi haavoittuvuuksien todentamisessa.

Opetuksen toteutuksen vastattava myös opiskelijoiden tarpeita, nuoriso- ja aikuispuolella tulee lähestymistapojen olla erilaiset. Aikuispuolella on sisällöissä mahdollista ylittää tutkinnon perusteiden vaatimukset.

Opettajien koulutustarpeet

Opettajien kiinnostus oman osaamisensa kehittämiseen on välttämätöntä ja sitä tulee tukea, koko ajan kehittyvällä alalla myös itsensä ajan tasalla pitäminen ja kehittäminen on elinehto. Opettajien koulutukseen koettiin löytyvän resursseja, enemmän haasteita koettiin sopivien koulutusten löytämisessä. Esimerkiksi yksityisten koulutustarjoajien kurssit harvoin osuvat opettajien tarpeisiin kovin suoraan. Koulutusten tulisi jollain tavalla hyödyntää koko opetustiimiä. Koulutuksissa voisi hyödyntää sertifiointeja sekä olemassa olevia viitekehyksiä.

Opettajien mentorointi ja verkostoituminen koettiin tärkeäksi, niin työelämään kuin muiden alan opettajien kesken. Haasteena on, että vain harvassa oppilaitoksessa opettajat voivat keskittyä kyberturvallisuuden kouluttamiseen, vaan heillä on myös muiden alojen koulutusvastuita. Tällöin alan osaamisen kehittämiseen löytyvää aikaa on vastaavasti vähemmän.

Opettajien on mahdollista mennä oppilaitoksen kustantamana harjoitteluun työelämään. Arvio harjoittelun kestosta vaihteli suuresti, toisaalta koettiin, että jo päivän mittainen harjoittelu antaa lisäpontta, mutta toisaalta taas todettiin, että vasta noin 2–4 viikon mittaisessa harjoittelussa pääsee kokemaan arjen kunnolla. Harjoittelussa olisi syytä käydä 3–4 vuoden välein. Opettajien osallistumismahdollisuuksia alan tutkimukseen liittyviin ryhmiin tulisi selvittää. Opettajien rekrytointi on koko ajan haasteellisempaa. Ammattilaiset eivät ehkä näe opetusta omana alanaan. Työelämästä opetukseen siirtyvät ammattilaiset toisivat tuoretta tietoa mukanaan.

Harjoittelu

Harjoittelupaikkojen saatavuus koettiin haastavaksi. Työelämän odotukset koulutusta ja opiskelijoita kohtaan ovat usein kovemmat, mitä koulutuksen myötä kyetään tarjoamaan. Toisaalta työelämä ei välttämättä kykene tarjoamaan harjoittelussa sellaisia tehtäviä, joissa annettua koulutusta pääsisi hyödyntämään. Esimerkiksi salassapitosäädökset ja asiakkaiden kanssa tehdyt sopimukset saattavat luoda tilanteita, joissa opiskelijaa ei voida täysimittaisesti hyödyntää. Opiskelijoiden suorittamat sertifikaatit voisivat selventää opiskelijoiden osaamistasoa harjoittelupaikkojen suuntaan.

Harjoittelupaikan koon osalta saatiin ristiriitaisia vastauksia, osa vastaajista koki, että pienempi toimija kykenee huomioimaan paremmin opiskelijan mahdollisuudet ja työtehtävät voivat olla laaja-alaisempia. Osa taas koki, että isolla toimijalla resursointi on paremmin huomioitu. Ohjaus on erittäin oleellinen osa harjoittelua.

Ylipäätään tärkeäksi koettiin yhteydenpito mahdollisiin harjoittelupaikan tarjoajiin, minkä lisäksi koettiin, että harjoitteluja voisi tuotteistaa sekä niihin liittyvistä näytöistä voisi tiedottaa enemmän, mitä kautta myös paikkoja tulisi lisää. Mahdollisuuksia on paljon, harjoitteluja ei tehdä pelkästään alaan keskittyneillä toimijoilla, vaan esimerkiksi suurissa teollisuuslaitoksissa löytyy usein hyvin mahdollisuuksia harjoitteluille. Lisäksi tulisi muistaa, että myös yhdistykset voivat tarjota hyviä harjoittelupaikkoja. Hyvin suoritettu harjoittelu voi johtaa työpaikkaan samassa organisaatiossa. Vaikka harjoitteluja ei kyettäisi toteuttamaan työelämässä, on kaikilla oppilaitoksilla sekä opetus/laboratorioverkkoja sekä hallinnollisia verkkoja, joissa harjoitteluja voidaan toteuttaa. Laboratorioverkon ylläpitoa voidaan toteuttaa IT-ylläpito-opiskelijoiden harjoituksina.

Yhteistyö, yhdessä tekeminen

Alan opettajien ja oppilaitosten välinen yhteistyö koettiin monella osa-alueella tärkeäksi. Sitä kautta käytäntöjä voisi jakaa ja oppilaitokset voisivat esimerkiksi vertailuanalysoida toisiaan. Oppilaitokset eivät ole koulutusmielessä toistensa kilpailijoita. Yhdessä tekeminen ja esimerkiksi vuosittaiset fyysiset tapaamiset nousivat esiin. Vertailukohtana voi pitää Tradenomikoulutuksen päivät -tapahtumaa. Yhteistyölle tarvitaan jokin alusta tai foorumi. Koulutus/laboratorioympäristöjen rakentamisessa yhteistyölle nähtiin myös mahdollisuuksia. Yhteistyön kautta myös kontakteja yrityksiin voitaisiin jakaa.

Koulutusmateriaali

Ylen tuottama Team Whack nousi esille useassa haastattelussa. Sen jaksoja käytetään yleisesti osana opetusta. Sarjan tapa esittää asioita ja esille nostetut teemat innostavat opiskelijoita. Varjopuolena on, että todellisuuden työelämässä ei ole tarjolla näin vauhdikkaita tehtäviä. Kyberturvallisuuskeskuksen tuottamaa Kybersäätä käytettiin yleisesti uhkiin tutustumisessa. Koulutusmateriaalien tuottamisessa koettiin, että oppilaitosten välillä voisi olla yhteistyötä, koska tutkintojen perusteetkin ovat samat. Toisaalta tunnistettiin, että opettajat haluavat opettaa asiat omalla tyylillään. Ciscon materiaaleja käytetään yleisesti.

Opetuksen synkronointi AMK:jen kanssa

Haastattelussa mainittiin, että koulutusasteiden erot tulisi saada mahdollisimman pieniksi. Opintojaksojen sisältöjä tulisi suunnitella siten, että niillä voisi korvata ammattikorkeakoulujen ensimmäisen vuoden opintoja. Arvioitiin että perustutkinnossa oleva kyberturvallisuuden 30 osp:n kokonaisuus vastaisi noin 10–15 opintopistettä AMK:ssa.

Etä/hybridiopetus

Opiskelijat ovat IT-alan tulevia ammattilaisia, joten yleisesti nähtiin, että erilaisten etäopiskelukäytäntöjen hallitseminen on perusedellytys. Toisaalta koettiin, että näissäkin perustaidoissa on kehittämistä. Työelämässä asioita tehdään paljolti etänä, joten siinäkin mielessä koulutuksessa näitäkin taitoja tulee kehittää. Etäopetuksessa on myös parempi mahdollisuus saada alan asiantuntijoita kertomaan opiskelijoille työstään. Etäopiskelu vaatii opiskelijoilta paljon. Peruskoulussa etäopetuksessa olleiden opiskelutaidot ovat heikommat.

4.4 Johtopäätökset ja kehittämislinjauksia

Kyberturvallisuuskoulutusta annetaan lähinnä IT-tuen, IT-asentajan ja tietoverkkoasentajan koulutuksissa. Haastateltavat pitivät kyberturvallisuuteen liittyviä tutkinnon perusteita hyvänä lähtökohtana opetukselle. Kyberturvallisuuden vaatimusten katsottiin olevan abstraktimpia kuin monet muut tieto- ja viestintätekniikan perusteet. Tätä pidettiin yleisesti hyvänä asiana, koska se mahdollistaa opetuksen sisältöjen sovittamisen myös muuhun opetukseen sekä ajan tasalla pitämisen. Perusteita pidettiin kuitenkin niin vaativina, että osaamisen osoittamiseen näyttöinä työpaikoilla ei juurikaan ole mahdollisuuksia, vaan näytöt suoritetaan oppilaitoksessa.

Kyberturvallisuuden osaamisalueita sisältyy ainoastaan tieto- ja viestintätekniikan perus-, ammatti- ja erikoisammattitutkintoihin, kaikkiin näihin valinnaisena osaamisalueena. Suomalaisen kyberturvallisuusosaamisen kasvattamiseksi suositamme, että kyberturvallisuuden koulutuksesta tulee pakollinen osa ICT-koulutusta. Lisäksi opetusta tulisi jatkossa integroida osaksi kaikkea muuta ammatillista opetusta systemaattisesti.

Opettajien kiinnostus oman osaamisensa kehittämiseen on välttämätöntä ja sitä tulee tukea, koko ajan kehittyvällä alalla myös itsensä ajan tasalla pitäminen ja kehittäminen on elinehto. Korkeakouluille tulee myöntää resurssia järjestää jatkuvan oppimisen mahdollisuuksia ammatillisille opettajille. Opettajien tutustumista työelämään tulee edistää.

Oppilaitosten yhteistyötä opettajalta opettajalle on kehitettävä ja sille on luotava alusta ja foorumi. Yhteistyöllä on nähtävissä monia hyötyjä. Tutkintojen perusteiden ollessa samat, on samoja koulutusmateriaaleja mahdollista hyödyntää. Koulutusympäristöjen kehittämistä voidaan tehdä yhteistyönä. Ajantasaista tietoa teknologian kehittymisestä on helppo jakaa. Yhteistyössä koottujen valmiiden mallien myötä madaltuu myös koulutuksen aloittamisen kynnys muissa oppilaitoksissa.

Työelämäyhteistyötä tulee kehittää. Tietoisuutta eri tutkinnoista (PT/AT/EAT) ja niihin sisältyvistä harjoitteluista tulee jakaa työelämälle.

Lähteet

Ammattikoulut.fi (2021). Ammattikoulut. https://www.ammattikoulut.fi/ Haettu 21.9.2021.

Finlex (2017a). Laki ammatillisesta koulutuksesta. 11.8.2017/531.

Finlex (2017b). Opetus- ja kulttuuriministeriön asetus ammatillisen koulutuksen tutkintorakenteesta. 680/2017.

Finlex (2017c). Valtioneuvoston asetus ammatillisesta koulutuksesta. 673/2017.

Finlex (2021). Valtioneuvoston asetus ammatillisesta koulutuksesta annetun valtioneuvoston asetuksen muuttamisesta. 583/2021.

Opetushallitus (2019). Tieto- ja viestintätekniikan perustutkinnon perusteet. Määräys OPH-2596-2019.

Opetushallitus (2020a). Tieto- ja viestintätekniikan ammattitutkinnon perusteet. Määräys OPH-2639-2020.

Opetushallitus (2020b). Tieto- ja viestintätekniikan erikoisammattitutkinnon perusteet. Määräys OPH-2640-2020.

Opetushallitus (2021). Tieto- ja viestintätekniikan perustutkinnon perusteet.docx (sic). Määräys OPH-4948-2021.

Opetushallitus (2022). Tutkintorakenne. https://www.oph.fi/fi/koulutus-ja-tutkinnot/tutkintorakenne. Haettu 28.4.2022.

Opintopolku (2021) Opintopolku haku. https://opintopolku.fi/konfo/fi/. Haettu 20.9.2021.

Opintopolku (2022) Opintopolku haku. https://opintopolku.fi/konfo/fi/. Haettu 16.4.2021.

Vipunen (2021). Koulutuksenjärjestäjä- ja oppilaitosverkko. Opetushallinnon tilastopalvelu. https://vipunen.fi/fi-fi/ammatillinen/Sivut/Koulutuksen-j%C3%A4rjest%C3%A4j%C3%A4--ja-oppilaitosverkko.aspx. Haettu 23.9.2021.

Vipunen (2022). Ammatillisen tutkinnon suorittaneet. Opetushallinnon tilastopalvelu. https://vipunen.fi/fi-fi/_layouts/15/xlviewer.aspx?id=/fi-fi/Raportit/Ammatillinen%20koulutus%20-%20tutkinnot%20-%20koulutusala.xlsb. Haettu 29.4.2022

5 Kyberturvallisuuden opetus ammattikorkeakouluissa

Suomen ammattikorkeakouluja ohjaa ja mittaa Opetus- ja kulttuuriministeriön (OKM) asettamat ohjauksen alat (Eduuni-wiki, 2021). Kyseiset ohjauksen alat johdetaan ISCED -koulutusalaluokituksista, jotka ovat käytössä esimerkiksi UNESCO:n tilastoinnissa (UNESCO, 2015). Samoja koulutusalaluokituksia on myös Euroopan Unioni määritellyt käytettäväksi jäsenvaltioissaan (Eurostat, 2020). Tätä kautta myös Suomen kansallinen tilastokeskus noudattaa koulutusalamäärityksiä (Tilastokeskus, 2022a).

5.1 Tutkimusaineisto

Aineistonkeruun rajaukseksi valittiin tietojenkäsittely ja tietoliikenne. Hyvin todennäköisesti tutkinto- ohjelmat, jotka sisältävät kyberturvallisuutta, keskittyvät tämän ohjauksen alan alle. Vastaavasti opiskelijat, jotka valitsisivat esim. valinnaisiksi opinnoiksi kyberturvallisuuden, valitsisivat sen kyseisten tutkinto-ohjelmien opintojaksotarjonnasta. Yleistettynä tietojenkäsittely ja tietoliikenne sisältää ammattikorkeakouluissa seuraavia tutkinto-ohjelmia:

- Insinööri (AMK), Tieto- ja viestintätekniikan tutkinto-ohjelma
- Tradenomi (AMK), Tietojenkäsittelyn tutkinto-ohjelma

Lisäksi molemmista tutkinnoista on ylempi korkeakoulututkinto mahdollinen esim. insinööri (YAMK) ja tradenomi (YAMK). Näitä tutkintoja tuottavien tutkinto-ohjelmien nimet vaihtelevat huomattavasti enemmän jokaisessa ammattikorkeakoulussa.

Rajausta noudatettiin pääsääntöisesti ja pelkästään sillä tutkinto-ohjelmia sekä niiden opetussuunnitelmia oli paljon läpikäytäväksi. Rajauksesta kuitenkin poikettiin tapauskohtaisesti, jos havaittiin että kyberturvallisuutta löytyi jonkun (esim. turvallisuus) alan koulutuksessa selkeästi.

Opetussuunnitelmista keskityttiin lähtökohtaisesti tarkastelemaan opintojaksojen nimiä eikä esim. opintojaksokuvauksesta asti osaamistavoitteita tai sisältöjä. Satunnaista tarkastelua opintojaksokuvaukseen tehtiin opetussuunnitelma-aiheista, jotka saattoivat liittyä kyberturvallisuuteen. Rajauksesta perusteella tutkinto-ohjelman määrät rajautuivat taulukon 2 mukaisiksi. Näiden tutkinto-ohjelmien lisäksi tarkasteltiin kunkin ammattikorkeakoulun erikoistumis-, täydennys- ja muuntokoulutus tarjontaa.

Taulukko 2. Tutkinto-ohjelmien määrä rajauksen jälkeen

Tutkinto-ohjelma	**Määrä**	**Sisäänotto 2022**
Ylempi ammattikorkeakoulututkinto	29 kpl	711
Insinööri (YAMK)	17 kpl	412
Tradenomi (YAMK)	12 kpl	269
Poliisi (YAMK)	1 kpl	30
Ammattikorkeakoulututkinto	64 kpl	3830
Insinööri (AMK)	17 kpl	2035
Tradenomi (AMK)	12 kpl	1375
Poliisi (AMK)	1 kpl	400
Kandidatexamen	2 kpl	20

5.2 Opetussuunnitelmat

Tutkinto-ohjelmat ja opetussuunnitelmat kerättiin kertaalleen syksyllä 2021 kunkin oppilaitoksen verkkosivuilta (esim. www.lapinamk.fi) ja julkaistuista opetussuunnitelmista (esim. ops.vamk.fi). Kevään 2022 yhteishaun aikana ja jälkeen listauksia vertailtiin vielä uudelleen esim. Opintopolku -järjestelmässä ilmoitettuihin arvoihin. Samalla tarkasteltiin myös keväällä julkaistut opetussuunnitelmat lukuvuonna 2022–2023 aloittaville, koska mahdollisia muutoksia oli saattanut tapahtua.

Yhteneväistä oli epäselkeys aloituspaikoista eri järjestelmien välillä. Julkaisujärjestelmissä oli selkeästi paikka paikoin epäyhteneväisyyksiä esim. korkeakoulun verkkosivuilla saattoi olla kevään 2021 aloituspaikkamäärät vaikka niitä oli selkeästi opintopolussa keväällä 2022 lisätty tai vähennetty. Näitä lukemia vertaillessa kyselyn arvioituihin aloituspaikkoihin oli selkeää, että tutkintovastaavillakin oli suuntaa-antavia tietoja aloittavien määristä suhteessa varsinaiseen sisäänottoon.

Tämän lisäksi ammattikorkeakoulujen tutkinto-ohjelmiin oli avattuna Opintopolku.fi -järjestelmässä ns. Erillishaku -kohteita. Nämä sisältävät esim. *avoimen ammattikorkeakoulun väyliä* tutkinto-ohjelman opiskelijaksi, *keskeneräisten tutkintojen* hakukohteita sekä *kansainvälisten opiskelijoiden sisäänottoja* esim. double degree ohjelmiin. Aineistonkeräykseen taulukoiduissa lukemissa päätettiin jättää nämä *Erillishaut* huomioimatta ja keskittyä varsinaisiin suoran haun aloituspaikkoihin (Yhteishaku), koska todennäköisesti nämä erillishaut olivat paikkaamaan esimerkiksi keskeyttävien määrää kyseisessä tutkinto-ohjelmassa. Liitteessä 2 on esitetty opetussuunnitelmien yksityiskohtainen läpikäynti ja kyberturvallisuuteen liittyvien opintojaksojen luettelointi.

5.2.1 Analyysi

Opetussuunnitelmien analysointimenetelmänä päätettiin käyttää tyypittelyä. Opetussuunnitelmien rakenteista käytiin läpi, miten kyberturvallisuutta oli sijoitettu pakollisiin, suuntautumisiin (tai ammattiopintoihin) ja vapaasti valittaviin opintojaksoihin. Tämän perusteella jokaisesta opetussuunnitelmasta tehtiin päätös minkä tyyppiseen malliin opetussuunnitelma kategorisoitui. Näiden opetussuunnitelmien luokittelu ja tarkennukset ovat selitetty taulukossa 3.

Taulukko 3. Analysoinnissa käytettävät kategorisointimallit tutkinto-ohjelmille

Malli	**Tarkennus**
A-malli	Kyberturvallisuuteen tähtäävä tutkinto-ohjelma ja oma hakukohteensa Opintopolussa
B-malli	Tutkinto-ohjelma oli suuntautumisena kyberturvallisuuteen tähtäävä
C-malli	Opetussuunnitelmassa oli pakollisissa opintojaksoissa kyberturvallisuutta, mutta tähtäsi eri tavoitteeseen (esim. robotiikka tai pelinkehitys)
D-malli	Opetussuunnitelmassa oli suuntautumisessa tai valinnaisena mahdollista ottaa kyberturvallisuuteen liittyvä opintojakso(ja)
E-malli	Opetussuunnitelmassa ei ollut mahdollista ottaa kyberturvallisuutta, mutta korkeakoulun rinnakkaisista opetussuunnitelmista löytyi kyberturvallisuutta
F-malli	Opetussuunnitelmasta eikä rinnakkaisista (saman tutkintotason) opetussuunnitelmista löytynyt kyberturvallisuutta

Opetussuunnitelmia läpikäytäessä oli selkeää, että myös mallien yhdistelmiä syntyi. Esimerkiksi tutkinto-ohjelman opetussuunnitelman pakollisissa opintojaksoissa saattoi olla kaikkia suuntautumisia yhdistävä ”Organisaation tietoturva” -opintojakso, mutta tutkinto-ohjelmassa oli myös tarjolla yksi suuntautuminen kyberturvallisuuteen. Tällöin opetussuunnitelma päätettiin olevan yhdistelmänä CD-mallinen.

5.2.2 Mallianalyysi YAMK tutkinto-ohjelmista

Ylemmän ammattikorkeakoulututkinnossa suoritetaan lähtökohtaisesti 60 tai 90 opintopistettä riippuen millä tausta tutkinnolla tutkintoon on haettu: insinöörien taustatutkinnossa on 240 opintopistettä ja tradenomeilla 210 opintopistettä. Tästä pienestä opintopistemäärästä valtaosa menee 30 opintopisteen opinnäytetyöhön. Jäljelle jäävistä opintopisteistä on hyvin usein muodostettu hyvin täsmällinen opintokokonaisuus. Taulukossa 4 on esitetty, miten tutkinto-ohjelmien läpikäynnissä opetussuunnitelmat sijoittuivat eri analyysimalleihin.

Neljä A-mallisia tutkinto-ohjelmia kyberturvallisuuteen nousi selkeästi aineistosta (aakkosjärjestyksessä):

- JAMK, Master’s Degree in Information Technology, Cyber Security, Insinööri (YAMK)
- Turku AMK, Ohjelmistotekniikka ja ICT
  - Insinööri (YAMK)
  - Tradenomi (YAMK)
- XAMK, Kyberturvallisuus, Insinööri (YAMK)

B-mallin tutkinto-ohjelmia ei havaittu, koska pienen opintopistemääränsä takia YAMK tutkinto-ohjelmat harvemmin sisälsivät suuntautumisia. C- ja D-malliseksi tuli useita tutkinto-ohjelmia, jotka olivat samassa korkeakoulussa rinnakkaisohjelmia. C-mallisessa YAMK tutkinnossa oli opintojaksossa joku pakollinen kyberturvallisuuden osio ja D-mallissa opiskelijoilla oli mahdollisuus valita vapaasti valittaviin opintoihinsa rinnakkaisen tutkinto-ohjelman pakollisia opintojaksoja. F-malliseksi jäi paljon tutkinto-ohjelmia. Näissä YAMK-ohjelmissa ei havaittu olevan tarjolla kyberturvallisuuden opintojaksoja.

Taulukko 4. Mallien tutkinto-ohjelmamäärät ja aloituspaikat YAMK:ssa

Malli	Tutkinto-ohjelmien määrä	Aloituspaikat	% aloituspaikoista
A-malli	4	79	11.11 %
B-malli	0	0	0 %
C-malli	8	150	21.10 %
D-malli	2	70	9.85 %
E-malli	6	182	25.60 %
F-malli	10	230	32.35 %

5.2.3 Mallianalyysi AMK tutkinto-ohjelmista

Ammattikorkeakoulututkinnoissa oli eniten läpikäytävää, koska tutkinto-ohjelma oli 240 opintopistettä ja saattoi sisältää vähintäänkin kompleksisia opetussuunnitelmarakenteita. Opetussuunnitelmien perusteella opiskelijoille selkeästi haluttiin esitellä opintojaksotarjontaa (esim. XAMK:ssa sadoittain vapaasti valittavia listattuna). Vaihtoehtoisesti suuntautumiset oli ladottu yhteen opetussuunnitelmaan, joista opiskelijoille tarjottiin moduulivalintoja (esim. JAMK ja Metropolian tieto- ja viestintätekniikka). Näissä usein piti korkeakoulun verkkosivujen kautta tulkita mitkä moduulit olivat pakollisia millekin suuntautumiselle. Myös toinen ääripää löytyi missä opetussuunnitelma oli hyvin tarkasti 240 opintopistettä sisältäen pelkät moduulit, jotka kyseiselle suuntautumiselle olivat pakollisia (esim. LapinAMK informaatiohallinnon Mallien tutkinto-ohjelmamäärät ja aloituspaikat AMK:ssa asiantuntija). Taulukossa 5 on esitetty, miten tutkinto-ohjelmien läpikäynnissä opetussuunnitelmat lukeutuivat eri analyysimalleihin.

Suuremmassa opintopistemäärässä on selkeästi mahdollisuutta tehdä suuntautumisia opetussuunnitelmaan. Tästä johtuen B-mallisia opetussuunnitelmia on huomattavasti enemmän. Yleisimmin tämä tarkoitti, että tutkinto- ohjelma oli tietojenkäsittely tai tieto- ja viestintätekniikka, mutta suuntautumisena oli kyberturvallisuus (tai vastaava). Kuitenkin B-mallisten ongelmana on tunnistaa, kuinka monta aloituspaikkaa oikeasti kohdentuu kyberturvallisuuteen. A-mallisissa tämä kohdentuminen on selkeämpää, koska kyberturvallisuus on suora hakukohde.

A-mallisessa opetussuunnitelmissa itseasiassa poiketaan Arene ry:n valintaperustesuosituksista (Arene, 2021), koska kyberturvallisuus on suora hakukohde opintopolussa. Vuoden 2016 valintaperustesuosituksissa oli selkeästi taulukoituna hakukohteiden mallit, joita tulisi käyttää Opintopolussa (esim. tieto- ja viestintätekniikka). Kuitenkin valintaperustesuosituksia tarkastellessa useammalta vuodelta on selkeää, että Arenen ohjaus valtakunnallisissa valintaperustesuosituksissa on löystynyt tältä osin. Heidän raporttinsa ei pidä enää niin tarkkaa listausta tutkinto-ohjelmista ja niihin sidotuista aloista. Tämä ”ohjauksen hiipuminen” koulutuksen hakukohteissa puolestaan näkyy selkeästi opintopolku palvelussa ja tässä analyysissä.

Taulukko 5. Mallien tutkinto-ohjelmamäärät ja aloituspaikat AMK:ssa

Malli	Tutkinto-ohjelmien määrä	Aloituspaikat	% aloituspaikoista
A-malli	3	85	2.22 %
B-malli	5	390	10.18 %
BC-malli	1	20	0.52 %
C-malli	11	752	19.63 %
CD-malli	12	618	16.14 %
CDE-malli	1	40	1.04 %
CE-malli	1	40	1.04 %
D-malli	13	1163	30.37 %
E-malli	12	447	11,67 %
F-malli	5	275	7.18 %

A- ja B-malliset opetussuunnitelmat painottuivat seuraaviin ammattikorkeakouluihin (aakkosjärjestyksessä):

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

C- ja D-mallisiin tutkinto-ohjelmiin jyvittyy suurin osa opetussuunnitelmista. Nämä ovat usein samassa korkeakoulussa olevia rinnakkaisia tutkinto-ohjelmia, jotka ovat pakollisissa saaneet yhden opintojakson kyberturvallisuutta tai valinnaisten listauksessa oli opintojakso tai kaksi aiheesta. Kuitenkin E- ja F-malliin mahtui mittava määrä tutkinto-ohjelmia, joissa kyberturvallisuutta ei sivuttu lainkaan opintojaksojen nimissä.

5.2.4 Opintojaksojen kirjavuus AMK- ja YAMK-opinnoissa

Ammattikorkeakoulujen opintojaksojen nimeäminen on hyvin kirjavaa. Samaa asiaa voidaan opettaa täysin erilaisen tai vain hieman poikkeavan opintojakson nimen alla. Tutkimuksessa löydettiin 135 eri nimeä eri kokoisille ammattikorkeakoulujen opintojaksoille, jotka käsittelevät kyberturvallisuutta. Aiheet ovat useilla opintojaksoilla kuitenkin hyvin lähellä toisiaan. Esimerkiksi kyberturvallisuuden perusteita käsittelevän opintojakson nimi voi olla ”Kyberturvallisuuden perusteet”, ”Johdanto kyberturvallisuuteen” tai ”Kyberturvallisuus”. Suurin osa opintojaksoista on viiden opintopisteen kokoisia. Tämä lienee osoitus siitä, että kokonaisuuksista halutaan tehdä standardimääriin sopivaksi. Opintojaksojen pistejakauma on esitetty taulukossa 6. Mikäli opintopisteiden määrä on näin samanlainen, myös sisällöt olisi luultavasti mahdollista kohdistaa yhden nimen alle.

Opintojaksoja on aiemmin tutkittu Kyberturvaaja-hankkeessa, joka on listannut hankkeeseen osallistuneiden suomalaisten korkeakoulujen opintotarjonnan teemoittain. (TAMK, 2020, 13–14) Lisäksi hanke on suunnitellut kurssikokonaisuudet eri kohderyhmille. (TAMK, 2020, 20) Selkeästi kuvattua kehikkoa ei ole otettu käyttöön, sillä nimeäminen on edelleen vaihtelevaa eri korkeakouluissa.

Taulukko 6. Kyberturvallisuuden opintojaksojen koko opintopisteinä

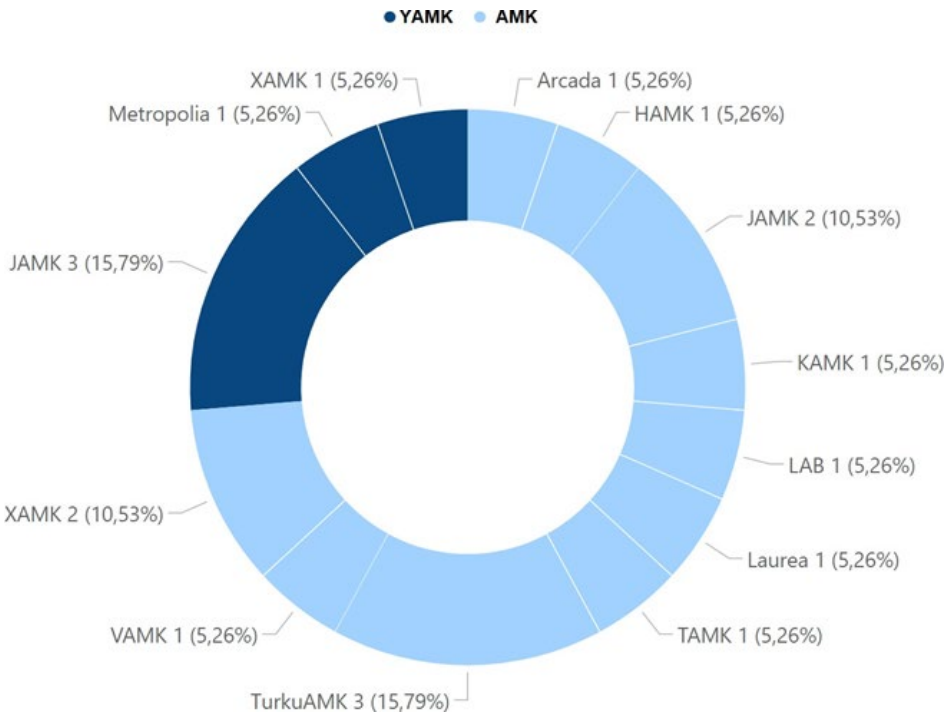
Opintopisteet	Esiintymiskerrat
15	1
10	2
5	115
4	4
3	9
2	2
1	2

5.3 Kyselytutkimuksen toteutus

Tutkimuksen kysely lähetettiin 51 tutkinto-/koulutusvastaavalle vuoden 2021 lopussa. Kysely kohdennettiin tietojenkäsittelyn ja tietoliikennealan AMK- ja YAMK-tutkintovastaaville kaikissa ammattikorkeakouluissa. Monessa ammatti- korkeakoulussa yksittäisellä tutkintovastaavalla saattoi olla useampia tutkinto- ohjelmia vastuualueenaan. Puolestaan joidenkin tutkinto-ohjelmien tapauksessa oli julkisilla verkkosivuilla ohjattu yhteydenotot hakutoimiston tai opiskelija- palveluiden kautta. Suurimmassa osassa tapauksia kysely pystyttiin kuitenkin lähettämään suoraan tutkintovastaavalle. Kyselyyn tuli yhteensä 19 vastausta, joten kyselyn vastausprosentiksi tuli noin 37 %.

Vastanneiden jakautumaa verratessa tutkinto-ohjelmien rakenteisiin, on selkeästi havaittavissa, että kyselyyn aktiivisemmin vastanneet ammattikorkeakoulut myös opettavat eniten kyberturvallisuutta (tutkinto-ohjelma A- tai B-mallinen). Muiden ammattikorkeakoulujen tapauksessa oli kohtalaisen läpinäkyvää, että kyselyyn vastasi vain yksi tutkintovastaava tai jätettiin vastaamatta kokonaan. Vastanneiden jakaumaa tarkasteltiin YAMK ja AMK-tutkinto-ohjelmien välillä. Kuva 22 näyttää tutkintotasot niistä ammattikorkeakouluista, joista vastaus tuli.

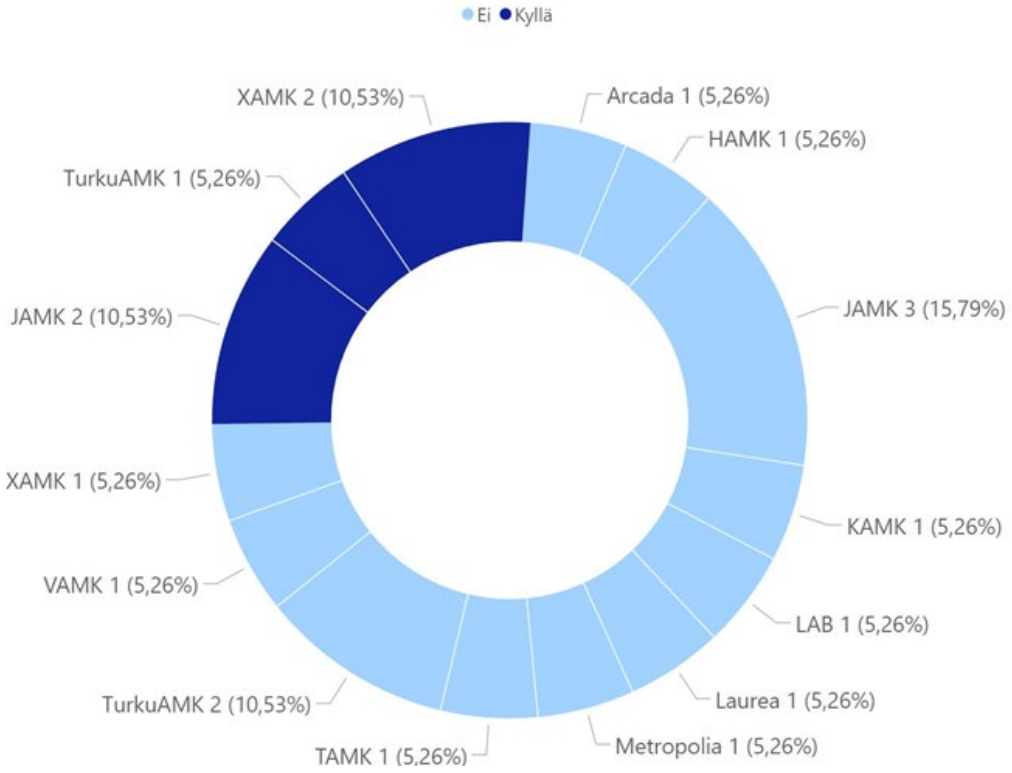
Kyselyyn vastanneiden perusteella YAMK tutkinnot tulevat JAMK, Metropolia ja XAMK:sta. AMK tutkinnot sijoittuvat useampaan ammattikorkeakouluun. Selkeästi on havaittavissa, että lähes 3/4 vastanneista edustaa siis AMK tutkintotasoa. YAMK vastanneet myös selkeästi edustavat ammattikorkeakouluja, jotka painottavat tutkinto-ohjelmissaan kyberturvallisuuden opetusta.



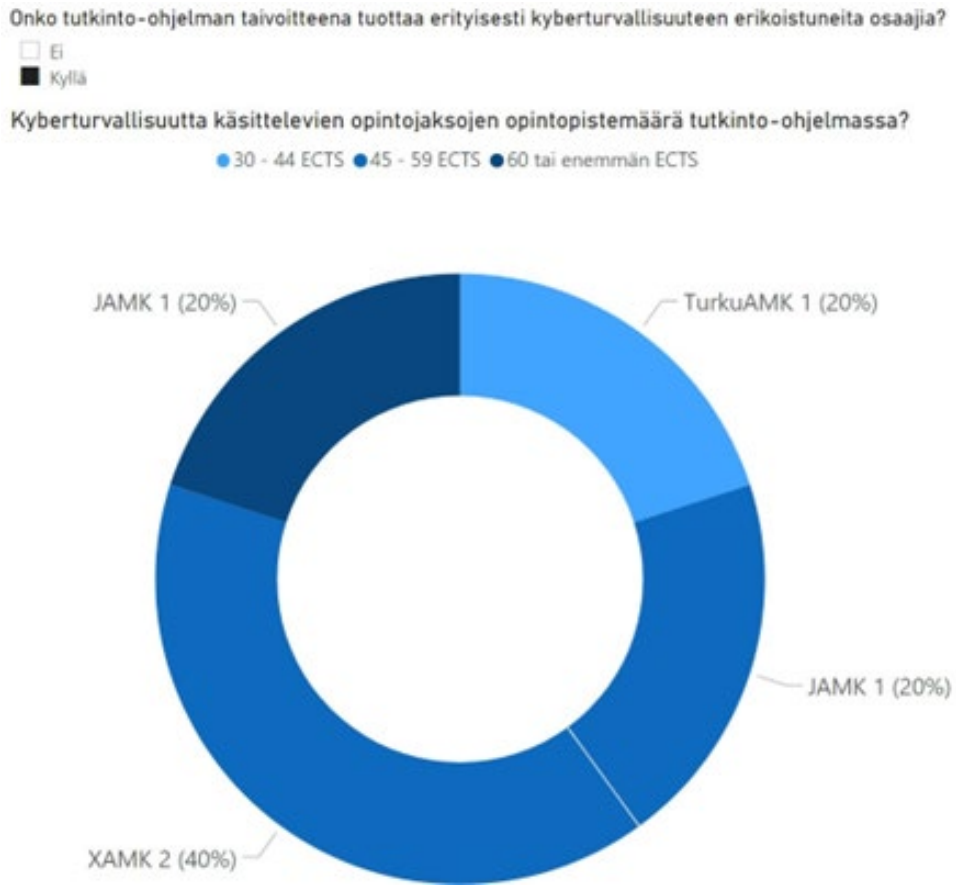
KUVA 22. Jakauma AMK/YAMK-tutkinto-ohjelmien kesken

Kysymyksessä, onko tutkinto-ohjelman tavoitteena tuottaa erityisesti kyberturvallisuuteen erikoistuneita osaajia, profiloitiin tutkinto-ohjelman pääpainotusta vastanneiden kesken, jotta voidaan eritellä, onko tutkinto-ohjelma kyberturvallisuuteen painottuva. Kuvassa 23 on selkeästi erotettavissa kolme ammattikorkeakoulua, jotka keskittyvät tutkinto-ohjelmassaan tuottamaan kyberturvallisuuden osaajia.

Kuvassa 24 on suodatettu näkymään pelkästään kyberturvallisuuteen painottuvat tutkinto-ohjelmat. Tutkinto-ohjelmista vastattiin, mikä on opintopisteiden määrä kyberturvallisuuteen painottuvissa opintojaksoissa. Kuvan 24 vastaukset on kuitenkin tulkittava suuntaa antaviksi. On tulkinnanvaraista, kuuluuko tämä painotus puhtaasti pakollisiin opintoihin vai onko vastauksessa yleinen tarjonta kyberturvallisuusopintoja, joista opiskelija valitsee itselleen soveltuvan määrän omaan tutkintoonsa. Selkeää on kuitenkin, että tutkinto-ohjelman painottaessa kyberturvallisuutta, on myös tarjottavat opinto- pistemäärät huomattavasti korkeammat.

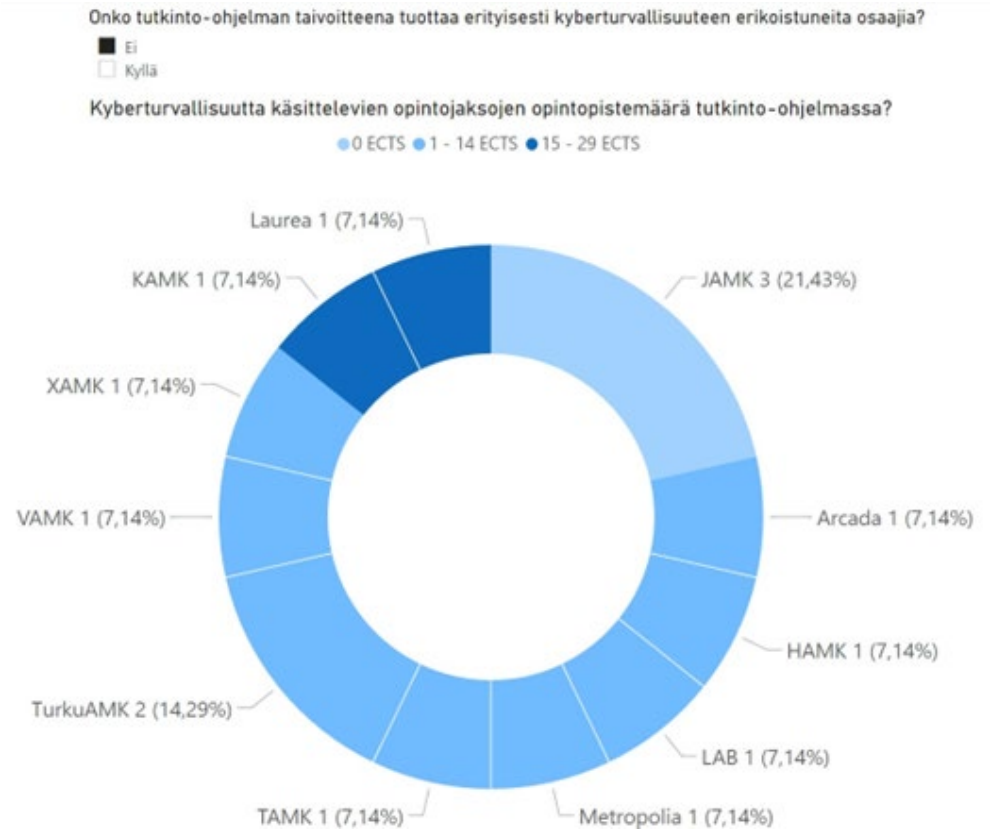


KUVA 23. Onko tutkinto-ohjelman tavoitteena kyberturvallisuus?



KUVA 24. Kyberturvallisuutta käsittelevät tutkinto-ohjelmat

Kuvassa 25 on puolestaan tarkasteltuna opintopistemäärät kyberturvallisuuden opintojaksoissa, kun tutkinto-ohjelma ei erikoista kyberturvallisuuteen. Kuvan 25 perusteella on selkeää, että monissa tutkinto-ohjelmissa kyberturvallisuus sivutaan pienemmässä roolissa. Suurin osa vastauksista on 1–14 opintopisteen välillä. Näissä tapauksissa kyberturvallisuus on yhdessä opintojaksossa. Näissä tapauksissa vastaus jää 1–14 ECTS väliin. Kahdessa tutkinto-ohjelmassa oli 15–29 ECTS kyberturvallisuusopintoja, mutta todennäköisesti näissä tapauksissa moduulit olivat tarjonnassa esim. syventävinä opintoina.



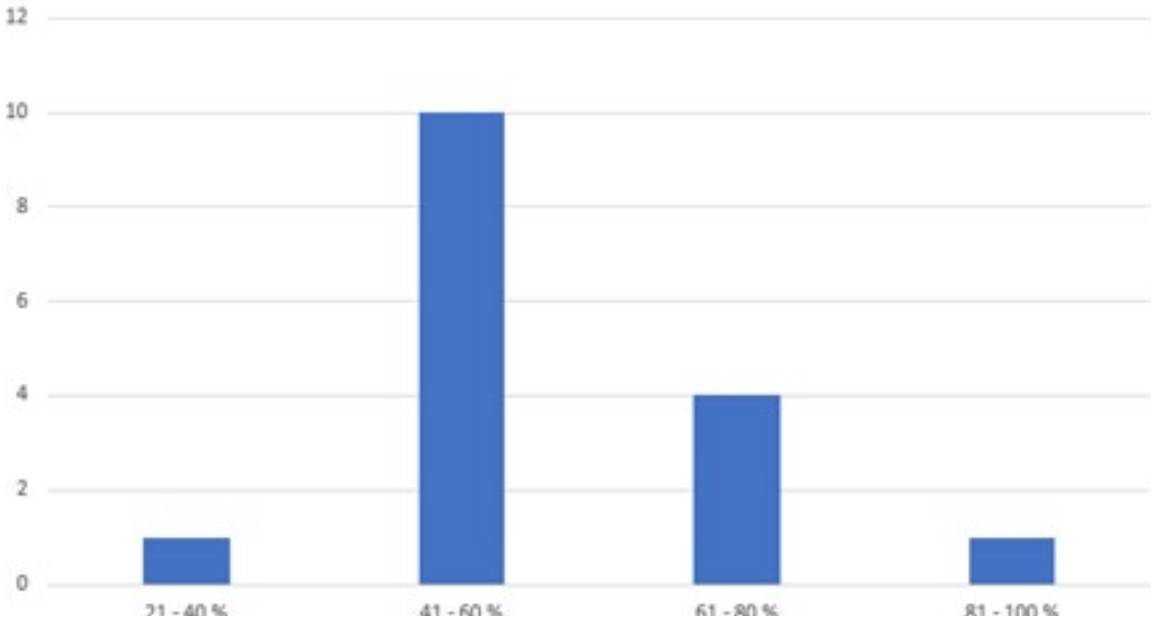
KUVA 25. Kyberturvallisuuden opintopistemäärät siihen muissa tutkinto-ohjelmissa

Korkeat keskeyttämismäärät ovat yleisesti tiedossa oleva ongelma varsinkin insinöörialoilla. Insinööriliitto ry, Ammattikorkeakoulujen rehtorineuvosto Arene ry, Energiateollisuus ry, Teknologiateollisuus ry, Kemianteollisuus ry, Metsäteollisuus ry sekä Rakennusinsinöörit ja -arkkitehdit RIA ry toimeksiantoivat tutkimuksen *Miksi opinnot viivästyvät ja keskeytyvät?* jonka toteutti E2 Tutkimus (2021). Tutkimuksen todettiin seuraavia:

- Tutkinnon suorittaa neljässä vuodessa vain joka neljäs opiskelija
- Tilastojen mukaan insinööriopiskelijoista vain hieman yli 60 prosenttia suorittaa tutkinnon

Koska tietojenkäsittely ja tietoliikenne on rajauksena, on tällä myös suora vaikutus kyberturvallisuusosaajien valmistumiseen ammattikorkeakouluista ja saatavuuteen työmarkkinoilla. Tähän vastatakseen ammattikorkeakoulut usein ottavat sisään enemmän opiskelijoita kuin tavoitevalmistuneet ovat. Tätä suurempaa sisäänottoa on kuitenkin hankala todentaa, koska OKM:n ja ammattikorkeakoulun väliset sopimukset yhdistävät alat keskimääräisiksi tutkintotavoitteiksi esim. luonnontieteet, tietojenkäsittely ja tietoliikenne, tekniikan alat sekä maatalous- ja metsätieteelliset alat.

