

Jukka Niemelä

**KYBERTURVALLISUUSALAN TYÖVOIMAN
KYSYNTÄ, SAATAVUUS JA KEHITTÄMINEN
VASTAAMAAN TYÖVOIMAN TARVETTA
SUOMESSA**

PRO GRADU



JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

TIIVISTELMÄ

Niemelä, Jukka

Kyberturvallisuusalan työvoiman kysyntä, saatavuus ja kehittäminen vastamaan työvoiman tarvetta Suomessa

Jyväskylä: Jyväskylän yliopisto, 2019, 62 s.

Kyberturvallisuus, pro gradu -tutkielma

Ohjaaja(t): Lehto, Martti

Tutkimuksessa selvitetään kyberalan työvoiman saatavuutta rekrytoivien organisaatioiden näkökulmasta. Tutkimus käy läpi työnantajien kokemuksen soveltuvan työvoiman tarjonnasta, työvoiman tarpeesta, osaamistasosta ja koulutuksen vastaavuudesta työmarkkinoiden tarpeisiin. Kyberalan työntekijän ominaisuuksista luodaan työntekijäprofiili sekä kartoitetaan kyberalan koulutustarjontaa Suomessa.

Teemahaastatteluna suoritettua laadullista tapaustutkimusta täydennetään kerätyllä kirjallisella aineistolla työpaikkamääristä, kompetensseista ja kyberalan oppilaitosten tarjonnasta. Tulosten perusteella kyberalan työvoiman saatavuus on heikolla tasolla. Rekrytoivat organisaatiot ovat joutuneet laskemaan odotuksia hakijoiden osaamistasosta, että ovat saaneet avoimet tehtävät edes pääosin täytettyä. Koulutusmäärät sekä opetuksen laatu täyttävät työnantajien vaatimukset vain melko hyvin.

Osaamisen tasoon ja laajuuteen on saatava merkittävää parannusta, jotta se täyttää työmarkkinoiden tarpeet. Kyberalan merkitys maailmassa kasvaa jatkuvasti. Heikolla työvoiman saatavuudella on kansallisesti merkitystä talouden ja turvallisuuden sektoreilla, jos osaamisen merkittävä vaje jatkuu pitkään.

Asiasanat: Kyberturvallisuus, Kyberala, Työvoima, Koulutus, Rekrytointi, Työntekijän profiili, Kompetenssi

ABSTRACT

Niemelä, Jukka

Demand, availability and development of the cyber security workforce respond to the need for labor in Finland

Jyväskylä: University of Jyväskylä, 2019, 62 pp.

Cyber Security, Master's Thesis

Supervisor(s): Lehto, Martti

This study explores the availability of cyber labor from recruiting organizations perspective. The study goes through the employers' experiences about availability of suitable workforce, how much workforce is needed, skill levels, and suitability of education to satisfy labor markets in cyber field. The cyber professional employee profile is gathered from required skills and qualities of recruiters. Current education of cyber studies in Finland is evaluated.

A qualitative case study conducted as a theme interview will be supplemented with collected written material on available jobs, competencies and the supply of cyber educational institutions. Based on the results, the availability of cyber labor is poor. Recruiting organizations have had to lower their expectations of applicants' skills, so that they have even partly filled their open jobs. Educational volumes and the quality of teaching meet employers' requirements only quite well.

Significant improvement in the level and scope of knowledge is required to meet the needs of the labor market. The importance of cyberspace in the world is constantly increasing. Weak labor availability has national importance in the economic and security sectors if the significant shortage of skills continues.

Keywords: Cybersecurity, Cyber field, Workforce, Labor, Education, Recruitment, Employee profile, Competence

KUVIOT

KUVIO 1 IT-alan osaamisvaje.....	21
KUVIO 2 The Iceberg Model of Competence	23
KUVIO 3 Havainnekuva työpaikkailmoitusten perusteella tehtävästä jaottelusta	33
KUVIO 4 Havainnekuva haastattelujen analysoinnista teemoittamalla.....	34

TAULUKOT

TAULUKKO 1 NCWF työtehtävät	25
TAULUKKO 2 Haastattelujen tulosten tiivistelmä tutkimuskysymysten osalta	43

SISÄLLYS

TIIVISTELMÄ	2
ABSTRACT	3
KUVIOT	4
TAULUKOT	4
SISÄLLYS.....	5
1 JOHDANTO.....	7
1.1 Tutkimuksen tarkoitus.....	9
1.2 Tutkimusongelma.....	10
1.3 Tutkimuksen rakenne	10
2 KIRJALLISUUS.....	12
2.1 Kyberalan koulutus	12
2.1.1 Kyberalan koulutus Suomessa	13
2.1.2 Kyberalan opinnot yliopistoissa.....	13
2.1.3 Kyberalan opinnot ammattikorkeakouluissa.....	14
2.1.4 Kyberalan opinnot avoimissa yliopistoissa ja ammattikorkeakouluissa	15
2.1.5 Muu kyberalan koulutus.....	15
2.1.6 Kyberalan koulutustarve.....	16
2.2 Työvoima ja rekrytointi	17
2.2.1 Työvoiman määritelmä	17
2.2.2 Kyberalan työvoiman määritelmä	18
2.2.3 Työvoiman rekrytointi	19
2.2.4 Kyberalan työvoiman tarve	20
2.3 Kyberalan työn jaottelu ja kompetenssit	22
2.3.1 Kompetenssin määritelmä	22
2.3.2 Kyberalan työtehtävien jaottelu ja työntekijöiden profilointi....	24
3 TUTKIMUSMENETELMÄT.....	27
3.1 Tutkimuksen tavoitteet ja rajaus	28
3.2 Tutkimusmenetelmien kuvaus	28
3.3 Tutkimuksen kohdejoukko	29
3.4 Aineiston kerääminen ja analysointi.....	30
4 TULOKSET.....	35
4.1 Työpaikkailmoitusten seuranta	35

4.2	Rekrytoijien haastattelut.....	37
4.3	Korkeakouluopetuksen selvitys ja kysely	44
4.3.1	Koulutuksen tulevaisuuden näkymät.....	45
5	JOHTOPÄÄTÖKSET	47
6	POHDINTA	50
	LÄHTEET	52
	LIITE 1 TUTKIMUSHAASTATTELUN KYSYMYKSET.....	63
	LIITE 2 TUTKIMUSHAASTATTELUUN OSALLISTUNEET ORGANISAATIOT65	
	LIITE 3 OPPILAITOSKYSELYN KYSYMYKSET	67

1 JOHDANTO

Tiedon ja tiedonsiirron turvallisuus nousee entistä suurempaan merkitykseen, mitä enemmän yhteiskunta tukeutuu sähköisiin palveluihin. Kriittinen infrastruktuuri, talous, terveydenhoito ja muut välttämättömät palvelut ovat tietoverkkojen ja -järjestelmien varassa. Samoin jokaisen ihmisen henkilökohtainen tieto ja toiminta ovat siirtyneet tietoverkkoihin. Tämän kokonaisuuden, kyber turvallisuuden, toteuttamiseen tarvitaan osaavaa työvoimaa.