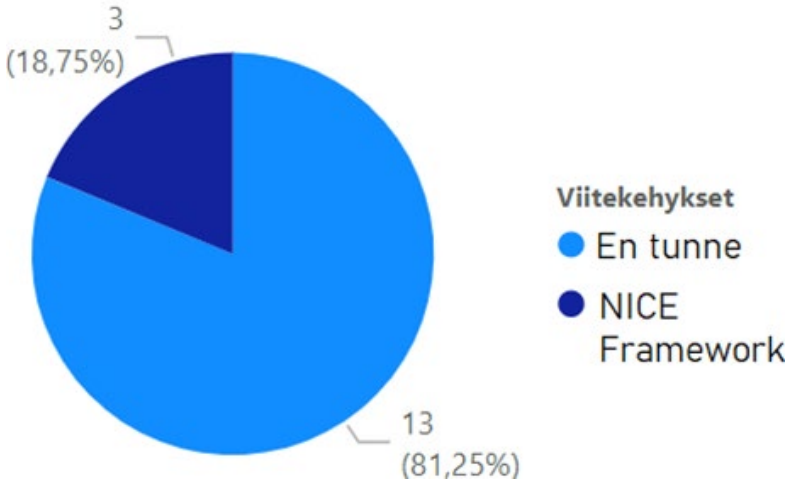
Kyselyssä haluttiin tietää tutkintovastaavien perspektiivistä arvioita keskeyttämisprosentista. Kuvassa 26 on havaittavissa tutkintovastaavien antamia suuntaa antavia arvioita valmistumisprosentista.



KUVA 26. Arviot valmistumisprosentista

Kyselystäkin selkeänä ilmiönä nousee arvio 41–60 % valmistuneista. Laskettuna keskiarvona valmistuminen tämän kyselynperusteella kallistuu hieman lähemmäksi 60 %, mikä on linjassa E2 Tutkimuksen toteamien kanssa. Huomioitavaa on että, kansallisesti kaikista tutkinto-ohjelmista ei ole vastauksia ja vastaus perustuu vastaajien "tuntumaan" aiheesta eikä viralliseen tietoon. Kuitenkin yleistyksenä voi kyselyn perusteella tulkita, että aloituspaikoista hieman päälle puolet valmistuvat.

Kyselyssä haluttiin tietää tuntevatko tutkinto-ohjelmien tutkintovastaavat kyberturvallisuusalaa koskevia viitekehyksiä. Tämän perusteella voi päätellä painottuvatko tutkinnot johonkin standardoituun rakenteelliseen malliin kyberturvallisuuden opetusta. Vastaus on esitetty kuvassa 27. Kolme tutkintovastaavaa (JAMK; XAMK, LAB) tunnisti NICE Frameworkin, mutta JSEC2017:a ei kukaan tuntenut.



KUVA 27. Viitekehysten tuntemus tutkintovastaavilla

5.4 Haastattelututkimuksen tuloksia

Tutkimusta varten haastateltiin tutkintovastaavia neljästä ammattikorkeakoulusta. Kysymys opetuksen lisäämisestä nosti vahvasti esiin valtakunnallisen osaajavajeen. Erityisenä huolena nousi esille kyberturvallisuuden opetusresurssien vajaus. Suurimpana ongelmana haastatellut näkivät alan yleisestä osaajapulasta johtuvan vaikeuden saada tarpeeksi osaavaa opetushenkilökuntaa. Lisäksi teollisuuden tarjoaman tehtävä- ja palkkakilpailun nähtiin vaikeuttavan rekrytointia. Ongelmaksi luettiin myös opettajien kyky pysyä kehityksen perässä, sillä kyber- turvallisuusala ja uhkakuvat muuttuvat jatkuvasti.

Koulutuksen tavoitteiksi kyber- ja tietoturvallisuuden alalla mainittiin osaavien insinöörien tuottaminen elinkeinoelämään ja ylipäänsä kyberturvallisuuden asiantuntijoiden tuottaminen ja kasvattaminen yhteiskunnan tarpeisiin. Ymmärrettävästi koulutuksen haluttiin antavan tarpeeksi taitoja suoriutua työtehtävistä. Ammattikorkeakoulujen tavoitteena nähtiin tuottaa palveluna osaajia yhteiskunnalle. Taulukossa 7 on esitetty haastattelussa yleisimmin esiintyneet aihekategoriat.

Kyberturvallisuuden aiheista tällä hetkellä merkittävimpinä nähtiin sen hallinta ja tietoverkkojen kyberturvallisuus. Myös varsinainen tekninen toimeenpano nähtiin tämänhetkisenä painopisteenä, luultavasti erotuksena hallinnolliseen puoleen verrattuna. Osaajien nähtiin tarvitsevan ongelmanratkaisukykyä siten, että kyberturvallisuus on taustalla vakaana perusoppina: hyökkäävä ja puolustava toiminta, liiketoiminnan näkökulmat ja projektiosaaminen ovat tavoiteltua osaamista. Lisäksi tarpeellisena opetettavana aiheena nähtiin SOC-toiminta (engl. Security Operations Center) eli tietoturvavalvomossa toimiminen. Kyberturvallisuuteen keskittyvissä ohjelmissa saatettiin myös nähdä kaiken muun opiskeltavan vievän tilaa itse asian osaamiselta. Esimerkiksi yleisemmän johtajuuden suuntaan meneminen saattaa viedä tilaa teknisemmältä osaamiselta. Opiskelijoita arvioitiin valmistuvan vähemmän per vuosi kuin heitä otetaan sisään. Tällaiselle kadolle esitettiin syitä. Ylempää ammattikorkeakoulututkintoa tavoittelevat opiskelijat tekevät tutkintoa usein työelämän ohessa, minkä nähtiin aiheuttavan esteitä opiskelulle. Alan opiskelijat kuitenkin siirtyvät työelämään hyvin. Esille nousivat myös teknisen osaamisen puute uudemmissa hakijoissa ja ohjelmointiosaamisen tärkeys. Opetuksen määrän nähtiin lisääntyneen, mutta tulevaisuudesta esiintyi kahdenlaista mielipidettä: toisaalta määrän nähtiin lisääntyvän, toisaalta taas ei nähty, jolloin viitattiin resurssointiin.

Taulukko 7. Haastattelussa yleisimmin esiintyneet aiheiden kategoriat

Aihe	**Esiintymiskerrat**
Kyberturvallisuuden opetusresurssien vajaus	8
Kyberturvallisuuden hallinta	3
Tietoverkon kyberturvallisuus	3
YAMK: työelämän ohessa esteitä opiskella	2
Opetuksen määrä on lisääntynyt	2
Tekninen toimeenpano painopisteenä	2
Kyberturvallisuuden opetus tulee lisääntymään määrällisesti	2
Trendi: tekoälyn rooli	2
Maailmantilanne eli Venäjän hyökkäys Ukrainaan	2
Ei ole tarpeeksi osaavia kouluttajia	2
Täydennyskoulutus: tutkintojen päivittäminen	2

Tulevaisuuden trendeistä tekoälyn rooli mainittiin kahdesti. Muita tärkeäksi nähtyjä tulevia aiheita olivat modernit verkot, kriittinen infrastruktuuri, etätyön vaikutus, identiteetin ja käyttöoikeuksien hallinta, luottamattomuuden periaate (Zero Trust), tilannekuva, kyberturvallisuustilanteen johtaminen sekä kyberrikostutkinta. Myös kriittisten sovellusalojen huomioiminen nähtiin parannettavana asiana, esimerkiksi merenkulku, energia, terveydenhuolto. Lisäksi suuren yleisön opastaminen tietoturvallisuuden pariin ilmeni tarpeellisena tulevaisuuden kehityskohteena. Ajankohtaisista aiheista maailmantilanne eli Venäjän hyökkäys Ukrainaan mainittiin asiana, jonka uskottiin lisäävän kyberturvallisuuskoulutuksen suosiota.

Täydennyskoulutuksen osalta tärkeimpänä havaintona oli tarve aikaisemmin suoritettujen tutkintojen päivittämiseen. Myös työttömille kerrottiin tarjottavan koulutusta, jotta kyberturvallisuuden taidot saadaan päivitettyä ajan tasalle. Avoimen yliopiston tarjonta nousi myös esille, sillä siellä on usein tarjolla samat kokonaisuudet kuin tutkinto-opiskelijoille. Usein ei kuitenkaan ole yleiskurssia eri aloille, ja tässäkin asiassa osaavien kouluttajien puute on esteenä.

Yleisenä havaintona kyberturvallisuuden koulutuksesta nousi esille Opetus- ja kulttuuriministeriöstä tuleva ohjaus. Ohjaus nähtiin ylhäältä tulevana ja koulutustarjontaa rajoittavana esimerkiksi resurssoinnin kannalta: tutkintomäärien tavoitteet ministeriöstä määrittelevät opetusmäärät. Opiskelijoiden lisäämisen kustannukset ammattikorkeakouluille vaatisi rahoituksen kohdentamista, sillä tutkintomäärien tavoitteet ministeriöstä määrittelevät opetusmäärät. Toisaalta myös jo olemassa oleva korkeakoulujen aloittama kyberturvallisuuskoulutuksen tarjonta oli havaittu haastateltavien keskuudessa.

5.5 Ammattikorkeakoulujen kokonaisanalyysi

Ammattikorkeakoulujen tutkintoon johtavien koulutusten opetussuunnitelmasisällöistä sekä tutkintovastaavien haastattelujen tuloksista voidaan todeta, että kyberturvallisuuden opetusta annetaan kattavasti AMK- ja YAMK-tasolla, mutta kyseinen opetus keskittyy vahvasti tiettyihin ammattikorkeakouluihin.

Kyberturvallisuusopetuksen laajamittaisten sisältöjen ja työelämävaatimuksiin vastaamisen osalta erottuvat kuitenkin Jyväskylän ammattikorkeakoulu, Kaakkois-Suomen ammattikorkeakoulu, Laurea-ammattikorkeakoulu ja Turun ammattikorkeakoulu. Opetussuunnitelmien perusteella tarjonta on laajaa sekä vastaa yhteiskunnan, teollisuuden ja elinkeinoelämän tarpeisiin. Eräs parannettava kohta olisi kuitenkin harmonisoida ns. ”kyberturvallisuuden opintojakso” kaikista tutkinto-ohjelmista. Toisin sanoen yhteneväinen opintojakso kyberturvallisuuden perusteista. Opetussuunnitelmien perusteella kaikilla on opintojakso tähän tarpeeseen, mutta hieman eri nimellä, aavistuksen eri opinto- pistemäärällä ja vähintäänkin eri osaamistavoitteilla.

Tästä huolimatta, vaikka yleisesti modulaariset opetussuunnitelmasisällöt sinällään vastaavat tunnistettuihin osaamiskapeikkoihin, on kansallisesti pula enemmänkin koulutusresursseista: esimerkiksi aloituspaikkojen määrä ja opetukseen käytettävien resurssien määrä ovat vajavaisia. Työvoiman saatavuuden niukkuudesta nouseva uhka liittyy vahvasti keskeyttämisten määrään. Tässäkin tutkimuksessa keskeyttämisten määrä suhteessa aloituspaikkoihin tarkoittaisi, että kyberturvallisuuden A- ja B-mallisten AMK- ja YAMK-tutkinto-ohjelmien osalta 554 aloittaneesta opiskelijasta noin 332 valmistuisi

(60 % keskeyttämisprosentilla). Tässä lukemassa on kuitenkin hieman ylimääräistä, koska tilannekuvaa hämärtää kuinka moni B-mallisissa oikeasti suuntautuu kyberturvallisuuden moduuleihin.

Vastauksena osaajapulaan on jo tämän tutkimuksen aikana vuoden 2021 lopulla tehty koulutuspoliittisia ratkaisuja. Joulukuussa 2021 opetusministeriö ilmoitti korkeakoulujen esityksiin perustuen lisäävänsä 2300 uutta aloituspaikkaa korkeakouluihin, näistä ammattikorkeakoulut saavat yhteensä 822 aloituspaikkaa, jotka kohdennetaan 21 ammattikorkeakouluun vuonna 2022 alkaviin koulutuksiin. Tällä toimenpiteellä pyritään vastaamaan korkean osaamistason osaajapulaan sekä toteuttamaan hallituksen tavoitetta osaamis- ja koulutustason nostosta. Lisäyksellä turvataan korkeakoulutuksen saatavuus eri puolilla Suomea, erityisesti työvoimapulasta kärsiville koulutusaloille vahvistamaan alueiden elinvoimaisuutta. (OKM, 2021b)

Uusien aloituspaikkojen erittelyssä voidaan nähdä, että tietojenkäsittely ja tietoliikenne -alalle kohdistetaan 9 ammattikorkeakouluun yhteensä 185 paikkaa (5–40 aloituspaikkaa ammattikorkeakoulusta riippuen). (OKM, 2021a) Taulukosta 8 voidaan todeta, kuinka aloituspaikkojen lisäys kohdistui kyberturvallisuuteen tähtääviin tutkinto-ohjelmiin. A- ja B-mallisista tutkinto-ohjelmista ainoastaan JAMK ja Turun AMK saivat aloituspaikkoja.

Tämän tutkimuksen pohjalta voidaankin sanoa, että OKM:n päätös on hyvä, mutta uusia paikkoja ja lisäresursseja koulutukseen tarvitaan myös tulevaisuudessa, sillä digitalisaation kehitys laajenee entisestään ja luo näin vaatimuksia kyberturvallisuusosaajille eri toimialoilla.

Kyberturvallisuuden osaamisessa on huomioitava, että meneillään olevan digitaalisen transformaation myötä tietotekniikan osaaja ei saa kaikkea työelämässä tarvittavaa osaamista koulussa. Alakohtaista osaamisen karttumista tapahtuu koko ajan työn ohessa työelämässä, ja osaamista pitää päivittää työuran aikana toimintaympäristön muuttuessa ja kehittyessä. Koulutuksen myötä saavutetaan kuitenkin tarvittava pohjaosaaminen, jonka avulla uudet tiedot ja taidot kyetään opiskelemaan ja osaamisrepertuaaria kartuttamaan.

Taulukko 8. Vuoden 2021 aloituspaikkojen lisäyksen vaikutus kyberturvallisuuteen tähtääviin tutkinto-ohjelmiin

AMK	**Tutkinto-ohjelma**	**Lisäys**	**Malli**
Haaga-Helia	Tradenomi (AMK), tietojenkäsittely	40	D
HAMK	Tieto- ja viestintätekniikka, insinööri, monimuoto	20	CD
JAMK	Tieto- ja viestintätekniikka, insinööri AMK	20	B
XAMK	Insinööri (AMK), Peliteknologia	30	D
KAMK	Insinööri (AMK), Tieto- ja viestintätekniikka	20	CD
Metropolia	Insinööri (AMK)	25	C
OAMK	Tradenomi (AMK), tietojenkäsittely	15	F
SAMK	Tradenomi	5	D
TurkuAMK	Tieto- ja viestintätekniikka, insinööri (AMK)	10	B

Pohdittavaksi jää kuitenkin, että kuinka paljon alakohtaista kyberturvallisuutta tulisi opettaa. Opetussuunnitelmista esiin nousi esim. *Tietosuoja ja turvallisuus sosiaali- ja terveydenhuoltojärjestelmässä* -opintojakso. Kuinka monelle muulle alalle soveltuvia, kohdistettuja opintojaksoja tulisi tuottaa? Lisäksi oli selkeää, että kyberturvallisuus oli esillä erikoistumis- tai täydennyskoulutuksena eri ammattikorkeakouluissa varsin mittavilla opintojaksokokonaisuuksilla.

5.6 Johtopäätökset ja suositukset

Kyberturvallisuudessa yksi tärkeimmistä ja arvokkaimmista suojattavista kohteista on osaava henkilöstö. Vaikka organisaatiolla olisi kuinka hyvät tekniset ratkaisut ja prosessit, niin ilman osaavaa henkilöstöä kyberresilienssiä ei synny. Tämä pätee kaikkien työntekijäroolien osalta, koska henkilöstön osaamattomuuden ja tietämättömyyden myötä organisaatio voi olla haavoittuva kyberulottuvuudessa.

Organisaatiot tarvitsevat teknisiä kyberturvallisuusasianatuntijoita esimerkiksi suunnittelemaan turvallisia järjestelmiä, ylläpitämään järjestelmiä, hankkimaan turvallisia järjestelmiä tai tunnistamaan hyökkäyksiä ja tunkeutumisia sekä suorittamaan eriasteisia kyberpoikkeamanhallinnan toimenpiteitä.

Maailmanlaajuisesti on tunnistettu pula osaavista kyberturvallisuusasiantuntijoista. Tämä sama asiantuntijapula kattaa niin Euroopan kuin kansallisesti Suomenkin. Maailmanlaajuisesti puhutaan miljoonien osaajien työvoimatarpeesta, joten Suomenkin osalta tarve on varmasti tuhansia osaajia.

Osaajapulan kannalta on huomioitava erilaiset osaamistarpeet eri tehtävissä. Kyberhyökkäysten tunnistamisessa ja poikkeamanhallinnassa tarvitaan erilaista kyberturvallisuusosaamista kuin kyberturvallisuusjohtamisessa tai uusien järjestelmien hankinnassa. Tämä jako on vielä karkea, jos asiaa tarkastellaan kyberturvallisuuden työvoimaa kuvaavan kehysmallin kautta. Esimerkiksi NICE Framework -kehyksen mukaisten tietojen, taitojen ja kykyjen perusteella huomataan, että osaamisvalikoima on melko laaja ja osaajan pitää erikoistua johonkin tiettyyn kokonaisuuteen.

Tämä on huomioitava koulutuksessa, eli mihin tehtävään valmistuvan osaajan oletetaan työllistyvän. Toki on ymmärrettävä, että koulutuksen kautta saavutetaan tietty perusosaaminen ja myöhemmin työtehtävien, erikoistumisen ja mahdollisten erikoiskoulutusten kautta saavutetaan syvempi erikoisasiantuntijuus kyseiseen aihealueeseen.

Ammattikorkeakouluissa annettava kyberturvallisuusopetus (AMK- ja YAMK-korkeakoulututkinto, sekä erikoistumis- täydennys- ja muuntokoulutus) on sisällöllisesti kattavaa ja kykenee modulaarisen rakenteen perusteella muuntautumaan teollisuuden tarpeisiin. Kuitenkin koulutuksen resursseihin pitää panostaa, jotta pystytään vastaamaan jatkuvasti laajenevan digitalisaation mukanaan tuomiin vaatimuksiin. Tämän myötä kyberturvallisuusosaamista tarvitaan yhä laajemmin eri digitalisoituvilla toimialoilla. Toimialojen osaamistarpeet tulevat laajenemaan myös vahvasti kyberturvallisuuden ja ohjelmistorobotiikan (tekoäly, neuroverkot, syväoppiminen) yhdistyessä.

Koulutuksen resursseja mietittäessä on myös huomioitava se, että ammattikorkeakoulut antavat pääsääntöisesti teknistä kyberturvallisuuskoulutusta, joka kouluttaa tekniseen osaamiseen. Tällainen insinööritieteiden opetus vaatii laajat ja monimutkaiset

oppimisympäristöt, jotka ovat kalliita hankkia ja ylläpitää. Jotta riittävä tekninen osaaminen voidaan taata, on tarvittavien oppimis- ja koulutusympäristöjen hankinta, kehitys- ja ylläpitokulut huomioitava resursoinnissa.

Opettajien määrän lisääminen on tärkeää, jos kyberturvallisuusalan opettamista halutaan lisätä. Haasteena opettajien määrän lisäämisessä on opetustyön houkuttelevuus tarpeeksi osaavien asiantuntijoiden rekrytoimiseksi. Nopeasti kehittyvän alan aiheiden täytyy tukea työelämää, ja tämän vuoksi aiheiden täytyy myös osaltaan tulla työelämän tarpeista.

Kyberturvallisuuden opetusta tulisi kohdentaa myös eri työelämän aloille. Näin tarvittavaa osaamista olisi käytettävissä yhteiskunnassa yleisellä tasolla. Tutkintoja päivittävä täydennyskoulutus vaatii myös opetusresursseja. Koulutuksen täytyy tuottaa tarpeeksi osaajia, jotta yhteiskunnalla on valmius vastata nykymaailman haasteisiin.

Koska ammattikorkeakoulut toimivat ennalta määrättyjen opetusmäärien pohjalta, täytyy jatkossa resursseja pystyä kohdistamaan kyberturvallisuuden koulutukseen hallinnollisten päätösten kautta, sillä se on suurin todellinen kannustin, jolla ammattikorkeakoulukenttä ryhtyy lisäämään tuotantoa.

Lähteet

Arene (2021). Ammattikorkeakoulujen valintaperustesuositukset 2021. Ammattikorkeakoulujen rehtorineuvosto (Arene). https://www.arene.fi/julkaisut/raportit/ammattikorkeakoulujen-valintaperustesuositukset/. Viitattu 02.04.2022.

Blažič, B. J. 2021. The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. Technology in Society 67, 101769. doi: https://doi.org/10.1016/j.techsoc.2021.101769.

CC (2020). Computing Curricula 2020 – CC2020: Paradigms for Future Computing Curricula (Draft, Version 36). https://cc2020.nsparc.msstate.edu/.

CSEC (2017). Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (Version 1.0). https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf.

E2 Tutkimus (2021). Miksi opinnot viivästyvät ja keskeytyvät? Selvitys AMK-insinööriopiskelijoiden opintojen viivästymisen ja keskeyttämisen syistä. https://www.ilry.fi/wp-content/uploads/2021/11/Miksi-opinnot_viivastyvat-ja-keskeytyvat-selvitys.pdf. Viitattu 02.04.2022.

ECSO (2017). Gaps in European Cyber Education and Professional Training. European Cyber Security Organisation (ECSO) https://ecs-org.eu/documents/publications/5fdb282a4dcbd.pdf.

ECSO (2021). European Cybersecurity Education and Professional Training: Minimum Reference Curriculum. European Cyber Security Organisation (ECSO). https://www.ecs-org.eu/documents/publications/61967913d3f81.pdf.

Eduuni-wiki (2021). OKM:n korkeakoulujen ohjauksen alat. Luku 7.2 julkaisussa Tiedonkeruun käsikirja 2021. https:// wiki.eduuni.fi/display/cscsuorat/7.2+OKM%3An+ohjauksen+alat+2021. Viitattu 22.04.2022.

ENISA (2021). Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education. European Union Agency for Cybersecurity (ENISA).

https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

Eurostat (2020). International Standard Classification of Education (ISCED). https://ec.europa.eu/eurostat/statistics-explained/index.php?title=International_Standard_Classification_of_Education_(ISCED). Viitattu 02.02.2022.

ISC2 (2021). A Resilient Cybersecurity Profession Charts the Path Forward. 2021 Cybersecurity Workforce Study, International Information Systems Security Certification Consortium (ISC)^2. https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.

JAMK (2022). CYBERDI. Jyväskylän ammattikorkeakoulu (JAMK). https://www.jamk.fi/fi/projekti/cyberdi. Viitattu 02.02.2022.

Lehto, M. & Niemelä, J. (2019). Kyberalan tutkimus ja koulutus Suomessa 2019. Informaatioteknologian tiedekunnan julkaisuja 83/2019. Jyväskylän yliopisto.

Newhouse, W., Keith, S., Scribner, B. & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. National Institute of Standards and Technology (NIST). https://doi.org/10.6028/nist.sp.800-181.

OKM (2015a). Opetus- ja kulttuuriministeriön tarkentavat ohjeet sopimuskauden 2017–2020 valmisteluun ja vuonna 2016 käytäviin neuvotteluihin. https://okm.fi/documents/1410845/4169434/OKM%2Bohje%2B2016%2Btarkentavat%2Bohjeet%2Bsopimuskauden%2B2014-2020%2Bvalmisteluun%2Bja%2Bvuonna%2B2016%2Bkäytäviin%2Bneuvotteluihin. Viitattu 02.02.2022.

OKM (2015b). Opetus- ja kulttuuriministeriön tarkentavat ohjeet sopimuskauden 2017–2020 valmisteluun ja vuonna 2016 käytäviin neuvotteluihin. Liite 1: Kauden 2017–2020 sopimusvalmistelua koskevat ohjeet https://okm.fi/documents/1410845/4169438/OKM%2Bohje%2B2016%2C%2BLiite%2B1%2BKauden%2B2017-2020%2Bsopimusvalmistelua%2Bkoskevat%2Bohjeet. Viitattu 02.02.2022.

OKM (2019). Opetus- ja kulttuuriministeriön tarkentavat ohjeet sopimuskauden 2021–2024 valmisteluun ja vuonna 2020 käytäviin neuvotteluihin. https://okm.fi/documents/1410845/15969577/OKM+kirje+2019+tarkentavat+ohjeet+sopimuskauden+2021-2024+valmisteluun+ja+vuonna+2020+k%C3%A4yt%C3%A4viin+neuvotteluihin.pdf/56d80980-046a-1928-4236-4f0e21a31be5/OKM+kirje+2019+tarkentavat+ohjeet+sopimuskauden+2021-2024+valmisteluun+ja+vuonna+2020+k%C3%A4yt%C3%A4viin+neuvotteluihin.pdf?version=1.2&t=1571396453000. Viitattu 02.02.2022.

OKM (2021a). Ammattikorkeakouluille myönnetyt uudet lisäpaikat vuodelle 2022. https://okm.fi/documents/1410845/4392480/AMK-uudet+lis%C3%A4paikat+2022.pdf/7a9befe4-8019-135c-fbb1-381094f5d67f/AMK-uudet+lis%C3%A4paikat+2022.pdf?t=1639985949325.

OKM (2021b). Korkeakoulujen aloituspaikkoja lisätään vuodelle 2022 noin 2 300:lla. https://okm.fi/-/korkeakoulujen-aloituspaikkoja-lisataan-vuodelle-2022-noin-2-300-lla.

Schmidt, C. (2004). The analysis of semi-structured interviews. Teoksessa U. Flick, E. von Kardorff & I. Steinke (toim.) A Companion to Qualitative Research. London, Thousand Oaks, New Delhi: SAGE Publications, 253–258.

TAMK (2020). Kyberturvaaja-hanke. Loppuraportit, tulokset, yhteenvedot ja tuotokset. Tampereen ammattikorkeakoulu (TAMK). https://projects.tuni.fi/uploads/2020/10/91c0d668-20201029_kyberturvaaja_tuotokset.pdf.

Tilastokeskus (2022a). Kansallinen koulutusala 2016. https://tilastokeskus.fi/fi/luokitukset/koulutusala/koulutusala_1_20160101/.

Tilastokeskus (2022b). Kuntapohjaiset tilastointialueet. Aineisto on ladattu Tilastokeskuksen rajapintapalvelusta 9.3.2022 lisenssillä CC BY 4.0.

UNESCO (2015). International Standard Classification of Education: Fields of education and training 2013 (ISCED-F 2013), detailed field descriptions. UNESCO Institute for Statistics. doi:10.15220/978-92-9189-179-5-en. http://uis.unesco.org/sites/default/files/documents/international-standard-classification-of-education-fields-of-education-and-training-2013-detailed-field-descriptions-2015-en.pdf.

6 Kyberturvallisuuden opetus yliopistoissa

Tässä osatutkimuksessa luotiin tilannekuva kyberturvallisuuden opetuksesta Suomen yliopistoissa. Tilannekuva kartoitettiin tutkimalla yliopistojen tutkinto-ohjelmia yliopistojen verkkosivujen perusteella ja strukturoidulla kyselylomakkeella. Lisäksi osatutkimuksessa toteutettiin haastattelut, joihin osallistui neljä kyberturvallisuuden asiantuntijaa yliopistosektorilta. Osatutkimuksessa luotiin tilannekuva myös yliopistojen tarjoamasta täydennyskoulutuksesta ja kartoitettiin FITech verkostoyliopiston kurssitarjontaa kyberalalta. Aineiston analyysiä ohjasi Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity ja siinä määritetyt kyberturvallisuuden osa-alueet:

- Data Security, Software Security,
- Component Security,
- Connection Security,
- System Security,
- Human Security,
- Organizational Security ja
- Societal Security.

Kyberturvallisuuteen keskittyneitä tutkinto-ohjelmia on määrällisesti niukasti ja opetus keskittyy ylempiin korkeakoulututkintoihin. Yliopistot tuottavat melko vähän kyberturvallisuuden osaajia suhteessa tunnistettuun osaajapulaan. Tutkinto-ohjelmia, joissa kyberturvallisuutta on sisällytetty tutkinto-ohjelman rakenteisiin valinnaisina- tai pakollisina opintoina 1–15 ECTS on runsaasti. Yliopistot tarjoavat vähäisissä määrin kyberalan täydennyskoulutusta. Haastatteluissa nousi esille muun muassa, että opiskelijoiden kiinnostus kyberturvallisuuden opiskeluun on lisääntynyt viime vuosina ja opetusyhteistyön kehittäminen yliopistojen välillä nähtiin kehityskohteena, johon kannattaisi lisätä resursseja. Lisäresurssit opetukseen ja tutkimukseen kehittäisivät kyberturvallisuuden opetusta Suomessa. Yhtenä resurssihaasteena koettiin kyberturvallisuuden osaajien rekrytointi.

6.1 Aineiston keruu

Aineiston keruun ensimmäisessä vaiheessa tarkasteltiin yliopistojen eri tiedekuntien ja laitoksien tutkinto-ohjelmia ja niiden sisältöjä. Ensimmäisen vaiheen perusteella rakentui lista tutkinto-ohjelmista, jonka perusteella kohdistettiin strukturoitu kyselylomake. Kyselyn vastaajiksi etsittiin tutkintovastaavia/tutkinto-ohjelmien johtajia/vastuuopettajia, joiden tutkinto-ohjelmassa on kyberturvallisuuden/tietoturvallisuuden/digitaalisen turvallisuuden opetusta. Tutkimushanketta varten haastateltiin myös kyberturvallisuuden asiantuntijoita neljästä yliopistosta ja yhteensä haastateltavia oli neljä.

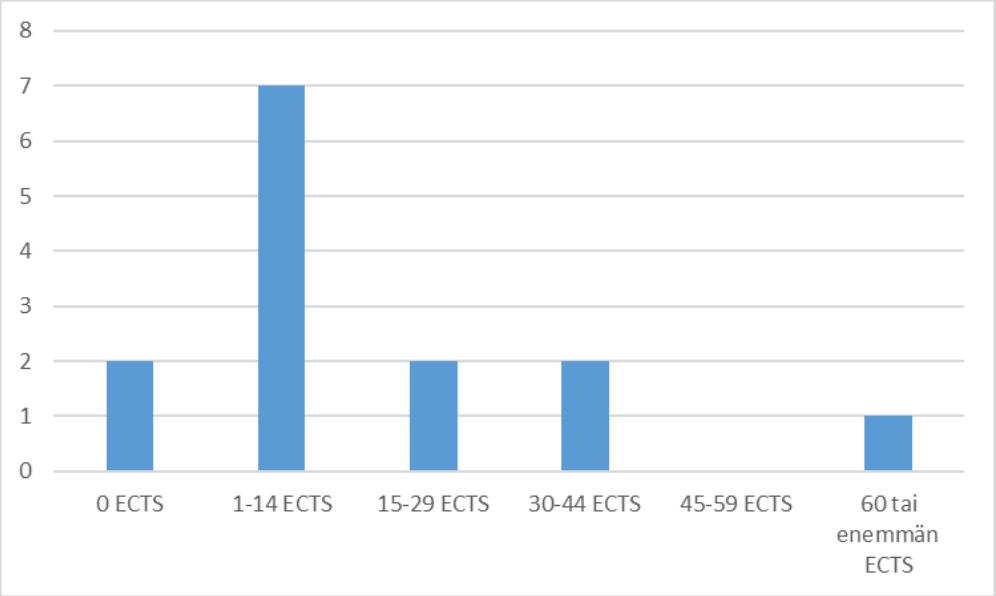
Aineiston analyysiä ohjasi Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Opetussuunnitelmassa määritetään standardinomaiset perusteet kyberturvallisuuden tutkinto-ohjelmille ja siinä on määritetty kyberturvallisuuden osaamisalueiksi: Data Security, Software Security, Component

Security, Connection Security, System Security, Human Security, Organizational Security ja Societal Security. (CSEC, 2017)

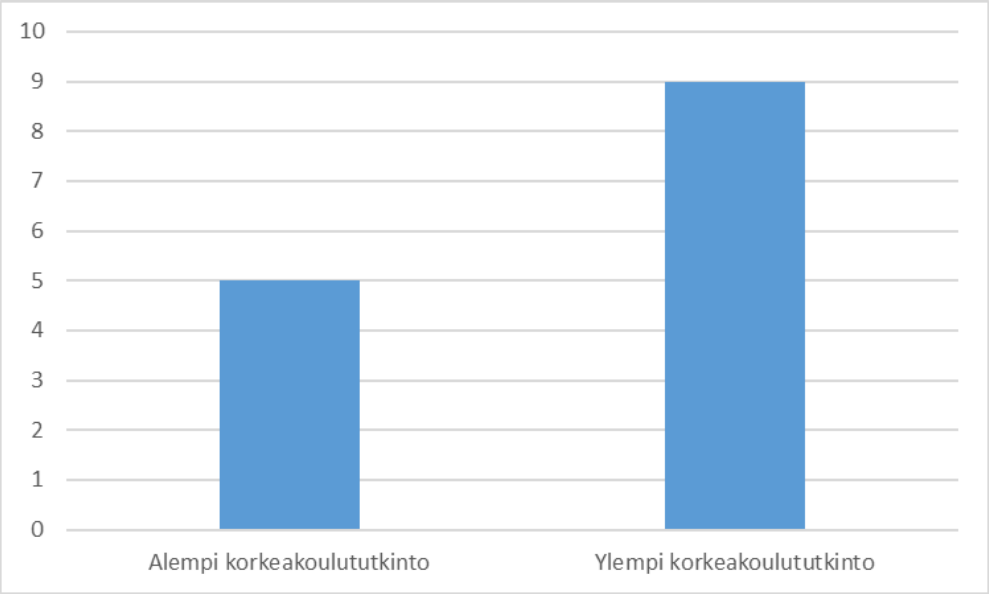
Aineiston keruun ja analysoinnin tuloksena rakentui lista kyber- ja tietoturvallisuuden kursseista ja tutkinto-ohjelmista, joissa niitä opetetaan. On mahdollista, että kyberturvallisuuden kursseja on enemmän kuin mitä tässä raportissa on määritelty. Lisäksi on mahdollista, että kyberturvallisuuden opetusta on tutkinto-ohjelmissa, mitä ei olla tässä raportoitu.

Hankkeessa on luotu tilannekuva myös yliopistojen tarjoamasta täydennyskoulutuksesta kyberturvallisuuden alalta. Täydennyskoulutuksen tilannekuva perustuu yliopistojen verkkosivujen kautta hankittuun tietoon ja haastatteluihin. Lisäksi tässä osatutkimuksessa on kuvattu keskeisten tutkinto-ohjelmien hakijamääriä ja sisäänottomääriä. Luvut perustuvat kevään 2022 hakijatilastoihin ja kyselylomakkeen tuloksiin. Tässä raportissa esitetyt luvut ovat suuntaa antavia, koska luvuissa ei olla huomioitu mahdollisia avoimen väylän ja siirtohaun kautta olevia opiskelupaikkoja. Lisäksi tutkinto-ohjelmissa on usein kandidaatin ja maisteri opinto-oikeuden lisäksi mahdollisuus hakea vain maisteriopintoihin oikeuttavaan opinto-oikeuteen, johon on oma kiintiönsä. Nämä tekijät vaikeuttavat lopullisten hakija- ja sisäänottomäärien arviointia ja sen vuoksi luvut ovat suuntaa antavia.

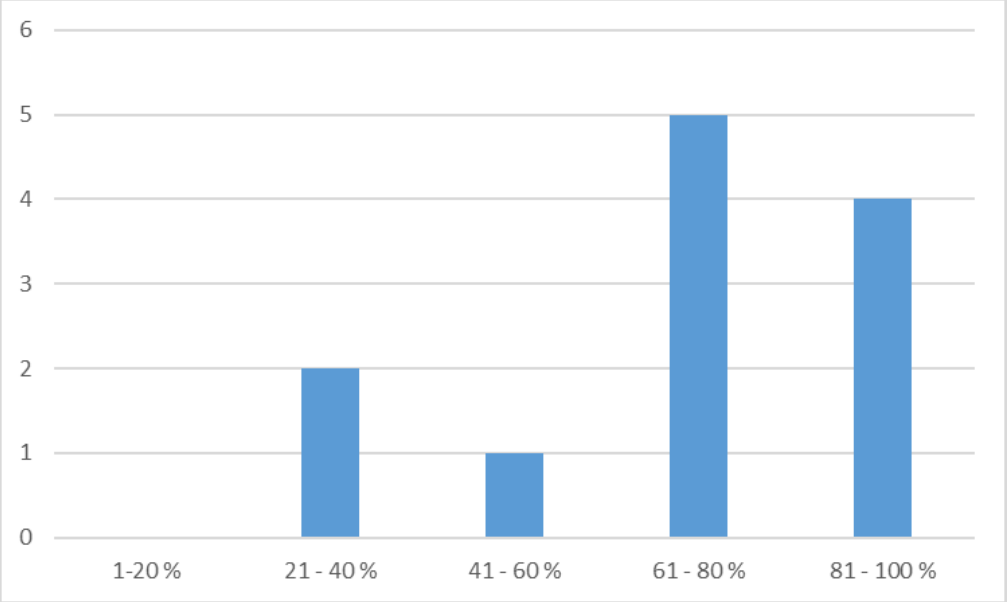
Kyselyssä selvitettiin, miten paljon tutkinto-ohjelmaan valitaan uusia opiskelijoita, miten paljon tutkinto-ohjelmasta valmistuu opiskelijoita suhteessa sisäänottomäärään ja miten paljon kyberturvallisuuden kursseja tutkinto-ohjelma sisältää. Suomessa on runsaasti tutkinto-ohjelmia, joissa kyberturvallisuutta on sisällytetty tutkinto-ohjelman rakenteisiin valinnaisina tai pakollisina opintoina 1–14 ECTS. Sen sijaan sellaisia tutkinto-ohjelmia on määrällisesti vähän, joissa kyberturvallisuus on pääpainopiste tai merkittävässä asemassa tutkinto-ohjelman sisältöä. Kuvassa 28 on esitetty kyberturvallisuuden kurssien määrä tutkinto-ohjelmissa.



KUVA 28. Kyberturvallisuuden kurssien määrä tutkinto-ohjelmissa



KUVA 29. Tutkinto-ohjelmien jakautuminen alempiin- ja ylempiin korkeakoulututkintoihin



KUVA 30. Arvio opiskelijoiden vuosittaisesta valmistumisprosentista suhteessa tutkinto-ohjelman sisäänottomäärään

Ylemmistä korkeakoulututkinnoista kurssitarjontaa oli eniten. Kuvan 29 mukaan kyberturvallisuuden opetus Suomen yliopistoissa on keskittynyt ylempiin korkeakoulututkintoihin.

Vastaajia pyydettiin arvioimaan, mikä on opiskelijoiden vuosittainen valmistumisprosentti suhteessa tutkinto-ohjelman sisäänottomäärään. Tulokset osoittavat, että on melko tyypillistä, että vuosittain valmistuneiden opiskelijoiden määrä tutkinto-ohjelmasta on alhaisempi kuin sisään otettava opiskelijamäärä (kts. kuva 30).

6.2 Yliopistoanalyysi

6.2.1 Aalto-yliopisto

Kyberalaan liittyvä opetus

Aalto-yliopiston tietotekniikan laitoksella on Master's Programme in Computer, Communication and Information Sciences tutkinto-ohjelma, johon sisältyy useita eri pääaineita/suuntautumisia mukaan lukien Security and Cloud Computing (Security). Pääaine/suuntautuminen tarjoaa opiskelijoille laajan ymmärryksen uusimmista ja myös tulevaisuuden teknologioista koskien turvallisia mobiileja (engl. secure mobile) ja pilvilaskentajärjestelmistä (engl. cloud computing systems). Opiskelijat saavuttavat sekä käytännön tekniset taidot että teoreettisen käsityksen turvallisesta järjestelmäsuunnittelusta (engl. secure systems engineering), tietoverkko- ja pilviarkkitehdistä sekä pilvi- ja mobiili alustoista. Tutkinto-ohjelmassa on erityinen huomio kiinnitetty turvallisuus- ja yksityisyys kysymyksiin, koska ne ovat kriittisiä vaatimuksia kehitettäessä ja käyttöön otettaessa palveluja avoimissa tietoverkoissa ja hajautetuissa järjestelmissä. (Aalto, 2021)

Pääaineessa on tarjolla useita kyber- ja tietoturvallisuuden kursseja pakollisina- ja valinnaisina opintoina. Tutkinto-ohjelmaan oli 194 hakijaa vuonna 2022 ja uusia opiskelijoita valittiin 11.

Aalto-yliopisto koordinoi myös Erasmus Mundus Joint Master Degree Programme in Security and Cloud Computing (SECCLO) tutkinto-ohjelmaa yhdessä viiden muun yliopiston kanssa. Tutkinto-ohjelman rakenne on kaksivaiheinen. Ensimmäisenä lukuvuotena suoritetaan 60 ECTS edestä opintoja Aalto-yliopistossa ja toisena lukuvuotena suoritetaan erikoistumisopinnot toisessa yhteistyöyliopistossa. Vaihtoehtoina on erikoistua tietoliikennetekniikkaan Ruotsissa (The Royal Institute of Technology), tietoturvaan Norjassa (The Norwegian University of Science and Technology), luotettaviin hajautettuihin järjestelmiin Tanskassa (Technical University of Denmark), kryptografiaan Virossa (University of Tartu) ja Big Data turvallisuuteen Ranskassa (EURECOM). Tutkinto-ohjelman omien verkkosivujen perusteella tutkinto-ohjelmaan haki ensimmäisellä hakukierroksella (24.11.2021-05.01.2022) yhteensä 735 hakijaa, joista 76 valittiin tutkinto-opiskelijaksi. (SECCLO, 2022)

Yksittäisiä kyber- ja tietoturvallisuuden kursseja on tarjolla valinnaisena tai pakollisena myös useissa muissa tutkinto-ohjelmissa. Näiden osalta on kuvattu tutkinto-ohjelman nimi ja onko kyberalaan liittyvä kurssi tutkinto-ohjelmassa pakollinen vai valinnainen.

Kyberalaan liittyvä täydennyskoulutus

Aalto PRO (Aalto, 2022) tarjoaa eri toimialojen koulutuksia niin uransa alussa oleville kuin jo pidempään vaativissa asiantuntijatehtävissä toimiville henkilöille. Erilaisia koulutuksia on tarjolla laaja-alaisesti mukaan lukien turvallisuusjohtamisen- ja digitaalisen turvallisuuden koulutuksia. Tällä hetkellä tarjonnassa ovat ainakin seuraavat turvallisuusalan koulutukset:

- Diplomia in Digital Security 21.09.2022-08.03.2023,
- Turvallisuusjohdon koulutusohjelma -TJK 09.11.2022-17.05.2024,

- Digitaalinen vastuullisuus ja teknologiat, sosiaalinen vastuullisuus ja eettisyys 21.04.2022-22.04.2022.

6.2.2 Helsingin yliopisto

Kyberalaan liittyvä opetus

Helsingin yliopistolla ei ole kyber- tai tietoturvallisuuteen keskittyneitä tutkinto-ohjelmia. Sen sijaan Matemaattis-luonnontieteellisessä tiedekunnassa voi opiskella kyber- ja tietoturvallisuutta osana tietojenkäsittelytieteen maisteriohjelmaa. Tutkinto-ohjelmassa pystyy suuntautumaan tietoverkkoihin, joka sisältää myös kyberturvallisuuteen keskittyneitä kursseja.

Tietojenkäsittelytieteen kandidaatin tutkinnossa tulee valita pakolliseksi kurssiksi joko tietoturvan perusteet- tai johdatus tekoälyyn kurssin. Tietoturvan perusteet kurssi järjestetään myös kaikille saatavilla olevana MOOC-kurssina. Lisäksi Master's Programme in Data Science sisältää valinnaisena Trustworthy Machine Learning kurssin.

Kyberalaan liittyvä täydennyskoulutus

Helsingin yliopisto (2022a) tarjoaa edellisessä luvussa mainitun tietoturvan perusteet MOOC-kurssin. Muita kyberalan täydennyskoulutuksia Helsingin yliopisto ei tarjoa tällä hetkellä. HY+ Oy, joka on yliopiston rahastojen omistama täydennyskoulutusyhtiö, tarjoaa täydennyskoulutusta seuraavista aihealueista:

- Viestintä ja vuorovaikutus
- Johtaminen, esihenkilötyö ja ohjaus
- Opetus ja oppiminen
- Hyvinvointi ja terveys
- Kestävä kehitys.

Lisäksi tarjolla on myös esimerkiksi ammatillisia jatkokoulutuksia sekä erikoistumiskoulutuksia useilta eri aloilta. (Helsingin yliopisto, 2022b)

6.2.3 Tampereen yliopisto

Kyberalaan liittyvä opetus

Tampereen yliopisto tarjoaa Advanced Studies in Information Security suuntautumisen (80 ECTS). Tutkinto-ohjelmissa, joissa tietoturvaan pystyy suuntautumaan, on tarjolla myös useita muita suuntautumisvaihtoehtoja. Tutkinto-ohjelmat, joihin opintokokonaisuus kuuluu ovat seuraavat:

- Master's Programme in Information Technology
- Tietojenkäsittelyopin maisteriohjelma
- Master's Programme in Computer Science

Tavoitteena on, että opiskelija saavuttaa opinnoista hyvän ymmärryksen digitaalisesta turvallisuudesta ja yksityisyydestä. Kyvyn arvioida turvallisuutta ja yksityisyyttä olemassa olevissa järjestelmissä. Kyvyn analysoida, suunnitella ja implementoida turvallisia järjestelmiä. Kyvyn osallistua turvallisuuden ja yksityisyyden tieteelliseen tutkimukseen. (Tampereen yliopisto, 2022a) Suuntautumiseen vuosittain valikoituva opiskelijamäärä on arvioitu olevan 1–30.

Tampereen yliopiston Johtamisen ja talouden tiedekunnassa on Master's Programme in Security and Safety Management tutkinto-ohjelma, jossa on tarjolla kaksi eri pääainetta:

- Safety Management and Engineering
- Security Governance

Opiskelijat, joiden pääaineena on Security Governance kehittyvät asiantuntijoiksi turvallisuuden hallinnassa ja johtamisessa yhteiskunnissa ja yhteisöissä kansainvälisessä, kansallisessa ja paikallisessa turvallisuusympäristöissä julkisissa organisaatioissa ja vapaaehtoissektorilla. Opiskelijat tulevat olemaan korkean tason asiantuntijoita, joilla on perusteellinen ymmärrys turvallisuudesta ja turvallisuuden johtamisesta, riskienhallinnasta, johtamisesta sekä julkisella että yksityisellä sektorilla paikallisesti, kansallisesti ja maailmanlaajuisesti. (Tampereen yliopisto, 2022b) Tutkinto-ohjelmaan oli 45 hakijaa vuonna 2022 ja tutkinto-ohjelmaan hyväksyttiin 8 uutta opiskelijaa.

Opiskelijat, joiden pääaine on Safety Management and Engineering kehittävät asiantuntemustaan tuotantoon, tuotteisiin ja palveluihin, joihin liittyvät turvallisuuden-, terveyden-, ja ympäristöriskien hallinta. Lisäksi he kehittävät asiantuntijuuttaan yrityksien turvallisuuteen ja riskienhallintaan sekä suunnitteluun, missä tyypilliset työkalut ovat käytössä. (Tampereen yliopisto, 2022c) Tutkinto-ohjelmaan oli 76 hakijaa vuonna 2022 ja tutkinto-ohjelmaan hyväksyttiin 8 uutta opiskelijaa.

Tampereen yliopiston Tekniikan ja luonnontieteiden tiedekunnassa on tarjolla automaatiotekniikan DI-ohjelma, jossa on useita suuntautumisvaihtoehtoja mukaan lukien automaation tietotekniikka. Tämä suuntautuminen sisältää pakollisina- ja valinnaisina opintoina kyber- ja tietoturvallisuuteen linkittyviä kursseja. Lisäksi tutkinto-ohjelmassa on kursseja, joissa tietoturvallisuus ei ole pääpainopiste, mutta yksi osa-alue kurssin sisältöä.

Tämän lisäksi Tampereen yliopisto tarjoaa useita pienempiä valinnaisia opintosuuntauksia tutkinto-ohjelmien sisällä, joissa on tarjolla valinnaisina opintoina kyber- ja tietoturvallisuutta käsitteleviä kursseja tai vaihtoehtoisesti kursseja, joissa teknologiaan liittyvä turvallisuus on yksi osa-alue kurssin sisältöä. Kyseisiä opintokokonaisuuksia voi opiskella useissa eri tutkinto-ohjelmissa. Edellä mainittuja opintokokonaisuuksia ovat ainakin: Intermediate Studies in Communication and Networking valinnaisina opintoina, Intermediate Studies in Health Informatics valinnaisina opintoina, lentokonetekniikan aineopintoja valinnaisina opintoina, turvallisuustekniikan aineopintoja valinnaisina opintoina, ohjelmistotuotannon syventävät opinnot valinnaisina opintoina ja tietoliikennetekniikan aineopinnot valinnaisina opintoina. Yksittäisiä kyber- ja tietoturvallisuuden kursseja on myös tarjolla pakollisina tai valinnaisina opintoina useissa tutkinto-ohjelmissa.

Kyberalaan liittyvä täydennyskoulutus

Tampereen yliopisto (2022d) tarjoaa kattavasti täydennyskoulutuksia usealta eri tieteenalalta, mutta tarkasteluhetkellä tarjonnassa ei ole kyberturvallisuuden täydennyskoulutuksia. Tampereen yliopiston täydennyskoulutusten koulutusalat ovat:

- Johtaminen ja esihenkilötyö
- Sosiaali- ja terveysala
- Opetus ja kasvatus
- Tekniikka ja teknologia

- Liiketoiminnan ja organisaation toiminnan kehittäminen
- Kulttuuri- ja media-ala.

6.2.4 Jyväskylän yliopisto

Kyberalaan liittyvä opetus

Jyväskylän yliopiston informaatioteknologian tiedekunnassa on tarjolla kyberturvallisuuden maisteriohjelma. Tutkinto-ohjelman tavoitteet ovat seuraavat: ”Kyberturvallisuuden maisteriohjelman tavoitteena on tarjota opiskelijalle vankka osaaminen työskentelyyn kyberturvallisuuden kokonaishallintaa vaativissa johtamis- ja kehittämistehtävissä. Koulutuksessa tarkastellaan kybermaailmaa ja sen turvallisuutta hallinnollisesta ja teknologisesta näkökulmasta. Maisteriohjelmassa sisällöllisiä painopistealueita ovat kyberturvallisuuden suunnittelu, johtaminen ja tietoturvallisuusriskien hallinta niin johtamisen kuin teknologiankin näkökulmasta”. (Jyväskylän yliopisto, 2022a) Tutkinto-ohjelmaan valitaan 45 uutta opiskelijaa ja hakijoita oli 184 vuonna 2022.

Informaatioteknologian tiedekunnassa on tarjolla myös turvallisuus- ja strategisen analyysin maisteriohjelma, joka sisältää kyberturvallisuuteen linkittyviä kursseja. Tutkinto-ohjelman kuvauksessa on sanottu seuraavaa: ”Maisteriohjelmassa koulutetaan laaja-alaisia turvallisuuden asiantuntijoita, jotka osaavat analysoida turvallisuuteen vaikuttavia muutoksia ja ilmiöitä globaalissa ympäristössä. Maisteriohjelman opinnoissa käsitellään turvallisuusympäristöä ja sen muutosta, kriisejä ja konflikteja sekä globalisaation, teknologian kehittymisen ja digitalisaation merkitystä niihin. Keskeinen osa maisteriohjelmaa on myös strategisen analyysin osaaminen: maisteriohjelma tarjoaa valmiudet turvallisuuteen liittyvän tiedon hankintaan, käsittelyyn ja analysointiin niin, että yhä monimutkaisemman turvallisuusympäristön ymmärtäminen, hallinta ja ennustaminen on mahdollista”. (Jyväskylän yliopisto, 2022b) Tutkinto-ohjelmaan valitaan 25 uutta opiskelijaa ja hakijoita oli 390 vuonna 2022.

Tiedekunnassa pystyy opiskelemaan myös tietotekniikan maisteriohjelmassa, joka sisältää kaksi eri suuntautumista:

- Ohjelmisto- ja tietoliikennetekniikka
- Teknis-matemaattinen mallintaminen ja päätösanalytiikka

Ohjelmisto- ja tietoliikennetekniikan pääaineessa on tarjolla valinnaisina opintoina kyber- ja tietoturvallisuuden kursseja. Tiedekunnassa on myös tieto- ja ohjelmistotekniikan kandidaatti ja diplomi-insinööri ohjelma, joka sisältää pakollisina- ja valinnaisina kursseina myös kyber- ja tietoturvallisuuteen linkittyviä kursseja. Tiedekunnassa pystyy opiskelemaan myös tietojärjestelmätieteitä, koulutusteknologiaa ja kognitiotiedettä. Lisäksi tarjolla on kaksi englanninkielistä maisteriohjelmaa; Information Systems ja Cognitive Computing and Collective Intelligence.

Kyberalaan liittyvä täydennyskoulutus

Jyväskylän yliopisto ei tarjoa kyber- ja tietoturvallisuuden täydennyskoulutusta. Yliopisto tarjoaa kattavasti erilaisia täydennyskoulutuksia kuten Avance Executive MBA -johtamiskoulutuksen, kesäyliopiston koulutustarjonnan, koulutusjohtamisen opinnot, opettajille suunnatut täydennyskoulutushankkeet (OKL), psykoteraupettikoulutuksen,

täydennyskoulutuksen liikunnan ja terveystiedon opettajille ja IT-alan täydennyskoulutusta. Tarkasteluhetkellä IT-alan täydennyskoulutuksessa ei ollut kyberturvallisuuden kursseja vuodelle 2022. (Jyväskylän yliopisto, 2022c)

6.2.5 Turun yliopisto

Kyberalaan liittyvä opetus

Turun yliopistolla on kyber- ja tietoturvallisuuteen keskittyneitä tutkinto-ohjelmia. Alan opetus keskittyy Teknilliseen tiedekuntaan, jossa on tarjolla tutkinto-ohjelmia tieto- ja viestintätekniikasta (TkK ja DI) ja tietojenkäsittelytieteistä (LuK ja FM). Kansainvälisenä hakukohteena Turun yliopistolla on tarjolla Master's Degree Programme in Information and Communication Technology tutkinto-ohjelma, jossa voi suuntautua seuraaviin pääaineisiin vuodesta 2022 alkaen:

- Cyber Security
- Cryptography
- Smart Systems
- Software Engineering
- Data Analytics

Cyber Security -pääainetta voi opiskella kokonaan Turussa järjestettävänä koulutuksena. Tutkinto-ohjelma on myös osa EIT Digital Master School kaksoistutkinto-ohjelmaa. EIT Digital Master School on kaksivuotinen maisteriohjelma, jossa on mukana 20 eurooppalaista huippuyliopistoa. Opiskelijat aloittavat kyberturvallisuuden opintonsa yhdessä yliopistossa. Ensimmäisenä lukuvuotena tarjotaan yhteinen perusosaaminen kaikille tutkinto-ohjelman opiskelijoille ja toisena lukuvuotena suoritetaan erikoistumisopinnot toisessa yliopistossa. Suomesta ei ole muita tutkinto-ohjelmia mukana EIT Digital Master School kaksoistutkinto-ohjelmassa. Cyber Security -pääaineessa opiskelija saavuttaa tietämystä, asiantuntijuutta ja käytännön osaamisen kokemusta turvallisuudesta, teknologiasta ja verkotetuista järjestelmistä. Tutkinto-ohjelman erikoistuminen keskittyy tulevaisuuden verkkojärjestelmiin ja sovelluksiin. Teknologisiin aihepiireihin kuuluvat älykkäiden ympäristöjen turvallisuus, järjestelmä- ja verkkoturvallisuus, tietoliikennejärjestelmien- ja -sovellusten turvallisuus sekä turvallisten järjestelmien suunnittelu. Opiskelija perehtyy alan teknologiseen ja teoreettiseen tieteelliseen tutkimukseen sekä osaa soveltaa niitä käytännössä. Valmistuneilla tulee olemaan vahva teknologinen ja teoreettinen käytännön ymmärrys kyberturvallisuudesta. (Turun yliopisto, 2022a)

Kryptografiassa tavoitteena on kouluttaa tutkimus- ja ICT alalle tulevaisuuden asiantuntijoita, joilla on vahva ja laaja tietämys kryptografian ja tietoturvan matemaattisista näkökohdista. Kryptografiaan erikoistuminen tarjoaa vankan taustan matemaattisten kryptografian klassisista ja moderneista näkökohdista. Nykyaikaisista symmetrisistä ja epäsymmetrisistä kryptojärjestelmistä (engl. cryptosystems) kehitetään syvällistä ymmärrystä. Opiskelijoille tarjotaan vahva akateeminen koulutus jatko-opintojen jatkamiseksi sekä IT-alan kyberturvallisuuden asiantuntijana työskentelyyn. Opiskelija oppii arvioimaan kryptografisten ratkaisujen vahvuuksia ja heikkouksia taustalla olevan syvän teoriaosaamisen pohjalla. Opiskelija osaa myös soveltaa kryptografisia algoritmejä ja protokollia tosielämän ympäristöihin. (Turun yliopisto, 2022b)

Master's Degree Programme in Information and Communication Technology tutkinto-ohjelmaan oli 522 hakijaa vuonna 2022, joista 130 haki Cyber Security -pääaineeseen ja 13 Cryptography -pääaineeseen. Lisäksi EIT Digital Master Schoolin kevään 2022 ensimmäisellä hakukierroksella Cyber Security -kaksoistutkinto-ohjelmaan oli 16 hakijaa. EIT:n toinen hakukierros (EU-hakijoille) on tätä kirjoittaessa vielä kesken. Cyber Security pääaineeseen valitaan 35 uutta opiskelijaa (sisältää EIT Digital Master School tutkinto-ohjelman aloituspaikat) ja kryptografiaan valitaan viisi uutta opiskelijaa.

Teknillisessä tiedekunnassa on tarjolla myös tieto- ja viestintätekniikan (DI) tutkinto-ohjelma. Tutkinto-ohjelman nimi muuttuu syksystä 2022 alkaen tietotekniikaksi. Tutkinto-ohjelmassa voi suuntautua seuraaviin pääaineisiin vuodesta 2022 alkaen:

- Tietoliikenne- ja kyberturvallisuusteknologia
- Ohjelmistotekniikka
- Älykkäät järjestelmät
- Data-analytiikka

Ennen vuoden 2020 opetussuunnitelman päivittämistä, tietoliikenne- ja kyberturvallisuusteknologian pääaine keskittyi tietoliikennetekniikkaan. Pitkän kehityskulun seurauksena tutkinto-ohjelma on kehittynyt lähemmäksi Cyber Security -pääaineen sisältöä ja se onkin nykyään sisällöltään lähes yhtenevä Cyber Security -pääaineen kanssa. Tutkinto-ohjelman kuvauksessa mainitaan, että: "Esineiden Internet ja kaiken sensorointi (esim. älykkäät tilat ja kaupungit), ja autonomiset järjestelmät/robotiikka ovat tuoneet uuden kovan osaamistarpeen tietoliikenteen ja kyberturvallisuuden osaajille. Tällä hetkellä koulutuksessa on erityispainotusta sensoriverkkoihin, IoT ja autonomisiin järjestelmin, sekä matalantehonkulutuksen toteutuksiin. Alakohtainen spesialisointi voidaan tehdä temaattisen moduulin kautta esimerkiksi data-analytiikkaan, terveysteknologiaan, konetekniikkaan, sekä älykkäisiin ja autonomisiin järjestelmiin. Temaattisessa moduulissa opiskelija voi myös suuntautua vahvemmin liike- ja innovaatiotoimintaan tai laajentaa osaamistaan kryptologiaan ja kyberturvallisuusjohtamiseen". (Turun yliopisto, 2022c)

Tieto- ja viestintätekniikan (DI) tutkinto-ohjelmaan valitaan 30 opiskelijaa. Arvion mukaan siitä noin 6–8 suuntautuu tietoliikenne- ja kyberturvallisuusteknologiaan.
Yhteishaun kautta voi hakea opinto-oikeutta tieto- ja viestintätekniikan (TkK + DI) tutkinto-ohjelmaan ja uusia aloituspaikkoja on tarjolla 120. Kandidaatin tutkinnon nimi muuttuu myös tietotekniikaksi syksystä 2022 alkaen. Kandidaatin tutkinnon suoritettuaan opiskelija voi valita suuntautumisen useasta eri linjasta mukaan lukien kyberturvallisuus, kryptografia ja tietoliikenne- ja kyberturvallisuusteknologia.

Useissa muissa tutkinto-ohjelmissa on myös mahdollista opiskella kyberturvallisuutta osana tutkinto-ohjelmaa. Tieto- ja viestintätekniikan DI-ohjelman ohjelmistotekniikan suuntautumisessa on pakollisina- ja valinnaisina kursseina kyber- ja tietoturvallisuuteen linkittyviä kursseja. Tiedekunnan tarjoamassa tietojenkäsittelytieteen (FM) tutkinto-ohjelman vuorovaikutusmuotoilun suuntautumisessa voi valita yhdeksi temaattiseksi moduuliksi tietoliikenne- ja kyberturvallisuusteknologian (20 ECTS). Turun kauppakorkeakoulun tietojärjestelmätieteen pääaineessa on tarjolla myös kyberturvallisuutta käsitteleviä kursseja.

Kyberalaan liittyvä täydennyskoulutus

Turun yliopistolla ei ole tällä hetkellä kyber- ja tietoturvallisuuteen keskittyneitä täydennyskoulutuksia tarjolla. Turun yliopiston täydennyskoulutuksia tarjotaan Brahea-keskuksen ja usean tiedekunnan kautta. Brahea-keskuksen opetustarjonnassa on koulutuksia tarjolla kolmesta kategoriasta vuonna 2022:

- Maahanmuutto ja kulttuurinen moninaisuus
- Meri ja merenkulku
- Opetus- ja kasvatusala

Seuraavat Turun yliopiston tiedekunnat tarjoavat täydennyskoulutuksia: kasvatustieteiden-, lääketieteellinen-, oikeustieteellinen-, Turun kauppakorkeakoulu-, ja yhteiskuntatieteellinen tiedekunta. (Turun yliopisto, 2022d)

6.2.6 Oulun yliopisto

Kyberalaan liittyvä opetus

Oulun yliopistossa ei ole tällä hetkellä kyber- ja tietoturvallisuuteen keskittynyttä tutkinto-ohjelmaa. Sen sijaan useassa tutkinto-ohjelmassa on kyber- ja tietoturvallisuuden kursseja pakollisina- ja valinnaisina opintoina. Tieto- ja sähkötekniikan tiedekunnassa voi opiskella muun muassa tietotekniikan kandidaatiksi ja diplomi-insinööriksi. Kandidaatin tutkinnossa voi opiskella tekoälyä, soveltavaa tietotekniikkaa ja tietokonetekniikkaa. DI-vaiheessa voi suuntautua tekoälyyn, soveltavaan tietokonetekniikkaan, tietokonetekniikkaa -laitteistot tai tietokonetekniikkaa -ohjelmistot.

Tietotekniikan kandidaatin ja diplomi-insinöörin tutkintojen rakenteisiin on sisällytetty joko pakollisia tai valinnaisia kyberturvallisuuden kursseja. Tietotekniikassa on tarjolla useita tietotekniikan erikoiskursseja ja moni näistä käsittelee kyber- ja tietoturvallisuutta. Oulun yliopiston Humanistisessa tiedekunnassa voi opiskella esimerkiksi informaatiotutkimusta (HuK ja FM), joka sisältää myös kyberalaan linkittyviä kursseja.

Kyberalaan liittyvä täydennyskoulutus

Oulun yliopisto (2022) tarjoaa täydennyskoulutusta useilta eri tieteenaloilta mukaan lukien tekniikan alalta. Oulun yliopiston tekniikan alan erikoisosaamista ovat esimerkiksi 6G-tutkimus, ohjelmointiosaamisen kehittäminen ja projektinhallinnan osaaminen. Kyber- ja tietoturvallisuus huomioidaan osana DigiHealth-täydennyskoulutuksessa (25 ECTS), joka järjestetään ainakin lukuvuotena 2021–2022. Opintokokonaisuus lukeutuu jatkuvan oppimisen, täydennyskoulutuksen ja erillisen opinto-oikeuden kategorioihin. Opintokokonaisuus antaa kattavan katsauksen lääkinnällisten laitteiden regulaatioon ja tietoturvaan, digitaalisen terveydenhuollon perusteisiin, soveltamiseen ja kehittämiseen sekä terveysdatan mallintamiseen ja hyödyntämiseen. Kurssit, jotka kuuluvat opintokokonaisuuteen ovat:

- Lääkinnällisen laitteen regulaatiot ja laadunhallinta 5 ECTS
- Connected Health and mHealth 5 ECTS
- Koneoppimisen käytön perusteet lääketieteessä 5 ECTS
- Biosignal Processing 5 ECTS
- Basics in eHealth 5 ECTS.

6.2.7 Itä-Suomen yliopisto

Kyberalaan liittyvä opetus

Itä-Suomen yliopistolla ei ole kyber- ja tietoturvallisuuteen keskittynyttä tutkinto-ohjelmaa. Yliopiston luonnontieteiden ja metsätieteiden tiedekunnassa on mahdollista opiskella muun muassa tietojenkäsittelytieteen kandidaatiksi (LuK) ja maisteriksi (FM). Osana tietojenkäsittelytieteen kandidaatin tutkintoa on pakollisena kurssina *Johdatus tietoturvaan* (5 ECTS). Tietojenkäsittelytieteen maisteriohjelmassa on mahdollista opiskella kursseja esimerkiksi tekoälystä, hahmontunnistuksesta, syväoppimisesta, konenäöstä ja katseenseurannasta.

Kyberalaan liittyvä täydennyskoulutus

Itä-Suomen yliopisto (2022a) ei tarjoa kyber- ja tietoturvallisuuteen keskittyneitä täydennyskoulutuksia. Itä-Suomen yliopiston täydennyskoulutusten koulutusalat ovat

- Yrityksen kasvu ja kehittäminen
- Johtaminen ja henkilöstön kehittäminen
- Juridiikka
- Lääkeala
- Kasvatus- ja opetusala
- Ympäristö ja teknologia
- Sosiaali- ja terveysala
- Kansainvälisyys.

Yliopisto tarjoaa myös erikoistumiskoulutuksia ja erillisiä opintoja useista eri tieteenaloista mukaan lukien SmartICT erikoistumiskoulutuksen ja automaatiotekniikan DI-ohjelman. Tarkasteluhetkellä koulutuksissa ei ollut kyberturvallisuuteen keskittynyttä erikoistumiskoulutusta. (Itä-Suomen yliopisto, 2022b)

6.2.8 Lappeenrannan teknillinen yliopisto

Kyberalaan liittyvä opetus

Lappeenrannan teknillisessä yliopistossa ei ole kyber- tai tietoturvallisuuteen keskittynyttä tutkinto-ohjelmaa. Laskennallisen tekniikan- ja tuotantotalouden kandidaatin tutkinnoissa sekä data-analytiikka päätöksenteossa- ja tuotannon johtamisen DI-ohjelmissa on mahdollista opiskella sivuopintoina ohjelmistotuotantoa (20 ECTS). Tähän kokonaisuuteen sisältyy valinnaisina opintoina ohjelmistojärjestelmän tietoturvaa- ja ohjelmistotestauksen periaatteita käsitteleviä kursseja. Edellä mainitut kaksi kyberturvallisuuteen linkittyvää kurssia on myös tarjolla tietotekniikan- ja Software and Systems Engineering (Lahti) kandidaatin tutkinnoissa.

Lisäksi Master’s Programme in Software Engineering and Digital Transformation- ja Master’s Programme in Product Management and Business (Lahti) tutkinto-ohjelmissa on pakollisena opintona Requirements Engineering (6 ECTS) ja valinnaisena opintona on tarjolla Quality Assurance in Software Development (6 ECTS).

Kyberalaan liittyvä täydennyskoulutus

Lappeenrannan teknillisessä yliopistossa ei ole kyber- ja tietoturvallisuuteen keskittyneitä täydennyskoulutuksia. Yliopiston koulutusohjelmat täydennyskoulutuksen osalta ovat LUT EMBA, KATI 16 – Johtamisen täydennyskoulutusohjelma, Controller asiantuntijaohjelma, hankintatoimen johtamisen asiantuntijaohjelma, tietojohtamisen asiantuntijaohjelma, talous ja rahoituksen ohjelma, leadership and management ohjelma ja innovaatiojohtamisen asiantuntijaohjelma. (Lappeenrannan teknillinen yliopisto 2022).

6.2.9 Åbo Akademi

Kyberalaan liittyvä opetus

Åbo Akademissa ei ole kyber- ja tietoturvallisuuteen keskittynyttä tutkinto-ohjelmaa. Yksittäisiä kyber- ja tietoturvallisuuteen linkittyviä kursseja on tarjolla pakollisina- ja valinnaisina opintoina useassa tutkinto-ohjelmassa. Lisäksi Åbo Akademi tarjoaa valinnaisena *Safety-Critical and Autonomous Systems* temaattisen moduulin useassa eri tutkinto-ohjelmassa. Temaattisessa moduulissa on tarjolla kyber- ja tietoturvallisuuteen linkittyviä kursseja. Yksittäiset kyberalaan liittyvät kurssit ovat kuvattu erillisessä taulukossa.

Kyberalaan liittyvä täydennyskoulutus

Åbo Akademilla ei ole kyber- ja tietoturvallisuuteen keskittyviä täydennyskoulutuksia. Tarkasteluhetkellä Åbo Akademi tarjoaa ainakin kaksi erikoistumiskoulutusta:

- Korkeakoulupedagogiikka
- Oikeuspsykologian erikoistumiskoulutus

Åbo Akademilla on Elinikäisen oppimisen keskus (Centret för livslångt lärande, CLL), joka on Suomen suurin ruotsinkielinen aikuiskouluttaja. Keskus on Åbo Akademin ja Yrkeshögskolan Novian (AMK) yhteinen keskus. Sen tarkoituksena on tuottaa tutkimusperustaisia kehittämis- ja koulutuspalveluja useilla aloilla. (Åbo Akademi, 2022)

6.2.10 Vaasan yliopisto

Kyberalaan liittyvä opetus

Vaasan yliopistolla ei ole kyber- ja tietoturvallisuuteen keskittynyttä tutkinto-ohjelmaa tai opintokokonaisuutta. Yksittäisiä kyber- ja tietoturvallisuuteen linkittyviä kursseja on tarjolla pakollisina- ja valinnaisina opintoina useissa eri tutkinto-ohjelmissa kuten esimerkiksi automaation, tietotekniikan (TkK), tietojärjestelmätieteen (KTM) ja teknisen viestinnän (KTM) tutkinnoissa.

Kyberalaan liittyvä täydennyskoulutus

Vaasan yliopistolla ei ole kyber- ja tietoturvallisuuteen keskittynyttä täydennyskoulutusta. Vaasan yliopisto tarjoaa useita Executive MBA ohjelmia, joista yksi on keskittynyt riskienhallintaan ja turvallisuuteen. Vaasan yliopiston (2022) ohjelmien erikoistumisopinnoissa voi suuntautua kahteen kokonaisuuteen:

- Riskienhallintaprosessi liiketoimintaympäristössä ja menetelmät 10 ECTS,

- Riskienhallinnan kehittäminen osana lakisääteisiä velvoitteita ja vaatimustenmukaisuutta 10 ECTS.

6.2.11 Lapin yliopisto

Kyberalaan liittyvä opetus

Lapin yliopiston oikeustieteellinen tiedekunta tarjoaa muun muassa hallinto-oikeuden ja oikeusinformatiikan opintoja. Oikeusnotaarin tutkintoon on sisällytetty yksi pakollinen kurssi hallinto-oikeudesta ja oikeusinformatiikasta. Puolestaan maisterin tutkintoon sisältyy valinnaisina opintoina kaksi oikeusinformatiikan kurssia.

Kyberalaan liittyvä täydennyskoulutus

Lapin yliopisto ei tarjoa tarkasteluhetkellä täydennyskoulutusta kyber- ja tietoturvallisuudesta. Täydennyskoulutuksia on saatavilla opetus- ja kasvatusalan osaajille, oikeusalan asiantuntijoille ja sosiaalialan asiantuntijoille. Lisäksi opintoja on mahdollista suorittaa avoimen yliopiston ja itsenäisesti suoritettavien MOOC-kurssien kautta. (Lapin yliopisto, 2022)

6.2.12 Maanpuolustuskorkeakoulu

Maanpuolustuskorkeakoulussa voi opiskella sotatieteiden- kandidaatiksi, maisteriksi ja tohtoriksi. Lisäksi tarjolla on esimerkiksi yleisesikuntaupseerin koulutus. Kyberturvallisuutta käsitellään sekä kandidaatin että maisteritutkinnon kursseilla. Enemmän alaa liittyvää opetusta on tarjolla maisteriohjelmassa.

Liitteessä 3 on esitetty yliopistojen kyberturvallisuuden koulutuksen sisältöjä.

6.2.13 FITech verkostoyliopisto

Finnish Institute of Technology (FITech) perustettiin vuonna 2017. Se toimii tekniikan alan verkostoyliopistona ja sen perustajajäseniä ovat seitsemän suomalaista yliopistoa, Teknologiateollisuus ry sekä Tekniikan akateemiset ry. Jyväskylän yliopisto liittyi jäseneksi vuonna 2019. Verkostoyliopiston tavoitteena on ohjata tekniikan alan osaajia Suomen kasvualoille ja vastata alan nouseviin osaajatarpeisiin. (FITech, 2022)

Alussa FITech keskittyi vastaamaan Lounais-Suomen teollisuuden yritysten osaajatarpeisiin. Sen myötä perustettiin FITech Turku -hanke syksyllä 2017. Tämän jälkeen toiminta on laajentunut aikuisopetukseen, kun konsortiossa käynnistettiin tuhansien suomalaisten ICT-osaamista kehittävä FITech ICT -hanke. Lisäksi käynnistettiin globaalin energiamurroksen aiheuttamiin osaamistarpeisiin vastaava FITech Energy Storage -hanke. Viimeisin hanke keskittyy 5G:hen ja sen opettamiseen. Opetus- ja kulttuuriministeriön rahoittamien hankkeiden toiminta jatkuu 2023 loppuun asti lukuun ottamatta FITech Turku -hanketta, joka päättyy lukuvuoden 2021–2022 lopussa. (FITech, 2022)

Verkostoyliopistojen tarjoamat kyberturvallisuuden kurssit lukuvuonna 2021–2022 ovat

- Aalto-yliopisto:
  - Information Security 5 ECTS 14.09-2021-28.10.2021
  - Cybersecurity 5 ECTS 19.04.2022-24.05.2022

  - Digital ethics and sustainability 1 ECTS 01.03.2022-03.06.2022

- Tampereen yliopisto:
  - Cyber Security II: Specialisation 5 ECTS 10.01.2022-29.04.2022
  - Kyberturvallisuus I: perusteet 5 ECTS 13.01.2022-31.07.2022
  - Secure Programming 5 ECTS 10.01.2022-31.05.2022
  - Standards, interoperability and regulations in health informatics 5 ECTS 10.01.2022-27.02.2022

- Jyväskylän yliopisto:
  - System vulnerabilities 5 ECTS 10.01.2022-13.03.2022

- Lappeenrannan teknillinen yliopisto:
  - Henkilökohtainen tietoturva, osa 1: Näin meitä huijataan 1 ECTS jatkuvasti käynnissä

- Oulun yliopisto:
  - Tietoturva 5 ECTS 11.01.2022-13.03.2022

- Turun yliopisto:
  - Privacy and Security for Software Systems 5 ECTS 25.10.2021-20.12.2021
  - System and Application Security 5 ECTS 30.08.2021-24.10.2021
  - Technologies and Security 5 ECTS 10.01.2022-27.02.2022.
  - Network Infrastructure Technologies and Security 5 ECTS 10.01.2022-27.02.2022
  - Protocol Processing and Security 5 ECTS 10.01.2022-31.05.2022

- Vaasan yliopisto:
  - Management of Cyber Security 5 ECTS kevät 2022
  - FITech 5G 30 ECTS

Helsingin yliopisto ja Åbo Akademi eivät tarjoa tarkasteluhetkellä aihepiirin opetusta lukuvuonna 2021–2022. Puolestaan Lapin- ja Itä-Suomen yliopistot eivät ole osa FITech verkostoyliopistoa. (FITech, 2022)

6.3 Haastattelututkimuksen analyysi

Tutkimushanketta varten haastateltiin neljää kyberturvallisuuden asiantuntijaa neljästä yliopistosta. Haastattelussa kartoitettiin muun muassa kyberturvallisuuden opetuksen tilannetta tutkinto-ohjelmissa, joissa he toimivat ja laajemminkin näkemyksiä kyberturvallisuuden opetuksen tilanteesta Suomen yliopistoissa.

Kolmessa haastattelussa todettiin, että opiskelijoiden kiinnostus kyberturvallisuuden opiskeluun on lisääntynyt viime vuosien aikana niissä tutkinto-ohjelmissa, joissa vastaajat toimivat. Yhdessä haastattelussa asia ei noussut keskusteluun. Haastateltava 2 edusti tutkinto-ohjelmaa, jossa kyberturvallisuus ei ole pääpainopiste ja sanoi kiinnostuksen kasvun näkyvän konkreettisesti esimerkiksi kandidaatin tutkielmissa ja Pro graduissa, joissa opiskelijat yhä enemmän käsittelevät tietoturvallisuutta.

Vastauksissa nousi esille, että lisäresursseille on tarvetta ja niillä saataisiin edistettyä ja lisättyä kyberturvallisuuden opetusta tutkinto-ohjelmissa. Käytännössä tämä voisi

vastausten perusteella näkyä lisääntyvänä kurssimääränä, mutta myös erilaisten kyberturvallisuuden käytännön taitoja kehittävien harjoitusten lisäämisenä nykyistä enemmän. Yhtenä resurssihaasteena nähtiin kyberturvallisuuden osaajien rekrytoiminen yliopistoihin. Haastateltava 4 nosti tähän liittyen yliopistojen haasteet kilpailla palkassa yksityisen sektorin kanssa. Haastateltava 3 nosti näkemyksen siitä, että Suomessa on määrällisesti vähän sellaisia kyberturvallisuuden alan asiantuntijoita, joiden osaaminen kohtaa tutkinto-ohjelmassa tunnistettuihin tarpeisiin, joita on esimerkiksi tieteelliseen tietoon perustuvat käytännön taitoja kehittävät kyberharjoitukset.

Haastateltavia pyydettiin kertomaan, miltä kyberturvallisuuden opetus näyttäytyy tällä hetkellä Suomen yliopistoissa. Vastauksissa nousivat esille opetuksen hajanaisuus, sitä on määrällisesti vähän ja yliopistojen välistä opetusyhteistyötä ei ole juuri lainkaan. Yhteistyön kehittäminen nähtiin myös kehityskohteena, johon kannattaisi laittaa resursseja. Haastateltava 4 nosti esille, että sen edistämistä voitaisiin lähestyä esimerkiksi kyberturvallisuuden korkeakoulutusverkoston luomisen hankkeella, jossa luodaan ja tiivistetään yhteistyötä eri toimijoiden ja sidosryhmien välillä. Haastateltava 3 nosti esille myös kansainvälisen yhteistyön kehittämisen. Hän korosti myös sitä, että yhteistyön kehittämisessä tulee huolehtia siitä, että se tuo todellista lisäarvoa opetukseen. Haastateltava 2 nosti esille myös yhteistyön kehittämisen eri yliopistoissa toimivien kyberturvallisuuden asiantuntijoiden kesken. Haastateltavat nostivat esille myös yliopistojen erikoistumisalat kyberturvallisuudessa ja sen merkityksen. Opetuksen näkökulmasta haastateltavat 1 ja 4 nostivat esille, että yliopistojen tämänhetkiset opetustarjonnat kyberturvallisuudesta mahdollistaisivat opiskelijoille laajemmat erikoistumisvaihtoehdot, jos opetukseen liittyvä yhteistyö olisi vahvempaa.

Haastateltava 3 nosti esille tarpeen resursoida enemmän huippututkimukseen siten, että yliopistot keskittyisivät eri kyberturvallisuuden osa-alueisiin. Tätä hän täsmensi sillä, että kyberturvallisuuden pelikenttä on hyvin laaja, jonka vuoksi yliopistojen erikoistumisilla saataisiin mahdollisimman moni kyberturvallisuuden osa-alueista täytettyä. Lisäksi haastateltava totesi, että olisi tärkeää saada myös puhe kyberturvallisuudesta spesifimmäksi, koska tällä hetkellä puhutaan vain kyberturvallisuudesta, mikä ei kerro sitä, missä sen osa-alueissa Suomi on tällä hetkellä hyvä ja missä on kehitettävää.

Haastatteluissa selvitettiin tutkinto-ohjelman tavoite ja tieteenala huomioiden, että onko sellaisia kyberturvallisuuteen liittyviä trendejä, joiden opettamiseen tulisi erityisesti varata resursseja. Tähän liittyen nostettiin esille hyvin erilaisia aihepiirejä, mikä toisaalta kertoo myös kyberturvallisuuden poikkitieteellisyydestä. Lisäksi haastateltava 1 nosti esille, että trendejä voisi opettaa esimerkiksi erikoiskurssina, mutta on tärkeämpää keskittyä sellaisiin perustaitoihin ja hyviin kysymyksiin, jotka mahdollistavat opiskelijaa kohtaamaan työelämässä erilaisia haasteita, koska trendit tulevat vaihtumaan pitkässä juoksussa.

6.4 Johtopäätökset ja suositukset

Keskeiset alan tutkinto-ohjelmat ja suuntautumiset, jotka on raportin työn aikana tunnistettu, on esitetty tiivistetysti taulukossa 9. Lisäksi niiden yliopistojen osalta, joissa alan tutkinto-ohjelmia ei ole, on huomioitu kyberalaa lähellä oleva tutkinto-ohjelma. Sisäänottomäärät ja hakijamäärät eivät ole täysin tarkkoja. Tämä johtuu siitä, että luvuissa ei olla huomioitu mahdollisia avoimen väylän ja siirtohaun kautta olevia opiskelupaikkoja. Lisäksi tutkinto-ohjelmissa on usein kandidaatin ja maisteri opinto-oikeuden lisäksi mahdollisuus hakea vain maisteriopintoihin oikeuttavaan opinto-oikeuteen, johon on oma kiintiönsä. Nämä tekijät vaikeuttavat lopullisen sisäänottomäärän arviointia ja sen vuoksi listan luvut ovat suuntaa antavia.

Taulukosta 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 ottaen tarjolla lukuisissa tutkinto-ohjelmissa pakollisina- tai valinnaisina opintoina.

Kokonaan Suomessa ja osittain ulkomailla suoritettavien kyberturvallisuuden ja turvallisuuden tutkinto-ohjelmien sisäänottomäärän voidaan arvioida olevan karkeasti noin 250 vuonna 2022. Tutkimuksen perusteella arvioidaan, että vuosittain yliopistoista valmistuu kyberturvallisuuden ja turvallisuuden osaajia hieman vähemmän kuin, mitä sisäänottomäärä on. Edellä mainitussa luvussa on huomioitu vain kyberturvallisuuden ja turvallisuuden alan tutkinto-ohjelmien sisäänottomäärät ja se rajaa ulkopuolelle alaa lähellä olevat tutkinnot kuten tietotekniikan. Kokonaisuudessaan yliopistojen tuottama osaajamäärä on melko vähäinen suhteessa tunnistettuun osaajapulaan.

Hakijamäärät keskeisiin alan tutkinto-ohjelmiin kuten Jyväskylän yliopiston kyberturvallisuuden maisteriohjelmaan, Aalto-yliopiston Security and Cloud Computing (Security) ja Turun yliopiston Cyber Security -pääaineeseen osoittavat, että kyberturvallisuus koulutusalana kiinnostaa ihmisiä merkittävissä määrin.

Yliopistot tarjosivat tarkasteluhetkellä vähäisissä määrin kyberturvallisuuden täydennys- ja erikoistumiskoulutusta. Poikkeuksena oli Aalto-yliopisto, jossa alaan liittyvää täydennyskoulutusta oli enemmän tarjolla. Sen sijaan FITech verkostoyliopiston kautta on mahdollista opiskella useita kyberturvallisuuden kursseja lukuvuotena 2021–2022. Toisaalta sen valikoima koostuu yksittäisistä kursseista, eikä sen kautta ole mahdollista opiskella erillisiä kokonaisuuksia kyberturvallisuudesta.

Haastatteluissa nousi esille muun muassa, että kyberturvallisuuden opetuksessa ei ole yliopistojen välistä yhteistyötä ja sen kehittämisen hyödyt nähtiin merkittävinä. Lisäresurssit kehittäisivät opetusta ja se näkyisi esimerkiksi kyberturvallisuuden käytännön taitojen kehittävien harjoitusten lisäämisenä opetukseen nykyistä enemmän. Yhtenä resurssihaasteena nähtiin kyberturvallisuuden osaajien rekrytointi.

Taulukko 9. Tiivistelmä keskeisistä kyberalan tutkinto-ohjelmista

Yliopisto	**Tutkinto-ohjelmat/keskeiset kurssi-kokonaisuudet**	**Sisäänottomäärä 2022**	**Hakija-määrät 2022**
Aalto-yliopisto	Security and Cloud Computing (Security)	11	194
Aalto-yliopisto	Security and Cloud Computing (SECCLO)	76 ensimmäisellä hakukierroksella	735 ensimmäisellä hakukierroksella
Helsingin yliopisto	Tietojenkäsittelytieteen maisteriohjelma	45	452
Tampereen yliopisto	Suuntaus: Advanced Studies in Information Security 80 ECTS	1–30	-
Tampereen yliopisto	Master's Programme in Security and Safety Management – Safety Management and Engineering	8	76
Tampereen yliopisto	Master's Programme in Security and Safety Management – Security Governance	8	45
Jyväskylän yliopisto	Kyberturvallisuuden maisteriohjelma	45	184
Jyväskylän yliopisto	Turvallisuuden ja Strategisen analyysin maisteriohjelma	25	390
Turun yliopisto	Cyber Security -pääaine + EIT Digital Master School kaksoistutkinto-ohjelma	35 (sisältää EIT Digital Master School kaksoistutkinto-ohjelman aloituspaikat)	130 + EIT Digital Master School -kaksoistutkinto-ohjelman hakijat
Turun yliopisto	Cryptography -pääaine	5	13
Turun yliopisto	Tietoliikenne- ja kybertuvallisuusteknologia -pääaine	Arviolta 6–8 tieto- ja viestintätekniikan DI-tutkinto-ohjelman hakijoista suuntautuu tähän.	Tieto- ja viestintätekniikan DI-ohjelmaan, jossa on useita suuntautumisia, haki 37
Oulun yliopisto	Tietotekniikka TkK + DI	100 (DIA-yhteisvalinta)	522 (DIA-yhteisvalinta)
Lapin yliopisto	Oikeusnotaari ja oikeustieteen maisteri	140	2888
Åbo Akademi	Temaattinen moduuli: Safety-Critical and Autonomous Systems 20 ECTS	-	-
Itä-Suomen yliopisto	Tietojenkäsittelytiede LuK + FM (Joensuu)	68	261
Vaasan yliopisto	Automaatio ja tietotekniikka TkK + DI	52	279
LUT-yliopisto	Tietotekniikka TkK + DI	82	444 (DIA-yhteisvalinta)

Kyberturvallisuuden osaajien määrää yhteiskunnassa voidaan lisätä vaikuttamalla useaan eri tekijään. Yhtenä keinona on lisätä alan tutkinto-ohjelmia ja kasvattaa tutkinto-ohjelmien sisäänottomääriä. Nämä toimenpiteet vaativat kuitenkin henkilöresurssien kasvattamisen. Lisäksi kyberturvallisuuden osaajien määrää voidaan lisätä kehittämällä yliopistojen täydennyskoulutusta ja FITech verkostoyliopiston kurssitarjontaa. Vaasan yliopisto järjestää FITech 5G (30 ECTS) kokonaisuuden ja tähän peilaten voitaisiin miettiä olisiko verkostoyliopiston kautta mahdollista järjestää vastaavia opintokokonaisuuksia kyberturvallisuudesta tulevaisuudessa. Lisäksi opetusyhteistyön syventäminen yliopistojen välillä mahdollistaisi opiskelijoita erikoistumaan monipuolisemmin eri kyberturvallisuuden osa-alueisiin.

Tutkimuksessa luotu tilannekuva ei ole täydellinen. Kyberturvallisuuden opetusta tarjotaan useissa eri tiedekunnissa ja yksittäisiä kyberalan kursseja on tarjolla lukuisissa tutkinto-ohjelmissa, mikä vaikeuttaa tilannekuvan luomista. Tämän vuoksi on mahdollista, että joitakin kyberturvallisuuden kursseja on jäänyt tunnistamatta ja myös tutkinto-ohjelmia, joissa kyberturvallisuutta on sisällytetty tutkinto-ohjelman rakenteisiin. Tilannekuvaa voitaisiin tarkentaa jatkotutkimuksessa, jossa jaotellaan olemassa olevat kyberturvallisuuden kurssit esimerkiksi Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity ja siinä määritettyjen kyberturvallisuuden osa-alueiden perusteella Data Security, Software Security, Component Security, Connection Security, System Security, Human Security, Organizational Security ja Societal Security -kategorioihin. Tämän perusteella pystyttäisiin havainnollistamaan, onko osa-alueiden opetuksessa määrällisiä eroja vai jakautuuko opetus tasaisesti eri osa-alueiden kesken.

Lähteet

Aalto (2022). Koulutukset. Aalto University, Professional Development. https://www.aaltopro.fi/avoimet-ohjelmat

Aalto (2022). Master's Programme in Computer, Communication and Informations Sciences – Security and Cloud Computing. Aalto University. https://www.aalto.fi/en/study-options/masters-programme-in-computer-communication-and-information-sciences-security-and

CC (2017). Cybersecurity Curricula. 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

FITech (2022). About FITech. https://fitech.io/en/about-fitech/. Haettu 20.1.2022.

Helsingin yliopisto (2022a). Täydennyskoulutus. https://www.helsinki.fi/fi/hakeminen-ja-opetus/taydennyskoulutus. Haettu 6.4.2022.

Helsingin yliopisto (2022b). Tutkintoa täydentävä koulutus. https://www.helsinki.fi/fi/hakeminen-ja-opetus/hae-tutkintoa-taydentaviin-koulutuksiin. Haettu 6.4.2022.

Itä-Suomen yliopisto (2022a). Täydennyskoulutus. https://www.uef.fi/fi/taydennyskoulutus?gclid=Cj0KCQjwl7qSBhD-ARIsACvV1X2Qwd07cj6731Bk-4IHI4Cpd9Y6071GL2jEdfYcceVisCHUzfsu9woaAl8oEALw_wcB. Haettu 20.1.2022.

Itä-Suomen yliopisto (2022b). Erikoistumiskoulutukset ja erilliset opinnot. https://www.uef.fi/fi/erikoistumiskoulutukset-ja-erilliset-opinnot. Haettu 7.4.2022.

Jyväskylän yliopisto (2022a). Kyberturvallisuuden maisteriohjelma, filosofian maisteri (2v). https://www.jyu.fi/fi/hakijalle/koulutustarjonta/kyberturvallisuuden-maisteriohjelma-filosofian-maisteri-2-v. Haettu 11.3.2022.

Jyväskylän yliopisto (2022b). Turvallisuus ja strateginen analyysi -maisteriohjelma. https://opinto-opas.jyu.fi/2021/fi/tutkintoohjelma/tsama2020/. Haettu 11.3.2022.

Jyväskylän yliopisto (2022c). Täydennyskoulutus. https://www.jyu.fi/fi/jatkuva-oppiminen/taydennyskoulutus. Haettu 19.4.2022.

Lappeenrannan teknillinen yliopisto (2022). Täydennyskoulutus. https://www.lut.fi/taydennyskoulutus#:~:text=LUT%2Dt%C3%A4ydennyskoulutus%20tuo%20yliopiston%20huippuosaamisen,my%C3%B6s%20teknii-kan%20ja%20talouden%20rajapinnoilla. Haettu 14.1.2022.