Maailman talous on nousussa ja työvoiman kysyntä on kasvanut Suomessa sen myötä merkittävästi viime aikoina. Suomessa eletään samaan aikaan korkean työttömyyden ja työvoimapulan ajassa (Nordea, 2018). Vaikka työttömiä työnhakijoita on runsaasti, työvoiman kysyntä ja tarjonta eivät kohtaa. Tärkeimpinä syinä ovat työvoiman liikkuvuuden puute, osaamistaso sekä sosiaaliturvan rakenteen muodostama kannustinloukku, missä työtä ei taloudellisesti kannata ottaa vastaan. (Sinko & Vihriälä, 2007). Rekrytointiongelmista kärsivät useat matalapalkka-alat, mutta myös korkeasti palkatuilla aloilla on vaikea löytää soveltuvaa työvoimaa. Kyberala on yksi soveltuvan työvoiman saatavuuden kanssa kamppailevista aloista (ISACA, 2018). Kyberalan rekrytointiongelman syitä on useita, osa maailman laajuisia, osa Suomeen tällä hetkellä kohdistuvia. Suomessa kyberalan työvoiman saatavuuteen vaikuttavat merkittävästi alan yleinen laajeneminen, koulutuksen riittämättömyys, uudet lait ja asetukset sekä osin Suomen maantieteellinen sijainti ja kieli.

Kyberala on suhteellisen uusi ja sitä ei ole määritelty tarkasti. Ala on laaja ja saanut uusia muotoja perinteisen tieto- ja tietoliikenneturvallisuuden lisäksi. Koska muutos on ollut nopea, ei alan koulutusta ja siten työvoimaa ole ollut saatavilla kaikilta osin riittävästi. Koko tietoteknisen alan koulutusmäärä on kohtuullisella tasolla, mutta kyberalan osalta määrä on riittämätön kattamaan tämän hetken tarvetta työmarkkinoilla. Erityisesti uusien teknologioiden osaaminen, tiedusteluosaaminen, kryptografia sekä koko kyberalan kentän laaja-alainen ymmärrys ja johtaminen ovat nousseet esille osaajapulasta keskusteltaessa (Tiihonen, 2018; Luukka, 2018). Koulutus on pyrkinyt uudistumaan ja laajentumaan vaadittujen muutosten mukana, mutta muutoksen nopeus ja resurssit eivät ole luoneet osaajakenttää, joka täyttäisi tyhjiön. Tutkimuksessa selvite-

tään kyberalan koulutusta Suomessa sekä yleisen kybertaidon lähteitä korkeakoulutuksen lisäksi.

Laajamittainen digitalisaatio Suomessa kehittyi jatkuvasti. Se luo uusia muotoja ja kasvaa uusille aloille. Valtion digihankkeita ovat mm. sähköinen ilmoitus- ja luvanhakupalvelu sekä tulorekisteri (Valtiovarainministeriö, 2018). Yrityspuolella palvelujen kirjo on laaja. Esimerkkinä toimivat mm. pankkien kehittyneet mobiilipalvelut, rahansiirrot ja uudet sähköiset maksupalvelut (Nordea, 2018; Danske Bank, 2018). Näiden erittäin sensitiivisten palveluiden kehitys vaatii äärimmäistä turvallisuutta kyberympäristössä ja siten korkean luokan osaamista niiden toteuttamisessa.

Suomeen on valmisteltu uutta tiedustelulainsäädäntöä vuodesta 2015 ja se astui voimaan 11.3.2019 (Eduskunta, 2019). Lakien tavoitteena on suojautua kansalliseen turvallisuuteen kohdistuvilta uhkilta. Tiedustelulaki antaa viranomaisille valtuuden tietoliikennetiedustelulla seurata Suomeen tulevaa ja Suomesta lähtevää viestiliikennettä sekä ulkomaan tietojärjestelmätiedustelulla tietojen hankkimiseen tietojärjestelmistä tietoteknisin menetelmin. (Puolustusministeriö, 2019; Suojelupoliisi 2019; Sisäministeriö, 2018). Koska laki avaa täysin uuden portin viranomaistyölle, se vaatii resursseja toteutuakseen. Suurin resurssi ovat osaavat työntekijät, joita tarvitsee rekrytoida nykyisen henkilökunnan lisäksi (Suihkonen, 2018). Samalla Euroopan Unioni on laatinut vuodesta 2012 alkaen uutta tietosuojasetusta (General Data Protection Regulation, GDPR) ja se astui voimaan 25.5.2018 (EUGDPR, 2018). Asetus ei lisää työvoiman tarvetta yhtä suoraviivaisesti, kuin tiedustelulait. Asetus levittäytyy kuitenkin laajalle rintamalle ja pakottaa lähes kaikki organisaatiot muokkaamaan omia toimintojaan, että ne voivat vastata asetuksen vaatimuksiin. Tämä lisää työvoiman tarvetta ainakin välillisesti.

Ulkomaisen työvoiman rekrytointi sisältää haasteita, joita tulisi pystyä lieventämään. Suomen syrjäisempi sijainti ja pohjoinen ilmasto, palkkataso ja verotus sekä vuorovaikutuksen ja sosiaalisten suhteiden rakentamisen vaikeus voivat nousta haasteeksi ulkomaista työvoimaa palkatessa (Raunio, 2002). Myös työvoiman tarveharkinta EU/ETA -alueiden ulkopuolelta vaikeuttaa ulkomaisen työvoiman hankintaa (Valtiovarainministeriö 2018). Vähäisempi kansainvälisyys, tutkimuksen pienempi määrä ja laatu tai yleinen mielikuva voivat vaikuttaa aivovuodon liikkumiseen Suomen suuntaan. Toisaalta vakaa yhteiskunta, kunnioittava työskulttuuri ja hyvä koulutusmaine ovat positiivisia piirteitä, jotka houkuttelevat muuttamaan Suomeen. (Raunio, 2002). Joillekin myös suomen kieli voi muodostua esteeksi työn hakemiselle tai saamiselle (Sinko ym., 2007, 73; Valtiovarainministeriö 2018). Työnantajien näkökulmasta ulkomailta rekrytoiminen on mahdollisuus ja haaste. Suurempi rekrytointialue tuo mukana mahdollisuuden löytää osaamista, jota Suomessa ei ole riittävästi sekä uudenlaista osaamista, jota Suomessa ei kouluteta. Haasteina ovat byrokratia, kielitaito, ulkomaisen koulutuksen todentaminen tai vastaavuus suomalaisessa koulutusjärjestelmässä (Sinko ym., 2007, 72-74). Kaikille työnantajille ulkomailta rekrytoiminen ei edes ole mahdollinen vaihtoehto kyberalan turvallisuusvaatimus-

ten vuoksi. Tutkimus ottaa kantaa kyberalan muutokseen ja käsittelee kyberalan työvoiman rekrytoinnin tilannetta.