Lapin yliopisto (2022). Jatkuva oppiminen. https://www.ulapland.fi/FI/Yhteistyo-ja-palvelut/Jatkuva-oppiminen. Haettu 18.3.2022.

Oulun yliopisto (2022). DigiHealth-täydennyskoulutus. https://www.oulu.fi/fi/joy/koulutushaku/digihealth-taydennyskoulutus. Haettu 20.1.2022.

SECCLO (2022). Selection results. https://www.secclo.eu/admission/selection-results/. Haettu 15.3.2022.

Tampereen yliopisto (2022a). Advanced Studies in Information Security. https://www.tuni.fi/opiskelijanopas/opintotiedot/opintokokonaisuudet/otm-31975feb-1d19-4168-aec5-183ea80a56e2?year=2021. Haettu 10.1.2022.

Tampereen yliopisto (2022b). Security Governance, Security and Safety Management. https://www.tuni.fi/en/study-with-us/security-governance-security-and-safety-management#expander-trigger--field-degree-study-objectives. Haettu 10.1.2022.

Tampereen yliopisto (2022c). Safety Management and Engineering, Security and Safety Management. https://www.tuni.fi/en/study-with-us/safety-management-and-engineering-security-and-safety-management#switcher-trigger--information. Haettu 10.1.2022.

Tampereen yliopisto (2022d). Täydennyskoulutus. https://www.tuni.fi/fi/tule-opiskelemaan/taydennyskoulutus?utm_source=google&utm_medium=cpc&utm_campaign=TAU_JOP_2020-2021_Taydennyskoulutus_GNX&gclid=Cj0KCQjwl7qSBhDARIsACvV1X2LGLAZXGADoeVjih3szRuYgioyhw0oHGp33UPy9Ju0sNHN-lFxiE1IaAm34EALw_wcB. Haettu 1.3.2022.

Turun yliopisto (2022a). MDP in Information and Communication, Cyber Security (Tech), 2020-2022. https://opas.peppi.utu.fi/en/programme/16075?period=2020-2022. Haettu 12.3.2022.

Turun yliopisto (2022b). MDP in Information and Communication, Cryptography (Tech), 2020-2022. https://opas.peppi.utu.fi/en/programme/16118. Haettu 12.3.2022.

Turun yliopisto (2022c). *Tieto- ja viestintätekniikka, Tietoliikenne- ja kyberturvallisuusteknologia (DI), 2020-2022. https://opas.peppi.utu.fi/fi/ohjelma/16282. Haettu 12.3.2022.

Turun yliopisto (2022d). Turun yliopiston täydennyskoulutustarjonta. https://www.utu.fi/fi/opiskelijaksi/turun-yliopiston-taydennyskoulutustarjonta. Haettu 15.1.2022.

Åbo Akademi (2022). Elinikäisen oppimisen keskus. https://www.abo.fi/fi/centret-for-livslangt-larande/. Haettu 17.2.2022.

Vaasan yliopisto (2022). Jatkuvan oppimisen koulutustarjonta. https://www.uwasa.fi/fi/koulutus/jatkuva-oppiminen/jatkuvan-oppimisen-koulutustarjonta?field_editors_target_id=All&lang=All&field_education_pricing_target_id=All&field=All&field_education_method_target_id=All&year=All&items_per_page=10. Haettu 18.2.2022.

7 Muiden toimijoiden kyberturvallisuuskoulutus

Tässä osassa selvitetään kansalaisen kyberturvallisuuden/digitaalisen turvallisuuden osaamisen kehittämisen tarjonta ja kehittämistarve. Aluksi tehtiin nykytilan kartoitus, jonka jälkeen nykytila analysoitiin. Aikaisempiin aineistoihin ja raportteihin sekä käynnissä oleviin hankkeisiin perustuen rakennettiin materiaali ja prosessi kansalaisten osaamisen vahvistamiseksi.

7.1 Aineiston keruu

Aineistoa kerättiin nykytilan kartoitusta varten yrityksiltä, kolmannen sektorin toimijoilta (yhdistykset, järjestöt, vapaa sivistystyö) sekä valtiollisilta ja kunnallisilta toimijoilta, jotka järjestävät kyberturvallisuuden koulutusta. Aiemmissa kartoituksissa, kuten Kyberalan tutkimus ja koulutus Suomessa (Lehto & Niemelä, 2019), on kartoitettu toimijoita, joilta tietoa lähdettiin keräämään. Tämän lisäksi kartoitettiin, onko kentälle tullut uusia toimijoita.

Aineistoa kerättiin verkosta etsimällä, sekä haastatteluiden ja kyselytutkimusten avulla. Kerätystä verkosta löytyvästä aineistosta muodostettiin ensin yleiskuva nykytilanteesta, jota lähdettiin tarkentamaan kyselyillä ja haastatteluilla.

Sellaisia organisaatioita, jotka järjestävät paljon kyberturvaisuuteen liittyvää koulutusta haastateltiin seuraavissa vaiheissa lisää. Verkossa tarjolla olevaa koulutustarjontaa tarkennettiin haastatteluilla, joilla lisäksi selvitettiin sitä, mihin suuntaan koulutustarjontaa ollaan kehittämässä ja kenelle se on erityisesti suunnattu.

Seuraavissa vaiheissa haastateltiin sellaisia asiantuntijoita, joilla on näkemystä kyberturvallisuuskoulutuksen tilasta ja tavoitetilasta, näitä asiantuntijahaastatteluja hyödynnettiin erityisesti kehitystarpeiden arvioinnissa.

Pienemmille organisaatioille, joita on paljon, ja jotka eivät erityisemmin mainosta järjestävänsä kyberturvallisuuteen liittyvää koulutusta suuremmassa mittakaavassa (kansalaisopistot, kesäyliopistot ja paikalliset yrittäjäjärjestöt) lähetettiin lomakemuotoinen kysely, jotta voitiin kartoittaa missä määrin kyberturvallisuuden koulutusta liittyy esimerkiksi muihin koulutussisältöihin.

7.2 Kolmannen sektorin toimijoiden järjestämä koulutustarjonta

Kolmannen sektorin toimijoista laajimmin kyberturvallisuuteen liittyvää koulutusta järjestää Maanpuolustuskoulutus – MPK. Muista kolmannen sektorin toimijoista osa kansalaisopistoista järjestää jonkin verran kyberturvallisuuteen liittyvää koulutusta, mutta esimerkiksi yrittäjäjärjestöjen osalta koulutus on satunnaista ja hyvin vähäistä.
Seuraavaksi esitellään kolmannen sektorin toimijoita:

Maanpuolustuskoulutus – MPK

MPK on Puolustusvoimien strateginen ja operatiivinen kumppani, joka osallistuu Suomen varautumiseen sekä turvallisuusasioista tiedottamiseen ja valistamiseen. Tässä alaluvussa esitetyt seikat perustuvat MPK:n edustajan haastatteluun, MPK:n Kyberturvallisuuden koulutusohjelmaan (MPK, 2021) sekä MPK:n verkkosivulta löytyviin tietoihin.

Vuonna 2022 MPK on vakiinnuttanut asemansa kansalaisten kyberturvallisuuskouluttajana, ja kouluttaa tuhansia ihmisiä vuosittain. Kyberkoulutuksen tavoitteena on toisaalta tarjota tavallisille kansalaisille perusvalmiudet ja toisaalta järjestää sotilaallisia valmiuksia palvelevaa koulutusta ja synnyttää puolustusvoimien reserviin kyberosaamista. MPK järjestää kaikille soveltuvaa matalan kynnyksen koulutusta edulliseen hintaan ja potentiaalia kasvattaa koulutettavien määrää löytyy, ongelmana onkin se, että ihmiset, jotka eivät ole tietoisia kyberturvallisuuteen liittyvistä seikoista, eivät myöskään osaa hakeutua koulutukseen. MPK on luonut kyberturvallisuuden koulutusohjelman, jonka osiot ovat:

1. Kyberturvallisuuden perusosaamisen koulutuskokonaisuus
2. Kyberturvallisuuden jatko-osaamisen koulutuskokonaisuus
3. Kyberturvallisuusosaamisen soveltamisen koulutuskokonaisuus
4. Puolustusvoimien johtama koulutus ja muu harjoitustoiminta
5. Kyberturvallisuuden kouluttajakoulutus

Peruskurssit ovat pääsääntöisesti kaikille avoimia TIVA – tai VARTU-kursseja ja jatko- ja erikoiskurssit ovat pääsääntöiset SOTVA-kursseja. Jatko- ja erikoistason kursseilla tarvitaan jo pohjatietoa, joka voi olla esimerkiksi siviiliammatin kautta hankittua tai MPK:n omalta, nousujohteiselta kurssipolulta saatua. Edellä mainittujen lisäksi yhdistys järjestää myös muita teemaan liittyviä koulutuksia ja seminaareja. Peruskursseille voivat tulla kaikki, ilman ennakkotietoja. (MPK, 2021)

Maanpuolustuskoulutuksen koulutusohjelman kuvauksessa kerrotaan, että koulutusohjelman tavoitteena on tarjota reserviläisille ja muille kansalaisille nousujohteinen kyberturvallisuuden koulutuspolku, joka vastaa sekä suomalaisen yhteiskunnan ja sen kokonaisturvallisuuden, että myös Puolustusvoimien kyberosaamiseen tarpeeseen. Kyberkoulutusohjelmaan liittyy myös tiedotus- ja valistuskoulutuksellinen näkökulma. MPK:ssa koulutus on lain mukaan tiedostuksen ja valistuksen (TIVA), vapaan yhdistystoimintaan liittyvää varautumis- ja turvallisuuskoulutusta (VARTU) sekä julkishallinnollisena yhteisönä toteutettavaa sotilaallista valmiutta palvelevaa koulutusta Puolustusvoimien ohjauksessa (SOTVA). Koulutusohjelman ensimmäisen kurssin verkkomateriaali on vapaasti kaikkien kansalaisten saatavilla itsenäistä oman osaamisen kehittämistä varten. Lisäksi MPK on julkaissut yhdessä Jyväskylän yliopiston kanssa kaikille kansalaisille tarkoitetun *Kyberin taskutieto — keskeisin kybermaailmasta jokaiselle* -oppaan. Siihen on koottu tärkeimmät kyberturvallisuusvinkit, joista voi olla hyötyä kenelle tahansa tavallisessa arkielämässä ja kriiseihin varautumisessa. (MPK, 2021)

MPK:n koulutuksen haasteena on se, että sellaiset henkilöt, jotka koulutusta tarvitsevat, eivät välttämättä siihen hakeudu. Myös yhdistyksen maanpuolustuksellinen ulottuvuus voi toimia joillekin karkottavana tekijänä. Koulutuksia ei välttämättä löydetä, ellei MPK ole tuttu, eikä esimerkiksi ymmärretä, että kursseja suorittaakseen ei tarvitse olla reserviläinen, eli ei tiedetä, että näihin koulutuksiin voi osallistua.

Haasteena onkin saada tieto koulutuksista kaikille kiinnostuneille ja tähän tarvittaisiin laajempaa markkinointia sekä näiden että muiden koulutusten osalta. Kaikille avoin koulutustarjonta olisi hyvä saada yhteen paikkaan, josta jokainen halukas voisi hakeutua koulutuksiin. Esimerkiksi kansalaisenkyberinfo.fi tai muu vastaava sivusto voitaisiin tätä tarkoitusta varten perustaa. (Panu Moilasen haastattelut, MPK:n verkkosivu, MPK:n koulutusohjelma) MPK:n kyberkoulutusohjelman tarkempi esittely on liitteessä 4.

Naisten valmiusliitto

Naisten valmiusliitto järjestää koulutusta yhdessä yhteistyökumppaniensa kanssa, yhteistyökumppaneita ovat mm. MPK, Puolustusvoimat, Lotta Svärd Säätiö, Maanpuolustuksen kannatussäätiö, Vapepa, SPEK ja Kova-toimikunta.

Valikoimassa on ajankohtaisia, naisille suunnattuja, turvallisuuteen keskittyviä kursseja. Vuosittain järjestetään kaksi suurempaa NASTA-harjoitusta sekä pienempiä PIKKU NASTA -harjoituksia. Tällä hetkellä valikoimassa on informaatiovaikuttamiseen liittyvä kurssi, jonka aikana tutustutaan informaatiovaikuttamisen eri muotoihin, informaatiosotaan ja propagandalta suojautumiseen. (Naisten valmiusliitto, 2021)

Vanhustyön keskusliitto

SeniorSurf rohkaisee ikääntyneitä ihmisiä tarttumaan tietokoneisiin ja nettiin. Sivustolla on koottuna opastusmateriaaleja ja ohjeita opastukseen hakeutumiseen. Sivuston sisällöissä ja järjestettävässä opastuksessa käsitellään myös kyberturvallisuustaitoja. (Vanhustyön keskusliitto, 2021)

Kauppakamari

Keskuskauppakamari tarjoaa verkkosivullaan Kansainvälisen kauppakamarin (International Chamber of Commerce, ICC) tuottaman Tietoturvaoppaan yrityksille kaikkien suomalaisten toimijoiden käyttöön. Opas on suunnattu yritysten omistajille, henkilöstölle ja johtajille. (Keskuskauppakamari, 2016)

Kauppakamarin verkkosivustolta on ostettavissa Tietoturva tavaksi -verkkokoulutus. Lisäksi paikalliset kauppakamarit ovat järjestäneet/järjestävät yksittäisiä kyberturvallisuuden koulutuksia, kuten esimerkiksi Tampereen kauppakamarin järjestämä Tietoturvariskeihin varautuminen ja tietomurtoon reagointi -koulutus. (Kauppakamari, 2021)

Suomen yrittäjät

Suomen yrittäjillä on ollut silloin tällöin kyberturvallisuuteen liittyvää koulutusta tarjolla. Kursseja on kuitenkin jouduttu perumaan vähäisen ilmoittautujamäärän vuoksi. Tutkimukseen ei saatu vastauksia. Arvion mukaan tieto- ja kyberturva-asiat ovat teemoina osana muita digiaiheisia koulutuksia, jolloin niitä ei välttämättä tunnisteta muiden aiheiden joukosta tai itsenäiseksi kokonaisuudekseen.

7.3 Kansalaisopistot ja kesäyliopistot

Suomessa on 177 kansalaisopistoa ja 18 kesäyliopistoa. Verkkohakujen perusteella selvisi, että kyberturvallisuuteen, informaatioturvallisuuteen tai digitaaliseen turvallisuuteen liittyvää koulutusta on jonkin verran tarjolla. Koulutustarjontaa päätettiin selvittää tarkemmin kyselyllä, jotta myös suunnitteilla oleva koulutustarjonta tulisi otetuksi huomioon. Kysely lähetettiin kaikille kansalaisopistoille ja kesäyliopistoille ja vastauksia saatiin 39 kappaletta.

7.3.1 Vastausten analyysi

1. Järjestättekö tällä hetkellä kursseja, jotka keskittyvät pääasiassa kyberturvallisuuteen, informaatioturvallisuuteen tai digitaaliseen turvallisuuteen?

   - Kyllä: 10,3 % vastaajaorganisaatioista
   - Ei: 89,7 % vastaajaorganisaatioista

2. Millaisia kursseja ja millaisilla sisällöillä?

   - *Tietoturva ja kyberturvallisuus; rikokset ja huijaukset Internetissä*
     - Tällä luennolla voit perehtyä tieto- ja kyberturvallisuuden perusteisiin tavallisten ihmisten näkökulmasta ja saada tietoja siitä, millaisia rikoksia ja huijauksia Internetin välityksellä tehdään.
   - *Teemallinen digityöpaja – Tietoturva*
     - Tietoturvasta huolehtiminen on tärkeää nykyisin monien laitteiden ja tilien aikana. Tule kuulemaan miten voit välttää pahimmat sudenkuopat ja mm. määrittää itsellesi turvalliset salasanat.
   - *Sähköiset asiointipalvelut -kurssi*
   - *Arjen tietotekniikka*
   - *Osuvat taidot kurssi*

Tämän lisäksi tietoturvallisuudesta puhutaan paljon tabletin, tietokoneen ja älypuhelimen peruskursseilla. Kohteina seniorit, lähinnä IT-turvallisuuteen liittyviä asioita. Käyttäjätunnukset, salasanat, tunnistautuminen. Virukset, madot, haittaohjelmat ym. Kurssien nimikkeet vaihtelevat. Lisäksi on ollut lyhyitä, luentotyyppisiä tietoiskuja tietoturvallisuudesta.

3. Käsitelläänkö kyberturvallisuuteen, informaatioturvallisuuteen tai digitaaliseen turvallisuuteen liittyviä asioita osana jotain kurssia?

   - Kyllä: 64 % vastaajaorganisaatioista
   - Ei: 36 % vastaajaorganisaatioista

4. Millä kursseilla näitä asioita käsitellään?

   - Senioreille kohdennetuilla digikursseilla käydään läpi yleisesti tietoturva-asioita.
   - Tietotekniikka-klinikka koulutuksia.

Kurssikuvaus: Opiskelijalle tarjotaan 3 x 45 min. opetuskokonaisuutta yksilöopetuksena. Kurssille mukaan henkilökohtainen laite (kannettava tietokone, tabletti tai älypuhelin), jonka opetusta halutaan. Kurssi räätälöidään oppilaan tarpeiden mukaan. Tämä kurssi sopii myös aloittelijoille.

Kohderyhmä on kaikki tietoteknisiä laitteita (älypuhelin, tabletti, tietokone) käyttävät kansalaiset, mutta erityisesti ikäihmiset, joille älylaitteiden käyttö tulee uutena haasteena vastaan. Tietoturva tulee näissä koulutuksissa aivan keskeisesti esille. Pelkästään tietoturvaan keskittyviä koulutuksia on järjestetty aiemmin, mutta tänä päivänä se kytketään osaksi laitekoulutusta.

5. Suunnitteletteko tulevaisuudessa lisäävänne kyberturvallisuuteen, informaatioturvallisuuteen tai digitaaliseen turvallisuuteen liittyvää koulutustarjontaa?

- Kyllä: 43,6 % vastaajaorganisaatioista
- Ei: 56,4 % vastaajaorganisaatioista

6. Millaisia koulutussisältöjä on suunnitteilla ja mille kohderyhmille?

Suunnitteilla on koulutusta senioreille, sekä erimerkiksi täydennyskoulutusta työikäisille. Lisäksi suunnitellaan myös koulutusta opettajille. Toisaalta koulutusjärjestäjätkin kaipaisivat lisätietoa aiheesta, koska aihepiirin koulutuksia ei välttämättä osata suunnitella.

7.3.2 Haasteet ja kehittämistarpeet

Kansalaisopistoilla on laaja opiskelijakunta ja valmiit markkinointikanavat koulutuksilleen. Kuitenkin vain harvat vastaajatahot järjestävät kyberturvallisuuteen, informaatioturvallisuuteen tai digitaaliseen turvallisuuteen liittyvää koulutusta tällä hetkellä.

Nykyiset sisällöt ovat kansalaisen perustaitojen kannalta hyviä ja ne olisikin hyvä saada laajemmin eri kansalaisopistoissa tarjolle. Kyberturvallisuuteen liittyviä asioita sivutaan tällä hetkellä 64 % vastaajaorganisaatioissa osana muiden kurssien sisältöjä, ja tätäkin osuutta olisi hyvä nostaa, jos varsinaisia, näihin teemoihin täysin keskittyviä kursseja ei esimerkiksi resurssien vähyydestä johtuen pystytä järjestämään.

Kansalaisopistoissa opiskelee paljon senioreita, ja heille suunnattuja kursseja onkin tarjolla. Kansalaisopisto on monille senioreille tuttu opiskelupaikka, joten seniorit tavoittavaa koulutussisältöä olisi hyvä järjestää ja markkinoida enemmänkin.

Alle puolet vastaajaorganisaatioista suunnitteli lisäävänsä kyberturvallisuuteen, informaatioturvallisuuteen tai digitaaliseen turvallisuuteen liittyvää koulutustarjontaa tulevaisuudessa. Tässä toki täytyy huomioida kyselyn ajankohta, joka oli vuoden 2021 loppupuolella. Tilanne on voinut tässä suhteessa parantua, sillä Ukrainan sodan myötä kyberasiat ovat saaneet huomattavasti enemmän medianäkyvyyttä ja herättäneet myös kansalaisten kiinnostusta.

Ne tahot, jotka suunnittelivat koulutuksen lisäämistä, suunnittelivat mm. täydennyskoulutusta työikäisille ja tilauskoulutusta, ja näille olisikin tarvetta, sillä erityisesti pk-yritysten työntekijät saattavat taloudellisista syistä jäädä koulutusta vaille, ja kansalaisopistojen koulutus on edullista, matalan kynnyksen koulutusta.

Vastauksissa mainittiin myös se, ettei kiinnostusta koulutuksiin osallistumiseen pienellä paikkakunnalla ole ja ettei kansalaisopistoilla ole itsellään tarpeeksi tietoa kyberturvallisuuskoulutuksesta.

7.4 Valtiollisten ja kunnallisten toimijoiden järjestämä kyberturvallisuuden koulutus

HAUS kehittämiskeskus Oy

eOppiva on valtionhallinnon yhteinen oppimisalusta, jota ylläpitää HAUS kehittämiskeskus Oy. Koulutukset on tarkoitettu valtionhallinnon työntekijöille ja oppimisympäristöön pääsy vaatii kirjautumisen. eOppivassa on kuitenkin myös kaikille avoimia koulutuksia.

HAUS kehittämiskeskus Oy:n tarjonnassa oleva kyberturvallisuuden koulutus tai koulutus, jossa on osana kyberturvallisuuden sisältöjä (sivustolla käytetään termiä digiturvallisuus). (HAUS, 2021)

Suurena kouluttajana HAUSia haastateltiin kyberturvallisuuteen liittyvästä koulutustarjonnasta ja siihen liittyvistä suunnitelmista. HAUSin kohderyhmänä ovat erityisesti valtion ja kuntien palveluksessa työskentelevät, joskin eOppivan koulutukset ovat pääosin kaikille avoimia ja esimerkiksi pk-yritykset voisivat niitä halutessaan hyödyntää.

HAUSilla aloitettiin kybermaailmaan, tarkemmin tietosuojaan liittyvä koulutus vuonna 2018. Sen jälkeen koulutustarjonta on kasvanut kattamaan laajasti erilaisia kyberturvallisuuden osa-alueita. HAUS markkinoi koulutuksia kohderyhmilleen ja osa koulutuksista on kohderyhmille myös ns. pakollisia.

HAUS suunnittelee lisäävänsä kyberturvallisuuteen liittyvää koulutusta tulevaisuudessa. Mahdollisuuksien mukaan järjestetään myös ei-verkkopohjaista koulutusta teemasta. Esimerkiksi asiantuntijoille voitaisiin järjestää yhteisiä Teams-koulutuksia ja valmennustuokioita ja lisäksi voitaisiin tarjota myös syventävää koulutusta ja pidempiä moduuleja kyberuhkia ennaltaehkäisevinä täydennyskoulutuksina kriittisissä tehtävissä työskenteleville henkilöille. HAUSin kyberturvallisuuskoulutusten piirissä on yli 100 000 henkilöä. Suorituksia on huhtikuussa 2022 yli 50 000.

HAUS mittaa koulutustoimintaansa jatkuvasti esimerkiksi kysymällä palautetta koulutuksiin osallistuneilta henkilöiltä. Osallistujat ovat erittäin tyytyväisiä koulutuksiin (asteikolla 1–5 92 % vastaajista antaa arvosanaksi 4 tai 5). Myös sisältö koetaan hyödylliseksi oman työn näkökulmasta. Osallistujat kiittelivät sitä, että sisällöt on esitetty mielenkiintoisesti ja koulutusten kysymykset/tehtävät auttavat miettimään teemoja käytännössä. Koulutuksen suorittajat pitivät erityisesi videoista, joita sisältyi verkkokoulutuksiin. (FT Petteri Kallion haastattelu)

Digi- ja väestötietovirasto

Digi- ja väestötietovirasto tarjoaa Digiturvallinen elämä -koulutuksia, joiden tavoitteena on opettaa turvallista toimintaa digimaailman uhkatilanteissa. Kokonaisuus sisältää verkkokoulutuksia organisaatioiden johdolle, digitaalisen turvallisuuden asiantuntijoille ja organisaatioiden koko henkilöstölle. Koulutuksia täydentää mobiilipeli, jonka avulla pääsee harjoittelemaan digiturvataitoja käytännöllisissä tilanteissa. Koulutuskokonaisuus on kaikille avoin ja maksuton. (DVV, 2021)

Lisäksi virastolla on JUDO-hanke, jonka tavoitteena on kehittää julkisen hallinnon digiturvan johtamista ja hallintaa, henkilöstön digiturvaosaamista sekä tarjoaa tukea turvallisempien palveluiden kehittämiseksi. Hanke tukee julkista hallintoa turvallisten ja luotettavien palveluiden kehittämisessä vuosina 2019–2023. Hankkeen puitteissa on toteutettu mm. verkkolähetyksiä ja työpajoja, joissa asiantuntijat kertovat parhaista käytännöistä ja antavat konkreettisia neuvoja digiturvallisuuden toteuttamiseen. (DVV, 2021)

TAISTO-harjoitukset ovat myös osa Digi- ja väestötietoviraston toimintaa. Näissä digitaalisen turvallisuuden harjoituksissa julkishallinnon toimijat harjoittelevat häiriötilanteissa toimimista kuvitteellisten tilanteiden kautta. (DVV, 2021)

Huoltovarmuuskeskus

Huoltovarmuuskeskus järjestää yhteistyössä muiden toimijoiden kanssa valtakunnallista Tieto-harjoitusta. Se on yritysten ja viranomaisten yhteistoimintaharjoitus laajojen kyberhäiriöiden varalta. Harjoituksia järjestetään joka toinen vuosi, ja ne kohdistetaan eri-

tyisesti erikseen valittaville toimialoille. Harjoittelulla tuetaan yritysten jatkuvuudenhallintaa, varautumista ja kehitetään sopimussuhteista yhteistyötä. (Huoltovarmuuskeskus, 2021)

Puolustusvoimat

Puolustusvoimilla on erillinen kybervarusmieskoulutus. Kybervarusmiehet saavat opetusta kyberpuolustuksen ammattilaisilta ja pääsevät kyberturvallisuuteen liittyviä töitä. Palveluksen aikana osallistutaan blue team / red team -harjoitustoimintaan, rakennetaan palveluja ja testataan niiden turvallisuutta sekä suoritetaan ohjelmointiprojekteja. (Puolustusvoimat, 2021a)

Lisäksi Puolustusvoimiin on perustettu Johtamisjärjestelmäkoulu, joka toimii johtamisjärjestelmätoimialan, kyberpuolustuksen ja informaatiopuolustuksen toimialakouluna. Koulu tukee Puolustusvoimien toimintaa ja tekee tiivistä yhteistyötä vastuualueellaan Maanpuolustuskorkeakoulun sekä puolustushaara-, toimiala- ja aselajikoulujen kanssa. (Puolustusvoimat, 2021b)

7.5 Yritysten tarjoama kyberturvallisuuden koulutus

2NS

2NS tarjoaa ns. perustasoista koulutusta yritysten henkilöstölle sekä tietoturvakoulutusta ohjelmistokehittäjille. Henkilöstön tietoturvakoulutusta myydään Kyberoppi-nimisenä verkkokoulutustuotteena, joka on tarkoitettu sekä yksityisille yrityksille että julkisille organisaatioille. Kyberoppi on saatavilla 14 eri kielellä ja koulutustuotteen piirissä on n. 100 000 käyttäjää. Koulutuksessa tutustutaan erilaisiin tietoturvatilanteisiin huumorin keinoin ja testataan omaa osaamista. (2NS, 2022)

Alma Talent

Alma Talent (2021) kouluttaa asiantuntijoita ja päättäjiä livenä ja verkossa. Yrityksen kyberturvallisuuteen liittyvät koulutukset:

- Tietosuojakursseja, tuotteisiin (kuten MS365) liittyviä tietoturvakursseja
- Privacy Pro -sertifikaatti
- Certified Information Privacy Professional/Europe (CIPP/E)
- Certified Information Privacy Technologist (CIPT)
- IT-riskienhallinta
- Tietosuojavastaavan koulutusohjelma
- Certified information privacy manager
- Toteuta onnistunut kyberharjoitus

Arrow ESC

Arrow ECS on Suomen ainoa virallinen EC-Council- koulutuskeskus. EC-Councilin hakkerointi- ja tietoturvakurssien tarkoituksena on laajentaa it-asiantuntijoiden osaamista tietoturvauhkiin ja niiltä suojautumiseen liittyen. (Arrow ESC, 2021)

Arter Oy

Yritys tarjoaa kursseja tietoturva-alan ammattilaisille. Tarjolla oleva kurssi: ISO 27001:2017 Tietoturvajärjestelmän rakentaminen. (Arter Oy, 2021)

CGI

CGI tarjoaa henkilöstökoulutusta yrityksille myös kyberturvallisuuteen liittyen. Lisäksi yrityksen tarjoamasta löytyy kyberturvallisuuteen keskittyvä, siirrettävä pakohuonepeli. Pakohuonepelin voi tilata toimipisteen parkkipaikalle mihin tahansa Suomessa. Peli räätälöidään organisaation tietoturvaohjeistusten mukaiseksi. (CGI, 2021)

Cyberwatch Finland

Cyberwatch Finland tarjoaa e-koulutuspalveluita ja konsultointia kybertietoisuuden ja -osaamisen parantamiseksi kaikilla organisaation tasoilla. Kyberjohtamisen peliharjoituksen avulla tuotetaan osaamista kyberturvallisuuden strategisella tasolla. Heillä on mahdollisuus tarjota myös yrityskohtaisesti räätälöityjä koulutuspaketteja. (Cyberwatch, 2021)

Elisa Santa Monica

Elisa Santa Monica (Elisa, 2021) tarjoaa kursseja ja koulutuspalveluja nimellä SantaCare Training Services. Tarjolla olevat kyberturvallisuuteen liittyvät kurssit:

- Henkilöstön tietoturvakoulutus,
- Johdon ja esimiesten perehdytys yritysten kyberuhkiin ja niiltä suojautumiseen,
- Johdanto kyberuhkien torjuntaan,
- Cyber threat intelligence and threat hunting,
- Tuotantoverkkojen kyberturvallisuuden perusteet,
- Yritysverkon tietoturva.

F-Secure

Cyber Security Base with F-Secure on Helsingin yliopiston yhteistyössä F-Secure Cyber Security Academyn kanssa järjestämä kurssisarja, joka keskittyy kyberturva-ammattilaisen työhön liittyvien ydintietojen ja kykyjen rakentamiseen. Kurssisarja on ilmainen ja avoin kaikille. Ei ilmoittautumista eikä osallistujamäärää ole rajoitettu. (Mooc.fi, 2021)

Lisäksi tarjolla on yritysten tarpeisiin räätälöityä koulutusta sekä valmiita ammattilaistason kursseja ja Capture the Flag -tapahtumia. Valmiit kurssisisällöt ovat (F-secure, 2021)

- Proactive Web Defense,
- Proactive Network Defense,
- Proactive First Response,
- Proactive Mobile Defense.

Granite

Granite (2022) tarjoaa koulutusta tietoturvan perusteista yritysten henkilöstölle. Verkkosivuston mukaan koulutuspalvelulla on yli 200 000 käyttäjää. Kurssikokonaisuudet ovat

- Tietoturvan perusteet 1: Teknologinen tietoturva
  - Verkkokoulutus tietoturvan teknologisista perusteista koko henkilöstölle.
- Tietoturvan perusteet 2: Tietoturva työssä
  - Työpaikan tietoturvallisuuden periaatteet ymmärrettävänä verkkokoulutuksena.
- Tietoturvan perusteet 3: Arki ja työmatka
  - Tietoturvallisuuden periaatteita käytännön esimerkkien kautta koko henkilöstön tarpeisiin.
- Tietoturvan perusteet 4: Tietoturva etätöissä
  - Etätyön kriittisimmät tietoturvakysymykset selkeänä verkkokoulutuksena.

Insta

Insta tarjoaa kyberturvallisuuden koulutusta yritysten henkilöstölle. Instan tarjoama koulutus on tarkoitettu lähinnä IT-alan ammattilaisille, mutta tilauksista yrityksille voidaan järjestää myös ns. perustason koulutusta. Koulutustarjonta on pääosin turvalliseen sovelluskehitykseen liittyvää täydennyskoulutusta. Lisäksi Insta järjestää kymmeniä kyberturvallisuusharjoituksia vuodessa. Jatkossa tarkoitus jatkaa saman tyyppisiä koulutuksia.

Kyberturvallisuustaitojen tulisi olla kansalaistaitoja, joiden kouluttaminen lähtee peruskoulutasolta. Julkinen sektori voisi tarjota enemmänkin kansalaisten taitoihin sekä omaan henkilökohtaiseen tietoturvaan liittyvää koulutusta. Useat ihmiset saavat kyllä koulutusta työpaikoillaan, ainakin jos työskentelevät suuremmissa yrityksissä. Pienempien yritysten työntekijöillekin olisi ilmaista tarjontaa verkossa, mutta sen löydettävyys on huono. (Insta, 2021; Elina Niemimaan haastattelu)

JYVSECTEC by JAMK

JYVSECTEC (Jyväskylä Security Technology) on Jyväskylän ammattikorkeakouluun kuuluva kyberturvallisuuteen ja tekoälykehitykseen keskittynyt tutkimus-, koulutus- ja kehityskeskus. JYVSECTEC tarjoaa kyberturvallisuuskoulutuksia ja kyberturvallisuusharjoituksia yrityksille ja julkisille toimijoille. JYVSECTEC on kehittänyt Suomen kansallisen Cyber Range -kyberharjoitusympäristön (Cyber Range on kansainvälinen termi kyberturvallisuuden tekniselle koulutus- ja harjoitusinfrastruktuurille). Lähes kaikissa JYVSECTEC:n järjestämissä koulutuksissa ja harjoituksissa hyödynnetään kansallista Cyber Range -ympäristöä RGCE (*Realistic Global Cyber Environment*).

JYVSECTEC tarjoaa monipuolista koulutusta tieto- ja kyberturvallisuuden eri osa-alueilla. Koulutusten tarkoituksena on lisätä henkilöstön tietoja ja taitoja sopeutua digitalisaation jatkuvaan muutokseen ja kyberuhkiin. Tarjottavissa koulutuksissa kehitetään yksilön osaamista valituista aiheista nykyaikaisilla harjoitusmenetelmillä ja käytännön harjoituksilla. Tarjottavia koulutuksia ovat *Ethical Hacking and Penetration Testing*

(kesto 3päivää), *Threat Hunting* (kesto 2 päivää)*, Cyber Incident Response* (kesto 2 päivää)*, Cyber Security Operations Center* (kesto 3 päivää) ja tämän lisäksi *räätälöityjä koulutuskokonaisuuksia* asiakastarpeen mukaisesti.

JYVSECTEC järjestää kyberturvallisuusharjoituksia yrityksille ja julkisille toimijoille. Vuodesta 2013 alkaen JYVSECTEC on järjestänyt kansallista kyberturvallisuusharjoitusta KYHA. KYHA-harjoitusten tarve ja määrä on kasvanut vuosittain ja vuonna 2022 kansallisia KYHA-harjoituksia järjestetään 4 kappaletta (Turvallisuuviranomaiset, Valtionhallinto, Terveydenhuolto, sekä Kuntasektori ja kriitiinen infrastruktuuri). KYHA-harjoitusten lisäksi JYVSECTEC tarjoaa kyberturvallisuusharjoituksia yrityksille ja julkisille toimijoille. Tarjottavia kyberturvallisuusharjoituksia ovat *Live Exercise*, *Digital Forensics and Incident Response (DFIR) Exercise* ja *Threat Hunting Exercise*.

JYVSECTEC tarjoaa myös FINCSC-sertifikaattia (Finnish Cyber Security Certificate). FINCSC on yrityksille ja yhteisöille luotu sertifiointijärjestelmä tietojen turvaamiseen ja liiketoiminnan jatkuvuuden varmistamiseen. Se on kohdistettu erityisesti PK-sektorille, mutta soveltuu käytettäväksi kaikenkokoisille organisaatioille niiden toimialaan katsomatta. Erityisesti koulutustarpeen kannalta huomattavaa on, että FINCSC-sertifiointi antaa kattavan tilannekuvan organisaation kyberturvallisuuden tasosta. (JYVSECTEC, 2022; FINCSC, 2022)

KPMG

KPMG (2021) tarjoaa tietoturvakursseja ja koulutuksia. Kurssit voivat tähdätä johonkin ammattitutkintoon kuten CISSP, CISM tai CPTE tai liittyä johonkin tiettyyn aiheeseen, esimerkiksi tietosuojavastaavan rooliin. Kouluttajina kursseilla ja koulutuksissa toimivat KPMG:n tietoturvan ja tietosuojan asiantuntijat. Koulutuksia ovat

- Tietoturvallisuuden ammattitutkintoihin valmentavat koulutusjaksot (CISSP, CISM, CPTE),
- Kattava tietoturvallisuuden koulutusohjelma, 10 pv (vaihtoehtoisesti yksittäisiä koulutusjaksoja),
- Sovelluskehityksen tietoturvallisuus-koulutusohjelma,
- Automaation tietoturva,
- Organisaation tietosuojariskien hallinta,
- Tietoturvallisuuden seminaarit ja ajankohtaistapahtumat,
- Koko henkilöstön tietoturva- tai tietosuojaperehdytys,
- Hankintojen/sovelluskehityksen tietoturvallisuus,
- Tietosuojavastaavan koulutus,
- Säännölliset ja jatkuvat koulutusohjelmat (esim. 2 kk välein aihe/osallistujaryhmä).

Navisec

Navisec tarjoaa tietoturva- ja tietosuojakoulutusta verkossa eri kohderyhmille. Koulutukset on suunnattu erityisesti yrityksille, kunnille ja julkisille organisaatioille, sosiaali- ja terveystoimelle sekä opetuksen ja varhaiskasvatuksen toimijoille. Navisec:n (2022) valikoimassa on seuraavia koulutuksia:

- Henkilöstön tietoturva- ja tietosuojakoulutus,

- Luottamushenkilöiden tietoturva ja tietosuoja,
- Turvallinen tiedonhallinta,
- Sosiaalihuollon tietoturva ja tietosuoja,
- Opetustoimen tietoturva ja tietosuoja,
- Varhaiskasvatuksen tietoturva ja tietosuoja,
- Turvallisen salasanan muistilista.

Nixu Oyj

Nixu Oyj tarjoaa koulutusta ja kyberharjoittelua organisaation toiveiden mukaisesti henkilöstölle. Koulutukset koostuvat esimerkiksi luennoista, harjoituksista, ryhmätöistä ja peleistä. Nixu tuottaa asiakasorganisaatioilleen myös koulutusmateriaaleja ja eLearningeja henkilöstön kouluttamiseen. Lisäksi koulutusvalikoimassa on esimerkiksi tietojenkalasteluyritysten simulointia ja tietoturvapakohuoneita. Koulutukset suunnitellaan organisaatioiden tarpeita ja esimerkiksi sertifiointeja vastaaviksi. Nixu järjestää myös tietoturvatapahtumia ja tarjoaa palveluita henkilöstön tietoturvatietoisuuden kehittämiseen. Kyberharjoitukset räätälöidään tilaajaorganisaatioiden tavoitteiden mukaisesti ja saatavilla on esimerkiksi laajoja toiminnallisia harjoituksia sekä pienimuotoisempia työpöytäharjoituksia ja näiden välimuotoja. (Nixu, 2021a)

Nixu Challenge -harjoitteluohjelma antaa nuorille mahdollisuuden päästä työskentelemään aitoihin kyberturva-alan töihin Nixun ammattilaisten rinnalla. Haku harjoitteluohjelmaan käynnistyy teknisen haasteen ratkaisemisella, jonka avulla hakijat osoittavat tekniset taitonsa ja ongelmanratkaisukykynsä. (Nixu, 2021b)

Lisäksi tarjolla on rekrykoulutusta kyberturva-alalle AW Academyn kautta. Koulutus kestää 12 viikkoa, jonka jälkeen koulutettavat aloittavat työskentelyn Nixulla traineina. (Anu Laitilan haastattelu)

Professio Finland Oy

Professio Finland Oy tarjoaa kyberturvallisuuteen liittyvää koulutusta erityisesti IT-alan ammattilasille, sekä julkisen puolen että yksityisen sektorin tarpeisiin. (Professio, 2022)

Salus Qualitas Consulting Oy

Salus Qualitas Consulting Oy on turvallisuuteen ja laatuun erikoistunut konsultointi- ja koulutuspalveluja tarjoava yritys. Yrityksen valikoimassa on sote-alan tietoturva- ja tietosuojakoulutusta. (Salus, 2021)

Saranen Consulting Oy

Saranen Cyber Security Academy on tietoturva-alan rekrykoulutusohjelma. Viiden kuukauden koulutusohjelmaan sisältyy lähiopetusta, etäopiskelua sekä työssäoppimista. Koulutusohjelman tavoitteena on, että ohjelman päätyttyä opiskelijat työllistyvät yhteistyöyrityksiin erilaisiin työrooleihin. Koulutuksen ensisijainen kohderyhmä on ICT-alan korkeakoulututkinnon suorittaneet tai työkokemuksen kautta vastaavan ammattitaidon omaavat TE-toimiston asiakkaat, jotka haluavat kehittää osaamistaan. (Saranen, 2021)

Silverskin Information Security Oy

Silverskin Academy tarjoaa kyberturvakoulutuksia yrityksille. Kyberturvatietoisuuskoulutukset kehittävät motivaatiota ja yksilöiden kykyä havaita kyberriskejä sekä toimia turvallisesti arjessa. Hallinnolle ja asiantuntijoille suunnatut koulutukset on suunniteltu kehittämään organisaation kyvykkyyttä ja taitoja puolustautua. Silverskinin (2021) tarjoamia koulutuksia ovat:

- Kyberturvatietoisuus,
- Turvallinen sovelluskehitys,
- Käytännön harjoitukset,
- Kyberturvademot,
- Luennot ja katsaukset.

Sovelto Oyj

Sovelto Oyj tarjoaa tietoturvakoulutuksia organisaatioiden tarpeisiin. Valikoimassa on laajasti kursseja eri aiheista, kuten web-palvelun haavoittuvuuksista, tietokantojen tietoturvasta, PKI:sta ja varmenteista. (Sovelto, 2021)

Sulava Oy

Sulava Oy on Microsoftin virallinen koulutuskumppani, joka tarjoaa luokkamuotoisia- ja online-koulutuksia, kartoituksia, testauksia, luentoja ja koulutusmateriaaleja. Valikoimassa on yleisiä Microsoft 365:een liittyviä koulutuksia, joissa käsitellään myös turvallisuusasioita, sekä yleisempiä koulutuksia, kuten ”Tietoturvakoulutus etätyötä tekeville”. (Sulava, 2021)

7.6 Muita toimijoita

Teknologiateollisuus

Teknologiateollisuuden MyTech-ohjelma on yläkouluille ja toiselle asteelle suunnattu oppimiskokonaisuus. Osana sitä on julkaistu yhteistyössä Maol:ryn kanssa kyberturvallisuuden pakopeli. Kyseessä on virtuaalinen oppimiskokonaisuus, jossa nuoret pääsevät pakopelin omaisesti tutustumaan kyberturvallisuuden maailmaan, kyberturva-alaan ja siihen liittyviin ammatteihin. (Teknologiateollisuus, 2021)

Tieto- ja viestintätekniikan ammattilaiset TIVIA ry

TIVIA järjestää IT-koulutuksia eri aiheista. Osa koulutuksista on TIVIAn järjestämiä ja osa TIVIAn yhteistyökumppaneiden järjestämiä. Koulutussisällöissä on koulutuksia myös tietoturvasta. (TIVIA, 2021)

7.7 Muiden EU-maiden malleja

National Cyber Security Index (NCSI) mittaa eri maiden kyberkyvykkyyttä, Suomi sijoittuu listauksessa kymmenenneksi ja Suomea edellä EU-maista ovat 1. Kreikka, 2. Liettua, 3. Belgia, 4. Tšekki, 5. Viro, 6. Saksa, 7. Portugali, 8. Espanja sekä 9. Puola. (NCSI, 2022)

Kreikka

Kreikan kyberturvallisuusstrategiassa todetaan, että tarkoituksenmukaista ja kohdennettua kyberturvallisuustietoisuuskoulutusta tulee järjestää kansalaisille. Tässä työssä pitää hyödyntää eri kanavia, jotta koulutus tavoittaa eri kohderyhmät. Kreikassa on luotu ”käyttäjä-kansalaisen” kyberturvallisuusohjelma, jonka toimeenpanoa valvoo kansallinen kyberturvallisuusviranomainen. Ohjelma sisältää informaatiokampanjoita sekä koulutusta yhteistyössä yliopistojen kanssa. (Cyberwiser, 2022; Greece, 2020, 12)

Liettua

Liettuan kyberturvallisuusstrategiassa korostetaan kansallisen kyberturvallisuuskulttuurin luomista ja vastuutetaan asiaa julkisen sektorin lisäksi myös yksityiselle sektorille, jotta esimerkiksi yritykset pitäisivät huolta kansalaistensa kyberosaamisesta. Julkisten puolen työntekijöille tarjotaan koulutusta ja kouluttautujien määrä kasvaa vuosittain. (Lithuania, 2018, 12–13)

Belgia

Belgian kyberturvallisuusstrategiassa todetaan, että erilaisia kyberturvallisuuteen keskittyviä koulutuksia tulee järjestää räätälöidysti eri ikäryhmille ja eri taitotason omaaville kansalaisille. Myös kampanjoita kyberturvatietoisuuden lisäämiseksi tulee järjestää. Belgian kyberturvallisuuskeskus tarjoaa ohjeita ja koulutusmateriaalia kodin kyberturvallisuudesta, kouluille, hallitukselle ja yhteiskunnan toiminnan kannalta kriittisten sektorien toimijoille. Belgiasta löytyy sivusto (www.sefeonweb.be), jonne tietoa ja koulutusta koordinoidusti kerätään. Belgian kansallisen kyberturvallisuuden vastuut on määritelty melko tarkasti, kyberturvallisuuskeskuksen vastuulla on hallinnoida projekteja ja koordinoida yhteistyötä sekä lisätä tietoisuutta uhkista ja niiltä suojautumisesta, lisäksi se konsultoi säännöllisesti Internet-palveluntarjoajia siitä, miten kansalaisten kyberturvallisuutta voidaan lisätä. (CCB, 2021)

Tšekki

Tšekissä kyberturvallisuuteen liittyvää tietoisuutta pyritään parantamaan kaikilla kansalaisten elämän osa-alueilla. Erityisesti opettajille tarjotaan ei-tutkintoon johtavaa täydennyskoulutusta, jotta he osaavat paremmin opettaa oppilaitaan. Lisäksi julkisten sektorin työtekijöille koulutetaan kyberturvallisuustaitoja. Iäkkäämmälle väestölle tarjotaan koulutusta teknologian turvalliseen käyttöön sekä disinformaation tunnistamiseen. Lisäksi kaikki suuren riskin ryhmät tarvitsevat räätälöityä koulutusta iästä riippumatta. Myös Tšekissä tehdään kyberiin liittyviä laajoja tai kohdennetumpia tietoisuuskampanjoita. Julkinen puoli tekee koulutus- ja tietoisuustyössä laajasti yhteistyötä yksityisen sektorin, akateemisen maailman sekä kolmannen sektorin toimijoiden kanssa. (Czech, 2021, 18–19)

Viro

Virossa sekä yksityisen sektorin, että julkisen sektorin kyberturvallisuuteen liittyvä tietoisuus ja osaaminen vaatii kehittämistä, jotta jokainen taho ymmärtää oman vastuunsa. Koulutuksen ja tutkimuksen ministeriön (Ministry of Education and Research

vastuulla on suunnitella elinikäisen oppimisen aktiviteetteja, mukaan lukien kyberosaamisen kehittämistä. Virossa tavoitteena on, että jokaisella kansalaisella on hyvä “kyberlukutaito” (cyber-literate society). Suunnitteilla on, että luodaan yhteinen alusta, josta löytää materiaalia itsenäiseen opiskeluun. Kuten Suomessa, Virossakin on ollut haasteena tiedon ja koulutuksen pirstaloituminen liian moneen paikkaan. Jatkossa päävastuu kansalaisen yleisen tietoisuuden lisäämisestä on RIA:lla (Estonian Information Security Authority). Myös kohdennetumpaa koulutusta tullaan tarjoamaan avainhenkilöille. Nykyään RIA järjestää säännöllisesti koulutuskampanjoita kansalaisille, esimerkiksi vuonna 2019 keskityttiin kouluttamaan vanhempaa väestöä ja vuonna 2020 pieniä ja keskisuuria yrityksiä, etätyöskentelytaitoja kaikille ja uudelleen senioreita. (Estonia, 2019, 65–71; Estonia, 2021)

Saksa

Saksassa tavoitteena on keskittyä siihen, että pienet ja keskisuuret yritykset, koulutusorganisaatiot, järjestöt, säätiöt ja tavalliset kansalaiset saavuttavat tarvittavat tiedot ja taidot turvalliseen toimintaan digitaalisessa ympäristössä. Koulutus tapahtuu paitsi formaaleissa oppilaitoksissa, myös työpaikoilla. Lisäksi käyttäjille on tarjolla kohderyhmäspesifejä koulutussisältöjä. Saksassa on myös mahdollista suorittaa ”DsiN digital driving licence” sertifikaatti digitaidoista (sisältäen turvallisuustaidot). Lisäksi käynnissä on useita hankkeita, jotka tähtäävät tiettyjen kohderyhmien, kuten haja-asutusalueiden senioreiden kybertaitojen parantamiseen. (BMI, 2021)

Portugali

Portugalissa on käynnissä “National Digital Skills Iniative e. 2030”, osana tätä hanketta tavoitteena on parantaa myös kansalaisten kyberturvallisuuteen liittyviä taitoja. Tätä työtä on kuitenkin tarkoitus tehdä myös erikseen kyberturvallisuustoimijoiden toimesta. Koulutussisältöjä ja tietoa tarjotaan erityisesti lapsille, nuorille, senioreille ja muille riskiryhmille. Kyberturvallisuuskoulutusohjelmia tarjotaan myös organisaatioille ja tavallisille kansalaisille. (Portugal, 2019, 2891–2893)

Espanja

Espanjassa toteutetaan tietoisuutta lisääviä kampanjoita kansalaisille sekä yrityksille ja tarjotaan eri kohderyhmille räätälöityä tietoa sekä koulutusta. Erityisesti keskitytään itsensä työllistäjiin sekä pieniin ja keskisuuriin yrityksiin. Lisäksi erityisesti organisaatioiden johtajien kyberturvallisuuteen liittyvää ymmärrystä pyritään lisäämään, jotta he voivat paremmin ymmärtää millaisia toimia ja koulutusta tarvitaan suojaamaan heidän organisaatioitaan. Median kanssa tehdään yhteistyötä, jotta erityisesti nuoret pystytään tavoittamaan. (Spain, 2019, 56–57)

Puola

Puolassa nähdään, että opettajien täydennyskoulutus kyberturvallisuuden saralla on tärkeää, jotta saadaan kasvatettua kansalaisia, jotka tunnistavat uhkat ja osaavat toimia digitaalisessa maailmassa. Hallinto pyrkii systemaattisesti kasvattamaan kansalaisten tietoisuutta kyberturvallisuudesta yhteistyössä kolmannen sektorin ja yksityissektorin

toimijoiden kanssa. Koulutusta järjestetään muun muassa digitaalisen ympäristön oikeuksista ja velvollisuuksista, kyberrikosten uhrien oikeuksista, sekä tietovuotojen tai muiden yksityisyyden loukkausten uhrien oikeuksista. Kyberturvallisuuskampanjoita kohdistetaan eri kohderyhmille, kuten lapsille, vanhemmille sekä senioreille. Kansalaisia pyritään valistamaan, jotta he osaavat tunnistaa disinformaation ja vaikuttamisyritykset. (Poland, 2019)

7.8 Käynnissä olevia kehittämishankkeita

Digivisio 2030

Hankekuvauksen mukaan ”Digivisio on kaikkien Suomen korkeakoulujen yhteinen hanke, joka avaa oppimisen kansalliset tietovarannot yksilön ja yhteiskunnan käyttöön” (Digivisio, 2022). Hankkeen myötä luotava ekosysteemi tuo koulutussisältöjä myös elinkeinoelämän ja yhteiskunnan käyttöön. Tavoitteena on myös mahdollistaa se, että jokainen oppija voi kerryttää osaamistaan tarkoituksenmukaisella tavalla. Tavoitteena on tarjota sisältöjä jatkuvaan oppimiseen. (Digivisio, 2022)

Kyberturvallinen Eurooppa -hanke

Liikenne- ja viestintäministeriö toteuttaa Aalto-yliopiston kanssa hankkeen, jossa tavoitteena on luoda EU-maille yhteinen kyberturvallisuuden kansalaistaitojen koulutuspaketti. Hankkeessa kartoitetaan nykytila koko EU:n alueella, ja tämän kartoitustyön pohjalta luodaan kaikille avoin verkkosivusto, josta löytyy koulutusmateriaalia kaikkien EU-maiden kielillä. Hanke alkaa vuonna 2022 ja kestää vuoden 2024 loppuun saakka. (Liikenne- ja viestintäministeriö, 2022)

Digikompassi

Euroopan unionin digitaalistrategian tavoitteena on valjastaa digitalisaatio palvelemaan ihmisiä ja yrityksiä sekä tukemaan tavoitetta tehdä Euroopasta ilmastoneutraali vuoteen 2050 mennessä. Tämän tueksi Euroopan komissio teki ehdotuksen EU:n digitaalisesta kompassista maaliskuussa 2021. Syyskuussa 2021 komissio esitti toimintaohjelmaa, jolla tavoitteet toteutettaisiin ja joka velvoittaisi jäsenmaita laatimaan omat etenemissuunnitelmat. Digitaalinen kompassi on jaettu neljään osa-alueeseen: osaaminen, turvalliset ja kestävät digitaaliset infrastruktuurit, yritysten digitaalinen muutos sekä julkisten palvelujen digitalisointi.

Suomen digitaalinen kompassi perustuu EU:n digitaaliseen kompassiin ja tätä koskevaan ohjelmaehdotukseen, jossa määritellään vaatimukset kansallisille tiekartoille. Ohjelmasta odotetaan päätöstä syksyllä 2022. Suomen digikompassi sisältää kansalliset tavoitteet, joilla tuetaan EU:n digikompassin tavoitteiden saavuttamista. Lisäksi digikompassiin on koottu kansallisia, EU-kompassista täydentäviä tavoitteita ja teemoja, jotka ovat tarpeellisia Suomen digitalisaatiokehityksen vauhdittamiseksi ja joista Suomi haluaa olla tunnettu.

7.9 Johtopäätöksiä ja kehittämisehdotuksia

7.9.1 Nykytila

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.

Lapset ja nuoret saavat tänä päivänä kyberturvallisuuteen liittyvää koulutusta osana omaa koulutuspolkuaan sekä peruskoulutuksessa että myöhemmissä opiskeluvaiheissa. Kuitenkin ne, jotka ovat opiskelleet aikana, jolloin kyberturvallisuus ei ollut osa peruskoulutusta tai myöhempiä opintoja, voivat tällä hetkellä jäädä täysin ilman kyberturvallisuuskoulutusta elleivät sitä työpaikkansa kautta saa.

Yrityksille ja muille organisaatioille koulutusta tarjoavia tahoja Suomessa on melko paljon. Suurten yritysten ja julkisten organisaatioiden työntekijät saavat työhönsä liittyen yleensä koulutusta, mutta pk-yritysten työntekijät, itsensä työllistäjät ja yrittäjät voivat jäädä sitä ilman. Tässä voi olla ongelmana myös se, että pk-yritysten johto tai yrittäjät eivät tunnista tarvetta koulutukselle tai esteenä voi olla myös koulutuksen hinta.

Pk-yrityksille on tarjolla erilaisia tukimuotoja sekä hyvinkin edullista koulutusta, mutta tarpeita ei mahdollisesti tunnisteta, eikä koulutusta osata kaivata. Suomen Yrittäjien edustaja totesi, että koulutusta on joskus yritetty järjestää, mutta se on peruttu liian vähäisen osallistujamäärän vuoksi.

Koulutustarjonta on hajallaan, ja kaikilla ei ole ymmärrystä siitä, millaista koulutusta he itse tarvitsisivat. Kansalaisopistot kouluttavat eri ikäryhmiä, mutta edes koulutusorganisaatioilla itsellään ei välttämättä ole käsitystä siitä, millaista koulutusta kannattaisi järjestää.

Huomionarvoista on myös se, että IoT -puolta ei tässä kartoituksessa läpikäydyissä koulutuksissa juurikaan käsitellä. Koska IoT-laitteisiin liittyy riskejä, joita tavallinen kuluttaja ei välttämättä ymmärrä, olisi tämän kaltaiselle koulutukselle selkeä tarve.

Suurten yritysten ja julkisten organisaatioiden osalta tilanne on hyvä. Suurilla yrityksillä on kyvykkyyttä ostaa henkilöstölleen kyberturvallisuuskoulutusta, ja sitä tarjoavat yritykset myös mielellään räätälöivät koulutuksen yrityksen henkilöstölle sopivaksi. Julkisella sektorilla HAUS tarjoaa laajan valikoiman kyberturvallisuuteen liittyvää koulutusta, jolla saadaan varmistettua henkilöstön perusosaaminen.

Suomessa tarvittaisiin lisää eri kohderyhmille suunnattua, ns. pehmeämpää (eiteknistä) koulutusta. Tällä hetkellä vanhemmille ikäluokille ei ole paljoa koulutustarjontaa. Myös saavutettavuus olisi tärkeä muistaa, ja mahdollistaa opiskelu eri kielillä. Esimerkiksi Ylellä, DVV:llä, MPK:lla ja monilla muilla tahoilla on tarjolla hyvää materiaalia, kansalaisille tarkoitettu koulutus olisikin hyvä saada yhden sateenvarjon alle, jotta löydettävyys paranisi, myös markkinointiin tarvitsisi vastuullisen sekä taloudellisia resursseja.

7.9.2 Suomen mallin kehittäminen

Suomen kyberturvallisuusstrategiassa todetaan, että valtakunnallista digiturvallisuuden koulutus- ja harjoitusjärjestelmää vahvistetaan osana julkisen hallinnon digitaalisen turvallisuuden koulutusta, jotta julkishallinnon, yritysten ja muiden sidosryhmien työntekijöiden sekä kansalaisten osaaminen kehittyy (Turvallisuuskomitea, 2019). Käytännössä Suomi eroaa monista tässä luvussa esitetyistä maista tällä hetkellä siinä, että koulutustarjonta on melko pirstaloitunutta, eikä välttämättä tavoita juuri niitä kohderyhmiä, jotka tietoa ja koulutusta eniten tarvitsisivat. Suomessa olisi hyvä nimetä kansalaisten kouluttamisesta ja kouluttamiseen liittyvän yhteistyön koordinoinnista vastaava taho, jolla olisi riittävät resurssit tämän tehtävän hoitamiseen. Esimerkiksi Kreikan ohjelma, joka tarjoaa jokaiselle kansalaiselle koulutuspolun yhdessä paikassa voisi olla Suomessakin hyvä vaihtoehto.

Edellä mainituissa EU-maissa yhteistyötä kansalaisten kouluttamiseksi tehdään laajasti, mutta koordinointi ja koontivastuu on määritetty selkeästi. Riskiryhmien tunnistamista ja heille räätälöityä koulutusta tehtiin monessa maassa, ja tällainen kohdennettu koulutus hyvin markkinoituna varmastikin tavoittaa kohderyhmänsä paremmin, kuin ns. yleinen koulutus.

Esimerkiksi Belgiassa kansalaisen kyberturvallisuustaitoja kehittävät koulutukset ja tietopaketit on koottu yhden sivuston alle, jonka päivittämisestä vastaa paikallinen Kyberturvallisuuskeskus. Sivustoa markkinoidaan aktiivisesti kansalaisille erilaisten kampanjoiden yhteydessä. Vastaava alusta on myös Virossa suunnitteilla.

Useissa maissa on tunnistettu se, että pienten ja keskisuurten yritysten työntekijät, jotka ovat jo päättäneet koulutuspolkunsa aikana, jolloin kyberturvallisuutta ei opetettu formaalissa koulutuksessa, jäävät helposti kyberturvallisuuskoulutusta vaille. Näin on tutkimusaineiston perusteella myös Suomessa.

Suomessa senioreiden kyberturvallisuuskoulutus on jäänyt paljolti kolmannen sektorin toimijoiden varaan ja olisi tärkeää pohtia, miten koulutusta voitaisiin kohdistaa ja tuoda saavutettavaksi senioreille paremmin.

Muissa EU-maissa tunnistetut riskiryhmät ja mahdollisesti tietoa ja koulutusta vaille jäävät tahot, kuten itsensä työllistäjät, pienten ja keskisuurten yritysten työntekijät, lapset, nuoret, maahanmuuttajat sekä seniorit olisi tärkeää huomioida räätälöidyllä koulutuksella myös Suomessa.

7.9.3 Pk-yritysten ja yrittäjien huomiointi

Valtion ja kuntien työntekijät sekä suurten yritysten työntekijät saavat useissa tapauksissa edes hieman kyberturvallisuuteen liittyvää peruskoulutusta työpaikkansa kautta. Vaikkakin tämä koulutus keskittyy usein työhön liittyviin turvallisuusseikkoihin, ovat koulutuksissa opitut asiat hyödynnettävissä myös vapaa-ajalla. Lisäksi yhä useammat työnantajat ovat kiinnostuneita kouluttamaan työntekijöilleen myös suoraan työhön liittymättömiä kyberturvallisuuden asioita, koska esimerkiksi etätyön lisäännyttyä merkittävästi, on myös kotiympäristön digitaalisella turvallisuudella työnantajan kannalta merkitystä.

Pk-yritysten henkilöstö, itsensä työllistäjät ja yrittäjät jäävät helposti vaille kyberturvallisuuteen liittyvää koulutusta. Näitä tahoja olisikin hyvä tukea siinä, että he ylipää-

tään ymmärtäisivät kyberturvallisuuskoulutuksen tärkeyden ja pystyisivät sitä hankkimaan joko maksuttomista tai maksullisista lähteistä. Esimerkiksi ns. palvelusetelit näiden koulutuspalveluiden hankintaan voisivat olla yksi vaihtoehto. Näitä toimijoita helpottaisi, jos tarjolla oleva kyberturvallisuuskoulutus olisi kerättynä esimerkiksi yhden verkkosivuston alle. Asiantuntijahaastatteluissa korostuikin tarve saada koulutustarjonta paremmin eri toimijoiden tietoon ja hyödynnettäväksi.

Keväällä 2022 kyberturvallisuusasiat ovat olleet esimerkiksi medioissa paljon esillä, mikä on todennäköisesti lisännyt ymmärrystä teeman tärkeydestä, mutta silti tarvitaan kohdennettua viestintää pk-yrityksille, itsensä työllistäjille ja yrittäjille kyberturvallisuuskoulutuksen merkityksestä liiketoiminnan riskien pienentäjänä. Viestintää näille tahoille voisi toteuttaa laajamittaisemmilla kampanjoilla sekä lisäksi järjestöjen, kuten Suomen yrittäjien, Kauppakamarin sekä muiden järjestöjen kanssa yhteistyössä.

7.9.4 Riskiryhmien huomiointi

Riskiryhmiksi/kriittisiksi kohderyhmiksi tässä kartoituksessa on tunnistettu erityisesti seniorit, lapset sekä pienten lasten vanhemmat ja maahanmuuttajat, joille ei ole tarjolla koulutusta omalla kielellään, sekä luonnollisesti työssään kyberriskejä kohtaavat henkilöt. Työssään riskejä kohtaavat henkilöt saavat tällä hetkellä koulutusta yleensä työnantajiensa kautta, mutta erityisesti seniorit ja lapset, sekä heidän vanhempansa ja maahanmuuttajat, joilla on heikko suomen kielen taito jäävät koulutuksen ulkopuolelle.

Riskiryhmille olisi hyvä järjestää koulutusta esimerkiksi yhteistyössä heidän kanssaan jo muutenkin työskentelevien tahojen, kuten esimerkiksi lasten osalta Lastensuojelun keskusliiton kanssa. Lisäksi kyberturvallisuusasioiden tärkeydestä tulisi viestiä erityisesti senioreille ja heidän kanssaan työskenteleville, sekä pienten lasten kanssa työskenteleville ja heidän vanhemmilleen. Tässäkin auttaisi, jos kaikille avoin koulutus olisi helposti kerättynä yhteen paikkaan ja eritelty selkeästi kohderyhmittäin.

Kansalaisopistot ovat suuri senioreiden kouluttaja, mutta kaikilla kansalaisopistoilla tai opettajilla ei itsellään ole riittäviä tietoja kyberturvallisuuden kouluttamisesta. Kansalaisopistojen opettajille (kuten muillekin opettajille) ja koulutussuunnittelijoille olisi hyvä tarjota täydennyskoulutusta kyberturvallisuuteen liittyen. Myös hinta nähtiin ongelmaksi kursseille osallistumisessa, joten sitäkin voisi pohtia voisiko kansalaisopistoja tukea kurssien järjestämisessä, jolloin ne voisivat olla osallistujille edullisia tai ilmaisia.

Myös maahanmuuttajat tulisi huomioida yhtenä riskiryhmänä, sillä koulutusta olisi hyvä olla tarjolla omalla kielellä. Tässä sekä viestinnällistä että koulutuksellista yhteistyötä voisi tehdä maahanmuuttajien kanssa työskentelevien tahojen kanssa.

7.9.5 Koordinaation selkeyttäminen

Kartoituksessa sekä haastatteluissa korostui tarve kansalaisen kyberturvallisuuskoulutuksen koordinoinnille. Suomessa olisi hyvä nimetä kansalaisten kouluttamisesta ja kouluttamiseen liittyvän yhteistyön koordinoinnista vastaava taho, jolla olisi riittävät taloudelliset ja henkilöresurssit tämän tehtävän hoitamiseen. Nykyisen koulutustarjonnan löydettävyys on koettu ongelmaksi, joten myös koulutusten tai koulutukset kokoavan sivuston markkinointiin tulisi panostaa.

Eri kohderyhmille suunnattu kyberturvallisuuskoulutus olisi hyvä saada kootusti yhdelle verkkosivustolle, jonka ylläpidosta ja päivittämisestä vastaisi kansalaisten kyberkouluttamisesta ja kouluttamiseen liittyvän yhteistyön koordinoinnista vastaava, nimetty taho. Sivuston kokoamisessa voi hyödyntää tätä kartoitusta eri koulutustarjoajien tarjonnasta, joskin sivuston ylläpito vaatii jatkuvaa koulutustarjonnan kartoitusta.

Sivustolla koulutukset olisi hyvä eritellä kohderyhmittäin ja pyrkiä myös viestimään kyberturvallisuuden merkityksestä jokapäiväisessä elämässä kunkin kohderyhmän kannalta.

7.9.6 Koulutus kohdentaminen

Muissa EU-maissa Suomen Kyberturvallisuuskeskusta vastaavat tahot ovat kohdentaneet sekä viestintää että koulutusta erityisesti niille tahoille, jotka muuten uhkaavat jäädä kyberturvallisuuskoulutuksen ulkopuolelle. Kohdennetun koulutuksen rakentamisessa on tärkeää huomioida kohderyhmien tarpeet ja kyvyt. Ns. yleinen kyberturvallisuuskoulutus ei sovi kaikille kohderyhmille.

Nämä koulutukset olisi hyvä suunnitella yhdessä esimerkiksi senioreiden, lasten ja maahanmuuttajien kanssa työskentelevien kanssa ja myös koulutusten markkinointi ja levittäminen olisi hyvä tehdä yhteistyössä kohderyhmät tuntevien tahojen kanssa.

Sekä koulutuksissa että koulutuksen tärkeyden viestimisessä tulisi huomioida kohderyhmien käyttämät kanavat, yleiset digitaidot sekä saavutettavuus.

7.9.7 Yhteistyön lisääminen

Muissa EU-maissa on luotu toimivia yhteistyöverkostoja yritysten, kyberturvallisuuskoulutusta koordinoivien valtiollisten tahojen sekä kolmannen sektorin toimijoiden kanssa. Suomessa olisi hyvä muodostaa kansalaisten kouluttamisesta ja kouluttamiseen liittyvän yhteistyön koordinoinnista vastaavan tahon johdolla yhteistyöverkosto kansalaisen kyberturvallisuustaitojen kehittämiseksi. Verkostoa voisi hyödyntää myös kyberkoulutukset kokoavan verkkosivuston suunnittelussa sekä ylipäätään kansalaisen kyberturvallisuuden kehittämisen konseptin jatkojalostuksessa.

Verkostoon kannattaisi kutsua mukaan ainakin tässä kartoituksessa esitetyt suurimmat koulutustarjoajat kaikilta sektoreilta sekä myös riskiryhmien ja pk-yritysten ja yrittäjien kanssa toimivien tahojen edustajat. Verkoston osaamista voisi hyödyntää lisäksi sekä koulutusten luomisessa että niiden markkinoinnissa.

Lähteet

2NS (2022). Tietoturvakoulutus. 2NS – Second Nature Security Oy. https://www.2ns.fi/palvelut/koulutus/. Haettu 20.3.2022.

Alma Talent (2021). Alma Talent koulutus. https://koulutus.almatalent.fi/. Haettu 16.10.2021.

Arrow ECS (2021). Arrow ECS Edu. https://edu.arrow.com/fi. Haettu 16.10.2021.

Arter Oy (2021). Koulutukset. https://www.arter.fi/koulutukset/. Haettu 16.10.2021.

BMI (2021). Cyber Security Strategy for Germany 2021. Federal Ministry of the Interior, Building and Community.

CCB (2021). Cybersecurity Strategy Belgium 2.0 2021–2025. Centre for Cyber Security Belgium.

CGI (2021). Tietoturva- ja kyberturvallisuus. CGI. https://www.cgi.com/fi/fi/tietoturva. Haettu 16.10.2021.

Cyberwatch (2021). Palvelut. Cyberwatch Finland. https://www.cyberwatchfinland.fi/fi/palvelut/. Haettu 17.10.2021.

Cyberwiser (2022). Greece (GR). Cyberwiser.eu. https://www.cyberwiser.eu/greece-gr. Haettu 1.4.2022.

Czech (2021). National Cyber Security Strategy of the Czech Republic. National Cyber and Information Security Agency.

Digivisio (2022). Digivisio 2030 -hanke. https://digivisio2030.fi/. Haettu 30.3.2022.

DVV (2021). Digiturvapalvelut. Digi- ja väestötietovirasto. https://dvv.fi/digiturva. Haettu 1.10.2021.

Elisa (2021). Elisa Santa Monican kurssit. https://yrityksille.elisa.fi/kurssit. Haettu 17.10.2021.

Estonia (2019). Cybersecurity Strategy. Republic of Estonia. Republic of Estonia Ministry of Economic Affairs and Communications.

Estonia (2021). Cybersecurity in Estonia 2021. Republic of Estonia Information System Authority.

FINCSC (2022). FINCSC - Finnish Cyber Security Certificate. https://www.fincsc.fi. Haettu 12.4.2022.

F-secure (2021). Consulting and training. https://www.f-secure.com/en/consulting/training. Haettu 17.10.2021.

Granite (2022). Tietoturvan perusteet -verkkokoulutukset. Granite. https://granite.fi/tietoturvan-perusteet/. Haettu 15.3.2022.

Greece (2020) *National Cybersecurity Strategy.* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Greece

HAUS (2021). eOppiva. HAUS kehittämiskeskus Oy. https://www.eoppiva.fi/. Haettu 20.10.2021.

Helsingin työväenopisto (2021). Tietotekniikka. https://www.hel.fi/sto/fi/opiskelu/tietotekniikka. Haettu 16.11.2021.

Huoltovarmuuskeskus (2021). Tieto20. https://www.huoltovarmuuskeskus.fi/a/tieto20-harjoitus-testaa-yhteistoimintaa-laajassa-kyberhairiotilanteessa. Haettu 13.10.2021.

Insta (2021). Kyberturvallisuus. https://www.insta.fi/palvelut/kyberturvallisuus/. Haettu 18.10.2021.

JYVSECTEC (2022). JYVSECTEC by Jamk. https://www.jyvsectec.fi. Haettu 12.4.2022.

Kauppakamari (2021). Verkkokoulutukset. https://koulutusonline.fi/course/index.php?categoryid=12. Haettu 15.11.2021.

Keskuskauppakamari (2016). Tietoturvaopas yrityksille. Keskuskauppakamari. https://kauppakamari.fi/wp-content/uploads/2020/06/tietoturvaopas-yrityksille.pdf

KPMG (2021). Tietoturvakurssit ja räätälöidyt koulutukset. KPMG. https://home.kpmg/fi/fi/home/palvelut/neuvontapalvelut/teknologiakonsultointi/tietoturva/tietoturvakoulutus.html. Haettu 18.11.2021.

Lehto M. & Niemelä, J. (2019). Kyberalan tutkimus ja koulutus Suomessa 2019. Informaatioteknologian tiedekunnan julkaisuja 83/2019, Jyväskylän yliopisto. https://www.jyu.fi/it/fi/tutkimus/julkaisut/it-julkaisut/kyberalan_koulutus_suomessa_verkkoversio.pdf

Liikenne ja viestintäministeriö (2022). Suomi kehittää kyberturvallisuuden kansalaistaitoja koko Euroopan unionin alueelle. https://valtioneuvosto.fi/-/suomi-kehittaa-kyberturvallisuuden-kansalaistaitoja-koko-euroopan-unionin-alueelle.

Lithuania (2018). National Cyber Security Strategy. Ministry of National Defence, Republic of Lithuania.

Mooc.fi (2021). Cyber Security Base with F-Secure. Course series. Mooc.fi. https://moocfi.github.io/courses/2017/cybersecurity/. Haettu 17.10.2021.

MPK (2021). Kyberturvallisuuden ja tiedustelun koulutusohjelma. MPK ak 132/1.04/7.9.2021, Maanpuolustuskoulutus – MPK.

MPK (2021). Kyber- ja informaatioturvallisuus. Maanpuolustuskoulutus – MPK. https://mpk.fi/koulutukset/kyber-ja-informaatioturvallisuus/. Haettu 1.10.2021.

Naisten valmiusliitto (2022). Koulutukset. https://naistenvalmiusliitto.fi/koulutukset/tapahtumakalenteri/. Haettu 20.2.2022.

NCSI (2022). Ranking. NCSI Project. https://ncsi.ega.ee/ncsi-index/?order=rank. Haettu 25.3.2022.

Nixu (2021a). Kyberharjoittelu ja koulutus. Nixu Oyj. https://www.nixu.com/fi/palvelut/kyberharjoittelu-ja-koulutus. Haettu 14.11.2021.

Nixu (2021b). Nixu Challenge. Nixu Oyj. https://thenixuchallenge.com/entry/. Haettu 14.11.2021.

Poland (2019). Cybersecurity Strategy of the Republic of Poland. Ministry of Digital Affairs.

Portugal (2019). National Strategy for Cyberspace Security 2019-2023. *Portuguese Official Journal*, Series 1 — No. 108 — 5 June, 2019.

Professio (2022). IT-koulutukset. Professio Finland Oy. https://professio.fi/it/. Haettu 20.2.2022.

Puolustusvoimat (2021a). Kybervarusmies. https://intti.fi/kybervarusmies-puolustusvoimien-johtamisjarjestelmakeskus. Haettu 10.11.2021.

Puolustusvoimat (2021b). Puolustusvoimiin perustetaan johtamisjärjestelmäkoulu. https://puolustusvoimat.fi/-/puolustusvoimiin-perustetaan-johtamisjarjestelmakoulu.

Salus (2021). Sotetraining-verkkokoulutukset. Salus Qualitas Consulting Oy. https://www.sotetraining.fi/. Haettu 18.11.2021.

Saranen (2021). Cyber Security Academy. Saranen Consulting Oy. https://www.saranen.fi/rekrytointikoulutus/cybersecurityacademy. Haettu 18.11.2021.

Silverskin (2021). Academy. Silverskin Information Security Oy. https://www.silverskin.com/fi/academy.html. Haettu 20.11.2021.

Sovelto (2021). Tietoturva – koulutukset. Sovelto Oyj. https://www.sovelto.fi/koulutukset/tietoturva/. Haettu 21.11.2021.

Spain (2019). National Cybersecurity Strategy. Prime Minister's Office, Government of Spain.

Sulava (2021). Tietoturvakoulutukset. Sulava Oy. https://sulava.com/kauppa/?category=tietoturva. Haettu 23.11.2021.

Teknologiateollisuus (2021). Kyberturvallisuus. https://mytechohjelma.fi/kyberturvallisuus/. Haettu 16.10.2021.

TIVIA (2021). Koulutukset ja tapahtumat. Tieto- ja viestintätekniikan ammattilaiset TIVIA ry. https://tivia.fi/koulutukset/. Haettu 12.11.2021.

Turvallisuuskomitea (2019). Suomen kyberturvallisuusstrategia 2019. Valtioneuvoston periaatepäätös 3.10.2019. https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf

Vanhustyön keskusliitto (2021). SeniorSurf. https://www.seniorsurf.fi/. Haettu 15.10.2021.

8 Osaamistarvekartoitus

Haastattelut, eri selvitykset ja laajemmat tutkimukset kertovat Suomen merkittävästä kyberosaajapulasta. Kilpailua osaajista vaikeuttaa se, että ongelma on globaali. Tässä luvussa arvioidaan pulan suuruutta henkilöittäin ja kohdentumista eri osaamisaloihin. Tulokset tukeutuvat aiempiin selvityksiin asiasta ja laajempiin tilastotietoihin. Erityisesti Liikenne- ja viestintäministeriölle tehdyn kyberosaamistarpeita kartoittaneen Osaamistarve-esiselvityksen (VN, 2020) aineistosta johdetaan, kuinka suuria valtakunnalliset osaamistarpeet voisivat olla. Tämä luku rajoittuu keskustelemaan tietyistä ammatti- ja koulutusnimikkeistä, mikä on vain näkyvin osa tarpeista. Kyberturvallisuus on poikkileikkaavaa, minkä vuoksi yhteiskunnan osaamisvajeet ja koulutuksen haasteet ovat tässä luvussa kuvattua laajemmat ja monisyisemmät. (ENISA, 2019; ENISA, 2021; CPO, 2020; CBR, 2020; NIST, 2017; UK Government, 2021; AustCyber, 2020)

8.1 Osaajatarve

Elinkeinoelämä, viranomaiset ja kolmas sektori tarvitsevat uusia kyberammattilaisia. LVM:n kyberosaamistarpeita kartoittavassa kyselyssä 73 % vastaajista näkee organisaatioissaan merkittävää osaajapulaa. Lähes kaikki vastaajat ottaisivat uusia ammattilaisia, jos heitä vain saisi. Kyselyn perusteella tarpeet vaihtelevat voimakkaasti. Vastaajat edustivat viittä eri ryhmää ja antoivat suuruusluokan rekrytointitarpeistaan. Kyselyvastauksia oli 273. Vastaajista noin puolet oli yrityskentästä, vajaa puolet oli julkiselta sektorilta ja kolmannelta sektorilta 5 %. Vastaajaryhmien perusteella kyselytuloksia on yleistetty, jotta saatiin arvio koko yhteiskunnan tarpeista. 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. Tieto- ja kyberturvatuotteita ja -palveluita tarjoavien yritysten ja organisaatioiden teknologiateollisuuden järjestön Kyberalan (FISC, 2021) kyselyn mukaan alan yrityksistä 87 % aikoi palkata kyberturvallisuusalan henkilökuntaa. Kyberalan 2021 jäsenkyselyn perusteella noin 35 % vastaajista ilmoitti osaavan työvoiman puutteen olevan merkittävin alan kasvua rajoittava tekijä. Brittiläisissä kyberturvallisuusyrityksissä vastaava luku oli 13 %. (UK Government, 2021)

Työvoimatarpeesta on tehty muutamia keskeisiä arvioita. Kyberalan (FISC) jäsenet työllistivät Suomessa vuonna 2020 arviolta 6 500–7 000 kyberturva-alan ammattilaista. Kyberturvallisuuteen liittyviä tuotteita ja palveluita tarjoavien yritysten rekrytoinnin kasvuprosentin vaihteluväli oli Osaamistarve-esiselvityksessä tyypillisesti 21 %-100 %. Vastauksista voidaan johtaa Suomessa noin 4 000 lisäosaajan tarve kyberturvallisuuteen keskittyvissä yhtiöissä. Laskelmat perustuvat vastausten jakaumaan ja aiempaan tietoon ammattilaisten nykymäärästä sekä näiden jakautumisesta. Aiemmassa VTT:n tutkimuksessa (Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2016) arvioitiin, että muissa yrityksissä ja julkisella sektorilla työskentelee täysipäiväisesti sama määrä kyberammattilaisia. Näiden tasavahvojen ryhmien lisäksi on hieman suurempi joukko niitä, jotka tekevät vastaavia tehtäviä muiden töiden lisäksi. Tämä tarkoittaa, että kyberammattilaisista 60 % tekee tämän kanssa töitä kokopäiväisesti ja 40 % osa-aikaisesti. *Cyber security skills in the UK labour market 2021* -tutkimuksessa arvioitiin kybertehtävien ja kyberosaamista

hyödyntävien suhdetta työmarkkinoilla. Rekrytointi-ilmoitusten perusteella (2 700 ja 5 000 kuukaudessa) suhde olisi 35 % ja 65 %.

Muissa vastaajaryhmissä (muut yksityiset, julkinen ja kolmas sektori) lisätarve on pienempi, alle 20 % eli 1 000–4 000 henkilöä lähivuosien aikana. Kokopäiväisten vaihteluväli on siten yhteensä 5 000–8 000 kokopäiväistä lisärekrytointia. Samoilla laskuperusteilla lisäystarve henkilöille, jotka tekevät näitä tehtäviä oman toimensa ohella, on 1000–5000. Yhteensä tarve on siten 6 000–13 000 kyberammattilaista parin seuraavan vuoden aikana.

Arviohaarukka ei poikkea paljoa muista suomalaisista laskelmista. Kyberturvallisuusalan sisäisen kyselyn ja muun materiaalin perusteella alan järjestö näki, että vuonna 2025 tarve olisi jopa 15 000:lle alan osaajalle. (FISC, 2020; ENISA, 2019; ISC2, 2021) Aiemman, Teknologiateollisuuden vuonna 2018 tekemän arvion mukaan sen jäsenyritykset tarvitsevat 11 400 uutta ICT-ammattilaista. Teknologiateollisuuden kyselyssä tietotekniikkaosaajien tilannetta arvioitiin koko teknologiateollisuuden intresseistä. (Teknologiateollisuus, 2018)

ICT-työpaikkojen ennakoitua kasvuvauhtia voidaan peilata Tilastokeskuksen työvoimatutkimuksen kanssa. Sen perusteella ICT-ala on trendinomaisessa kasvussa mutta nousu on lähinnä ohjelmistojen, konsultoinnin sekä siihen liittyvän toiminnan varassa. Valmistus, televiestintä ja tietopalvelutoiminta eivät ole viime vuosina kasvaneet. (FiCom, 2021) Edellä mainittujen raporttien perusteella kaivatuista ICT-ammattilaisista suurin osa päätyisi työskentelemään kyberturvallisuuden parissa.

Kansainvälisen työvoimakyselyn (ISC2, 2021) mukaan valtiot ovat vastanneet kasvaneeseen kysyntään. Vuoden aikana alalle on näissä maissa tullut 700 000 osaajaa, erityisesti Saksa on kasvattanut voimakkaasti osaajapohjaa. Talouden ja väestön koon suhteen Suomen kokoisessa Irlannissa kyberammattilaisia on 15 000. Irlannissa alan työntekijöiden määrän kasvu vuodessa oli 800 henkilöä. (ISC2, 2021)

8.2 Ammattilaisten sijoittuminen eri osaamisalueisiin

Yritysten osaamistarpeiden kirjo on laaja. Osaamistarve-esiselvityksessä kysyttiin, mihin erityisosaamisaloihin vastaajat suuntaisivat uudet rekrytointinsa. Jaottelussa käytettiin yleistä NCWF-kehikon[1] mukaista luokittelua. Amerikkalaista viitekehystä on laajasti hyödynnetty kuvaamaan kyberturvallisuuteen liittyviä osaamisen pääluokkia tai osaamiskategorioita sekä näiden alla olevia erityisosaamisaloja. Seuraavaksi tarkastellaan eri pääluokkien ja joidenkin erityisosaamisalojen suhteellista kiinnostavuutta rekrytoitavien organisaatioiden näkökannalta. Näin saatuja tuloksia suhteutetaan aiemmin johdettuun henkilömäärien arviointiin. (Niemelä, 2019) Osaamisen pääluokat ovat:

1. Turvallinen tuotanto (Securely Provision),
2. Operointi ja ylläpito (Operation and Maintain),
3. Kokonaisuuden valvonta ja johtaminen (Oversee and Govern),
4. Suojaaminen ja puolustus (Protect and Defend),

[1] Viitekehikosta käytettiin kyselyssä nimeä NIST. Kyseessä on Yhdysvaltojen National Institute of Standards and Technologyn (NIST), National Initiative for Cybersecurity Education (NICE) -ohjelmaan liittyvä National Cybersecurity Workforce Framework (NCWF).

5. Analysointi (Analyze),
6. Tiedonkeruu ja operointi (Collect and Operate),
7. Tutkinta (Investigate).

Näissä kussakin on useita erityisosaamisaloja. Kyselyssä vastaaja pystyi merkitsemään niin pääluokan kuin erityisalojakin. Oman pääluokkansa tärkeimmät erityisosaamisalat mainitaan seuraavissa kappaleista, jos vastaajista useampi kuin joka neljäs merkitsi sen ao. alueen osaamispulaksi.

Ensimmäinen pääluokka, turvallinen tuotanto, on lähestulkoon yhtä tärkeä eri vastaajaryhmille. Kyberturvallisuuden tuotteita ja palveluita muille tuottavat tuottavien yritykset painottivat tätä hieman samalla kun koulutus- ja tutkimusorganisaatioihin kuuluvat organisaatiot alipainottivat tätä pääluokkaa. Tärkeimpiä erikoistumisaloja tässä pääluokassa olivat kyselyn perusteella järjestelmäarkkitehtuuri (engl. Systems Architecture), riskinhallinta (engl. Risk Management) ja ohjelmistokehitys (engl. Software Development).

Toisessa pääluokassa eli operoinnissa ja ylläpidossa organisaatioiden tausta vaikutti enemmän tarpeisiin. Erityisesti alueellisen tason organisaatiot merkitsivät tämän alan työvoimatarpeita selkeästi useammin (17 %) kuin tämän ryhmän osuus vastaajista olisi antanut olettaa (13 %). Tämän pääluokan erikoisosaamisaloista kysytyimmät ovat suuruusjärjestyksessä datan hallinta (engl. Data Administration), järjestelmäympäristön hallinta (engl. Systems Administration) ja verkkoympäristön hallinta (engl. Network Services).

Kokonaisuuden valvonta ja johtaminen eli kolmas pääluokka nousi erityisesti valtiolla tärkeäksi osaamistarpeeksi. Erikoistumisalueista ylivoimaisesti merkittävin oli kyberturvallisuuden hallinta (engl. Cybersecurity Management). Myös kyberturvallisuus/tietoturvajohtaja engl. (Executive Cybersecurity Leadership) sekä strateginen suunnittelu ja linjaukset (engl. Strategic Planning and Policy) olivat kysyttyjä erikoisaloja.

Neljänteen luokkaan eli suojaamiseen ja puolustukseen eri vastaajaryhmät vastasivat lähestulkoon painoarvojensa mukaisesti. Haavoittuvuusarviointi ja hallinta (engl. Vulnerability Assessment and Management), tapahtumiin vastaaminen (engl. Incident Response), järjestelmien ja tietojen suojaustarpeiden analysointi (engl. Cybersecurity Defense Analysis) sekä kyberturvallisuuden puolustusinfrastruktuuri (engl. Cybersecurity Defense Infrastructure Support) nousivat esille tärkeimpinä alakategorioina.

Koko vastaajajoukosta joka toinen vastaaja (47 %) ilmoitti, että heillä on osaajapulaa 2–3 vuoden kuluttua viidennen pääluokan eli analysoinnin eri erikoisosaamisalueissa (engl. Threat, Exploitation, All-Source, Target, Language Analysis). Tämä nousi erityisesti valtiollisten organisaatioiden ja kolmannen sektorin vastauksissa tärkeäksi tehtäväkokonaisuudeksi. On huomattava, että kysely tehtiin, kun Vastaamo-tapausta käsiteltiin julkisuudessa. Vastausten ajallisessa jakaumassa huomattiin, että suurempi medianäkyvyys lisäsi vastauksia tähän kohtaan. Alajaottelua analyysin erityisaloihin ei kysytty, koska amerikkalaisen viitekehyksen yksityiskohtaisuus tässä osaamisalueessa katsottiin liian pikkutarkaksi suomalaiseen ympäristöön.

Tiedonkeruu ja operointi eli kuudes pääluokka oli kyberturvallisuuden tuotteita tai palveluja ensisijaisesti muille myyville yrityksille kohtuullisen tärkeä. Yksikään erikoistumisala ei noussut kyselyssä kuitenkaan esille.

Viimeinen pääluokista on tutkinta, jota nostivat esille erityisesti valtiollisia organisaatioita edustaneet vastaajat. Erityisaloista kybertutkinta (engl. Cyber Investigation)

nostettiin esille. Noin 11 % vastaajista kirjoitti valmiiden vaihtoehtojen lisäksi muista osaamistarpeista. Vapaassa tekstiosuudessa esiintyivät mm. seuraavat aiheet: kryptologia, viestintä, opetus sekä erilaiset maininnat kokonaisuuden hahmottamisesta.

8.3 Rekrytointitarve pääluokittain ja erikoistumisalueittain

Lisärekrytointitarpeet konkretisoituvat henkilöinä. Aluksi kokonaistarve jaetaan osaamisen pääluokkien mukaan. Laskelmat on tehty sekä kokopäiväisen henkilöstötarpeen (5 000–8 000) sekä kokonaistarpeen (yhteensä 6 000–13 000) mukaan. Jälkimmäisessä kokopäiväisiin on lisätty henkilöt, jotka tekevät kyberturvallisuutta oman toimensa ohella.

Kokopäiväiset uudet työntekijät jakaantuisivat pääluokkien tai osaamiskategorioiden 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.

Suurempi rekrytoitavien joukko, 6 000–13 000 henkilöä jakaantuisi vastaavasti seuraavasti:

1. Turvallinen tuotanto 1 100–2 400 henkilöä,
2. Operointi ja ylläpito 900–1 900 henkilöä,
3. Kokonaisuuden valvonta ja johtaminen 1 000–2 200 henkilöä,
4. Suojaaminen ja puolustus 1 000–2 300 henkilöä,
5. Analysointi 800–1 700 henkilöä,
6. Tiedonkeruu ja operointi 600–1 300 henkilöä,
7. Tutkinta 600–1 300 henkilöä.

Mainintojen suhteellisten osuuksien osuvuutta voidaan arvioida vertailemalla lukuja kansainvälisiin ja eri menetelmällä hankittuihin lähteisiin. Samaa NCWF-viitekehystä on käytetty esimerkiksi tutkittaessa avoimia kyberturvallisuuden työpaikkoja Yhdysvalloissa ja nykyisiä työpaikkoja tutkaavassa kansainvälisessä ISC-kyselyssä

Eri aineistoja voidaan verrata jakamalla kokonaistarve (100 %) eri osaamisluokkiin. Prosenttiosuudet osaamiskartoituksen kyselystä, amerikkalaisista työpaikkailmoituksista ja kansainvälisestä ISC-kyselystä ovat samansuuntaisia. (CyberSeek, 2022; ISC2, 2021) Jakauma on esitetty taulukossa 10.

Edellä mainitussa suomalaisessa kyselyaineistossa ennakoidaan lähivuosia ja kahdessa kansainvälisessä aineistossa arvioidaan nykytilaa. Havaitut erot kuvastanevat sektoreiden ja niiden kypsyystasojen kansallista erilaisuutta. Ainoat selkeästi suomalaiset poikkeamat ovat kahden viimeisen pääluokan - tiedonkeruun ja operoinnin sekä tutkinnan - koettu tärkeys. Tiedonkeruu ja operointi ovat tärkeitä kyberturvallisuustuotteita ja palveluita tuottaville yrityksille, tutkinta taasen valtiollisille toimijoille.