1.1 Tutkimuksen tarkoitus

Mediassa on keskusteltu kyberalan noususta ja sen levittäytymisestä kaikkialle. Kodit, työpaikat, liikenne, media, logistiikka, kulutustuotteet, lääketiede, finanssiala, puolustusvoimat ja monet muut asiat ovat saaneet tuntea muutoksen, jonka tietotekniikan kehittyminen, langattomat tietoverkot ja esineiden internet ovat tuoneet. Tämä muutos vaatii uutta osaamista, uutta ajattelua, uutta koulutusta ja uusia työntekijöitä.

Suomesta on haluttu luoda kyberalan edelläkävijä. Kunnianhimoinen visio vaatii paljon uutta ja kyvykästä työvoimaa, joka mahdollistaa edelläkävijän roolin. Ala on loppujen lopuksi paljolti kiinni osaamisesta. Vaikka rahalla voi ostaa ja kehittää tekniikkaa, se ei korvaa ihmisten kyvykkyyttä innovoida ja hyödyntää teknologian suomaa mahdollisuuksia.

Suomessa työvoimapolitiikka on viime vuodet elänyt murroskautta. Väestö ikääntyy ja suuret ikäluokat ovat eläköitymässä. Samalla työn luonne on muuttunut ja uudet teknologiset vaatimukset ovat tulleet lähes jokaiseen ammattiin. Asiantuntijatyön määrä kasvaa ja työntekijöiltä vaaditaan monien eri toimintojen hallitsemista, enää ei riitä, että osaa ydintyön vaan täytyy osata hahmottaa kokonaisuuksia.

Työvoimapula on jo todellisuutta monella alalla. Tätä kuvaa mm. Työ- ja elinkeinoministeriön ammattibarometri. (Ammattibarometri, 2019). Monilla aloilla työvoiman puutetta pystytään korvaamaan erilaisin keinoin, kuten hyödyntämällä eläköitynyttä ja ulkomaista työvoimaa tai pikakouluttamalla tarpeen mukaan. Kyberala poikkeaa näistä luonteensa vuoksi. Siellä ei ole runsaasti vanhaa työvoimaa, ala kasvaa nopeasti, koulutus on uutta sekä ala vaatii yhä enemmän kybermaailman ja organisaation ydintoiminnan yhtäaikaista ymmärrystä. Lähes aina, kyberala vaatii myös korkea-asteen koulutuksen, jota ei voi niin helposti tuottaa nopealla syklillä.

Aikaisempaa tutkimusta kyberalan työvoimasta Suomessa ei laajasti ole vielä tehty. Työvoimaan liittyvää tietoa on yleisesti runsaasti ja se on jaoteltu myös aloittain. Kyberala ei kuitenkaan nouse esiin muusta IT- tai turvallisuusalan työstä tilastoissa. Rekrytointiin liittyvää tutkimusta tehdään runsaasti. Suomessa kyberalaan liittyvää rekrytointitutkimusta ei kuitenkaan löytynyt. Maailman laajuisesti löytyy tutkimusta jo jonkin verran, koska ala on tällä hetkellä keskiössä maailman poliittisen tilanteen sekä tekniikan jatkuvan kehityksen vuoksi. Esimerkiksi ISACA (Information Systems Audit and Control Association) julkaisee omaa tutkimusta kyberalan kansainvälisestä työvoiman saatavuudesta. Yhdysvalloissa aiheetta on tutkittu erityisesti kansallisen turvallisuuden näkökulmasta. Suomen koulutusjärjestelmä on korkeatasoista maailmanlaajuisessa vertailussa ja siten koulutusta eri tasoilla on tutkittu paljon. Kyberalan osaamista eri näkökulmista on tutkittu. Myös koulutuksen ja tutkimuk-

sen tarjontaa on Suomessa kartoitettu viime vuosina. Koulutuksen tavoitteiden toteutumista työmarkkinoiden näkökulmasta ei kyberalalta ole vielä tehty. Ala on uusi ja vasta viime vuosina saavuttanut laajemman huomion korkeakouluisa. Kyberalan työvoiman ja koulutuksen nykytilasta sekä tulevaisuuden odotuksista ja suuntauksista tarvitaan tutkimusta, jolla voidaan tukea organisaatioiden kyberalan kehitystä Suomessa.

1.2 Tutkimusongelma

Työvoiman saatavuus ja tarve eivät aina kohtaa. Tätä ongelmaa ratkaistaessa tarvitaan tutkimusta siitä, miten suuri työvoiman tarve on ja mihin suuntaan se mahdollisesti on kehittymässä. Lisäksi on tarpeen löytää keinoja, joilla työvoiman kysyntä ja tarjonta saadaan kohtaamaan nykyistä paremmin.

Kyberalan määrittelemättömyys ja jatkuva nopea muutos tekevät työvoiman hankinnasta haastavan. Ala vaatii lähes aina korkeakoulutuksen tai vastaavan osaamistason. Korkeakoulutuksen kesto ja sitoutuminen tiettyyn koulutusohjelmaan opintojen alkuvaiheessa vaikeuttavat tulevan työvoiman mukautumista tarpeeseen. Koulutusta on sen lisäksi ollut verrattain lyhyen aikaa tarjolla. Ala laajenee vauhdilla ja määrällinen osaajatarve kasvaa.

Tutkimuksella kartoitetaan kyberalan organisaatioiden työvoiman tarvetta, rekrytoinnin vaikeutta sekä tämän hetken koulutustarjontaa ja tulevaisuuden suuntauksia. Tutkimuksen avulla kyberalan opiskelijat sekä nykyiset työntekijät voivat kouluttautua ja profiloitua kyberalan tarpeen mukaan. Oppilaitokset voivat kohdentaa omaa opintotarjontaansa vastaamaan työnantajien tarvetta. Työnantajat saavat kuvaa alan tämän hetken tilanteesta, jonka mukaan ne voivat muokata omaa toimintaan rekrytointikilpailussa ja osaajien kehittämisessä.

Päättökysymys:

- Miten nykyinen työvoiman tarjonta vastaa työnantajan näkökulmasta kyberalan työvoiman tarvetta?

Alakysymykset:

- Miten kyberalan koulutusta tulisi mukauttaa vastaamaan paremmin työnantajan tarvetta?
- Millaista työvoimaa kyberalalle haetaan nyt?

1.3 Tutkimuksen rakenne

Tutkielma rakentuu seuraavasti: johdanto, kirjallisuus, tutkimusmenetelmät, tulokset, johtopäätökset ja pohdinta. Ensimmäinen luku esittelee tutkimuksen

taustan, merkityksen ja tavoitteet. Siinä ilmaistaan myös tutkimuskysymykset. Toinen luku käy läpi aiheeseen liittyvää kirjallista materiaalia läpi. Luku käy läpi kyberalan koulutusta, työvoimaa sekä työn jaottelua ja kompetensseja. Kolmannessa luvussa kuvataan tutkimuksessa käytetyt tutkimusmenetelmät, tutkimuksen kohteet sekä tutkimusmateriaalin kerääminen ja analyysimenetelmät. Neljäs luku esittelee tutkimuksen tulokset eri tutkimusosioihin jaettuna. Viides luku sisältää tutkimuksesta kerätyt johtopäätökset sekä kuudes luku pohdintaa tutkimukseen liittyen. Viimeisessä luvussa esitellään myös ideoita jatkotutkimuksille.