Taulukko 10. Osaajien kokonaistarve jakaantuminen eri osaamisluokkiin

Osaamisluokka	**Kysely**	**USA työpaikka-ilmoitukset**	**ISC2 kysely**
Turvallinen tuotanto	19 %	22 %	18 %
Operointi ja ylläpito	14 %	26 %	14 %
Kokonaisuuden valvonta ja johtaminen	17 %	18 %	28 %
Suojaaminen ja puolustus	17 %	16 %	16 %
Analysointi	13 %	10 %	8 %
Tiedonkeruu ja operointi	10 %	4 %	6 %
Tutkinta	10 %	3 %	4 %

Niemelä (2019) luokitteli suomalaisia työpaikkailmoituksia vastaavasti. Pääluokkien osuus oli siinä seuraava: 1. 35 %, 2. 30 %, 3. 23 %, 4. 4 %, 5. 3 %, 6. 0 % ja 7. 6 %. Niemelän aineiston (168 ilmoitusta) perusteella suomalaisten työnantajien huomio keskittyi vain muutamaan pääluokkaan. Työpaikkailmoituksia hyödynnettiin myös Digibarometri 2020: Kyberturvan tilannekuva Suomessa -selvityksessä (Mattila ym., 2020). Silloin kyberalan ilmoituksissa etsittiin erityisesti järjestelmäarkkitehtuurin, alan liiketoiminnan, ohjelmistojen sekä ylläpidon ja valvonnan ammattilaisia.

Esiselvitys osoittaa myös pääluokkien alla olevien erikoistumisalojen tärkeysjärjestyksen, mistä voidaan johtaa myös lukumääräisiä arvioita. Taulukossa 11 näkyy arviot erityisosaamisaluetarpeista. Sarakkeissa näkyy alan jälkeen sen osuus omasta pääluokastaan, jota seuraa henkilötasolle tehdyt arviot neljässä tapauksessa. Ensin on haarukka kokopäiväisistä kyberosaajista ja sitten lukuun on lisätty myös ammattilaiset, jotka tekevät kybertyötä muun tehtäviensä ohella.

Alakohtaisen tarkastelun piirteenä on se, että pienemmissä pääluokissa koulutustarve keskittyy. Suuremmissa pääluokissa tarpeet ja vastaajien huomio levittäytyvät laajemmalle, ja mahdollisesti siksi yhden yksittäisen erityisosaamisalueen merkitys on pienempi. Laskelman perusteella eniten tutkinnan pääluokassa olevan kybertutkinnan (engl. Cyber Investigation) osaajia, tarve voi olla jopa 760 henkilöä. Suuruusjärjestyksessä seuraavat ovat suojaamisen ja puolustuksen pääluokan erityisosaamisalueen haavoittuvuusarviointi ja hallinta (engl. Vulnerability Assesment and Management), tarve 260–660 henkilöä, tapahtumiin vastaaminen (engl. Incident Response), tarve 230–590 henkilöä ja järjestelmien ja tietojen suojaustarpeiden analysointi (engl. Cybersecurity Defense Analysis), tarve 230–590 henkilöä. Tärkeimmän pääluokan eli turvallisen tuotannon erityisosaamisalueet jakaantuivat tasaisesti. Järjestelmäarkkitehtuuri (engl. Systems Architecture), tarve 180–470 henkilöä, riskinhallinta (engl. Risk Management), tarve 150–390 henkilöä, ohjelmistokehitys (engl. Software Development), tarve 140–370 henkilöä) olivat yleisimmät erityisosaamisalueet ensimmäisessä pääluokassa.

Taulukko 11. Arvio erityisosaamistarpeesta

Erityisosaamistarve	**Osuus pääluo-kasta**	**Koko-päiv. min**	**Koko-päiv. max**	**Koko ja OTO min**	**Koko ja OTO max**
1. Turvallinen tuotanto		900	1500	1100	2400
1.1. Turvallinen tuotanto – Riskinhallinta	16 %	147	244	179	391
1.2. Turvallinen tuotanto - Ohjelmistokehitys	15 %	137	229	168	367
1.3. Turvallinen tuotanto - Järjestelmäarkkitehtuuri	20 %	176	293	215	469
1.4. Turvallinen tuotanto - Teknologioiden tutkimus ja kehitys	9 %	82	137	101	220
1.5. Turvallinen tuotanto - Vaatimusmäärittely	13 %	114	189	139	303
1.6. Turvallinen tuotanto - Arviointi ja testaus	14 %	126	211	155	337
1.7. Turvallinen tuotanto - Järjestelmäkehitys	13 %	117	196	143	313
2. Operointi ja ylläpito		700	1100	900	1900
2.1. Operointi ja ylläpito - Datan hallinta	23 %	161	253	207	436
2.2. Operointi ja ylläpito - Tietämyksenhallinta	14 %	100	157	128	271
2.3. Operointi ja ylläpito - Asiakaspalvelu ja tekninen tuki	7 %	49	77	63	133
2.4. Operointi ja ylläpito - Verkkoympäristön hallinta	20 %	138	217	178	376
2.5. Operointi ja ylläpito - Järjestelmäympäristön hallinta	21 %	144	227	186	392
2.6. Operointi ja ylläpito - Järjestelmäanalyysi	15 %	108	169	139	293
3. Kokonaisuuden valvonta ja johtaminen		800	1300	1000	2200
3.1. Kokonaisuuden valvonta ja johtaminen - Lainopilliset palvelut	14 %	114	185	142	313
3.2. Kokonaisuuden valvonta ja johtaminen - Harjoittelu, koulutus ja tietoisuuden lisääminen	13 %	106	172	133	292
3.3. Kokonaisuuden valvonta ja johtaminen - Kyberturvallisuuden hallinta	25 %	202	329	253	557
3.4. Kokonaisuuden valvonta ja johtaminen - Strateginen suunnittelu ja linjaukset	16 %	129	210	161	355
3.5. Kokonaisuuden valvonta ja johtaminen - Projektinhallinta ja hankintaosaaminen	14 %	114	185	142	313
3.6. Kokonaisuuden valvonta ja johtaminen – Kyberturvallisuus-tietoturvajohtaja	17 %	135	219	169	371

(taulukko 11 jatkuu)

Erityisosaamistarve	**Osuus pääluo-kasta**	**Koko-päiv. min**	**Koko-päiv. max**	**Koko ja OTO min**	**Koko ja OTO max**
4. Suojaaminen ja puolustus		900	1400	1000	2300
4.1. Suojaaminen ja puolustus - Järjestelmien ja tietojen suojaustarpeiden analysointi	25 %	229	357	255	586
4.2. Suojaaminen ja puolustus - Kyberturvallisuuden puolustusinfrastruktuuri	20 %	180	280	200	460
4.3. Suojaaminen ja puolustus - Tapahtumiin vastaaminen	26 %	232	361	258	592
4.4. Suojaaminen ja puolustus - Haavoittuvuusarviointi ja hallinta	29 %	259	403	288	662
5. Analysointi		600	1000	800	1700
5.1. Analysointi – kaikki, mm. uhkien ja tunkeutumisen analysointi	100 %	600	1000	800	1700
6. Tiedonkeruu ja operointi		500	800	600	1300
6.1. Tiedonkeruu ja operointi - Tapahtumatietojen keruu	29 %	145	233	174	378
6.2. Tiedonkeruu ja operointi - Kyberoperaatiosuunnittelu	38 %	188	301	226	489
6.3. Tiedonkeruu ja operointi - Kyberoperaatiot	33 %	167	267	200	433
7. Tutkinta		500	800	600	1300
7.1. Tutkinta - Kybertutkinta	59 %	294	470	352	764
7.2. Tutkinta - Digitaalinen rikostutkinta	41 %	206	330	248	536

Viitekehikko rajaa koulutusalueet selvästi, mutta toisaalta pienet ryhmät voivat vaikeuttaa yleiskuvan hahmottamista. Vastauksista voidaan koostaa laajempia klustereita suuremman selkeyden saamiseksi. Voidaan nähdä, että vastaajajoukossa kysyntää oli erityisesti a) kokonaisuuden hallinnasta (erityisalat kuten järjestelmäarkkitehtuuri, kyberturvallisuuden hallinta, strategiat sekä niitä hoitavat kyberturvallisuus- tai tietoturvajohtajat) ja b) operatiivisemmasta osaamisesta, jossa painottuu järjestelmien suojaus sekä sitä tukeva analyysi. Julkinen sektori hakee suhteellisesti enemmän hyvin laajasti katsovia johtaja- ja riskinhallintaosaajia, kun taas elinkeinoelämä hakee hallinta- ja arkkitehtuuriosaajia.

Kuntasektorilla nähtiin muita suurempaa tarvetta asiakaspalvelun ja teknisen tuen sekä projektinhallinnan ja johtamisen kyberosaajille. Viimeksi mainitut alat eivät olleet muiden sektoreiden vastauksissa yhtä yleisiä. Kolmannen sektorin toimijoita oli vastaajien joukossa vähän, mutta heille datan hallinta ja analysointi olivat erityisen tärkeitä erityisosaamisalueita.

Kyberala (FISC) ry:n oman jäsenkyselyn (2020) perusteella kyberturvallisuuden tuotteita ja palveluita tarjoavat vastaajat tarvitsivat osaajia seuraavilla alueilla: ohjelmisto-osaaminen, liiketoiminnallinen osaaminen, strateginen kyberturvallisuusosaaminen, kryptografia/kryptologia, tekninen kyberturvallisuus, ylläpidon ja valvonnan osaaminen sekä järjestelmäarkkitehtuurin osaaminen. Osaamistarpeet-esiselvityksessä havainnot olivat samoja: yritykset, jotka tuottavat kyberturvallisuuden palveluita tai tuotteita tarvitsevat enemmän ohjelmistokehittämisen ja järjestelmäarkkitehtuurin ammattilaisia.

Muut selvitykset osaamistarpeista ovat samansuuntaisia. Huoltovarmuusorganisaation selvityksessä tarkasteltiin huoltovarmuuden kannalta keskeisten toimialojen kyberturvallisuuden kypsyystasoa. Siinä havaittiin, että tärkeimmät yhtenevät kehityskohteet liiketoiminnan näkökulmasta olivat 1. yrityksen kyberturvallisuusstrategia, 2. kyberturvallisuusarkkitehtuuri ja 3. tekninen jäljitettävyys eli lokien seuranta.

Teknologiateollisuuden osaaja- ja osaamisselvitys 2021 (Teknologiateollisuus, 2018) kysyi laajemmin ICT-osa-alueiden osaamistarpeita. Yritykset nostivat esille erityisesti seuraavat aihepiirit: robotiikka ja automaatio, tuotteiden/palveluiden älykkyyden kehittäminen, toiminnanohjaus/tuotetietojärjestelmät, pilvipalvelut sekä data-analytiikka.

Laaja brittitutkimus (2021) laventaa osaamispulan hyvinkin erilaisiin kyberyritysten ammattinimikkeisiin. Siellä eniten haettiin turvallisuusinsinöörejä (engl. Security Engineer, 37 %), analyytikoita (engl. Security Analyst 18 %), esimiehiä (engl. Security Manager 14 %) ja turvallisuusarkkitehtejä (engl. Security Architect 11 %). Saman tutkimuksen mutta eri aineiston mukaan 37 % kybertehtävistä on ollut vaikea täyttää. Näistä vaikeasti täytettävistä tehtävistä useimmat ovat olleet yleisesti kyberturvallisuustehtäviä ja päällikkötason töitä, mutta myös penetraatiotestaajia, turvallisuusarkkitehteja ja myyjiä. Tehtävistä kaikki eivät olleet täysipäiväisiä kyberammattilaisia, mutta heiltä odotettiin silti alan osaamista. Tehtävien täyttöä oli joka toisessa tapauksessa vaikeuttanut se, että kandidaateilta on puuttunut tekniset tiedot tai taidot. Joka kolmannelta on puuttunut työkokemusta (35 %) tai asenne ei ole sopinut tehtävään (30 %). (UK Government, 2021)

Enterprise Strategy Group – Information Systems Security Associationin (2021) tutkimuksen mukaan suurin kyberosaamispula koettiin pilvipalvelujen turvallisuudessa

(Cloud Computing Security 39 %), analyysissä ja tutkimuksessa (engl. Security analysis and Investigations, 30 %) ja sovellusten turvallisuudessa (engl. Application Security 30 %). Aineisto keskittyi Pohjois-Amerikkaan. (Oltsik, 2021)

Globaalin ISC-kyselyn (2021) mukaan osaamispula pysyy kriittisenä globaalisti. Joka toinen vastaaja nosti esiin tuotannon (engl. Securely Provision, 48 %), analysoinnin (engl. Analyze, 47 %), suojaamisen ja puolustuksen (engl. Protect and Defend). Muut pääkategoriat tulevat lähellä perässä. (ISC2, 2021)

8.4 Johtopäätökset ja kehittämistarpeet

Aiemmista kotimaisista aineistoista johdettuja lukuja on verrattu myös kansainvälisiin lähteisiin. Tulosten uskottavuutta parantaa, että ne ovat johdonmukaisia myös ulkomaalaisten lähteiden kanssa.

Osaajapula on todellisuutta, vaikka sen tasoa on vaikea tarkasti ennustaa. Lähtötietojen perusteella voidaan arvioida, että tarvitsemme 5 000–8 000 kyberturvallisuuden ammattilaista lähivuosina. Tämän lisäksi 1 000–5 000 uutta ammattilaista tulee tekemään vastaavia töitä muiden töiden ohessa. Nämä kaikki tarvitsevat alan koulutuksen.

Turvalliseen tuotantoon tarvitaan eniten uusia osaajia. Tarkemmin 6 000–13 000 uuden kyberammattilaisen ryhmä voidaan jakaa pääkoulutuksensa mukaan seuraavasti:

1. Turvallinen tuotanto 1 100–2 400 henkilöä,
2. Operointi ja ylläpito 900–1 900 henkilöä,
3. Kokonaisuuden valvonta ja johtaminen 1 000–2 200 henkilöä,
4. Suojaaminen ja puolustus 1 000–2 300 henkilöä,
5. Analysointi 800–1 700 henkilöä,
6. Tiedonkeruu ja operointi 600–1 300 henkilöä,
7. Tutkinta 600–1 300 henkilöä.

Osaamisprofiili jakaantuu varsin tasaisesti kaikille kyberturvallisuuden osaamisalueille. Tämä tarkoittaa tarvetta laaja-alaiselle koulutukselle. Korkeakoulujen tutkintokoulutuksen sekä muunto- ja täydennyskoulutuksen tulee kattaa kaikki nuo osa-alueet, jotta osaamistarve voidaan tyydyttää.

Kyberturvallisuuskoulutuksen sisäänottovahvuuksien nostaminen edellyttää resursseja sekä koulutukseen että tutkimukseen. Haasteena on nopealla aikataululla saada rekrytoitua tutkijoita ja opettajia korkeakouluihin. OKM-rahoittaa ammattikorkeakoulujen aloituspaikkojen lisäystä seuraavasti:

- AMK-opiskelija 6 000 €/vuosi/ opiskelija,
- YAMK-opiskelija 9 000 €/vuosi/opiskelija,
- ETA-alueen ulkopuolelta tuleville AMK tutkinto-opiskelijoille tutkintomaksu on 8 000 €/vuosi.

Yliopistotasolla kustannusvaikutus syntyy, kun sisäänotto kasvaa kymmenillä opiskelijoilla. Kandidaattitasolla kustannus on noin 6 000 €/vuosi/ opiskelija ja maisteritasolla 9 000 €/vuosi/opiskelija.

Lähteet

AustCyber (2020). Australia's Cyber Security: Sector Competitiveness Plan 2020. Australian Cyber Security Growth Network. https://www.austcyber.com/resources/sector-competitiveness-plan.

CBR (2020). Europe's Cybersecurity Skills Gap Has Doubled. Report. https://www.cbronline.com/news/cybersecurity-job-gap.

CPO (2020). Study Reveals That Cybersecurity Skills Gap Affects About Three-Quarters of Organizations and Still Worsening. CPO Magazine. https://www.cpomagazine.com/cyber-security/study-reveals-that-cybersecurity-skills-gap-affects-about-three-quarters-of-organizations-and-still-worsening/ .

CyberSeek (2022). Cybersecurity Supply/Demand Heat Map: Job openings by NICE Cybersecurity Workforce Framework Category. https://www.cyberseek.org/heatmap.html.

ENISA (2019). Cybersecurity Skills Development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database. European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union

ENISA (2021). Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education. European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

Oltsik J. (2021). The Life and Times of Cybersecurity Professionals 2021, Vol. V. ESG Research Report. https://2ll3s9303aos3ya6kr1rrsd7-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Jul-2021.pdf

FiCom (2021). ICT-alan työlliset 19.11.2021. Lähde: Tilastokeskuksen työvoimatutkimus, FiCom ry.

FISC (2020). Jäsenkysely. Finnish Information Security Cluster (FISC).

FISC (2021). Kyberosaajatarvekysely. Finnish Information Security Cluster (FISC).

ISC2 (2021). A Resilient Cybersecurity Profession Charts the Path Forward. 2021 Cybersecurity Workforce Study. International Information Systems Security Certification Consortium (ISC)^2. https://www.isc2.org/Research/Workforce-Study.

Mattila J., Mäkäräinen K., Pajarinen, M., Seppälä T., Ali-Yrkkö J., Tervo E. (2020). Digibarometri 2020: Kyberturvan tilannekuva Suomessa. Helsinki: Taloustieto Oy.

Niemelä J. (2019). Kyberturvallisuusalan työvoiman kysyntä, saatavuus ja kehittäminen vastaamaan työvoiman tarvetta Suomessa. Pro gradu, Jyväskylän yliopisto.

NIST (2017). Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future. National Institute of Standards and Technology (NIST). https://www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf

Teknologiateollisuus (2018). 9 ratkaisua Suomelle: Teknologiateollisuuden Koulutus ja osaaminen -linjaus 2018. https://teknologiateollisuus.fi/sites/default/files/file_attachments/teknologiateollisuus_koulutus_ja_osaaminen_linjaus_2018.pdf.

UK Government (2021). Cybersecurity skills in the UK labour market 2021. https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2021.

VN (2020). Kyberosaamistarpeet – esiselvitys. VN/20895/2020, Valtioneuvosto.

Liite 1 Esimerkkejä valinnaisten aineiden opetussuunnitelmista perusopetuksessa

Kuntien ja koulujen paikalliset opetussuunnitelmat ovat tärkeä osa ohjausjärjestelmää, nimittäin sillä on keskeinen merkitys sekä valtakunnallisten tavoitteiden että paikallisesti tärkeinä pidettyjen tarpeiden ja näkökulmien toteuttamisessa. Paikallinen opetussuunnitelma on työkalu, joka luo yhteisen perustan ja suunnan päivittäiselle koulutyölle. Paikallinen opetussuunnitelma voi liittää koulujen toiminnan muuhun paikalliseen toimintaan lasten ja nuorten hyvinvoinnin ja oppimisen edistämiseksi.

Kyselyyn osallistuneiden kaupunkien paikallisen opetussuunnitelman tieto- ja viestintäteknologiaan suuntavan valinnaisaineen sisältö tietoturvallisuuden tavoitteiden näkökulmasta on esitetty seuraavaksi.

Huomioitavaa on, että kaikilla kaupungeilla ei ole kaupunkikohtaisia valinnaisaineiden opetussuunnitelmia, jolloin tutkimuksessa on haettu eri kaupunkien koulujen omasta valinnaisainetarjonnasta tieto- ja viestintätekniikkaan liittyvien valinnaisaineiden sisältökuvauksia.

Espoo

Kaupungin valinnaisainejärjestelmä noudattaa Espoon koulutuslautakunnan hyväksymää linjausta, jonka mukaan valinnaisina aineina tarjotaan mahdollisimman paljon taito- ja taideaineita sekä aineita, jotka ovat koulun painotuksen tai profiilin mukaisia. Koulujen tulee tämän linjauksen mukaan pyrkiä tarjoamaan valinnaiset aineet nk. pitkinä valintoina, jolloin valinnaisainetta opetetaan yhteensä vähintään kaksi vuosiviikkotuntia yläkoulun aikana. Vuosiluokille 8–9 tarjottavan valinnaisaineen tavoitteet liittyen tietoturvallisuuteen ovat:

- Työskennellään tietoturvan, informaation haun ja -kriittisyyden parissa.
- Tietotekniikan opiskelussa keskitytään tietotekniikan perusteiden ymmärtämiseen ja toisaalta kokonaisvaltaiseen lähestymistapaan niin, että tiedot ja taidot ovat sovellettavissa jatkuvasti kehittyvässä tietoteknisessä maailmassa myös tulevaisuudessa.
- Ymmärretään Internetin ja yleensä tietoverkkojen perustoimintaperiaatteet, mikä luo pohjan tietoturvan merkityksen ymmärtämiselle.
- Ohjataan oppilasta käyttämän turvallisesti erilaisia sähköisiä oppimisympäristöjä.
- Ohjataan oppilasta sosiaalisen median ja nettietiketin käyttöön.
- Ohjataan turvalliseen tiedon hankintaan ja tiedon jakamiseen.

Helsinki

Vuosiluokille 8–9 tarjottavan valinnaisaineen tavoitteet liittyen tietoturvallisuuteen ovat:

- Oppiaineen tavoitteena on antaa oppilaalle valmiudet tietotekniikan hyödyntämiseen elämän eri osa-alueilla kuten koulussa, kotona ja jatko-opinnoissa sekä työelämässä.

- Oppilas tutustuu tietojenkäsittelyn keskeisiin osa-alueisiin ja perehtyy jokapäiväisen elämän tietoteknisiin sovelluksiin ja käyttöesimerkkeihin.
- Oppiaineen sisällössä seurataan tietotekniikan kehitystä.

Joensuu

Vuosiluokille 8–9 tarjottavan valinnaisaineen tavoitteet liittyen tietoturvallisuuteen ovat:

- Pilvitallennus ja sen hyödyntäminen työskentelyssä
- Sähköpostin käyttö
- Koulun verkkoon liittyminen / langattomat ilmaiset verkot
- Tiedonhaku netistä
- Netiketti

Kuopio

Vuosiluokille 8–9 tarjottavan valinnaisaineen tavoitteet liittyen tietoturvallisuuteen ovat:

- Netiketti ja lähdekritiikki sisältyvät luonnollisena osana oppiaineeseen.
- Tietotekniikan ohjelmistojen monipuolinen hallinta tukee sekä oppilaan opiskelua, että parantaa tulevaisuuden työelämätaitoja.

Lappeenranta

Vuosiluokille 8–9 tarjottavan valinnaisaineen tavoitteet liittyen tietoturvallisuuteen ovat:

- Tutustutaan tekijänoikeuslainsäädäntöön.
- Ymmärretään tietotekniikan monipuolinen käyttäminen ja mahdollisuudet sekä myös tietoturvalliset riskit.
- Harjoitellaan Internetin turvallista käyttöä.

Tampere

Vuosiluokille 8–9 tarjottavan valinnaisaineen tavoitteet liittyen tietoturvallisuuteen ovat:

- Opetuksessa pyritään kokonaisvaltaista ja kriittistä ajattelua kehittävään lähestymistapaan, siten että oppilas ymmärtää tietotekniikan perusteet, sovellutuksia, rajoja ja tulevaisuuden haasteita ja osaa itsenäisesti opiskella uutta tietotekniikan saralla.
- Oppilasta ohjataan ja kasvatetaan kohti tietoyhteiskunnan täysipainoista kansalaisuutta, johon kuuluvat tietotekniikan käytännön taitojen lisäksi tiedonhallintataidot, yhteistyö- ja vuorovaikutustaidot sekä tietoturvan ja etiikan pohtiminen ja hallinta.
- Tieto- ja viestintätekniikan nopea kehitys vaativat myös opetukselta ajan hermolla olemista ja sen vuoksi opetusta kohdennetaan ja painotetaan kulloinkin ajankohtaisiin ja keskeisiin aihealueisiin.

Turku

Vuosiluokille 8–9 tarjottavan valinnaisaineen tavoitteet liittyen tietoturvallisuuteen ovat:

- Tavoitteena on antaa oppilaalle tietoyhteiskunnassa hyvät valmiudet vastaanottaa, prosessoida ja tuottaa tietoa.
- Oppitunneilla käydään läpi tietotekniikan perusteet (käyttöjärjestelmät, työvälineohjelmat, tietoliikenne ja tietoturva).

Pori

Vuosiluokille 8–9 tarjottavan valinnaisaineen tavoitteet liittyen tietoturvallisuuteen ovat:

- Tavoitteena on antaa hyvät perustaidot tietotekniikan tärkeimmistä osa-alueista siten, että opetus sisällöllisesti ja vaadittavan osaamistason suhteen vastaa kehittyvän tietoyhteiskunnan vaatimuksiin. Tavoitteina on ymmärtää tietotekniikan merkitys yhteiskunnassa sekä tiedostaa sen vaikutukset koulutukseen, työelämään ja vapaa-aikaan.
- Tutustutaan verkkojen käyttöä ohjaavaan netikettisäännöstöön sekä tietoturvaan eri suojautumismenetelmien kautta.
- Oppilas ymmärtää tekijänoikeudet ja henkilötietolain pääkohdat sekä ymmärtää nettikiusaamisen seuraukset ja ehkäisyn.
- Oppilas on saanut perustiedot palomuurista, netiketistä, tietokoneviruksista ja niiden torjunnasta.

Lahti

Vuosiluokille 7–9 tarjottavan valinnaisaineen tavoitteet liittyen tietoturvallisuuteen ovat:

- Oppilas tutustuu tekijänoikeuksiin ja ymmärtää sosiaalisen median käyttömahdollisuudet hyvien tapojen ja normien mukaan.
- Oppilas tutustuu erilaisiin tietoturvan käsitteisiin samalla huolehtien käyttämistään laitteista.
- Oppilas opettelee arvioimaan internetissä olevien asioiden luotettavuutta.
- Oppilas harjoittelee luvallisen materiaalin hankintaa verkosta.

Jyväskylä

Vuosiluokille 8–9 tarjottavan valinnaisaineen tavoitteet liittyen tietoturvallisuuteen ovat:

- ohjataan oppilasta turvalliseen ja eettisesti kestävään tieto- ja viestintäteknologian käyttöön.
- tutustutetaan oppilas tietoturvariskeihin ja niiltä suojautumiseen.
- syvennetään oppilaan osaamista tietosuoja- ja tekijänoikeusasioissa.
- ohjataan oppilasta lähdekriittisyyteen.

Oulu

Vuosiluokille 8–9 tarjottavan valinnaisaineen tavoitteet liittyen tietoturvallisuuteen ovat:

- Oppilas perehtyy asialliseen käyttäytymiseen ja tietoturvaan sekä verkossa että sen ulkopuolella (esim. haittaohjelmat, salasanat, sosiaalinen media).
- Oppilas kunnioittaa tekijänoikeuksia.
- Oppilas ymmärtää, että verkkoon kerran laitettua materiaalia ei ehkä koskaan saada sieltä pois.
- Oppilas ymmärtää, että kaikki verkosta löytyvä ei välttämättä pidä paikkaansa.

Liite 2 Ammattikorkeakoulujen opetussuunnitelmat

1. Yrkeshögskolan Arcada

Arcadan tutkinto-ohjelmat sijoittuvat Uudellamaalla Helsingin kampukselle. AMK-tutkinto-ohjelmiin oli 2022 haussa 88 paikkaa päivätoteutukseen ja YAMK tutkinto-ohjelmiin 20 monimuotototeutukseen. Opetussuunnitelmien sivulta voi tarkastella vain tiettyä opetussuunnitelmaa, mutta niiden kategorisointi eri ISCED-aloihin puuttui. Verkkosivujen perusteella tutkinto-ohjelmat kuuluivat "Department of Business Management and Analytics":n alle, vaikka tutkinto- ohjelmasta valmistuu Bachelor/Master of Engineering -tutkinnolla.

Ylempi ammattikorkeakoulu - EQF7

Arcadassa on tutkinto-ohjelma *Big Data Analytics*, mutta kyseinen tutkinto- ohjelma ei sisällä kyberturvallisuutta.

Tutkinto-ohjelman kategoria: F.

Ammattikorkeakoulu - EQF6

Information Technology, Insinööri (AMK) opetussuunnitelmassa kyberturvallisuuteen liittyvä opintojakso kuului "Advanced Studies"(eli suuntautumisen) valinnaksi Service Oriented Architectures and Analytical Methods -nimisen moduulin alle.

Arcada, Information Technology, Insinööri (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
IA-2-010	Network Protocols and Security(V)	5

Tutkinto-ohjelman kategoria: D.

Erikoistumisopinnot

Arcada tarjoaa *Big Data Analytics* YAMK tutkinto-ohjelmaansa myös täydennyskoulutuksena. Kyberturvallisuutta ei havaittu täydennys tai erikoistumiskoulutuksen tarjonnassa tutkimuksen aikana.

2. Centria ammattikorkeakoulu

Centrian tutkinto-ohjelmat painottuvat Keski-Pohjanmaalla Kokkolan kampukselle, Pohjanmaalla Pietarsaareen ja Pohjois-Pohjanmaalla Ylivieskaan. AMK-tutkinto-ohjelmiin oli 2022 haussa 66 paikkaa ja YAMK tutkinto-ohjelmiin 50.

Ylempi ammattikorkeakoulu - EQF7

Centriassa YAMK -tutkinnot jakaantuvat suomenkieliseen *Digitalisaation johtamiseen* ja englanninkieliseen *Cloud-based Software Engineering*. Opetussuunnitelmien perus-

teella Centrian ylempiin ammattikorkeakoulututkintoihin ei sisältynyt kyberturvallisuuteen keskittyviä opintojaksoja. Molemmat opetussuunnitelmat kategorisoituivat F-malliin.

Ammattikorkeakoulu - EQF6

Tieto- ja viestintätekniikka, insinööri (AMK). Tutkinto-ohjelmat hajaantuvat monimuoto (39 aloituspaikkaa) ja päivätoteutusten (27 aloituspaikkaa) välillä, sekä suomenkielisten että englanninkielisten (Information Technology, Bachelor of Engineering). Opetussuunnitelmat eri hakukohteiden kesken olivat kohtalaisen identtiset. Kaikissa opetussuunnitelmissa kuitenkin kyberturvallisuuden opintojaksot ovat:

Centria, Tieto- ja viestintätekniikka, insinööri (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
IT00AK39	Cybersecurity and data privacy(P)	3
IT00AL57	CCNA: Network Security(V)	5

Tutkinto-ohjelman kategoria: CD.

Erikoistumiskoulutukset

Centriassa ei ollut kyberturvallisuuteen liittyviä erikoistumiskoulutuksia tarjolla.

3. Haaga-Helia ammattikorkeakoulu

Haaga-Heliassa koulutus sijoittuu Helsingin Pasilan kampukseen ja tietojenkäsittelyn tradenomitutkintoihin. Vastaavasti YAMK -tutkinnot ovat Tradenomi (YAMK) -ohjelmia. Opiskelijamäärät kevään 2022 haussa oli 265 opiskelijaa AMK tutkinto-ohjelmiin, josta monimuodossa 102 aloituspaikkaa ja päivätoteutuksessa 163 (eng+fin) aloituspaikkaa. YAMK tutkinto-ohjelmat monimuotona ja 70 aloituspaikalla varustettuna.

Ylempi ammattikorkeakoulu - EQF7

Liiketoiminnan teknologiat, Tradenomi (YAMK). Kyberturvallisuus näkyi tutkinto-ohjelman suuntautumisessa seuraavalla opintojaksolla.

Haaga-Helia, Liiketoiminnan teknologiat, Tradenomi (YAMK), liittyvät opintojaksot

Course Code	Course Name	ECTS
CT4HM003	Tietoturvan perusteet luottamuksesta lohkoketjuun(V)	5

Sama opintojakso (ja opetussuunnitelma) on myös identtisellä englanninkielisellä *Business Technologies* -tutkinto-ohjelmalla. Molempien tutkinto-ohjelmien kategoria: D.

Ammattikorkeakoulu - EQF6

Tietojenkäsittely, Tradenomi (AMK) tutkinto-ohjelmassa kyberturvallisuuteen liittyvät opintojaksot kuuluvat asiantuntijaosaamisen (valitaan 90 op opintoja) alla "ICT infra ja pilvipalvelut- moduuliin, josta valitaan 30–60 opintopistettä.

Haaga-Helia, Tietojenkäsittely, Tradenomi (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
ICI002AS2A	Tietoturvan perusteet(V)	5
ICI004AS3A	Tietoturvan hallinta(V)	5
ICI005AS3A	Tunkeutumistestaus(V)	5

Suomenkielisen tutkinto-ohjelman kategoria: D.

Business Information Technology, Bachelor of Business Administration englanninkielisessä tutkinto-ohjelmassa on tarjottuna pelkästään Tietoturvan perusteet (engl. Data Security). Muut opintojaksot suomenkielisestä opetussuunnitelmasta eivät ole syystä tai toisesta ole tarjolla englanninkielisille toteutuksille.

Business Information Technology, Bachelor of Business Administration, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
ICT4TF022	Data Security(V)	5

Tutkinto-ohjelman kategoria: D.

Erikoistumiskoulutukset

Kyberturvallisuuteen liittyviä opintokokonaisuuksia tai opintojaksoja ei ollut tarjolla Haaga-Helian erilliset opintokokonaisuudet ja vapaasti valittavat -tarjonnassa. Täydennyskoulutuksessa oli ”Turvallisuus kuuluu kaikille!” - opintokokonaisuus, jonka sisällöt vaikuttivat olevan yhteistyöhankkeesta. Tässä opintokokonaisuudessa oli 2 opintopistettä ”oppilaitoksen kyberturvallisuus” -opintokokonaisuuteen varattu.

4. Hämeen ammattikorkeakoulu

Hämeen ammattikorkeakoulussa opetus jakaantui Kanta-Hämeessä Hämeenlinnan ja Forssan välille tradenomi (AMK)- ja insinööri (AMK) -koulutukseen. Näihin opiskelijamäärät olivat 272 aloituspaikkaa. YAMK tutkinto-ohjelma oli vain insinööri (YAMK):lle tietojenkäsittely ja tietoliikenne -alassa. Kyseisen tutkinto- ohjelman sisäänotto oli 40 opiskelijaa.

Ylempi ammattikorkeakoulu - EQF7

Hämeen ammattikorkeakoulussa *Tietojohtaminen ja älykkäät palvelut* -tutkinto-ohjelmassa ei ollut kyberturvallisuuteen liittyviä opintojaksoja tarjolla.

Tutkinto-ohjelman kategoria: F.

Ammattikorkeakoulu - EQF6

Tietojenkäsittelyn koulutus, tradenomi (AMK) opetussuunnitelma on rakennettu kolmeportaiseksi ydinaineopintojen, valinnaisten ydinaineiden ja profiloivan osaamisen suhteen. Kyberturvallisuutta löytyi ydinaineopinnoista pakollisena ja profiloivasta osaamisesta valinnaisena suuntautumisena.

HAMK, Tietojenkäsittelyn koulutus, tradenomi (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
TK00DW10	Tietoverkot ja tietoturva(P)	3
TK00DL87	Kyberturvallisuus pilviympäristössä(V)	4

Tutkinto-ohjelman kategoria: CD.

Englanninkielinen tutkinto-ohjelma *Computer Applications, Bachelor of Business Administration* noudatti lähes identtistä opetussuunnitelmaa. Yhteensä aloituspaikkoja tradenomi (AMK) -tutkinnoissa oli 130.

Tieto- ja viestintätekniikka, insinööri (AMK). Hämeenlinnassa koulutettava tutkinto-ohjelma ottaa sisään 62 opiskelijaa vuonna 2022. Tutkinto-ohjelma ei sisältänyt kyberturvallisuuteen liittyviä opintojaksoja. Samassa kaupungissa tapahtuva tradenomikoulutus kuitenkin sisältää kyberturvallisuutta, eli oletettavasti opiskelijoilla on mahdollisuus valita sitä korkeakoulunsa sisältä.

Tutkinto-ohjelman kategoria: E.

Tieto- ja viestintätekniikka, biotalous, Insinööri (AMK), tämä biotalouteen painottuva tieto- ja viestintätekniikan tutkinto-ohjelmaa järjestetään Forssassa. Tutkinto-ohjelma ei sisältänyt kyberturvallisuuteen liittyviä opintojaksoja. Vaikka tutkinto-ohjelma on eri kaupungissa, on todennäköistä, että opiskelijat voivat ilmoittautua tradenomi tutkinto-ohjelmien opintojaksoille.

Tutkinto-ohjelman kategoria: E.

Erikoistumiskoulutukset

Hämeen ammattikorkeakoulussa oli avoimessa ammattikorkeakoulussa tarjolla *Kyberturvallisuus -opintojakso* (5 op). Tämä oli erikoista, koska sitä ei ollut missään rajauksen tutkinto-ohjelmassa vastaavassa koossa. Opinto-oppaan opintojaksohaun perspektiivistä tämä kyberturvallisuus -opintojakso ryhmittyi CampusOnline/vapaasti valittavat kategoriaan. Silti tätä tarjontaa ei ollut "kiinnitetty" rakenteeseen missään opetussuunnitelmassa.

5. Jyväskylän ammattikorkeakoulu

Jyväskylän ammattikorkeakoulun toiminta tietojenkäsittelyssä ja tietoliikenteessä painottuu Jyväskylässä sijaitseville kampuksille. Keväällä 2022 AMK-tutkinto-ohjelmissa on 200 aloituspaikkaa tarjolla ja YAMK-tutkinto-ohjelmissa 70 aloituspaikkaa.

Ylempi ammattikorkeakoulu - EQF7

70 aloituspaikkaa jakaantuu kolmeen eri tutkinto-ohjelmaan. Erityismainintana rajauksen ulkopuolelle jäävä Robotiikan YAMK -tutkinto-ohjelma, jossa on yksi opintojakso automaation tietoverkot ja kyberturvallisuus. Rajauksen sisällä olevat tutkinto-ohjelmat seuraavasti.

Artificial intelligence and data-analytics, insinööri (YAMK) tutkinto-ohjelmassa ei ole mainittavia kyberturvallisuuteen liittyviä opintojaksoja. Tutkinto-ohjelma mahdollistaa vapaasti valittavia 5 opintopistettä, jotka on mahdollista ottaa rinnakkaisesta tutkinto-ohjelmasta.

Tutkinto-ohjelman kategoria: E.

Cyber security, insinööri (YAMK), tässä kyberturvallisuuden YAMK tutkinto-ohjelmaan otetaan sisään syksyllä 2022 opintopolun mukaan 30 opiskelijaa.

Cyber security, insinööri (YAMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
YTCP0300	Auditing and Testing Technical Security(P)	5
YTCP0400	Cyber Security Exercise(P)	5
YTCP0210	Cyber Security Implementation in Practice(P)	5
YTCP0100	Security Management in Cyber Domain(P)	5

Tutkinto-ohjelman kategoria: A.

Full stack software development, Insinööri (YAMK) ei sisällä mainittavia kyberturvallisuuteen liittyviä opintojaksoja. Tutkinto-ohjelma mahdollistaa vapaasti valittavia 5 opintopistettä, jotka on mahdollista ottaa rinnakkaisesta tutkinto-ohjelmasta.

Tutkinto-ohjelman kategoria: E.

Ammattikorkeakoulu - EQF6

Tutkinto-ohjelmat jakaantuvat insinööri (AMK) -tutkinto-ohjelmaan ja tradenomi (AMK) -tutkinto-ohjelmaan.

Tieto- ja viestintätekniikan tutkinto-ohjelma, insinööri (AMK) on yksi hakukohde, jonka sisällä on useita eri suuntautumisvaihtoehtoja perustuen moduulivalintoihin. Kaikille pakollisissa opintojaksoissa Kyberturvallisuus, mutta matematiikassa voi valita vaihtoehtoisista itselleen sopivimman.

Tieto- ja viestintätekniikan tutkinto-ohjelma, insinööri (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
TTC1020	Kyberturvallisuus(P)	4
TZLM7020	Sovellettu matematiikka: Kryptologia(V)	3

Tutkinto-ohjelma sisältää suuntautuvat moduulit, josta opiskelija valitsee erikoistumisensa. Huomioitavaa on, että moduulien välillä jotkut opintojaksot toistuivat (esim. kyberuhkatieto ja data-analytiikka-opintojakso).

Tieto- ja viestintätekniikan tutkinto-ohjelma, insinööri (AMK), kyberpuolustus -moduulin opintojaksot

Course Code	Course Name	ECTS
TTC6010	Tietoturvakontrollit(V)	5
TTC6020	Kyberturvallisuuden hallinta(V)	5
TTC6030	Kyberuhkatieto ja data-analytiikka(V)	5

TTC6040	Hyökkäykset ja puolustusmenetelmät sekä suojaaminen(V)	5
TTC6050	Koventaminen(V)	5
TTC6060	Poikkeamien hallinta ja kyberturvakeskukset(V)	5

Tieto- ja viestintätekniikan tutkinto-ohjelma, insinööri (AMK), eettinen hakkerointi -moduulin opintojaksot

Course Code	Course Name	ECTS
TTC6500	Web-sovellusten turvallisuus(V)	5
TTC6510	Takaisinmallintaminen(V)	5
TTC6520	Ohjelmistohaavoittuvuudet ja niiden hyväksikäyttö(V)	5
TTC6530	CTF-haaste(V)	5
TTC6540	Salaustekniikat ja -järjestelmät(V)	5
TTC6550	Auditointi, Penetraatiotestaus ja Red Team - toiminta(V)	5

Tieto- ja viestintätekniikan tutkinto-ohjelma, insinööri (AMK), forensiikka ja analysointi -moduulin opintojaksot

Course Code	Course Name	ECTS
TTC7010	Haittaohjelmien analysointi(V)	5
TTC7020	Uhkien havainnointi ja vastetoiminta(V)	5
TTC7030	Uhkien metsästys(V)	5
TTC7040	Edistynyt forensiikka(V)	5
TTC7050	Digitaalinen forensiikka ja poikkeamienhallinta(V)	5
TTC6030	Kyberuhkatieto ja data-analytiikka(V)	5

Tieto- ja viestintätekniikan tutkinto-ohjelma, insinööri (AMK), kyberturvallisuusharjoitus -moduulin opintojaksot

Course Code	Course Name	ECTS
TTC7510	Kyberturvallisuusharjoitusten perusteet(V)	5
TTC7520	Kyberturvallisuusharjoituksen suunnittelu(V)	5
TTC7530	Kyberturvallisuusharjoitus(V)	5
TTC6060	Poikkeamien hallinta ja kyberturvakeskukset(V)	5
TTC6030	Kyberuhkatieto ja data-analytiikka(V)	5
TTC6550	Auditointi, Penetraatiotestaus ja Red Team toiminta(V) -	5

Moduulirakenteesta ja verkkosivuista päätellen tutkinto-ohjelma tähtää vahvasti kyberturvallisuuteen. Tutkinto-ohjelman kategoria: B.

Tietojenkäsittelyn tutkinto-ohjelma, tradenomi (AMK) perustuu Fullstack -ohjelmointiin, DATA&AI ja Game Production suuntautumisiin. Kyberturvallisuuden opintojaksoja ei ole kiinnitettynä opetussuunnitelmassa, vaikka insinööri tutkinto-ohjelmissa niitä on tarjolla.

Tutkinto-ohjelman kategoria: E.

Erikoistumiskoulutukset

Avoimessa ammattikorkeakoulussa JAMK tarjoaa kyberturvallisuusopintokokonaisuutta (30 op). Alkuun moduuli koostui osittain perusopinnoista ja osittain syventävistä kurs-seista, joiden päätarkoituksena oli antaa perustietämys kyberturvallisuudesta sekä tieto-taitoa, siitä miten voit suojata ja auditoida kyberympäristöä.

Avoimen AMK:n kyberturvallisuus 30 op -paketti

Course Code	Course Name	ECTS
TTZW0410	Git -versionhallinta ja Gitlab -projektien hallintaympäristö	1
TTC1040	Linux käyttö ja hallinta	5
TTC2030	Ohjelmoinnin perusteet	5
TTC1030	Tietoverkot	5
TTC1020	Kyberturvallisuus	4
TTC6550	Auditointi, Penetraatiotestaus ja Red Team –toiminta	5
TTC6040	Hyökkäykset ja puolustusmenetelmät sekä suojaaminen	5

Nykyään opinnoissa mennään astetta pidemmälle ja sisältö koostuu kuudesta syventä-västä kurssista, jotka on jaettu kahteen eri erikoistumiskokonaisuuteen. Ensimmäisessä erikoistumismoduulissa keskitytään yrityksen kyberturvallisuuden hallintaan.

Kyberturvallisuus erikoistumismoduuli 1

Course Code	Course Name	ECTS
TTC6010	Tietoturvakontrollit(V)	5
TTC6020	Kyberturvallisuuden hallinta(V)	5
TTC6040	Hyökkäykset ja puolustusmenetelmät sekä suojaaminen(V)	5

Toisessa erikoistumismoduulissa kohteena on Security Operations Center-toiminta.

Kyberturvallisuus erikoistumismoduuli 2

Course Code	Course Name	ECTS
TTC6030	Kyberuhkatieto ja data-analytiikka(V)	5
TTC6060	Poikkeamien hallinta ja kyberturvakeskukset(V)	5
TTC6050	Koventaminen(V)	5

Kokonaisuudet ovat tutkinto-ohjelman osia tarjottuna avoimessa kanavassa.

6. Kaakkois-Suomen ammattikorkeakoulu

Laajemmin tarkastellessa oppilaitoksen turvallisuuteen tai tietotekniikkaan painottuvat tutkinto-ohjelmat hajaantuivat kolmelle eri alalle:

- Kauppa, hallinto ja oikeustieteet (turvallisuusala, data-analytiikan koulutus)
- Tekniikan alat (Robotiikka ja tekoäly)
- Tietojenkäsittely ja tietoliikenne (ns. normaalit ICT ja tietojenkäsittely)

Rajauksesta johtuen ylimmät kaksi rajautuivat pois, mutta sisälsivät satunnaisesti kyber-turvallisuuteen liittyviä opintojaksoja. Esim. turvallisuusalalla oli täydentävässä suuntau-tumisessa kyberturvallisuus ja kriisinhallinta -moduuli. Data-analytiikan koulutuksessa

sekä robotiikassa ja tekoälyssä oli tarjolla ao. mukainen tarjonta. XAMK esittää opetussuunnitelmansa vapaasti valittavat opintojaksot muiden tutkinto-ohjelmien tarjonnasta. Esimerkiksi kaikkien AMK-tason opetussuunnitelmien rakenteessa oli nähtävissä 400 eri valittavaa opintojaksoa.

Ylempi ammattikorkeakoulu - EQF7

YAMK tutkinto-ohjelmat rajauksen alueella sijoittuivat Mikkeliin ja Kotkaan. Kyberturvallisuus, insinööri (YAMK) Kotkassa järjestettävä tutkinto-ohjelma oli sisäänoton perusteella 25 aloituspaikan kokoinen.

Kyberturvallisuus, insinööri (YAMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
BY00CW36	Johdatus kyberturvallisuuteen(V)	5
CS00DO70	Kyberturvallisuusauditointi ja kyberhygienia(V)	5
CS00CU79	Puolustava kyberturvallisuus(V)	5
CS00CU80	Hyökkäävä kyberturvallisuus(V)	5
CS00EO20	Tietoverkkojen kyberturvallisuus(V)	5

Tutkinto-ohjelman kategoria: A.

Tiedonhallinnan ja sähköisen arkistoinnin koulutus, tradenomi (YAMK), tähän Mikkelissä järjestettävä tutkinto-ohjelma ei sisältänyt kyberturvallisuuden opintojaksoja pl. vapaasti valittavien tarjonta.

Tutkinto-ohjelman kategoria: E.

Ammattikorkeakoulu - EQF6

XAMK:ssa tieto- ja viestintätekniikan, insinööri (AMK) tutkinto-ohjelma jakautuu neljään erilliseen opetussuunnitelmaan (tai suuntautumiseen). Jokainen näistä on oma hakukohteensa. Tällöin jokainen suuntautuminen voidaan kategorisoida mallien mukaisesti, koska opiskelija valitsee jo hakuvaiheessa erikoistumisensa. Tieto- ja viestintätekniikka, insinööri (AMK) Kotkassa järjestettävään kyberturvallisuuskoulutukseen oli 25 aloituspaikkaa syksyllä 2022.

Tieto- ja viestintätekniikka, insinööri (AMK), kyberturvallisuuden koulutus, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
KT00DN41	Aloitusprojekti, kyberturvallisuus(P)	5
KT00DN42	Kyberturvallisuuden perusteet(P)	5
KT00DN46	Turvallisten tietoverkkojen ylläpito(P)	5
KT00BI12	Tietoturva(P)	5
KT00DN47	Turvallisten tietoverkkojen suunnittelu(P)	5
KT00BI22	Kyberturvallisuuden matematiikka ja fysiikka(P)	5
KT00DN48	Turvalliset web-palvelut(P)	5
KT00BI23	Kyberturvallisuus(P)	5
TI00BI24	Tietoturvalaitteet(P)	5
KT00BI25	Penetraatiotestaus(P)	5

KT00DN54	Turvalliset reititysverkot(P)	5
KT00EO18	Kyberturvallisuusprojekti 1(P)	5
KT00BI33	Kehittynyt kyberturvallisuus(P)	5
KT00BI26	Turvalliset yritysverkot(P)	5
KT00EO19	Kyberturvallisuusprojekti 2(P)	5

Tutkinto-ohjelman kategoria: A.

Mikkelissä järjestettävään ohjelmistotekniikan suuntautumiseen oli 25 aloituspaikkaa syksyllä 2022.

Tieto- ja viestintätekniikka, insinööri (AMK), ohjelmointitekniikka kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
OT00EK08	Ohjelmistojen tietoturva(P)	5

Tutkinto-ohjelman kategoria: CD.

Peliohjelmoinnin koulutus & peliteknologian tutkinto-ohjelmassa molemmat suuntautumiset olivat erilliset hakukohteensa ja ne ovat luonteeltansa opetussuunnitelmissa hyvinkin samankaltaiset. Varsinkin kyberturvallisuutta tarkastellessa molemmat opetussuunnitelmat sisälsivät täydentävässä *Peliteknologiat ja digiturvallisuus* -moduulissa.

Tieto- ja viestintätekniikka, insinööri (AMK), peliohjelmointi ja peliteknologia, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
PO00EP08	Digiturva ja kyberhygienia(V)	5

Tutkinto-ohjelman molempien suuntautumisten kategoria: D.

Tietojenkäsittely, päivätoteutuksen Mikkeliin sijoittuva, mutta puhtaasti verkko-opetuksena (2022 perusteella) järjestettävä tietojenkäsittelyn tutkinto-ohjelma ei sisältänyt mainittavia kyberturvallisuuden opintojaksoja. Opetussuunnitelma nojautui vapaasti valittavan tarjonnan kautta kyberturvallisuuteen.
Tutkinto-ohjelman kategoria: E.

Information Technology, Bachelor of Engineering, tämä Mikkelissä järjestettävä englanninkielinen tutkinto-ohjelma tieto- ja viestintätekniikasta sisälsi hyvin yksilöllisen tutkinto-ohjelman, josta löytyi pakollisena yksi opintojakso.

Information Technology, Bachelor of Engineering, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
IT00CO77	Security Fundamentals(P)	5

Muussa tarjonnassaan tutkinto-ohjelma nojautui täydentävän osaamisen (valinnaisen) opintotarjontaan.

Tutkinto-ohjelman kategoria: CD.

Täydentävä osaaminen (valinnainen)

XAMK:n täydentävä osaaminen (valinnaiset) kurssit

Course Code	Course Name	P/V	ECTS
MA00AA07	Tietoturvatietoisuus	V	5
MO00DS12	Tietoturvallisuus	V	5
VV00DM10	Esimies ja tietoturva	V	5

Erikoistumiskoulutus

Ei kyberturvallisuuteen liittyviä täydennyskoulutuksia. Avoimessa AMK:ssa opinto-oppaan perusteella digitalisaation alla samoja kuin opetussuunnitelmien täydentävässä osaamisessa.

7. Kajaanin ammattikorkeakoulu

Ylempi ammattikorkeakoulu - EQF7

Tietojenkäsittelyn ja liiketoimintaosaamisen koulutus, tradenomi (YAMK) tutkinto-ohjelmassa aloittaa syksyllä 2022 opintopolun perusteella 15 opiskelijaa. Tutkinto-ohjelmassa ei ole kyberturvallisuuteen liittyviä opintojaksoja toteutuksessa eikä niitä havaittu muissa tutkinto-ohjelmissa. Tutkinto-ohjelman kategoria: F.

Ammattikorkeakoulu - EQF6

KAMK:ssa tietojenkäsittely, tradenomi (AMK) -tutkinto-ohjelma jakautuu kahteen erilliseen opetussuunnitelmaan (tai suuntautumiseen) ja tieto- ja viestintätekniikan, insinööri (AMK) -tutkinto-ohjelma jakautuu kolmeen erilliseen opetussuunnitelmaan (tai suuntautumiseen). Kukin näistä oli opintopolussa oma hakukohteensa. Yhteensä aloituspaikkoja näissä tutkinto-ohjelmissa ja niiden suuntautumisissa on 165. Opetus sijoittui lähtökohtaisesti Kainuuseen, mutta poikkeuksena Pohjois- Pohjanmaalla Raahessa suoritettava Pelialan koulutus 20 aloituspaikalla.

Tietojenkäsittely, tradenomi (AMK) tutkinto-ohjelman Datacenter -suuntautumisen opetussuunnitelma sisälsi kohtalaisen paljon kyberturvallisuuteen liittyviä opintojaksoja.

Tietojenkäsittely, tradenomi (AMK), datacenter, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
KTPT012	Organisaation tietoturva(P)	3
TT00BM11	Tekninen tietoturva(P)	3
TT00CB32	Palomuurin perusteet(P)	2
TT00CB34	Kyberturvallisuus I(V)	5
TT00CB35	Kyberturvallisuus II(V)	5

Tutkinto-ohjelman kategoria: BC.

PELIALA-suuntautumisen opetussuunnitelmassa oli yksi opintojakso pakollisena kyberturvallisuudesta.

Tietojenkäsittely, tradenomi (AMK), peliala, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
KTPT012	Organisaation tietoturva(P)	3

Oletettavasti rinnakkaisesta tutkinto-ohjelmasta oli mahdollista ottaa opintojaksoja, vaikka ne ei ollut pelialan opetussuunnitelmaan sidottuna.

Tutkinto-ohjelman kategoria: CE.

Tieto- ja viestintätekniikka, insinööri (AMK) tutkinto-ohjelmassa poiketen esim. XAMK:n ja JAMK:n mallista, KAMK:n ICT insinööri tutkinnon suuntautumiset omasivat omat opetussuunnitelmansa, mutta silti olivat yhtenäinen hakukohde opintopolussa keväällä 2022. Hakukohteeseen ilmoitettiin opiskelupaikkoja 40, joten oletettavasti ne jakaantuivat puoliksi suuntautumisten kesken. Datasta tekoälyyn suuntautuminen oli kuitenkin itsenäinen hakukohde 20 aloituspaikalla.

ÄLYKKÄÄT JÄRJESTELMÄT -suuntautumisessa on yksi pakollinen ja yksi vapaasti valittava opintojakso kyberturvallisuuteen liittyen.

Tieto- ja viestintätekniikka, insinööri (AMK), älykkäät järjestelmät, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
TT00BW68	Tietoturva IoT -ratkaisuissa(P)	5
TYW391	Tietoturvaohjelmointi(V)	4

Tutkinto-ohjelman kategoria: CD.

PELITEKNOLOGIA-suuntautumisen opintosuunnitelma ei sisältänyt kyberturvallisuuden opintoja. Tutkinto-ohjelman kategoria: E.

DATASTA TEKOÄLYYN -suuntautuminen tarjottiin keväällä 2022 opintopolussa omana hakukohteenaan: päiväopintoina Kajaanissa 20 aloituspaikkaa ja monimuoto-opintoina pääkaupunkiseudulle 20 aloituspaikalla. Tutkinto-ohjelmassa oli pakollisena yksi kyberturvallisuuteen liittyvä opintojakso.

Tieto- ja viestintätekniikka, insinööri (AMK), datasta tekoälyyn, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
TT00BX21	Tietoturva, kyberturvallisuus ja etiikka(P)	3

Tutkinto-ohjelman kategoria: C.

Erikoistumisopinnot

Kajaanin ammattikorkeakoulun tarjonnassa ei ollut kyberturvallisuuteen liittyviä erikoistumis- tai täydennyskoulutuksia.

8. Karelia-ammattikorkeakoulu

Tietojenkäsittelyn ja tietoliikenteen ala koostuu Kareliassa vain tietojenkäsittely, tradenomi (AMK) -tutkinto-ohjelmasta. Kyseisen sisäänottona on 60 opiskelijaa.

Ylempi ammattikorkeakoulu - EQF7

Karelian ammattikorkeakoulu ei tarjoa YAMK-tutkinto-ohjelmia tietojenkäsittelyn ja tietoliikenteen alalta. Lähimmät tutkinto-ohjelmat ovat:

- Teknologiaosaamisen johtaminen, insinööri (YAMK)
- Johtaminen ja liiketoimintaosaaminen, tradenomi (YAMK)

Kummassakaan tutkinto-ohjelmassa ei ole kyberturvallisuuteen liittyviä opinto- jaksoja toteutuksessa.

Ammattikorkeakoulu - EQF6

Tietojenkäsittely, tradenomi (AMK) tutkinto-ohjelma opetetaan verkkototeutuksena (kevään haun 2022 perusteella), mutta fyysinen kampus on Wärtsilä Joensuussa.

Tietojenkäsittely, tradenomi (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
LTD6043	Johdatus tietoturvaan(P)	5
DTI0021	Tietoturva sovelluskehityksessä(V)	5

Ydinopintoihin kuului yksi opintojakso kyberturvallisuutta ja suuntautumiseen (valinnaiset ammattiopinnot 1) myös yksi opintojakso.

Tutkinto-ohjelman kategoria: CD.

Erikoistumiskoulutus

Vuonna 2019 Kareliassa on ollut avoimessa ammattikorkeakoulussa kolme tieto- ja viestintätekniikan (60 op) kokonaisuutta: ABLOYxIT, SmartICT ja Digiosaajan ICT -taidot. Kaikissa näissä on Johdatus tietoturvaan -opintojakso, mutta ei muita kyberturvallisuuteen liittyviä opintojaksoja.

9. LAB-ammattikorkeakoulu

Korkeakoulun tutkinto-ohjelmat jakaantuivat Etelä-Karjalan Lappeenrantaan ja Päijät-Hämeen Lahteen. Yhteensä 272 aloituspaikkaan.

Ylempi ammattikorkeakoulu - EQF7

Kahdessa tutkinto-ohjelmassa oli sisäänotto 55 kpl keväällä 2022

- IoT:stä tekoälyyn, Insinööri (YAMK)
- Liiketoiminnan digitaaliset ratkaisut, Tradenomi (YAMK)

Molemmissa tutkinto-ohjelmissa käsiteltiin informaation, digitaalisuuden ja datan käsittelyä, mutta tieto-/kyberturvallisuus puuttuu aiheena.

Tutkinto-ohjelman kategoria: F.

Ammattikorkeakoulu - EQF6

Insinööri-tutkinto-ohjelmiin aloituspaikoista jakaantui 152 ja tradenomi-tutkinto-ohjelmiin 65 aloituspaikkaa.

Tieto- ja viestintätekniikka, Insinööri (AMK) tutkinto-ohjelma jakaantui päivätoteutukseen ja verkkototeutukseen. Molemmissa noudatettiin samaa opetussuunnitelmaa, mutta ensimmäisen vuoden lopussa haarauduttiin suuntautumisiin. Suuntautumiset eivät kuitenkaan painottuneet kyberturvallisuuteen.

Tieto- ja viestintätekniikka, Insinööri (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
AT00BT77	Tietoliikenteen ja tietoturvan perusteet(P)	5
AT00BY11	Lähiverkkojen perusteet ja turvallisuus(V)	5

Kaikille oli yksi opintojakso pakollisena ydinopinnoista ja tietoverkot suuntautumiselle vielä erikseen valinnaisena lähiverkkojen perusteet ja turvallisuus.

Tutkinto-ohjelman kategoria: CD.

Industrial Information Technology, Bachelor of Engineering on LAB:ssa tarjolla oleva englanninkielinen tutkinto-ohjelma, mikä oli toteutukseltaan poikkeava suomenkieliseen tutkinto-ohjelmaan.

Industrial Information Technology, Bachelor of Engineering, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
AT00CK38	Virtualization: Networks and Security(P)	15

Tutkinto-ohjelman kategoria: CDi.

Tietojenkäsittely, Tradenomi (AMK) tutkinto-ohjelmassa ei ilmentynyt kyberturvallisuuteen liittyviä opintojaksoja. Tutkinto-ohjelman kategoria: E, koska rinnakkaisissa tutkinto- ohjelmissa oli mahdollisesti vapaasti valittavaksi opintojaksoja.

Erikoistumiskoulutus

Ei erikoistumis- tai täydennyskoulutusta kyberturvallisuuteen liittyen.

10. Lapin ammattikorkeakoulu

Ylempi ammattikorkeakoulu - EQF7

Lapin AMK:n YAMK tutkintorakenne on mielenkiintoinen. Opintosuunnitelmien opintojaksot ovat taustatutkintoriippuvaista, mutta useammasta taustatutkinnosta voi hakea yhteen YAMK ohjelmaan.

Tiedolla johtamisen asiantuntijuus -tutkinto-ohjelmasta löytyy pakollisena yksi opintojakso.

Kyberturvallisuuteen liittyvä opintojakso Lapin AMK:n YAMK-tutkinto-ohjelmista

Course Code	Course Name	ECTS
R599Y32	Etiikka ja vastuullisuus tiedolla johtamisessa(P)	5

Opintojakso on vapaasti valittavana kaikkien muiden YAMK tutkinto- ohjelmien (yht. 10 kpl) opetussuunnitelmarakenteessa.

Ammattikorkeakoulu - EQF6

Tieto- ja viestintätekniikka, Insinööri (AMK). Tutkinto-ohjelma haarautuu kolmeen eri suuntautumiseen, mutta on yhdistetty hakukohde:

- Informaatiohallinnon asiantuntija
- Kyberfyysisten järjestelmien kehittäjä
- Ohjelmistokehittäjä

Informaatiohallinnon asiantuntijan -suuntautumisen opetussuunnitelmarakenteessa löytyy kaksi kurssia.

Tieto- ja viestintätekniikka, Insinööri (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
R504TL155	Organisaation tietoturva(V)	5
R504TL156	Salausmenetelmät(V)	5

Moduuli on kuitenkin vaihtoehtoinen ja tutkinto-ohjelma ei itse painota kyberturvallisuuteen.

Tutkinto-ohjelman kategoria: D.

Machine Learning and Data Engineering, Bachelor of Engineering opetussuunnitelma on saman rakenteinen kuin suomenkielinen, mutta siitä löytyy kyberturvallisuuden pakollisena.

Machine Learning and Data Engineering, Bachelor of Engineering, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
R504D74	Cyber Security(P)	5

Opintojakson kuvaus ei vastaa kumpaakaan suomenkielistä opintojaksokuvausta, eli eri osaamistavoitteet kuin *Organisaation tietoturvassa* suomenkielisessä.

Tutkinto-ohjelman kategoria: C.

Tietojenkäsittely, Tradenomi (AMK) koulutus perustuu Tornioon monimuoto- ja verkkototeutuksena. Tradenomeilla on eriävä opintojakso suhteutettuna insinööri tutkinto-ohjelmiin.

Tietojenkäsittely, Tradenomi (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
T42T157OJ	Tietoturvan perusteet	5

Tutkinto-ohjelman kategoria: C.

Erikoistumiskoulutus

Ei erikoistumis- tai täydennyskoulutusta kyberturvallisuuteen liittyen.

11. Laurea-ammattikorkeakoulu

Ylempi ammattikorkeakoulu - EQF7

Laureassa vain yksi tutkinto-ohjelma tuli tietojenkäsittelyn ja tietoliikenteen alalle, johon sisäänotto 30 opiskelijaa.

Tulevaisuuden innovatiiviset digitaaliset palvelut, Tradenomi (YAMK) tutkinto-ohjelmassa ei ole kyberturvallisuuteen liittyviä opintojaksoja opetussuunnitelmassa.

Merkittävänä mainintana kuitenkin Turvallisuusjohtamisen, Tradenomi (YAMK) -tutkinto-ohjelma palvelualojen alalta, joka sisälsi Kyberturvallisuuden Johtaminen -opintojakson (5 op).

Oletettavasti opintojaksoon on mahdollista ilmoittautua korkeakoulun sisältä, jolloin YAMK tutkinto-ohjelmissa on yksi opintojakso kyberturvallisuutta mahdollisena.

Tutkinto-ohjelman kategoria: E.

Ammattikorkeakoulu - EQF6

Tradenomi (AMK) -koulutus jakautuu useampaan eri tutkinto-ohjelmaan, jotka on tilastoitu eri alojen alle. Kaikki ovat erillisiä hakukohteita.

- Tietojenkäsittely ja tietoliikenne
    - kyberturvallisuus
    - digitaalisten palvelujen kehittäminen
- Palvelualat (poikkeus rajauksesta, koska selkeästi kyberturvallisuuteen liittyvä)
    - Turvallisuuden ja riskienhallinnan koulutus

Kaikista tutkinto-ohjelmista on myös englanninkieliset toteutukset.

Kyberturvallisuus, Tradenomi (AMK) pakollisissa opintojaksoissa:

Kyberturvallisuus, Tradenomi (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
R0242	Tietoverkot ja tietoturva(P)	5

Täydentävissä moduuleissa seuraavia vapaa valintaisia opintojaksoja:

Information infrastructure and security, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
TO00BR88	Internet Infrastructure and Security(V)	10

Information security management, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
TO00BR89	Introduction to Information Security(V)	5
TO00BR90	Information Security Management(V)	5

Cybersecurity technologies, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
TO00BR94	Systems Security(V)	5
TO00BR93	Network and Applications Security(V)	5

TO00BR91	Enterprise Security and Practitioners(V)	5
TO00BR92	Cybersecurity Analyst(V)	5

Cybersecurity work-life practices, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
TO00BS11	Cybersecurity Project(V)	5
TO00BR95	Cybersecurity Hackathon Project(V)	3
TO00BR96	Cybersecurity Working Life Practices(V)	2

Kyberturvallisuuden tutkinto-ohjelma tähtää kyberturvallisuuteen ja on oma hakukohteensa Tutkinto-ohjelman kategoria: A. Tutkinto-ohjelmalla on myös lähestulkoon identtinen englanninkielinen vastine omana hakukohteenaan.

Digitaalisten palvelujen kehittäminen, Tradenomi (AMK) suuntautumisessa on yksi opintojakso "muuna täydentävänä IT-osaamisena".

Digitaalisten palvelujen kehittäminen, Tradenomi (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
TO00BR89	Introduction to Information Security	5

Tutkinto-ohjelman kategoria: D. Tutkinto-ohjelmalla on myös lähestulkoon identtinen englanninkielinen vastine omana hakukohteenaan.

Turvallisuuden ja riskienhallinnan koulutus, Tradenomi (AMK) oli rajauksen ulkopuolelta (Palvelualat), mutta selkeästi nousi esiin kyberturvallisuusaspektinsa vuoksi. Erikoisuutena kuitenkin, että tämä tutkinto-ohjelma ei jaa identtisiä opintojaksoja vaan sillä on hyvin omannäköiset opintojaksot.

Turvallisuuden ja riskienhallinnan koulutus, Tradenomi (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
HT00BN81	Tieto- ja kyberturvallisuus(P)	5
TO00BN70	Tieto- ja kyberturvallisuuden hallinta(V)	10

Tutkinto-ohjelmalla on myös lähestulkoon identtinen englanninkielinen vastine omana hakukohteenaan.

Erikoistumisopinnot

Täydennyskoulutuksessa Laurealla oli tarjonnassa seuraavat koulutukset:

- Risk Manager -koulutus, 5 op
- Riskienhallintaa ja resilienssiä - Risk Managerin täydennyskoulutus, 1 op
- Katakri-pääauditoijakoulutus, 15 op
- Laurea Certified Risk Officer, 5 op

12. Metropolia ammattikorkeakoulu

Ylempi ammattikorkeakoulu - EQF7

Tutkinto-ohjelmat jakaantuivat insinööreille suunnatumpaan *Information Technology* -ohjelmaan ja tradenomeille suunnatumpaan *Business Informatics* - ohjelmaan. Tutkinto-ohjelmat eivät kuitenkaan poissulje opiskelijataustan perusteella hakua ristiin.

Master's Degree Programme in Information Technology, Networking and Services tutkinto-ohjelmaan sisäänotto on 30 opiskelijaa.

Master's Degree Programme in Information Technology, Networking and Services, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
IT00DV52	Cyber Security(P)	5

Tutkinto-ohjelman kategoria: C.

Master's Degree Programme in Information Technology, Medical Technology opetussuunnitelmassa ei ole kyberturvallisuuden opintojaksoja.

Tutkinto-ohjelman kategoria: E.

Master's Degree Programme in Business Informatics tutkinto-ohjelmaan ei sisälly kyberturvallisuuden opintojaksoja, mutta se on tarkoitettu insinööri (AMK) ja tradenomi (AMK) taustaisille.

Tutkinto-ohjelman kategoria: E.

Ammattikorkeakoulu - EQF6

Tieto- ja viestintätekniikan tutkinto-ohjelma jakautui suomenkieliseen päivätoteutukseen (sisäänotto 143), monimuotototeutukseen (sisäänotto 120), ja englanninkieliseen päivätoteutukseen (sisäänotto 75). Pakolliset opinnot eivät sisältäneet kyberturvallisuutta, mutta ammatillisissa suuntautumisissa on kyberturvallisuutta seuraavasti:

Ohjelmistotuotanto -suuntautuminen:

Ohjelmisto- tuotanto, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
TX00EX84	Eettinen hakkerointi(V)	5

Älykkäät IOT -järjestelmät -suuntautuminen:

Älykkäät IoT- järjestelmät, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
TX00EY35	IoT-tietoturva(V)	5
TX00EX92	Tietoturvalliset yritysverkot(V)	5
TX00EX94	Kyberturvallisuuden erikoiskurssi(V)	5
TX00EY35	Eettinen hakkerointi(V)	5
TX00EX99	Käytännön kyberturvallisuus(V)	5

Tutkinto-ohjelman kategoria: C.

Erikoistumiskoulutus

Metropoliasta järjestetään *Kyberturvallisuuden erikoistumiskoulutus* (30 opintopistettä), jonka opintojaksoja ei ole tutkintoon johtavissa koulutuksissa.

Metropolian kyberturvallisuuden erikoistumiskoulutuksen opintojaksot

Course Code	Course Name	ECTS
TX00CO64	Johdatus kyberturvallisuuteen	5
TX00CO63	Kyberturvallisuusliiketoiminta	5
TX00CO61	Puolustava kyberturvallisuus	5
TX00CO67	Offensiivinen kyberturvallisuus	5
TX00CO65	Tietoverkkojen kyberturvallisuus	5
TX00CO62	Kyberturvallisuusprojekti	5

Avoimessa ammattikorkeakoulussa tarjolla oli myös seuraava lista yksittäisiä opintojaksoja: Tietoturvallisuuden perusteet, Eettinen hakkerointi, Cyber Defence Professional, CISSP: Certified Information System Security Professional ja Tietoturvaratkaisut.

13. Oulun ammattikorkeakoulu

Ylempi ammattikorkeakoulu - EQF7

Degree Programme in Data Analytics and Project Management -tutkinto-ohjelma on tarjolla tradenomi ja Insinööri -pohjakoulutuksella. Tämän vuoksi opintokokonaisuus vaihtelee 60 ja 90 opintopisteen välillä. Kyberturvallisuus sisältyy osana datan keräämistä.

Degree Programme in Data Analytics and Project Management, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
KA00DA48	Towards Data Mining(V)	5

Tutkinto-ohjelma painottui vahvasti muuhun kuin kyberturvallisuuteen.

Tutkinto-ohjelman kategoria: C.

Degree Programme in Printed Intelligence: Ei kyberturvallisuuteen liittyviä opintojaksoja.

Hyvinvoinnin digitaaliset ratkaisut tutkinto-ohjelma on tarjolla tradenomi ja insinööri -pohjakoulutuksella. Tämän vuoksi opintokokonaisuus vaihtelee 60 ja 90 opintopisteen välillä. Kyberturvallisuus löytyi tietosuojan ja tietoturvan ylläpitämisen kautta sosiaali- ja terveydenhuoltojärjestelmien digitaalisissa ratkaisuissa.

Hyvinvoinnin digitaaliset ratkaisut tutkinto-ohjelma, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
OU00CV36	Tietosuoja ja turvallisuus sosiaali- ja terveydenhuolto-järjestelmässä(V)	5

Ammattikorkeakoulu - EQF6

OAMK:ssa tietojenkäsittely ja tietoliikenne opetus jakaantui kahteen tutkinto- ohjelmaan

- Tietotekniikan tutkinto-ohjelma,
    - Laite- ja tuotesuunnittelun suuntautumisvaihtoehto
    - Ohjelmistokehityksen suuntautumisvaihtoehto (fi, en)
- Tietojenkäsittelyn tutkinto-ohjelma

Kyberturvallisuus (tai tietoturvallisuus) ei ollut mainittavasti minkään tutkinto- ohjelman opintojakson nimessä.

Tutkinto-ohjelmien kategoria: F.

Erikoistumiskoulutukset

Ei tarjontaa kyberturvallisuuden opinnoissa.

14. Satakunnan ammattikorkeakoulu

Ylempi ammattikorkeakoulu - EQF7

SAMK:ssa ei ollut tietojenkäsittelyn ja tietoliikenteen tutkinto-ohjelmia tarjolla 2022–2023 ylemmässä ammattikorkeakoulussa.

Ammattikorkeakoulu - EQF6

SAMK:ssa tietojenkäsittelyn ja tietoliikenteen opetus painottuu Tradenomi (AMK) -tutkinto-ohjelmaan kahdella eri painotuksella:

- Tietojenkäsittely
- Artificial Intelligence

Näistä *Artificial Intelligence* opetussuunnitelma ei sisältänyt kyberturvallisuuteen liittyviä opintojaksoja.

Tutkinto-ohjelmien kategoria: E.

Tietojenkäsittely tutkinto-ohjelman modulaarissa rakenteessa kyberturvallisuus sijoittuu "Infraosaamisen-alle (57 op) ja siellä "Pilvi-moduuliin seuraavilla opintojaksoilla.

Tietojenkäsittely, Tradenomi (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
IC210212	Tietoturva(V)	5
IC210213	NG palomuurin hallinta(V)	5

Tieto- ja viestintätekniikan Insinööri (AMK) tutkinto-ohjelmaa ei ole, mutta erikoisuutena sähkö- ja automaatiotekniikan, insinööri (AMK) tutkinto-ohjelma käyttää samoja moduulirakenteita Tradenomi -tutkinnosta esimerkiksi tämän "Infraosaamisen" osalta.

Tutkinto-ohjelman kategoria: D.

Erikoistumiskoulutus

Ei erikoistumis- tai täydennyskoulutusta kyberturvallisuuteen liittyen.

15. Savonia-ammattikorkeakoulu

Ylempi ammattikorkeakoulu - EQF7

Savoniassa YAMK tutkinto-ohjelmat sisältävät ns. "Valinnaiset yhteiset opinnot" opintojaksojen tarjonnan, josta voi valita täyttöä kuhunkin tutkinto-ohjelmaan. Näissä yhteisesti valittavissa opinnoissa ei kuitenkaan kyberturvallisuuteen painottuvia opintojaksoja löydy.

Digitalisaation asiantuntija sosiaali- ja terveysalalla (YAMK), samaan tutkinto-ohjelma rakenteeseen voi hakea eri pohjilta. Tämän perusteella valmistutaan joko insinööri (YAMK), tradenomi (YAMK) tai sosiaali- ja terveysalan (YAMK). Opintokokonaisuudessa pakollisena opintojaksona (pohjatutkinnosta riippumatta on):

Digitalisaation asiantuntija sosiaali- ja terveysalalla (YAMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
4 TYDA20	Tietoturva ja tietosuoja digitaalisissa järjestelmissä(P)	5

Ammattikorkeakoulu - EQF6

Tutkinto-ohjelmat painottuivat insinööritieteisiin, johon yhteensä 104 aloituspaikkaa syksylle 2022.

- Bachelor’s Degree Programme in Information Technology (Internet of Things)
- Tietotekniikan tutkinto-ohjelma

Tietotekniikan tutkinto-ohjelman kyberturvallisuuteen painottavat opintojaksot:

Tietotekniikan tutkinto-ohjelma, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
ETX7200	Johdatus tietoturvaan(P)	5
ETN0140	CyberOps Associate(V)	5

Johdatus tietoturvaan oli kaikille pakollisissa ammattiopinnoissa, mutta CyberOps Associate sijoittui tietoverkkotekniikan ammattiopintoihin (suuntautumiseen). Hakukohteena kaikki hakivat tutkinto-ohjelmaan ja tarkemmat suuntautumisten oppilasmäärät olivat epäselvät verkkosivujen perusteella.

Tutkinto-ohjelman kategoria: C.

Bachelor’s Degree Programme in Information Technology (Internet of Things) -tutkinto-ohjelmassa ei ole kyberturvallisuuteen liittyviä opintojaksoja.

Tutkinto-ohjelman kategoria: E.

Erikoistumiskoulutus

Ei erikoistumis- tai täydennyskoulutusta kyberturvallisuuteen liittyen.

16. Seinäjoen ammattikorkeakoulu

Ylempi ammattikorkeakoulu - EQF7

Seinäjoen ammattikorkeakoulussa ei ole YAMK tutkinto-ohjelmia tarjolla tietojenkäsittelyn tai tietoliikenteen aloilla 2022–2023. Tekniikan alan YAMK tarjonnassa ei myöskään löytynyt kyberturvallisuuden opintojaksoja.

Ammattikorkeakoulu - EQF6

Erikoismainintana löytyy *tekniikan alojen* alta insinööri (AMK), *automaatiotekniikasta* tietoliikenne ja tietoturva (4 op) opintojakso sekä *sähköautomaatiosta* että *koneautomaation* suuntautumisesta. Lisäksi *kauppa, hallinto ja oikeustieteet* alta liiketalous, Tradenomi (AMK) sisältää tietojenkäsittelyyn yhdistettäviä moduuleja. Näistä "Digitaalinen liiketoiminta ja ohjelmointi 1: IT- infrastruktuuri" moduulissa on tietoturva ja juridiikka (3 op) opintokokonaisuus.

Tietotekniikka, insinööri (AMK) tutkinto-ohjelmassa on yksi kyberturvallisuuden opintojakso.

Tietotekniikka, insinööri (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
KL00CQ36	Tietoturva	3

Tutkinto-ohjelman kategoria: C.

Erikoistumiskoulutus

Ei erikoistumis- tai täydennyskoulutusta kyberturvallisuuteen liittyen.

17. Tampereen ammattikorkeakoulu

Ylempi ammattikorkeakoulu - EQF7

Tietojenkäsittelyyn ja tietoliikenteen -alaan liittyviä YAMK ohjelmia ei ollut tarjolla TAMK:ssa. Kaikki tutkinto-ohjelmat oli sijoitettu Tekniikan ja liikenteen - alalle.

Lähimpänä tietojenkäsittelyä ja tietotekniikkaa oli *Dataosaamisen ja tekoälyn* ylempi tutkinto-ohjelma, johon ei liittynyt kyberturvallisuuteen liittyviä opintojaksoja.

Tutkinto-ohjelman kategoria: F.

Ammattikorkeakoulu - EQF6

Tietotekniikan tutkinto-ohjelma, Insinööri (AMK) kaikille pakollisena oli tietoturvalliset järjestelmät - opintojakso ICT-insinöörin perusosaaminen moduulissa. Suuntaaviin ammatillisiin moduuleihin sijoittui Turvalliset tietoverkot ja kyberturvallisuustoiminnot - opintojaksot.

Tietotekniikan tutkinto-ohjelma, Insinööri (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS

5G00ET64	Tietoturvalliset järjestelmät(P)	5
5G00EV20	Turvalliset tietoverkot(V)	5
5G00EV10	Kyberturvallisuustoiminnot(V)	5

Tutkinto-ohjelman kategoria: CD.

Degree Programme in Software Engineering - englanninkielinen tutkinto-ohjelma oli selkeästi karsitumpi. Kyberturvallisuus ei ollut aiheena pakollisissa eikä ammatillisissa suuntautumisissa. Opetus- suunnitelman perusteella kyberturvallisuuteen liittyvä opintojakso oli vain vapaasti valittavissa opinnoissa.

Degree Programme in Software Engineering, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
5G00DM21	Introduction to Cybersecurity(V)	5

Tutkinto-ohjelman kategoria: D.

Tietojenkäsittely, Tradenomi (AMK) tutkinto-ohjelma painottui selkeästi peliteollisuuteen, mutta täysin vapaasti valittavissa opintojaksoissa oli listattuna kyberturvallisuutta.

Tietojenkäsittely, Tradenomi (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
4A00FA67	Kyberturvallisuuden perusteet(V)	3
4A00FA78	Tietoturvan yleiset perusteet(V)	3

Tutkinto-ohjelman kategoria: D.

Erikoistumiskoulutus

TAMK:lla on ollut vuonna 2020 kyberturvallisuuden erikoistumiskoulutus 30 opintopistettä, mutta 2021 ja 2022 ei havaittu käynnistyneitä koulutuksia.

18. Turun ammattikorkeakoulu

Ylempi ammattikorkeakoulu - EQF7

Tarjottava *Ohjelmistotekniikka ja ICT*-tutkinto-ohjelma YAMK:ssa on sama molemmille taustatutkinnoille.

- Ohjelmistotekniikka ja ICT
    - Insinööri (YAMK)
    - Tradenomi (YAMK)

Taustatutkinnosta riippuen opetussuunnitelman sisällä on 60 op ja 90 op ero, mutta molemmille taustatutkinnoille on merkitty pakolliseksi Tietoturva-moduuli.

Ohjelmistotekniikka ja ICT, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
MS00BP19	Tietoturvan perusteet(P)	5
MS00BP20	Tietoturvan riskien hallinta ja yksityisyyden suoja(P)	5

Tutkinto-ohjelman nimessä on ensimmäisenä ohjelmistotekniikka, vaikka itse ohjelmistotuotanto ja sovellusarkkitehtuurit moduuli on esim. insinööri (AMK) taustaisille sijoitettu opetussuunnitelmassa "laajentavaan osaamiseen". Tulkinnan mukaan tutkinto-ohjelma siis tähtää kyberturvallisuuteen ja siksi sen kategoria on A.

Ammattikorkeakoulu - EQF6

Tieto- ja viestintätekniikan koulutus, insinööri (AMK) tutkinto-ohjelmaan hakeudutaan yhtenä hakukohteena, mutta kyseinen tutkinto-ohjelma jakautuu viiteen eri suuntautumiseen (tai "osaamispolkuihin").

- Game and Interactive Technologies
- Embedded Software and IoT
- Terveysteknologia
- Data Networks and Cybersecurity
- Software Engineering and Project Management

Kaikille opiskelijoille on kuitenkin pakollisena yksi opintojakso kyberturvallisuutta.

Tieto- ja viestintätekniikan koulutus, insinööri (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
5051215	Tietoverkkojen ja tietoturvan perusteet(P)	5

Terveysteknologia -suuntautumisessa opintojaksotarjonnassa yski kurssi.

Terveysteknologia, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
5051252	Tietoturva ja tietosuoja(V)	5

Data Networks and Cybersecurity -suuntautumisessa oli eniten kyberturvallisuuden opintojaksoja.

Data Networks and Cybersecurity, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
TT00BO26	Programming for networks and information security(V)	5
TE00BL63	Network Security(V)	5
TE00BU43	Enterprise Networking, Security and Automation(V)	5
5051244	Information Security Testing and Assessment(V)	5
5051245	Operational Security(V)	5
TE00BZ70	Cybersecurity Situational Awareness(V)	5
5000BL89	Advanced Project on Networking and Cyber Security(V)	5

Muissa suuntautumisissa ei kyberturvallisuutta ollut tarjolla.

Bachelor's Degree in Information and Communications Technology -tutkinto-ohjelmassa oli tarjolla Cyber Security and IoT suuntautuminen Salossa. Sisäänotto jakaantui vuosien välillä: -/30 (vuosi 2022), 335/30 (vuosi 2021), 365/40 (vuosi 2020). Kyseinen suuntautuminen on ollut omana tutkinto-ohjelmanaan 2021 asti, mutta 2022 vaikuttaa yhdistyneen suomenkielisen tutkinto-ohjelman rakenteisiin.

Tietojenkäsittelyn koulutus, Tradenomi (AMK) tutkinto-ohjelma jakautuu kolmeen eri suuntautumiseen (tai "osaamispolkuihin").

- Ohjelmistotekniikka ja Projektinhallinta
- Tietoverkot ja kyberturva
- Ohjelmistojen kehittäminen Näistä kaikille pakollisena on

Tietojenkäsittelyn koulutus, Tradenomi (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
5051215	Tietoverkkojen ja tietoturvan perusteet(P)	5
3011580	Data Protection and Privacy(P)	5

Ohjelmistotekniikka ja projektinhallinta -suuntautumisessa ei ole kyberturvallisuuteen liittyviä opintojaksoja.

Ohjelmistojen kehittäminen ja tietojärjestelmät -suuntautumisessa yksi kyberturvallisuuteen liittyvä opintojakso.

Tietojenkäsittelyn koulutus, Tradenomi (AMK), ohjelmistojen kehittäminen ja tietojärjestelmät suuntautumisen kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
3011640	Application Security(V)	5

Tietoverkot ja kyberturva -suuntautuminen noudattaa lähestulkoon täysin insinööri (AMK) -tutkintoa kyberturvallisuuden opintojaksojen osalta.

Tietojenkäsittelyn koulutus, Tradenomi (AMK), tietoverkot ja kyberturva, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
TT00BO26	Programming for networks and information security(V)	5
TE00BL63	Network Security(V)	5
TE00BU43	Enterprise Networking, Security and Automation(V)	5
5051244	Information Security Testing and Assessment(V)	5
5051245	Operational Security(V)	5
TE00BZ70	Cybersecurity Situational Awareness(V)	5
3011369	Information Security Risk Management(V)	5
TE00BZ69	Cybersecurity for Industrial Networks(V)	5

Tutkinto-ohjelman kategoria: B.

Erikoistumiskoulutukset

TurkuAMK:ssa järjestetään Kyberturvallisuuden erikoistumiskoulutus (30 opintopistettä), jonka opintojaksoja ei ole tutkintoon johtavissa koulutuksissa.

Erikoistumiskoulutukset, kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
5231001	Johdanto kyberturvallisuuteen	5
5231005	Kyberturvallisuus ja liiketoiminta	5

5231003	Puolustava kyberturvallisuus	5
5231002	Hyökkäävä kyberturvallisuus	5
5231004	Tietoverkkojen kyberturvallisuus	5
5231006	Kyberturvallisuus projekti	5

19. Vaasan ammattikorkeakoulu

Ylempi ammattikorkeakoulu - EQF7

VAMK:ssa oli esim. digitalisaation johtaminen ja vastaavia YAMK tutkinto-ohjelmia, mutta niiden sisällössä ei kyberturvallisuuteen liittyviä opintojaksoja löydy.

Ammattikorkeakoulu - EQF6

VAMK:ssa tutkinto-ohjelmat jakautuvat seuraavasti:

- Tietojenkäsittelyn koulutus, Tradenomi (AMK)
- Information Technology, Insinööri (AMK)
- Tietotekniikan koulutus, Insinööri (AMK) Tietojenkäsittelyn koulutus, Tradenomi (AMK)

Tietojenkäsittely sisältää yhden opintojakson kyberturvallisuudesta pakollisessa "perus- ja ammattiosaaminen-moduulissa.

Tietojenkäsittelyn koulutus, Tradenomi (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
TK00BG66	Tietoturvallisuus(P)	5

Kyberturvallisuus ei ole aiheena syventävissä ammattiopinnoissa.

Tutkinto-ohjelman kategoria: C.

Tietotekniikan koulutus, Insinööri (AMK) tutkinto-ohjelman "Perusopinnot-moduulissa oli pakollisena kaksi opintojaksoa ja syventävissä opinnoissa "Tietoverkkotekniikkamoduulissa yksi opinto- jakso.

Tietotekniikan koulutus, Insinööri (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
ITTP0904	Ohjelmistotestaus(P)	5
IITP0310	Kyberturvallisuus(P)	3
TT00BI87	Tietoverkkojen turvallisuus(P)	5

Tutkinto-ohjelman kategoria: CD.

Information Technology, Bachelor of Engineering opetussuunnitelma noudattaa kieliä lukuun ottamatta lähes täysin suomenkielistä opetussuunnitelmaa tietotekniikasta.

Erikoistumiskoulutus

Ei erikoistumis- tai täydennyskoulutusta kyberturvallisuuteen liittyen.

20. Yrkeshögskolan Novia

Novia ei tarjoa tietojenkäsittelyyn tai tietoliikenteen alaan liittyviä tutkintoja AMK- tai YAMK-tasolla. Huomioitavaa on kuitenkin, että Novian tekniikan alan koulutuksen sähkö- ja automaatioalan tutkinto-ohjelma sisältää moduulin informaatioteknologiasta. Kyseisessä moduulissa ei kuitenkaan ole käsiteltävänä aiheena kyberturvallisuus.

21. Högskolan på Åland

Ahvenanmaan ammattikorkeakoulu tarjoaa tietotekniikan (Informationsteknik) tutkintoa poikkeuksellisesti 210 (Systemvetare) tai 240 (IT-Ingenjör) opintopisteen pituuksilla. Kumpaankaan opetussuunnitelmaan ei kuulunut kyberturvallisuuteen liittyviä opintojaksoja.

22. Poliisiammattikorkeakoulu

Ylempi ammattikorkeakoulu - EQF7

Tutkinto-ohjelman opetussuunnitelmassa ei esiinny kyberturvallisuutta.

Tutkinto-ohjelman kategoria: F.

Ammattikorkeakoulu - EQF6

Poliisi (AMK) tutkinnossa ilmentyi kyberturvallisuutta täysin vapaasti valittavissa opintojaksoissa.

Poliisi (AMK), kyberturvallisuuteen liittyvät opintojaksot

Course Code	Course Name	ECTS
-	E-FIRST-verkkokurssi -poliisina kybertoimintaympäristössä	1

Kyberturvallisuus ja kyberrikollisuus ovat sivutavoitteena opintojaksolla *Pakkokeinot ja tiedonhankinta* 3,5 op.

Tutkinto-ohjelman kategoria: D.

Erikoistumisopinnot

Poliisiammattikorkeakoulussa on menossa "Kyberrikostorjunnan erikoisopinnot (Kyber-EOP) -hanke, jossa "Tarkoituksena on kehittää ja lisätä Poliisiammattikorkea- koulun kyberkoulutustarjontaa, minkä myötä käynnistetään erikoistumisopintokokonaisuus kyberrikostorjunnan alalle syyslukukaudella 2022.". Kyseistä erikoistumisopintokokonaisuutta ei ole kuitenkaan julkaistu raportin kirjoittamisen vaiheessa.