2 KIRJALLISUUS

2.1 Kyberalan koulutus

Koulutus on polku, joka etenee vaiheittain perusopetuksesta lukioon ja ammatilliseen koulutukseen sekä niiden kautta korkea-asteen koulutukseen. Koulutuksen jälkeen kertyy kokemusta, osaamista ja taitoja työelämässä. Omaehtoinen tiedonhankinta ja jatkokouluttaminen ovat tärkeä osa nykyistä kehityspolkuja ammatillisessa kehityksessä. Kyberturvallisuuden kansallinen osaaminen -raportti painottaa kyberturvallisuuden osaamisen olevan osa kansalaistaitoja (Lehto & Kähkönen, 2015). Kyberturvallisuus ei ole vain ammatillinen osaamisalue, jota tarvitaan vain tietyissä teknisissä työtehtävissä. Se on osa kaikkien arkea tavalla tai toisella.

Alakoulussa opetellaan tieto- ja viestintätaitoja. Näihin opintoihin kuuluu laitteisiin ja ohjelmistoihin tutustuminen sekä palveluiden, kuten tiedonhaun, käyttöä. Mukana on myös viestintäteknologian käyttöä eri vuorovaikutustilanteissa. Myös ikäkaudelle sopivaa ohjelmointia harjoitellaan matematiikan opiskelun ohella. Myöhemmin perehdytään tiedon rakentumiseen ja itsenäisempään tiedonhakuun. Yläkoulussa edellisiä aiheita syvennetään sekä perehdytään eettiseen tieto- ja viestintäteknologian käyttöön. Samalla tutustutaan myös tietoturvariskeihin ja niiltä suojautumiseen. (Opetushallitus, 2014).

Toisen asteen koulutusta ohjaa vahvasti linjavalinta. Lukio ja ammattikoulu toimivat eri pohjalla, mutta molempien tavoitteina on tehdä opiskelijoista tietoisempia medianlukijoita sekä tietoteknisesti valveutuneempia. Lukiossa teknologista kehitystä seurataan, tutustaan sen luomiin mahdollisuuksiin ja opitaan tekemään järkeviä ratkaisuja teknologiaa koskevissa valinnoissa. Kyberturvallisuus sinänsä ei opinnoissa vielä näy, mutta ohjelmointi ja tietotekniikka voivat tulla jo laajastikin tarjolle valinnaisina aineina. (Opetushallitus, 2015).

Korkeakouluasteella linjavalinta sekä opiskelijan omat kurssivalinnat korostuvat entisestään. Kyberalan opintoja tarjotaan yleensä osana tietoteknisiä aloja, mutta myös muiden alojen opiskelijoille yksittäisinä kursseina ja opinto-

kokonaisuuksina. Kyberalan tutkinnon voi suorittaa Jyväskylän yliopistossa sekä ammattikorkeakoulussa Jyväskylässä ja Kaakkois-Suomessa (JY, 2018; JAMK, 2018; XAMK, 2018). Näiden lisäksi kyberalaan liittyviä opintoja on tarjolla ainakin yhdeksässä muussa yliopistossa ja seitsemässä ammattikorkeakoulussa.

Perustietämystä varsinaisen oppipolun lisäksi tai sen jälkeen on saatavilla myös kansalaisopistoissa (Kansalaisopistot.fi, 2018), varusmiespalveluksessa (Varusmies, 2018), maanpuolustuskoulutusyhdistyksen kursseilla (MPK, 2018) sekä tietoturvaoppaista, kuten Kyberin taskutieto (Lönnqvist & Moilanen, 2017) ja Kodin kyberopas (Laitinen, 2017).

Yksityiskohtainen kuvaus kyberturvallisuusalan koulutuksesta yliopistoissa ja ammattikorkeakouluissa on esitetty tämän työn rinnalla tehdyssä tutkimustyössä: M. Lehto, J. Niemelä, Kyberturvallisuuden kansallinen osaaminen, Jyväskylän yliopisto, Informaatioteknologian tiedekunta, tutkimusraportti, joka julkaistaan kevään 2019 aikana.

2.1.1 Kyberalan koulutus Suomessa

Kyberalaan liittyvää koulutusta on Suomessa tarjolla ympäri maata yliopistoissa ja ammattikorkeakouluissa. Koulutus on laaja-alaista ja levittäytyy eri tekniikan aloille. Yhdeksästätoista korkeakoulusta kolme tarjoaa varsinaisen kyberturvallisuuden koulutusohjelman. Kaikissa muissa korkeakouluissa kyberalan koulutus on osana jotakin muuta koulutusohjelmaa. Kyberalan koulutus on usein sidoksissa tietotekniikan, tietojenkäsittelyn tai muihin matemaattisluonnontieteellisten aineiden koulutukseen. Koulutus elää jatkuvaa muutosvaihetta, kun oppilaitosten koulutuksen sisällöt hakevat pysyvämpiä muotoja.

2.1.2 Kyberalan opinnot yliopistoissa

Kyberalaan liittyvää koulutusta on tarjolla ainakin kymmenessä yliopistossa:

- Aalto-yliopisto (Aalto)
- Helsingin yliopisto (HY)
- Itä-Suomen yliopisto (UEF)
- Jyväskylän yliopisto (JY)
- Lappeenrannan yliopisto (LUT)
- Maanpuolustuskorkeakoulu (MPKK)
- Oulun yliopisto (OY)
- Tampereen yliopisto (TUNI)
- Turun yliopisto (TY)
- Vaasan yliopisto (Y)

Yliopistoista Jyväskylän yliopisto tarjoaa pisimmälle vietyä kyberalan koulutusta, missä kyberturvallisuus on omana maisteriohjelmana. Kyberturvallisuuden opinnoissa Jyväskylän yliopisto tarjoaa kaksi suuntautumisvaihtoehtoa: kyber-

turvallisuuden opintosuunta sekä kokonaisturvallisuuden ja strategisen tiedustelun opintosuunta. (JY, 2018). Opinnot tarjoavat laaja-alaisen ymmärryksen kyberturvallisuuden maailmaan teknologisesta ja hallinnollisesta näkökulmasta. Kyberalan tietoturvaan liittyvää koulutusta on tarjolla mm. Aalto yliopistossa, Tampereen teknillisessä yliopistossa sekä Turun yliopistossa. Turussa maisteritason opinnoissa voi erikoistua kryptografiaan ja tietoturvaan (TY, 2018). Siten opinnot keskittyvät kohdennetulle erikoisalalle kyberturvallisuuden kentässä. Tampereen yliopiston opetus kohdentuu automaation, elektroniikan ja ohjelmoinnin turvallisuuden yhdistämiseen (TTY, 2018). Aalto yliopiston painotuksena ovat eri verkkojen turvallisuus (Aalto, 2018). Muuten yliopistojen kyberkoulutus on osa jotakin muuta koulutusohjelmaa eikä siitä ole erikseen koulutusohjelmaa tai pääainetta. Kyberopintojen painotuksissa on pieniä eroja. Ne on suunniteltu tukemaan varsinaista koulutusohjelmaa tai yleisopinnoiksi lisäämään alan yleistä tietoisuutta.