Liite 3 Yliopistojen opetussuunnitelmat

1. Aalto yliopisto

Kyberalaan liittyvät kurssit

Security and Cloud Computing (Security)

Tietotekniikan laitos	**Master's Programme in Computer, Communication and Information Sciences**	**Security and Cloud Computing (Security)**
Kurssikoodi	**Kurssinimi**	**ECTS**
Pakolliset opinnot:		
CS-C3130	Information Security	5
CS-E4190	Cloud Software and Systems	5
CS-E4000	Seminar in Computer Science	5
Vapaasti valittavat pääaineopinnot:		
MS-E1687	Advanced Topics in Cryptography	5
CS-E4660	Advanced Topics in Software Systems	5
CS-E4640	Big Data Platforms	5
CS-E4340	Cryptography	5
CS-E5480	Digital Ethics	5
CS-E4670	Full Stack Development	5
CS-E4470	Informaatiomanipulaatio	5
ELEC-E7320	Internet Protocols	5
CS-E4160	Laboratory Works in Networking and Security	5
CS-E5370	Law in Digital Society	5
CS-C3240	Machine Learning	5
CS-E4650	Methods of Data Mining	5
CS-E4260	Multimedia Services in Internet	5
CS-E4300	Network Security	5
CS-E4350	Security Engineering	5
CS-E4003	Special Assignment on Computer Science	1-10
CS-E4002	Special Course in Computer Science	1-10
CS-E4330	Special Course in information Security	2-10
CS-C3170	Web Software Development	5

Kyberturvallisuuden kurssit muissa Aalto-yliopiston tutkinto-ohjelmissa

Kurssikoodi	**Kurssinimi**	**ECTS**	**Tutkinto-ohjelma ja kurssin pakollisuus** **P= Pakollinen** **V= Valinnainen**
MS-E2117	Riskianalyysi	5	Master's Programme in Advanced Energy Solutions, Sustainable Energy-Systems and Markets (V) Master's Programme in Mathematics and Operations Research (V)
CS-E5480	Digital Ethics	5	Bachelor's Programme in Science and Technology, Data Science (P) Teknistieteellinen kandidaattiohjelma, Tietotekniikka (V) Master's Programme in Computer Communication and Information Sciences, Software and Service Engineering (V)
ISM-E2003	Information Security Management	6	Master's Programme in Information and Service Management (V)
CS-C3130	Information Security	5	Teknistieteellinen kandidaattiohjelma, Tietotekniikka (V) Master's Programme in Computer, Communication and Information Sciences, Computer Science (V)
CS-E5370	Law in Digital Society	5	Teknistieteellinen kandidaattiohjelma, Tietotekniikka (V) Master's Programme in Computer Communication and Information Sciences, Software and Service Engineering (V)
ELEC-E7470	Cybersecurity P	5	Master's Programme in Computer, Communication and Information Sciences, Communication Engineering (V)
CS-E4960	Software Testing and Quality Assurance	5	Master's Programme in Computer, Communication and Information Sciences, Software and Service Engineering (V)
CS-E4340	Cryptography	5	Master's Programme in Computer, Communication and Information Sciences, Computer Science (V) Master's Programme in Mathematics and Operations Research, Applied Mathematics (V)

Kurssikoodi	Kurssinimi	ECTS	Tutkinto-ohjelma ja kurssin pakollisuus P= Pakollinen V= Valinnainen
MS-E1687	Advanced Topics in Cryptography	5	Master's Programme in Computer, Communication and Information Sciences, Computer Science (V) Master's Programme in Mathematics and Operations Research, Mathematics major (V) Master's Programme in Mathematics and Operations Research, Applied Mathematics (V)
CS-E4160	Laboratory Works in Networking and Security	5-10	Master's Programme in Computer, Communication and Information Sciences, Computer Science (V)
CS-E4350	Security Engineering	5	Master's Programme in Computer, Communication and Information Sciences, Human-Computer Interaction (V)

2. Helsingin yliopisto

Kyberalaan liittyvät kurssit

Tietojenkäsittelytieteen maisteriohjelman valinnaiset kyberturvallisuuden kurssit

Matemaattis-luonnontieteellinen tiedekunta	Tietojenkäsittelytieteen maisteriohjelma	Suuntaus: Tietoverkot
Kurssikoodi	**Kurssinimi**	**ECTS**
CSM13201	Mobile Systems Security	5
CSM13202	Cryptography in Networking	5
CSM13203	Software Security	5
CSM13204	Cyber Security II	5
CSM13280	Special Topics in Security	5
CSM132041	Cyber Security Base: Advanced Topics	3
CSM132042	Cyber Security Base: Course Project II	1
CSM132043	Cyber Security Base: Capture the Flag	1

Muut Helsingin yliopiston kyberturvallisuuden kurssit

Kurssikoodi	Kurssinimi	ECTS
-	Tietoturvan perusteet (MOOC-kurssi)	5
DATA20019	Trustworthy Machine Learning	5

3. Tampereen yliopisto

Kyberalaan liittyvät kurssit

Advanced Studies in Information Security (80 ECTS)

Informaatioteknologian ja viestinnän tiedekunta	**Master's Program in Information Technology** **Tietojenkäsittelyopin maisteriohjelma** **Master's Programme in Computer Science**	**Advanced Studies in Information Security (80 ECTS)**
Kurssikoodi	**Kurssinimi**	**ECTS**
Pakolliset opinnot:		
COMP.SEC.100	Cyber Security I: Fundamentals	5
COMP.SEC.110	Cyber Security II: Specialisation	5
Alla olevista kursseista valitaan 20–30 ECTS:		
COMP.SEC.300	Secure Programming	5
COMP.SEC.210	Cryptography Engineering II	5
TIJO.410	Information Security Management	5
COMP.CE.450	Internet of Things	5
COMP.SEC.200	Cryptography Engineering I	5
COMP.SEC.220	Security Protocols: Helping Alixe and Bob to Share Secrets	5
COMP.SEC.400	Digital Shadow: Privacy and Anonymity	5
Täydentäviä kursseja:		
COMM.NET.210	Networking Laboratory I	5
COMP.520	Special Topics on Computing	1-5
COMM.NET.200	Computer Networking I	5
COMM.NET.400	Computer Networking II	5
MATH.MA.450	Algebra	5
COMP.SE.620	Software Engineering Project 2	5

Automaatiotekniikan DI-ohjelma, automaation tietotekniikan kyberturvallisuuden kurssit

Tekniikan ja luonnontieteiden tiedekunta	**Automaatiotekniikan DI-ohjelma, automaation tietotekniikka**	**P= Pakollinen V= Valinnainen**
Kurssikoodi	**Kurssinimi**	**ECTS**
AUT 440	Automaation turvallisuus (P)	5
AUT 410	Tietoverkkopohjainen automaatio (P)	5
AUT 420	Automaation reaaliaikajärjestelmät (P)	5
COMP.SE.200	Ohjelmistojen testaus (V)	5
COMP.SEC.110	Cyber Security II: Specialisation (V)	5
COMP.SEC.100	Kyberturvallisuus I: perusteet (V)	5
COMM.NET.400	Computer Networking II (V)	5
BBT.MJS.144	Standards, Interoperability and Regulations in Health Informatics (V)	5

Safety Management and Engineering -pääaineen kyberturvallisuuteen linkittyvät kurssit

Johtamisen ja talouden tiedekunta	**Master's Programme in Security and Safety Management, Safety Management and Engineering**	**P= Pakollinen V=Valinnainen**
Kurssikoodi	**Kurssinimi**	**ECTS**
SAFER.310	Introduction to Security Studies, Governance and Safety Management (P)	3
SAFER.330	Current Trends in Security and Safety Management (P)	5
KONE.630	Systems RAMS Engineering (P)	5
SAFER.SME.310	Safety Engineering (P)	5
SAFER.SME.320	Enterprise HSEQ Management (P)	5
SAFER.SME.330	Safety and Risk Analysis (P)	5
KONE.640	System Reliability Centered Maintenance (V)	5
TIJO.410	Information Security Management (V)	5

Security Governance -pääaineen kyberturvallisuuteen linkittyvät kurssit

Johtamisen ja talouden tiedekunta	**Master's Programme in Security and Safety Management, Security Governance**	**P= Pakollinen V=Valinnainen**
Kurssikoodi	**Kurssinimi**	**ECTS**
SAFER.310	Introduction to Security Studies, Governance and Safety Management (P)	3
SAFER.330	Current Trends in Security and Safety Management (P)	5
SAFER.SG.310	Societal Security: Contemporary Challenges (P)	5
SAFER.SG.320	Governance Security (P)	5
SAFER.SG.340	Current Themes in International Security (P)	5
SAFER.SG.350	Crisis Management and Leadership (P)	5

Turvallisuustekniikan aineopintojen kyberturvallisuuteen linkittyvät kurssit

Opintosuuntaus: Turvallisuustekniikan aineopintoja valinnaisina opintoina **Taulukkoon listattu: opintosuuntaukseen sisältyvät kurssit, jotka linkittyvät kyber- ja tietoturvallisuuteen**			**P= Pakollinen** **V= Valinnainen**
Kurssikoodi	**Kurssinimi**	**ECTS**	**Tutkinto-ohjelmat, joissa opintosuuntauksen pystyy valitsemaan.**
TUTA.270	Riskienhallinta (P)	5	Teknis-taloudellinen koulutus (TkK), Tuotantotalous Tietojohtamisen DI-ohjelma, Tiedon ja osaamisen johtaminen Tietojohtamisen DI-ohjelma, Tietojärjestelmien johtaminen Tietojohtamisen DI-ohjelma, Liikenne, logistiikka ja informaatio Tuotantotalouden DI-ohjelma, International Sales and Sourcing Tuotantotalouden DI-ohjelma, Strateginen teknologia- ja projektijohtaminen Tuotantotalouden DI-ohjelma, Talouden ja liiketoiminnan hallinta Tuotantotalouden DI-ohjelma, Tuotannon ja toimitusketjujen hallinta
AUT.440	Automaation turvallisuus (V)	5	

Ohjelmistotuotannon syventävien opintojen kyberturvallisuuteen linkittyvät kurssit

Opintosuunta: Ohjelmistotuotannon syventävät opinnot valinnaisina opintoina **Taulukkoon listattu: opintosuuntaukseen sisältyvät kurssit, jotka linkittyvät kyber- ja tietoturvallisuuteen**			**P= Pakollinen** **V= Valinnainen**
Kurssikoodi	**Kurssinimi**	**ECTS**	**Tutkinto-ohjelmat, joissa opintosuuntauksen pystyy valitsemaan.**
COMP.CE.450	Internet of Things (V)	5	Tietojohtamisen DI-ohjelma, Tietojärjestelmien johtaminen Tietojohtamisen DI-ohjelma, Tiedon ja osaamisen johtaminen Tietojohtamisen DI-ohjelma, Liikenne, logistiikka ja informaatio Tuotantotalouden DI-ohjelma, Tuotannon ja toimitusketjujen hallinta Tuotantotalouden DI-ohjelma, Strateginen teknologia- ja projektijohtaminen Tuotantotalouden DI-ohjelma, Talouden ja liiketoiminnan hallinta Tuotantotalouden DI-ohjelma, International Sales and Sourcing
COMP.SE.200	Ohjelmistojen testaus (V)	5	
COMP.SEC.300	Secure Programming (V)	5	

Tietoliikennetekniikan aineopintojen kyberturvallisuuteen linkittyvät kurssit

Opintosuuntaus: Tietoliikennetekniikan aineopinnot valinnaisina opintoina **Taulukkoon listattu: opintosuuntaukseen sisältyvät kurssit, jotka linkittyvät kyber- ja tietoturvallisuuteen**			**P= Pakollinen** **V=Valinnainen**
Kurssikoodi	**Kurssinimi**	**ECTS**	**Tutkinto-ohjelmat, joissa opintosuuntauksen pystyy valitsemaan.**
COMP.SEC.100	Kyberturvallisuus I: perusteet (V)	5	Teknis-taloudellinen kandidaattiohjelma, Tietojohtaminen Teknis-taloudellinen kandidaattiohjelma, Tuotantotalous Tietojohtamisen DI-ohjelma, Tietojärjestelmien johtaminen Tietojohtamisen DI-ohjelma, Tiedon ja osaamisen johtaminen Tietojohtamisen DI-ohjelma, Liikenne, logistiikka ja informaatio Tuotantotalouden DI-ohjelma, Tuotannon ja toimitusketjujen hallinta Tuotantotalouden DI-ohjelma, Strateginen teknologia- ja projektijohtaminen Tuotantotalouden DI-ohjelma, Talouden ja liiketoiminnan hallinta Tuotantotalouden DI-ohjelma, International Sales and Sourcing
COMM.NET.400	Computer Networking II (V)	5	
COMP.SEC.220	Security Protocols: Helping Alice and Bob to Share Secrets (V)	5	
COMP.SEC.200	Cryptography Engineering I (V)	5	

Health Informatics opintojen kyberturvallisuuteen linkittyvät kurssit

Opintosuuntaus: Intermediate Studies in Health Informatics as Free Choice Studies **Taulukkoon listattu: opintosuuntaukseen sisältyvät kurssit, jotka linkittyvät kyber- ja tietoturvallisuuteen**		**P= Pakollinen** **V= Valinnainen**	
Kurssikoodi	**Kurssinimi**	**ECTS**	**Tutkinto-ohjelmat, joissa opintosuuntauksen pystyy valitsemaan.**
BBT.MJS.144	Standards, Interoperability and Regulations in Health Informatics (V)	5	Teknis-taloudellinen kandidaattiohjelma, Tietojohtaminen Teknis-taloudellinen kandidaattiohjelma, Tuotantotalous Tietojohtamisen DI-ohjelma, Tietojärjestelmien johtaminen Tietojohtamisen DI-ohjelma, Tiedon ja osaamisen johtaminen Tietojohtamisen DI-ohjelma, Liikenne, logistiikka ja informaatio

			Tuotantotalouden DI-ohjelma, Tuotannon ja toimitusketjujen hallinta Tuotantotalouden DI-ohjelma, Strateginen teknologia- ja projektijohtaminen Tuotantotalouden DI-ohjelma, Talouden ja liiketoiminnan hallinta Tuotantotalouden DI-ohjelma, International Sales and Sourcing

Lentokonetekniikan aineopintojen kyberturvallisuuteen linkittyvät kurssit

Opintosuuntaus: Lentokonetekniikan aineopintoja valinnaisina opintoina **Taulukkoon listattu: opintosuuntaukseen sisältyvät kurssit, jotka linkittyvät kyber- ja tietoturvallisuuteen**			**P= Pakollinen** **V= Valinnainen**
Kurssikoodi	**Kurssinimi**	**ECTS**	**Tutkinto-ohjelmat, joissa opintosuuntauksen pystyy valitsemaan.**
KONE.760	Aircraft Computer Systems and Situational Awareness (V)	5	Teknis-taloudellinen kandidaattiohjelma, Tuotantotalous Tietojohtamisen DI-ohjelma, Tietojärjestelmien johtaminen Tietojohtamisen DI-ohjelma, Tiedon ja osaamisen johtaminen Tietojohtamisen DI-ohjelma, Liikenne, logistiikka ja informaatio Tuotantotalouden DI-ohjelma, Tuotannon ja toimitusketjujen hallinta Tuotantotalouden DI-ohjelma, Strateginen teknologia- ja projektijohtaminen Tuotantotalouden DI-ohjelma, Talouden ja liiketoiminnan hallinta Tuotantotalouden DI-ohjelma, International Sales and Sourcing
KONE.630	Systems RAMS Engineering (V)	5	
KONE.640	Systems Reliability Centered Maintenance (V)	5	

Intermediate Studies in Communications and Networking suuntautumisen kyberturvallisuuteen linkittyvät kurssit

Opintosuuntaus: Intermediate Studies in Communications and Networking as Free Choice Studies **Taulukkoon listattu: opintosuuntaukseen sisältyvät kurssit, jotka linkittyvät kyber- ja tietoturvallisuuteen**			**P= Pakollinen** **V= Valinnainen**
Kurssikoodi	**Kurssinimi**	**ECTS**	**Tutkinto-ohjelmat, joissa opintosuuntauksen pystyy valitsemaan.**

COMP.SEC.220	Security Protocols: Helping Alice and Bob to Share Secrets (V)	5	Bachelor's Programme in Science and Engineering, Computing and Electrical Engineering Bachelor's Programme in Science and Engineering, Natural Sciences and Mathematics Teknis-taloudellinen koulutus (TkK), Tietojohtaminen Teknis-taloudellinen koulutus (TkK), Tuotantotalous Tietojohtamisen DI-ohjelma, Tiedon ja osaamisen johtaminen Tietojohtamisen DI-ohjelma, Tietojärjestelmien johtaminen Tietojohtamisen DI-ohjelma, Liikenne, logistiikka ja informaatio Tuotantotalouden DI-ohjelma, International Sales and Sourcing Tuotantotalouden DI-ohjelma, Strateginen teknologia- ja projektijohtaminen Tuotantotalouden DI-ohjelma, Talouden ja liiketoiminnan hallinta Tuotantotalouden DI-ohjelma, Tuotannon ja toimitusketjujen hallinta

4. Jyväskylän yliopisto

Kyberalaan liittyvät kurssit

Kyberturvallisuuden maisteriohjelma

Informaatioteknologian tiedekunta	**Kyberturvallisuuden maisteriohjelma**	
Kurssikoodi	**Kurssinimi**	**ECTS**
Kyberturvallisuuden tutkimusosaaminen, valitaan 40 ECTS		
TJTS5001	Tutkimusmenetelmät	5
KYBS5502	Pro Gradu -tutkielma	30
KYBS5503	Maturiteetti	0
KYBS5505	Pro Gradu -seminaari	5

Kyberturvallisuuden johtaminen, valitaan 15 ECTS		
TJTSM51	Information Security Management	5
TJTSM56	Advanced Course on Information Security Management	5
KYBS3020	Legal Aspects of Security and Privacy	3-5
Kyberturvallisuuden teknologian moduuli, valitaan 15 ECTS		
ITKST56	Järjestelmähaavoittuvuudet	5
TIES327	Tietoverkkoturvallisuus	3-7
KYBS1201	Kyberturvallisuusteknologiat	5
Valitaan joko sosiaalinen tai tekninen syventyminen (10 ECTS)		
Sosiaalinen syventyminen (10 ECTS)		
TJTS4903	Business Continuity and ICT Resilience	5
TJTS4902	Ethics and Information Technology	5
KYBS3040	Cyber Security Psychology	5
KYBS3041	Privacy in the light of Cybersecurity and Digitalization	5
KYBS3042	Trends in Cyber Security	5
Tekninen syventyminen (10 ECTS)		
ITKS6400	IoT/Embedded Security	5
ITKST55	Kyberhyökkäys ja sen torjunta	5
ITKA2050	Ohjelmistoturvallisuuden perusteet	5
ITKST53	Ohjelmistoturvallisuus	3
ITKST50	Secure Systems Design	5
KYBS3050	Koneoppimismenetelmiä kyberturvallisuuteen	5
KYBS7041	Anomalian havaitseminen	3-5
KYBS2001	Introductory Penetration Testing and Security Assessment	5
KYBS2002	Advanced Penetration Testing and Security Assessment	5
KYBS2003	Cybersecurity “continuous learning” with CTF (Capture the Game) gamification	5
KYBS2004	Authentication, passwords and applied cryptography	5
Viestintä- ja kieliopinnot (5 ECTS)		
Informaatioteknologian perusosaaminen (0-20 ECTS)		

Turvallisuuden ja strategisen analyysin maisteriohjelman kyberturvallisuuteen linkittyvät kurssit

Informaatioteknologian tiedekunta	**Turvallisuuden ja strategisen analyysin maisteriohjelma**	**P= Pakollinen V=Valinnainen**
Kurssikoodi	**Kurssinimi**	**ECTS**
TSAS7010	Turvallisuuden käsite ja sen muutos (P)	5
CRIA5001	Crises, Conflicts and Security (P)	5
TSAS7031	Tiedustelun perusteet (P)	5
TSAS7032	Tiedusteluanalyysi I (P)	5
TSAS7033	Tiedustelutuotteet ja tiedolla johtaminen (P)	5
TSAS7034	Tiedusteluanalyysi II (V)	5
TSAS7035	Monitieteinen tiedusteluprojekti (V)	5
TSAS7037	Tiedustelun erikoiskysymyksiä (V)	5
TSAS7011	Resilienssiajattelu ja yhteiskunnan turvallisuus (V)	3
TSAS7022	Hybridivaikuttaminen ja turvallisuus (V)	5
TSAS7041	Digitaalinen maailma ja turvallisuus (V)	5
TSAS7055	Turvallisuuspeli (V)	2
ITKP0001	Näkökulmia digitalisaatioon (V)	2
ITKP0007	Kansalaisen kyberturvallisuus (V)	2

Ohjelmisto- ja tietoliikennetekniikan pääaineen kyberturvallisuuden kurssit

Informaatioteknologian tiedekunta	**Tietotekniikan maisteriohjelma, Ohjelmisto- ja tietoliikennetekniikka**	**P= Pakollinen V= Valinnainen**
Kurssikoodi	**Kurssinimi**	**ECTS**
TIES546	Ohjelmistotestaus (P)	5
TIES327	Tietoverkkoturvallisuus (P)	3-7
ITKST53	Ohjelmistoturvallisuus (V)	3
ITKST56	Järjestelmähaavoittuvuudet (V)	5
ITKS6400	IoT/Embedded Security (V)	5
TIES5362	IoT-järjestelmän tietoturvallinen suunnittelu (V)	3

5. Turun yliopisto

Kyberalaan liittyvät kurssit

Master's Degree Programme in Information and Communication Technology, Cryptography

Teknillinen tiede-kunta	**Master's Degree Programme in Information and Communication Technology, Cryptography**	
Kurssikoodi	**Kurssinimi**	**ECTS**
Cryptography moduuli, valitaan 20 ECTS		
MATE5341	Foundations of Cryptography	5
MATE5396	Cryptography I	5
MATE5397	Cryptography II	5
MATE5344	Algebraic Structures in Cryptography	5
MATE5345	Selected Topics in Cryptography	5
Security of Networked Systems and Security Management (20 ECTS)		
Pakolliset opinnot (17 ECTS)		
DTEK8025	System and Application Security	5
TJS17	Enterprise Architecture	6
TJS13	Management of Information System Security	6
Valinnaiset opinnot (5 ECTS)		
DTEK8063	Firewall and IPS Technology	5
DTEK0039	Security Engineering	5
DTEK2029	Human Element in Information Security	5
Pro Gradu (30 ECTS)		
Pakolliset syventävät opinnot (10 ECTS)		
Temaattinen moduuli tai sivuaine (20–25 ECTS) - **Information Technology management** - **Discrete Mathematics** - **Data Science** - **Interactive Systems**		
Valinnaiset kurssit (15–20 ECTS)		
KIFF0003	Suomen intensiivinen alkeiskurssi I	5
DTEK2036	Industrial Seminar on Future Technologies	5

Master's Degree Programme in Information and Communication Technology, Cyber Security

Teknillinen tiedekunta	**Master's Degree Programme in Information and Communication Technology, Cyber Security**	
Kurssikoodi	**Kurssinimi**	**ECTS**
Security of Networked Systems, valitaan 20 ECTS		
DTEK8025	System and Application Security	5
DTEK8063	Firewall and IPS Technology	5
DTEK0039	Security Engineering	5

DTEK2029	Human Element in Information Security	5
Cryptography and Management, valitaan 22 ECTS		
DTEK8025	System and Application Security	5
MATE5396	Cryptography	5
TJS13	Management of Information System Security	6
TJS17	Enterprise Architecture	6
Yleiset opinnot: Information and Communication Technology (10 ECTS)		
DTEK0045	Internship	1-5
DTEK0088	Capstone	10
KIFF0003	Suomen intensiivinen alkeiskurssi I	5
Valinnaiset opinnot (15-20 ECTS)		
DTEK8060	Protocol Processing and Security	5
DTEK8096	Network Infrastructure Technologies and Security	5
DTEK8097	Secure Sensor Network Systems	5
DTEK2034	Communication Technologies and Security in IoT	5
DTEK8112	Special Course on Cyber Security	5
DTEK8102	Privacy and Security for Software Systems	5
DTEK0045	Internship	1-5
DTEK0088	Capstone	10
DTEK2036	Industrial Seminar on Future Technologies	5
DTEK1020	Diplomityöseminaari	0-5
Pro Gradu (30 ECTS)		
Temaattinen moduuli tai sivuaine (20-25 ECTS): • Information Technology Management • Innovation and Business Creation • Data Science • Game Development • Interactive Systems • Safety-critical and Autonomous Systems		

Tieto- ja viestintätekniikka, tietoliikenne- ja kyberturvallisuusteknologia (DI)

Teknillinen tiedekunta	**Tieto- ja viestintätekniikka, Tietoliikenne- ja kyberturvallisuusteknologia (DI)**	
Kurssikoodi	**Kurssinimi**	**ECTS**
Tietoliikenne- ja kyberturvallisuusteknologia, valitaan 20 ECTS		
DTEK8025	System and Application Security	5
DTEK8096	Network Infrastructure Technologies and Security	5
DTEK8097	Secure Sensor Network Systems	5
DTEK2034	Communication Technologies and Security in IoT	5

Tietoliikenne- ja kyberturvallisuusteknologian syventävät opinnot, valitaan 10 ECTS		
DTEK8063	Firewall and IPS Technology	5
DTEK0039	Security Engineering	5
Tutkinto-ohjelman yhteiset syventävät opinnot (15 ECTS)		
DTEK1020	Diplomityöseminaari	0–5
YH000201	Knowledge and Innovation Management	5
Valitaan yksi (10 ECTS)		
DTEK0088	Capstone	10
DTEK2037	Lean Platform Business Design	10
Diplomityö (30 ECTS)		
Temaattinen kokonaisuus tai sivuaine 20-25 ECTS: - **Cryptography and Management** - **Data-analytiikka** - **Konetekniikka** - **Teknologiajohtaminen** - **Työelämän ja henkilöstöasioiden opintokokonaisuus**		
Vapaavalintaiset opinnot (15-20 ECTS)		
DTEK8060	Protocol Processing and Security	5
DTEK2029	Human Element in Information Security	5
DTEK8112	Special Course on Cyber Security	5
DTEK8102	Privacy and Security for Software Systems	5
MATE5341	Foundations of Cryptography	5
MATE5396	Cryptography I	5
DTEK0045	Internship	1-5
DTEK2036	Industrial Seminar on Future Technologies	5

Turun kauppakorkeakoulun tietojärjestelmätieteen kyberturvallisuuden kurssit

Turun Kauppakorkeakoulu	**Tietojärjestelmätiede**	**P= Pakollinen** **V=Valinnainen**
Kurssikoodi	**Kurssinimi**	**ECTS**
TJS16	Information Technology and Ethics (V)	6
TJS13	Management of Information System Security (V)	6

6. Oulun yliopisto

Kyberalaan liittyvät kurssit

Oulun yliopiston tietotekniikan erikoiskurssit kyberturvallisuudesta

Tietotekniikan erikoiskurssit		
Kurssikoodi	**Kurssinimi**	**ECTS**
521252S	Tietotekniikan erikoiskurssi 4 – International Crisis Management	5
521253S	Tietotekniikan erikoiskurssi 5 – Tietoturvaprojekti	5
521254S	Tietotekniikan erikoiskurssi 6 – Kryptografiset järjestelmät ja niiden heikkoudet	5
521256S	Tietotekniikan erikoiskurssi 8 – Tekoälyn etiikka, yksityisyys ja lainsäädäntö	5
521257S	Tietotekniikan erikoiskurssi 9 – Fundamentals of Sensing, Tracking and Autonomy	5
521244S	Tietotekniikan erikoiskurssi 12 – Modern Cryptography	5
521246S	Tietotekniikan erikoiskurssi 13 – Empirical Research in Computer Security	5

Kyberturvallisuuden kurssit muissa Oulun yliopiston tutkinto-ohjelmissa

Kurssikoodi	**Kurssinimi**	**ECTS**	**Tutkinto-ohjelma ja kurssin pakollisuus** **P= Pakollinen** **V= Valinnainen**
811168P	Tietoturva	5	Tietotekniikka (DI) (V) Informaatiotutkimus (HuK) (V) Computer Science and Engineering, DP in Digitalization, Computing and Electronics (TkK) (P) Information Processing Science, Degree Programme in Digitalisation, Computing and Electronics (TkK) (P) Tietojenkäsittelytieteet (LuK) (P) Tietotekniikka (TkK) (V) Wireless Communications Engineering,M.SC. (TECH), RAN (V) Wireless Communications Engineering,M.SC. (TECH), RF (V)
694679A	Informaatio-lainsäädäntö ja -etiikka	5	Informaatiotutkimus (HuK) (P)
555377S	Risk Management	5	Tuotantotalous (DI), Tuotehallinta (V) Tuotantotalous (DI), Projektijohtaminen (V) Tuotantotalous (DI), Tuotannon ja toimitusverkkojen johtaminen (V)

811306A	Ohjelmistojen laatu ja testaus	5	Tietojenkäsittelytieteet (LuK) (P)
811602S	Advanced Software Quality and Security	5	Software, Systems and Development in the Global Environment GS3D (MSc), Information systems (P) Software, Systems and Development in the Global Environment GS3D (MSc), Software Engineering (P) Tietojenkäsittelytiede (FM), Information Systems (P) Tietojenkäsittelytiede (FM), Software Engineering (P) European Masters in Software Engineering, EMSE (P)
	ICT and Behaviour Change	5	Tietotekniikka (DI) (V) Tietojenkäsittelytiede (FM) (V)

7. Itä-Suomen yliopisto

Kyberalaan liittyvät kurssit

Itä-Suomen yliopiston kyberturvallisuuden kurssit

Luonnontieteiden ja metsätieteiden tiedekunta	**Tietojenkäsittelytieteen kandidaatti (LuK)**	**P= Pakollinen** **V= Valinnainen**
Kurssinimi		**ECTS**
Johdatus tietoturvaan (P)		5

8. Lappeenrannan teknillinen yliopisto

Kyberalaan liittyvät kurssit

Lappeenrannan teknillisen yliopiston kyberturvallisuuden kurssit

Lappeenrannan teknillinen yliopisto		
Kurssikoodi	**Kurssinimi**	**ECTS**
CT60A5521	Ohjelmistojärjestelmän tietoturva	3–4
CT60A4160	Ohjelmistotestauksen periaatteet	3
CT70A20000	Requirements Engineering	6
CT60A5500	Quality Assurance in Software Development	6

9. Åbo Akademi

Kyberalaan liittyvät kurssit

Safety-Critical and Autonomous Systems

Temaattinen moduuli: Safety-Critical and Autonomous Systems, 20 ECTS			
Kurssikoodi	**Kurssinimi**	**ECTS**	**Tutkinto-ohjelmat, joissa moduuli on valinnaisena tarjolla**
IT00CE01	Real-Time Systems	5	Double Degree NISS: Nordic Master Programme in Intelligent Software Systems, Master of Science (Technology) Double Degree: INSA Rennes, Master of Science (Technology) Master's Degree Programme in Information Technology: Computer Engineering in Åbo, Master of Science (Technology) MDP in Information Technology: Computer Science, Master of Science
IT00CE02	Software Safety	5	
IT00CE04	Reliable Distributed Systems	5	
IT00CE05	Autonomic Software and Systems	5	
IT00CD99	Multidimensional Sensing Techniques	5	
IT00CD86	Security Engineering (UTU)	5	

Kyberturvallisuuden kurssit muissa Åbo Akademin tutkinto-ohjelmissa

Kurssikoodi	**Kurssinimi**	**ECTS**	**Tutkinto-ohjelmat ja kurssin pakollisuus** **P= Pakollinen** **V= Valinnainen**
IT00CE12	Software Testing	5	Double Degree NISS: Nordic Master Programme in Intelligent Software Systems, Master of Science (Technology) (P) Master's Degree Programme in Information Technology: Computer Engineering in Åbo, Master of Science (Technology) (P) Double Degree ESIGELEC: Embedded Systems, Master of Science (Technology) (V)
IT00CE13	Software Quality	5	Double Degree NISS: Nordic Master Programme in Intelligent Software Systems, Master of Science (Technology) (P)

			Double Degree EDISS: Engineering of Data-intensive Intelligent Software Systems, Master of Science (Technology) (V) Master's Degree Programme in Information Technology: Computer Engineering in Åbo, Master of Science (Technology) (P)
IT00CD86	Security Engineering (UTU)	5	Datateknit, teknologie kandidatexamen (P)
IT00CE02	Software Safety	5	Double Degree EDISS: Engineering of Data-intensive Intelligent Software Systems, Master of Science (Technology) (V)

10. Vaasan yliopisto

Kyberalaan liittyvät kurssit

Kyberturvallisuuden kurssit Vaasan yliopiston tutkinto-ohjelmissa

Kurssikoodi	**Kurssinimi**	**ECTS**	**Tutkinto-ohjelma ja kurssin pakollisuus** **P= Pakollinen** **V= Valinnainen**
ICAT1090	Järjestelmien turvallisuus	3	Automaatio ja tietotekniikka (TkK) (P) Sähkö- ja energiatekniikka (TkK) (P) Tuotantotalous (TkK) (P)
TECH1020	Engineering Ethics, Norms and Regulations	1	Automaatio ja tietotekniikka (TkK) (P) Energia- ja informaatiotekniikka, automaatio ja tietotekniikan opintosuunta (DI) (P) Smart Energy, Master of Science (P) Sähkö- ja energiatekniikka (TkK) (P) Energia- ja informaatiotekniikka, energiatekniikan opintosuunta (DI) (P) Tuotantotalous (TkK) (P) Industrial Systems Analytics, Master of Science (P)
ICATC2040	Software Testing	5	Automaatio ja tietotekniikka (TkK) (V) Energia- ja informaatiotekniikka, automaatio ja tietotekniikan opintosuunta (DI) (V) Tietojärjestelmätiede (KTK) (V)

MATH2070	Salaustekniikan algebralliset piirteet	5	Energia- ja informaatiotekniikka, automaatio ja tietotekniikan opintosuunta (DI) (V)
ICAT3240	Security of Embebbed and Distributed Systems	5	Energia- ja informaatiotekniikka, automaatio ja tietotekniikan opintosuunta (DI) (P) Smart Energy, Master of Science (V)
TITE3370	Management of Cyber Security	5	Smart Energy, Master of Science (V) Tietojärjestelmätiede (KTM) (V) Tekninen viestintä (KTM) (V)
TITE3410	Computers, Ethics and Society	5	Tekninen viestintä (KTM) (V) Tietojärjestelmätiede (KTM) (V)

11. Lapin yliopisto

Kyberalaan liittyvät kurssit

Lapin yliopiston kyberturvallisuuteen linkittyvät kurssit

Tutkinto	**Kurssinimi**	**ECTS**
Oikeusnotaari	Hallinto-oikeus ja oikeusinformatiikka	10
Oikeustieteen maisteri	Oikeusinformatiikka – Ajankohtaista viestintäoikeutta ja informaatio-oikeutta	5
Oikeustieteen maisteri	Oikeusinformatiikka	10

Liite 4 MPK:n kyberturvallisuuden koulutusohjelma

1. Kyberturvallisuuden perusosaamisen koulutuskokonaisuus

Kansalaisen kyberturvallisuuskurssi

Kurssi toteutetaan verkkokurssina yhteistyössä Jyväskylän yliopiston kanssa. Kurssin materiaali on vapaasti kaikkien saatavilla verkossa. Kurssisuoritus perustuu oppijan tunnistamisen mahdollistavassa oppimisympäristössä suoritettavaan tenttiin, jonka hyväksytty suoritus vastaa kurssin suorittamista ja josta oppijalle annetaan suoritustodistus. Jyväskylän yliopisto myöntää kurssin hyväksytysti suorittaneille näiden niin halutessa yliopistollisen opintosuorituksen erillisellä opinto-oikeudella, josta peritään maksu siten, kun siitä säädetään valtioneuvoston asetuksessa yliopistojen toiminnassa perittävistä maksuista (1082/2009).

Kurssin osaamistavoitteet: Kurssin suoritettuaan osallistuja tuntee kansalaisen kyberturvallisuuden perusteet ja osaa tärkeimmät tekniset ja muut suojaustoimenpiteet niin kotona kuin mobiilissakin yksityishenkilön arjen näkökulmasta kuin muuallakin kuten kotona ja koulussa. Kurssin sisältö:

1. Digitalisaatio,
2. Kaiken taustalla on internet ja sen tekniikka,
3. Kyberturvallisuus kuuluu kaikille,
4. Kyberturvallisuus ja sen tasot,
5. Kokonaisturvallisuuden malli,
6. Sosiaalinen media, yksityisyys ja OSINT,
7. Digitaalinen osana kriisejä ja sotia,
8. Kyberturvallisuuden tuottaminen Suomessa

Kurssin oli suorittanut maaliskuun 2022 loppuun mennessä 703 henkilöä. Tässä vaiheessa ilmoittautuneita oli 2060.

Taistelijan kyberturvallisuuskurssi

Taistelijan kyberturvallisuuskurssi toteutetaan verkkokurssina PVMOODLE-oppimisympäristössä. Kurssin osaamistavoitteet: Kurssin suoritettuaan osallistuja: tuntee 1) operaatioturvallisuutta vaarantavat riskitekijät kyberturvallisuuden kontekstissa 2) julkisen infrastruktuurin (erityisesti Internetin) rakenteelliset perusheikkoudet, osaa: 1) Toimia kyberympäristössä operaatioturvallisuutta vaarantamatta 2) Viestivälineiden (ml. arjen välineet) vaatimukset ja niiden käytön. 3) Signaalitiedustelulta suojautumisen. 4) Sosiaalisen median operaatioturvallisen käytön sekä 5) Opastaa myös muita taistelijoita operaatioturvalliseen toimintaan

Kurssin sisältö: Internet, sen historia ja teknologia. Kyberpuolustus ja kyberoperaatiot. Yksilön toiminnan arjen välineet ja niiden kyberturvallisuus. Signaalitiedustelun perusteet ja suojautuminen.

Kyberturvallisuuden peruskurssi

Kurssin osaamistavoitteet: Kurssin tavoitteena on käydä kyberturvallisuutta opettamalla infranhallinnan ja ylläpidon parhaita käytäntöjä ja miten välttää yleisimpiä sudenkuoppia Kurssin suoritettuaan kurssilainen osaa tietoturvan perusteita sekä tietää käytännön toimen- piteitä näiden toteuttamiseksi. Kurssi antaa työkaluja syventävälle peruskurssille tai jatkokurssille etenemistä varten osaamisen tason mukaan. Kurssi antaa työkaluja syventävälle peruskurssille tai jatkokurssille etenemistä varten osaamisen tason mukaan.

Sisältö: 1) Tietoturva sekä kyberturvallisuus, 2) Salasanojen käyttö, 3) Kyberuhat, 4) Oma turvallinen toiminta, 5) Viranomaisten toiminta, 6) Langattomien verkkojen toiminta. Rastikoulutukset: 1) Salasanapaja, 2) Verkon liikenteen seuranta ja sen demot, 3) Oman koneen ”koventaminen”, 4) Kotireitittimen konfigurointi.

Kyberturvallisuuden syventävä peruskurssi

Kurssin osaamistavoitteet: Kurssin tavoitteena on syventää peruskurssin tietoja ja taitoja erityisesti painottamalla käytännön harjoituksia. Kurssin käytyään kurssilainen osaa soveltaa käytännössä tietoturvallisuutta lisääviä toimenpiteitä henkilökohtaisessa tietojenkäsittelyssä kuten omassa koneessaan, mobiililaitteissa, kotiverkossa ja siihen liitetyissä laitteissa. Kurssi antaa paremmat edellytykset jatkokurssille etenemiseen.

Kurssin sisältö: Kurssilla harjoitellaan henkilökohtaisten tietokoneiden suojaamista. Kurssilla voidaan ottaa mukaan esim. mobiililaitteiden koventamiset. Kurssin sisältö koostuu pääasiassa Kyberturvallisuuden peruskurssin aiheista siten, että painopiste on käytännön harjoituksilla.

Rastikoulutukset: 1) Mobiililaitteen koventaminen, 2) Kotiverkon segmentointi, 3) Palomuurien ominaisuuksien läpikäyminen. Näiden kurssien käyminen luo edellytykset koulutusohjelman muihin osioihin osallistumiseen.

Laaja-alainen vaikuttaminen ja turvallisuus

Kurssin osaamistavoitteet: Kurssin aikana käsitellään erityisesti kyber- ja informaatiovaikuttamista sekä sitä, miten ne liittyvät muihin vaikuttamisen muotoihin muodostaen laaja-alaisena vaikuttamisena tunnetun kokonaisuuden.

Kurssin sisältö: 1) Turvallisuus, sen muutos ja kokonaisturvallisuusajattelu, 2) Laaja-alaisen vaikuttamisen käsite, 3) Laaja-alaisen vaikuttamisen vastainen toiminta, 4) Huoltovarmuus 5) Laaja-alainen vaikuttaminen ja tiedustelu.

2. Kyberturvallisuuden jatko-osaamisen koulutuskokonaisuus

Kyberturvallisuuden jatkokurssien kokonaisuus on suunnattu ensisijaisesti tietoturvasta ja kyberturvallisuudesta kiinnostuneille reserviläisille. Jatko-osaamisen kokonaisuus on MPK:ssa jatkokurssitason koulutusta ja sen kurssit ovat pääasiassa SOTVA-kursseja.

Kyberturvallisuuden jatkokurssi

Kyberturvallisuuden jatkokurssin sisältö on lähtökohtaisesti tekninen.

Kurssin osaamistavoitteet: Kurssin tavoitteena on käydä kyberturvallisuutta opettamalla infranhallinnan ja ylläpidon parhaita käytäntöjä ja miten välttää yleisimpiä sudenkuoppia Kurssin suoritettuaan kurssilainen osaa tietoturvan perusteita sekä tietää käytännön toimenpiteitä näiden toteuttamiseksi. Kurssi antaa perusteet syventävälle jatkokurssille.

Kurssin sisältö: Kurssilla harjoitellaan tietoverkkojen tutkimista ja poikkeamien havainnointia. Kurssilla opetetaan kyberturvallisuuteen liittyvää lainsäädäntöä sekä operaatioturvallisuutta.

Kyberturvallisuuden syventävät jatkokurssit

Kurssien osaamistavoitteena on syventää yhden tai useamman sovelluksen osaamista (esim. NIDS, Moloch, HIVE, jne.). Kurssin jälkeen kurssilainen tuntee suhteellisen syvällisesti aiheina olleiden sovellustyökalujen toimintaa.

Kyberturvallisuuden eriytyvät jatkokurssit

Osaamistavoitteena on syventää osaamista joillain kyberturvallisuuden erityisalueilla kuten esimerkiksi N/SOC-toiminnoissa tai forensiikassa. Esitietovaatimuksena on kyberturvallisuuden jatkokurssien suorittaminen.

3. Kyberturvallisuusosaamisen soveltamisen koulutuskokonaisuus

Paikallisia, soveltavia ja pienimuotoisia kyberturvallisuuden harjoituksia, joissa on Puolustusvoimien kanssa sovittu tavoite, voidaan järjestää SOTVA-koulutuksena. SOTVA-ERIYTYVÄ koulutus on kyberturvallisuuden syventävää, jatko- ja erikoistason koulutusta. Koulutus toteutetaan tiiviissä yhteistyössä Puolustusvoimien kanssa. Kurssien kouluttajat ovat joko PV:n henkilöstöä tai MPK:n kouluttajia, joilla on PV:n kyberturvallisuuden kouluttaja -sertifikaatti. Tavoitteena on perehtyä johonkin kyber- tai informaatioturvallisuuden aiheen erityiskysymykseen. Koulutus sisältää myös mm. kyberturvallisuuden soveltamiseen painottuvat erikoiskurssit (harjoitukset, sotapelit).

Kyberturvallisuuden harjoitus

Rajoitetulle joukolle tarkoitettu harjoitus, jonka tavoitteet on sovittu Puolustusvoimien kanssa.

Kybermaailman sotapeli

Sotapelin tarkoitus on tarjota koulutusohjelmiin osallistuneille harjoitus, jossa voidaan soveltaa aikaisemmilla kursseilla opittuja tietoja ja taitoja.

Laaja-alaisen vaikuttamisen harjoitus

Harjoituksen tarkoitus on tarjota laaja-alaisen vaikuttamisen kursseille osallistuneille harjoitus, jossa voidaan soveltaa aikaisemmilla kursseilla opittuja tietoja ja taitoja.

4. Muu koulutus- ja harjoitustoiminta

Muu koulutus- ja harjoitustoiminta sisältää erilaisia tiedotus- ja valmistustoimintaan liittyviä (TIVA) seminaareja ja mm. erilaisiin Puolustusvoimien johtamien kansallisiin tai kansainvälisiin kyberharjoituksiin osallistumista.

Kyberturvallisuuden seminaari

Osana kyberturvallisuuden koulutusohjelmaa voidaan pitää myös erillisiä yhden päivän tilaisuuksia, jotka ovat nimetty Kyberturvallisuuden-seminaariksi. Seminaari voi käsitellä jotain tiettyä aihetta ja se voidaan kohdentaa tietylle joukolle. Seminaari voi olla myös yhden päivän tilaisuus, jossa annetaan kansalaisille tietoa siitä, mitä kyberturvallisuus tarkoittaa.

Informaatioturvallisuuden seminaari

Informaatioturvallisuuden seminaari on päivän mittainen koulutus, jossa luokkaopetuksena käydään läpi jonkin teeman kautta informaatioturvallisuutta. Teemojen kautta kurssille osallistuva osaa tulkita mediasta saamaansa tietoa ja ymmärtää minkälaisia keinoja ja menetelmiä voidaan käyttää sekä tunnistaa, kun itse saattaa olla informaatiovaikuttamisen kohteena.

Laaja-alaisen vaikuttamisen seminaari

Osana laaja-alaisen vaikuttamisen koulutuksen kokonaisuutta yhden päivän seminaari käsittelee laaja-alaista vaikuttamista ja siltä suojautumista sekä torjuntaa, poikkeusoloihin varautumista sekä informaatiovaikuttamista ja kriisiviestintää.

Kansalliset ja kansainväliset kyberturvallisuuden harjoitukset

Osallistujat valitaan näihin aikaisempien koulutuksiin osallistumisten perusteella. Varsinkin kansainvälisten harjoitusten perustamiset tapahtuvat pääasiassa Puolustusvoimien aloitteesta.

TIETO-harjoitus on joka toinen vuosi pidettävä kansallinen yritysten ja viranomaisten yhteistoimintaharjoitus laajojen kyberhäiriöiden varalta. Harjoituskokonaisuudessa harjoitellaan kulloinkin harjoitettavien yhteiskunnan huoltovarmuuden kannalta merkittävien toimialojen yritysten jatkuvuudenhallintaa, varautumista ja kriisi- viestintää kyberhäiriötilanteissa.

Locked Shields on kansainvälinen kyberturvallisuusharjoitus, jossa mukana on kymmeniä eri maita. Harjoituksessa käytetään vuosittain huipputeknologiaa ja tehdään toiminnallisia harjoitteita. MPK osallistuu harjoitukseen yhteistyössä Puolustusvoimien kanssa.

Cyber Coalition NATO:n kumppanivaltioille tarkoitettu kyberpuolustusharjoitus, jonka tarkoituksena on vahvistaa kansainvälistä ja kansallista yhteistyötä sekä yhteistoimintaa erilaisissa kyberhäiriötilanteissa. MPK on tarkoitus osallistua harjoitukseen yhteistyössä Puolustusvoimien kanssa. MPK osallistuu myös muihin alan harjoituksiin mahdollisuuksien mukaan.

5. Kouluttajakoulutus

Lähtökohtaisesti kouluttajien perusosaaminen tulee MPK:n yleisen kouluttajakoulutuksen kautta. Tämän lisäksi kyberturvallisuuden kouluttajaosaamista kehitetään kouluttajakoulutuksessa, jossa substanssi on ensisijainen koulutuskohde.

Kouluttajakoulutus jaetaan kolmeen kategoriaan:

1. MPK:n kyberturvallisuuden kouluttajakoulutus
2. Eriytyvä kouluttajakoulutus
3. Erikoiskouluttajakoulutus

Kouluttajakoulutuksen aiheina ovat muun muassa: 1) Kyberturvallisuuden koulutuksen rakenne ja prosessit, 2) Käytettävissä olevat koulutusympäristöt, 3) Kaluston ja järjestelmien hyödyntäminen, b) Kyberturvallisuuden virtuaalikoulutusympäristön hyödyntäminen, 4) Kyberturvallisuuden verkkokoulutus

Informaatioteknologian tiedekunnan julkaisuja
No. 93/2022

ISBN 978-951-39-9336-8 (verkkoj.)
ISSN 2323-5004

JYVÄSKYLÄN YLIOPISTO