2.1.3 Kyberalan opinnot ammattikorkeakouluissa

Kyberalaan liittyvää koulutusta on tarjolla ainakin yhdeksässä ammattikorkeakoulussa:

- Centria-ammattikorkeakoulu (Centria)
- Jyväskylän ammattikorkeakoulu (JAMK)
- Kaakkois-Suomen ammattikorkeakoulu (XAMK)
- Laurea ammattikorkeakoulu (Laurea)
- Metropolia ammattikorkeakoulu (Metropolia)
- Oulun ammattikorkeakoulu (OAMK)
- Poliisiammattikorkeakoulu (POLAMK)
- Tampereen ammattikorkeakoulu (TAMK)
- Turun ammattikorkeakoulu (TURKUAMK)

Ammattikorkeakoulujen alempi ammattikorkeakoulututkinto (AMK) keskittyy opintotarjonnan perusteella pääosin kyberturvallisuuden perusteisiin ja sivuainemaisiin opintokokonaisuuksiin. Niitä tarjotaan muun IT-alan opintojen ohessa. Jyväskylän ammattikorkeakoulussa kyberturvallisuus on omana suuntautumisvaihtoehtona. Siellä on kehitetty teknistä kyberturvallisuuden koulutusta ja tutkimusta mm. luomalla ammattikorkeakoulun sisäinen Jyväskylä Security Technology-keskus (JYVSECTEC). JAMK on ammattikorkeakouluista kyberturvallisuuden koulutuksessa kärjessä. (JAMK, 2018).

Jyväskylän ammattikorkeakoulun lisäksi laajempaa koulutusta tietoturvaan ja kyberturvallisuuteen liittyen tarjoavat myös Kaakkois-Suomen ammattikorkeakoulu, Laurea ammattikorkeakoulu, Tampereen ammattikorkeakoulu sekä Turun ammattikorkeakoulu (XAMK, 2018; Laurea, 2018; TAMK, 2018; TURKUAMK, 2018).

Osa ammattikorkeakouluista tarjoaa myös ylempää ammattikorkeakoulututkintoa (YAMK). Näissä kyberturvallisuus on omana koulutusohjelmana ainakin Kaakkois-Suomen ja Jyväskylän ammattikorkeakouluissa, joissa keskity-

tään pääosin tietoturva- ja tietoturvavaivoittuvuuksiin sekä tunkeutumisen ja puolustautumismenetelmiin. Näissä kahdessa kyberalan opetus on kaiken kaikkiaan pitkälle vietyä ja kattavaa. JAMK ja XAMK tarjoavat perusopetuksen ohella myös kyberharjoituksia suljetuissa verkkoympäristöissä. (JAMK, 2018; XAMK, 2018).

2.1.4 Kyberalan opinnot avoimissa yliopistoissa ja ammattikorkeakouluissa

Osa avoimista yliopistoista ja ammattikorkeakouluista tarjoaa kyberalaan liittyviä opintoja. Tarjonta on usein vastaavaa tai yhdessä järjestettyä varsinaisen yliopiston tai ammattikorkeakoulun kanssa. Siten se ei laajenna opetustarjontaa, mutta avaa mahdollisuuden opiskeluun tutkinto-opiskelun rinnalle. Kursseja on tarjolla mm. Aalton, Helsingin ja Jyväskylän avoimissa yliopistossa sekä Turun, Tampereen, Jyväskylän ja Kaakkois-Suomen avoimissa ammattikorkeakouluissa (Aalto, 2018; HY, 2018; JY, 2018; TURKUAMK, 2018; TAMK, 2018; JAMK, 2018; XAMK, 2018).

2.1.5 Muu kyberalan koulutus

Kyberalan osaamista voi kartuttaa tutkintokoulutuksen lisäksi muulla opiskelulla. Sertifikaattikoulutuksilla on IT-alalla vakiintunut asema, joilla todistetaan omaa osaamista joltakin spesifiltä osa-alueelta. Tietoturvaan ja kyberalaan liittyviä sertifikaatteja ovat esimerkiksi The International Information System Security Certification Consortiumin ((ISC)²) tarjoamat: CISSP (Certified Information System Security Professional), CISM (Certified Information Security Manager), CIPP/E (Certified Information Privacy Professional/Europe), CIPT (Certified Information Privacy Technologist). ((ISC)², 2018).

Yksi merkittävä koulutusten tarjoaja on The SANS Institute. Sen kurssien kautta on mahdollista suorittaa SANS Instituten omia sertifikaatteja, joita löytyy perustasosta ylöspäin ja hyvin laajalta skaalalta eri tietoturvan osa-alueisiin suuntautuen. Kurssitarjonnasta löytyviä aiheita ovat mm. tietoturva, kyberturvallisuus, ohjelmistoturvallisuus, penetraatiotestaus sekä digitaalinen rikosten-tutkintatekniikka. (The SANS Institute, 2018).

Näiden lisäksi tietoliikenne- ja tietoturva-alan laite- ja järjestelmävalmistajat järjestävät koulutusta ja myöntävät sertifikaatteja omien laitteiden ja ohjelmistojen konfigurointiin ja hallintaan liittyen. Suomessa on myös erilaisia perustason valmiuksia tarjoavia sertifikaatin luontoisia koulutuksia, kuten Tietoturvallisuuskortti (Tietoturvallisuuskortti, 2018) ja Tietosuojakortti (Alertum, 2018).

Korkeakoulujen ja sertifikaattikoulutusten lisäksi kyberalaan liittyvää opetusta on saatavilla yksityisten yritysten työllistämiskoulutuksena. Yhtenä esimerkkinä Barona-konserniin kuuluva Saranen Consulting Oy järjestää rekrytointikoulutusta kyberturvallisuuden alalla. Koulutus sisältää tietoturvakoulutusta sekä työssä oppimista. (Rekrytointikoulutus, 2018). Hyvin vastaavalla formaatilla toimii myös KPMG Oy Ab:n tarjoama IT-konsulttikoulutus. Siinä yhdistyvät työnantajan järjestämä koulutus ja määräaikainen työsojimus.

(KPMG, 2018). Telealan toimijat ovat laajentaneet palvelutoimintaansa ja tarjoavat myös väylän tietoturva-alalle. Elisa Santa Monica Networks sekä Telian hankkima Cygate tarjoavat IT-alaa opiskelleille mahdollisuuden erikoistua ja työllistyä omien trainee-ohjelmien kautta (Elisa Santa Monica, 2018; Academic Work Academy, 2018).

Maanpuolustuskoulutusyhdistys (MPK) antaa mm. kyberturvallisuuden koulutusta. Kurssit ovat suunnattu kaikille suomalaisille ja niillä pyritään lisäämään kansalaisten perusvalmiuksia kybermaailmassa. (MPK, 2018). Puolustusvoimissa varusmiehille tarjotaan mahdollisuutta hakeutua yhtenä erikoiskoulutuksena kybervarusmiespalvelukseen. Kybervarusmiehet saavat koulutusta Puolustusvoimien johtamisjärjestelmäkeskuksessa. Tehtävä sisältää koulutusta mm. tietoturvatestauksesta, tietoliikenteestä sekä blue team vs. red team -toiminnasta. Palvelusaika antaa hyödyllistä työkokemusta alalta. (Varusmies, 2018).

2.1.6 Kyberalan koulutustarve

Väestön rakenteellisen kehityksen myötä Suomessa korkeakoulutetun työvoiman kysynnän ennustetaan kasvavan lähivuosina. Syynä on suurelta osin työvoiman eläköityminen. Samaan aikaan korkeakouluopiskelijoiden määrä on ollut lievässä laskussa (Tilastokeskus, 2016). Tämä selittyy pääosin pitkään jatkuneesta syntyvyyden laskulla, jolloin syntyperäisten suomalaisten opiskelijoiden määrä luonnollisesti vähenee. (Sinko ym., 2007, 99).

Suomessa alakohtaista koulutustarvetta ennakoidaan työ- ja opetusministeriöiden toimesta keskipitkällä aikavälillä. Oppilaitoskohtaiset aloituspaikkojen määrät kytetään koulutustarvearvioon. Se on kuitenkin ongelmallista nopeasti muuttuvien suhdanteiden vuoksi koulutuksen kestäessä useita vuosia. (Sinko ym. 2007, 101). Kyberalan koulutuksen määrällistä tarvetta ei tilastoida alan määrittelemättömyyden vuoksi

Kaiken kaikkiaan Suomessa on laaja opetustarjonta tietotekniikasta, tietojenkäsittelystä ja matematiikasta. Vuonna 2017 yliopistoissa suoritettiin Tietojenkäsittely ja tietoliikenne (ICT) -aloilla yhteensä 1881 tutkintoa (Opetushallinnon tilastopalvelu, YO, 2017). Ammattikorkeakouluissa vastaavaa luku on 1696 (Opetushallinnon tilastopalvelu, AMK, 2017). Koulutuksen jakaantuminen yhdeksääntoista korkeakouluun tuo laajaa yleisosaamista mm. tietoliikenteestä ja tietoturvasta. Se voi kuitenkin heikentää osaamiskeskittymien muodostamista korkeatasoisen tutkimuksen keskuksiksi. Opetustarjonta saattaa jäädä perustasolle ja ammattilaiseksi kehittymien vaatii pitkää työssäoppimista tai jatkokoulutusta. Kyberosaaminen Suomessa - Nykytila ja tiekartta tulevaisuuteen selvitys nostaa esiin kaksi ristiriidassa olevaa tarvetta kyberalalla. Toisaalta tarvitaan laaja-alaista näkemystä ja toisaalta pitkälle erikoistunutta täsmäosaamista. (Pelkonen ym., 2016). Koulutuksen suunnittelun ongelmana on vastata näihin molempiin tarpeisiin. Samaan aikaan koulutuksen laadun lisäksi vaaditaan opiskelijoiden määrän kasvua. Osana muutosta aikuis-, muunto- ja jatkokoulutusta on kehitettävä. Yliopistojen ja ammattikorkeakoulujen tulisi mahdollistaa korkeasti

koulutetun työvoiman täydentävää koulutusta nykyistä aktiivisemmin (Sinko ym., 2007, 114). Pekka Neittaanmäen mukaan yliopistojen IT-alan opiskelijoiden sisäänottomääriä tulisi kasvattaa nykyisestä 1500:sta ainakin 2500:an henkilöön (Mäntylä, 2017).

Kokonaisuutena ajatellen kyberalan koulutusta tulee olla useilla tasoilla. Perustason ymmärrystä tulee lisätä kaikille opiskelijoille sekä aikuiskoulutuksen kautta kaikille kansalaisille. Kybertietoisuudesta tulee Suomessa muodostua kansalaistaito (Pelkonen ym., 2016). Kyberalan ammattiosaamista tulee laajentaa kahdella tasolla: laaja-alaisen kyberosaamisen lisääminen sekä kriittisten erityisalojen osaamisen laajentaminen ja laadullinen kehitys.

2.2 Työvoima ja rekrytointi

2.2.1 Työvoiman määritelmä

Tilastokeskus laskee työvoimaan ne 15-74 -vuotiaat henkilöt, jotka ovat tutkimusviikolla työllisiä tai työttömiä. Työllisiin lasketaan henkilöt, jotka ovat tutkimusviikolla tehneet työtä vähintään tunnin palkkaa tai luontoisetua vastaan. Myös tietyt poissaolot lasketaan työllistymiseksi, kuten perhevapaat. Työttömiksi lasketaan henkilöt, jotka tutkimusviikolla ovat vaille työtä, mutta etsivät työtä aktiivisesti ja ovat valmiita aloittamaan työn kahden viikon kuluessa. (Tilastokeskus, 2018). Työnhakijat koostuvat työttömistä työnhakijoista sekä muista henkilöistä, jotka hakevat työtä, mutta eivät kuulu työttömiin. Työvoiman tarjonta muodostuu työnhakijoista.

Työssäoloaste muodostuu työssä olleiden prosenttiosuudesta kaikista työllisistä laskettuna. Työttömyysaste on työttömien prosenttiosuus saman ikäisestä työvoimasta eli työllisistä ja työttömistä. Koko väestön työttömyysaste lasketaan 15-74-vuotiaiden työttömien prosenttiosuutena saman ikäisestä työvoimasta. Työttömiä oli Tilastokeskuksen mukaan vuoden 2018 huhtikuussa 240 000. Työttömyysaste oli 8,8%. (Tilastokeskus, 2018). Koska työttömyysaste on varsin korkea ja palkkakehitys on ollut maltillista, (Tilastokeskus, 2018) työvoiman saatavuuden puutteet johtunevat kysynnän ja tarjonnan kohtaamattomuudesta (Sinko ym., 2007, 13). Siten työvoimapulan voidaan päätellä liittyvän vain tiettyihin toimialoihin tai tehtäviin. Kohtaamattomuuden ongelma johtuu yleensä työvoiman sopimattomuudesta, riittämättömästä työvoiman liikkuvuudesta tai kannustimien puutteesta.

Työvoiman rakenteellinen muutos vaikuttaa uusien työtehtävien syntymiseen. Työttömänä olevilla ei useinkaan ole uusiin työtehtäviin vaadittavia taitoja tai ominaisuuksia. (Sinko ym., 2007, 13). Osaavan työvoiman muodostumiseen vaikuttaa pääosin koulutus ja työkokemus. Avautuviin työtehtäviin tulee siten hankkia henkilöitä kaikkien työnhakijoiden joukosta, joita työttömien työnhakijoiden lisäksi ovat töissä olevat. Lisäksi työvoimaa haetaan työvoiman ulkopuolelta, mm opiskelijoiden joukosta. (Sinko ym., 2007, 53).

Rekrytoinnin kohdistaminen eri ryhmiin:

- Työttömät työnhakijat, joilla on vaadittavat ominaisuudet tai kyky saavuttaa ne perehdyttämällä.
- Työlliset, joilla on vaadittavat ominaisuudet tai kyky saavuttaa ne perehdyttämällä, ja halu vaihtaa työpaikkaa.
- Opiskelijat, joilla on vaadittavat ominaisuudet tai kyky saavuttaa ne perehdyttämällä, mutta eivät ole vielä työmarkkinoilla.
- Ulkomailta rekrytoitavat henkilöt, joilla on vaadittavat ominaisuudet tai kyky saavuttaa ne perehdyttämällä.

2.2.2 Kyberalan työvoiman määritelmä

Sanalla kyber ei ole huomattavaa merkitystä ilman yhdyssanan perusosaa. Sitä käytetäänkin määriteosana, jolla viitataan digitaalisessa muodossa olevan informaation käsittelyyn. Kybertoimintaympäristöllä kuvataan yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuvaa toimintaympäristöä. Kyberturvallisuudesta puhuttaessa viitataan yleisesti tavoitetilään, jossa kybertoimintaympäristö on vakaa ja luotettava. (Sanastokeskus TSK ry, 2018). Työvoiman näkökulmasta kyberaluetta ei ole selkeästi määritelty. Kyberala työvoimaan liittyvänä työn osa-alueena on siten uusi ja pääosittain rajaamaton. Tässä tutkielmassa kyberala-termiä käytetään kuvaamaan laajasti kyberturvallisuuteen ja kybertoimintaympäristöön liittyviä työtehtäviä.

Koska kyber on määrittelemätön termi työvoiman alueella, lähin vastaus löytyy ICT-sektorilta (engl. Information and Communication Technology). Se pitää sisällään tavarantuotannon ja palvelutuotannon. Näistä kahdesta kyber on lähempänä palvelutuotantoa, jonka piiriin kuuluvat mm. tietojenkäsittely, teleliikenne, ohjelmistotuotanto, verkonhallinta ja tietoturva. Tavarantuotanto keskittyy enemmän elektroniikan valmistukseen. (Tilastokeskus, 2018). Koska palvelutuotantokin rajautuu tiedonkäsittelyyn, tietoliikenteeseen ja tallennukseen, siitä jää pois kyberalalle ominaiset muut osat. Näihin voidaan laskea turvallisuuden, rikostekniikan, tiedustelun, huoltovarmuuden ja maanpuolustuksen osa-alueita.

Tilastokeskuksen määritelmän mukaan *”Tietotekniikka-ammattilaisella tarkoitetaan henkilöä, jolla on kyky määritellä, suunnitella, kehittää, asentaa, käyttää, tukea, ylläpitää, hallinnoida, arvioida tai tutkia tietotekniikkaa tai tietojärjestelmiä. Tietotekniikka on heidän päätyönsä.”* (Tilastokeskus, 2018). Tämä rajaus sulkee osan kybertoimintaympäristöstä pois ja siten ei toimi täysin kyberalan ammattilaisuutta määriteltäessä. Epäselvää siis on, ketkä työntekijät kuuluvat kyberalan alle ja tullaanko kyberalan työtä terminä eriyttämään muusta IT-alan työstä.

Wilsonin ym. (2011) mukaan kyberalan ammattilaiset rakentavat ja ylläpitävät tietokonejärjestelmiä, jotka liittyvät informaatioturvallisuuteen. He nostavat myös esiin henkilön oman kokemuksen omasta työstään. Siten henkilö voi itse määritellä olevansa kyberalan ammattilainen. (Wilson & Wilson, 2011).

Myös Wilsonin ja Wilsonin määrittely on vajavainen ja ottaa huomioon lähinnä perinteisen tietoturva-alan työn.

Kyberalaa on vaikea laittaa kattavasti yhden kuvauksen alle. Siksi esimerkiksi Yhdysvaltojen puolustusministeriön (U.S. Department of Defence, DoD) oma The DoD Cyber Workforce Framework (DCWF) jakaa kyberalan työn neljään eri osa-alueeseen

- Cyberspace IT Workforce
- Cybersecurity Workforce
- Cyberspace Effects Workforce
- Intelligence Workforce (Cyberspace).

Puolustusministeriön jako kuvaa yhden, useita kybertoimintoja kattavan, organisaation näkemyksen kyberalan työn määrittelyyn. Kyberympäristön informaatiotekniikan, kyberturvallisuuden, kyberympäristön vaikutuksiin varautumisen sekä kyberympäristön tiedustelun tehtävien vaatimukset työssä suoriutumiseksi ovat hyvin vaihtelevat. Siten yksiselitteinen työn kuvaaminen ymmärrettävästi on ongelmallista. (The Department of Defense, 2018).

2.2.3 Työvoiman rekrytointi

Rekrytointia organisaatioihin tehdään pääosin kahdella tavalla, suorilla ja epäsuorilla menetelmillä. Suoria rekrytointimenetelmiä ovat mm. työpaikkailmoitukset ja mainostaminen, suoramaku eli head hunting, rekrytointitoimistojen käyttö sekä omat trainee-ohjelmat. Epäsuoria rekrytointimenetelmiä ovat mm. organisaation urasivut omilla internetsivuilla, avoimet haut, sosiaalisen median hyödyntäminen sekä organisaation työnantajabrändin rakentaminen. (Newell Brown, 2011).

Suorat menetelmät ovat tyypillisempiä ja niillä haetaan pääosin henkilöä tiettyyn avoinna olevaan tehtävään. Tyypillisesti työpaikka ilmoitetaan internetin työpaikkasivustoilla, joista työnhakijat pääsevät etsimään työtä. Työtehtäviä saatetaan mainostaa eri kanavissa, kuten lehdissä tai sosiaalisessa mediassa sen lisäksi, että ne on julkaistu työhakusivustoilla. Organisaatio voi myös ulkoistaa rekrytointiprosessin rekrytointitoimistoille, joilla on omat kanavansa etsiä potentiaalisia hakijoita ja omat listat jo tiedossa olevista työnhakijoista. Yleistyvä trendi on suoramaku eli head hunting, missä kontaktoidaan valikoituja haluttuja henkilöitä suoraan ja tiedustellaan heidän mielenkiintoaan tehtävää kohtaan. Työtä ei siten välttämättä ilmoiteta hakuun missään avoimessa kanavassa. Head hunting on aiemmin ollut tapa rekrytoida johtajia, mutta se on levinnyt laajasti myös asiantuntijoita rekrytoitaessa. Toinen laajaneuva tapa on trainee- eli harjoitteluohjelmat, joissa koulutetaan henkilöitä, osin työn ohessa, ja siten avautuu väylä päästä koulutuksen jälkeen suoraan töihin. Koulutuksen ajalta saatetaan maksaa palkkaa tai korvausta, mutta henkilöä ei suoraan palkata tehtävään ja organisaatioon. (Newell Brown, 2011).

Epäsuorat menetelmät rekrytinnissa ovat usein pitkäkestoisempia strategisia valintoja, missä yrityskuvaa pidetään yllä. Työnantajabrändiä rakennetaan

hallitusti houkuttelemaan parhaita osaajia organisaatioon. Sitä voidaan tukea sosiaalisen median kanavissa, joista mm. LinkedIn on erikoistunut ammatillisen verkostoitumisen kanavana. Samoin kaikki muutkin sosiaalisen median kanavat ja blogit voivat olla osa epäsuoraa rekrytointia. Myös työnhakijoiden kohtaaminen kasvokkain on hyvä tapa edistää työnantajabrändiä. Tämä voi tapahtua rekrytointimessuilla, kouluyhteistyön kautta tai järjestämällä tapahtumia tai ideointikilpailuja. Usein organisaatiot tarjoavat myös mahdollisuuden avoimen hakemuksen jättämisen internetsivuillaan. Siten potentiaalisia hakijoita voidaan kontaktoida suoraan, kun soveltuvia työtehtäviä tulee tarjolle. Samoin erilaiset urapolut tarjoavat mahdollisuuden työn vaihtamiseen, kun kokemusta ja osaamista kertyy työuran varrella. (Newell Brown, 2011).

Tulevaisuudessa työnhakijoiden haku voi tapahtua yhä enemmän suora-
haulla, missä työnhakijat tekevät profiilin verkkopalveluun. Siten työnantajat voivat etsiä omilla hakukriteereillä tai automaattisilla algoritmeilla sopivia hakijoita työntekijäpoolista. Sama metodi toimii jo nyt head huntingissa, jossa käytetään mm. LinkedIn-sivustoa. Tulevaisuudessa se voi vaan olla keskite-
tympää ja automatisoidumpaa; avoin hakemus koko työnantajakentälle.

Rekrytointipanostuksista huolimatta sopivaa hakijaa ei aina löydy. Rekrytointiongelmasta puhutaan, kun avoimeen työtehtävään on vaikeuksia löytää pätevä työntekijä. Kansainvälisesti termi skill shortage kuvaa tilannetta usein tarkemmin. Työvoimapulasta, eli labour shortage, voidaan puhua vasta, kun avoimeen työtehtävään ei löydy yrityksestä huolimatta soveltuvaa työntekijää. Kokemus rekrytointiongelmasta voi muodostua emootiosta, jossa työnantaja ei koe saavansa valmista työvoimaa riittävän nopeasti tai sillä panostuksella, jonka hän on tehnyt. Siten ajatus työvoimapulasta voi muodostua virheellisesti. Tilanne voi olla vain ajallisesti tilapäinen, maantieteellisesti paikallinen tai ratkaistavissa työnantajan omalla perehdytyksellä. (Sinko ym., 2007).

Tietoteknisten alojen mahdollinen työvoimapula ei näy tilastoissa. Alalla on työttömiä työnhakijoita. (Tilastokeskus, 2018). Kyberalan työvoimaa ei ole eritelty ja se olisi kokonaisuudessa pieni osa, joten se ei tilastoissa nousisi näkyvästi esiin. Alan nopean muutoksen ja huippuosaajien vähyyden vuoksi voi työnantajalle muodostua kuva työvoiman saatavuuden ongelmasta, erityisesti tilanteessa, missä haetaan seniortason osaajia tai yhdenkin asiantuntijan poistussa työnantajan palveluksesta.

2.2.4 Kyberalan työvoiman tarve

Työvoiman tarve pitkällä aikavälillä Suomessa tulee kasvamaan. IT-ala kasvaa ennusteiden mukaan erittäin nopeasti (Mäntylä, 2017). Sen mukana kasvaa myös kyberala. Ala on nyt kovassa nosteessa ja sen kasvupotentiaali on erittäin vahva. Suomessa on useita kansallisesti ja kansainvälisesti tunnettuja kyberalan toimijoita (CyberLab Oy, 2016). Kaupallisesta näkökulmasta Suomessa tarvitaan uusien kyberteknologioiden osaamista kasvavissa määrin täyttämään tulevaisuuden työpaikat. Lisäksi kyber linkittyy muihinkin kuin ainoastaan IT-alan

työtehtäviin, kuten fyysisen turvallisuuden, huoltovarmuuden ja sotilaallisen tason tehtäviin. Myös näissä tarve kybertietoiselle työvoimalle kasvaa.

Päivi Kinnunen ja Pekka Neittaanmäki tutkivat vuosien 2006-2015 IT-alan työttömyyden kehitystä ja koulutustasoa. Tutkimuksen mukaan työttömyys IT-alalla kasvoi kymmenen vuoden ajanjaksolla. Koulutuksen taso näkyi työttömyysprosentteissa selkeästi. Työnhakijoista keskiasteen tai alimman korkeasteen koulutuksen suorittaneita oli 51%, alemman korkeakouluasteen suorittaneita 20%, ylemmän korkeakouluasteen suorittaneita 15%. (Kinnunen & Neittaanmäki, 2016). Sen mukaan voidaan todeta koulutuksen tasolla olevan selkeä suhde työllistymiseen. Vaikka työttömyys on vuodesta 2017 ollut IT-alalla laskussa, alalla on edelleen työttömyyttä (Tilastokeskus, 2018; Ammattibarometri, 2019). Silti alan osaajien vajeen arvioidaan kolminkertaistuvan kahdeksassa vuodessa. Jo vuonna 2022 vaje olisi yli 20 000 henkilöä. (Mäntylä, 2017).

Kuviossa 1 on ennuste IT-alan työvoiman vajeen kasvusta.



KUVIO 1 IT-alan osaamisvaje (Mäntylä, 2017)

Kansainvälisesti kyberalan työvoiman tarpeesta on puhuttu jo useamman vuoden ajan. Maailmanlaajuisesti kyberalan työvoiman kehitystä seuraa ISACA (Information Systems Audit and Control Association). Sen neljän vuoden aikana tekemissä State of Cybersecurity -selvityksissä on havaittavissa toistuva vaje kyberturvallisuusalan osaamisessa. Viimeisimmän, vuonna 2018 tehdyn, kyselyn mukaan ISACA:n jäsenyrityksissä soveltuvan työvoiman löytäminen on ollut haasteellista. Erityisesti oikeanlaiset taidot omaavien yksilöiden rekrytoiminen on vaikeaa. Keskimäärin työpaikka on auki vähintään kolme kuukautta ennen soveltuvan hakijan löytämistä. Osa työpaikoista jää täyttämättä, koska soveltuvaa työvoimaa ei löydy. Suurin puute on työnhakijoiden yksilöllisissä teknisissä taidoissa. Siten voidaan todeta, että työnhakijoilla, joilla on suurimmat tekniset valmiudet, työllistyvät varmimmin. Työkokemus ei ole niin merkittävä tekijä ISACA:n tutkimuksen mukaan, kuin tekninen osaaminen. Tämä viittaa työnantajan uskoon siitä, että henkilöt kehittyvät työssä ollessaan ja voivat sitä kautta siirtyä vaativampiin tehtäviin ajan myötä. Koska työvoiman

saanti on haastavaa, osa tehtävistä pyritään korvaamaan automatisaatiolla, jolloin oleva työvoimaa voidaan vapauttaa muihin tehtäviin. (ISACA, 2018).

ISACA:n tutkimusten lisäksi erilaisia kybertyövoiman vajeeseen liittyviä tutkimuksia on tehty eri näkökulmista Libicki, Senty ja Pollak (2014) nostavat esiin valtiollisen turvallisuuden uhkan, jos valtiollisiin virkoihin tai valtion yhteistyöyrityksiinsä ei saada riittävän osaavaa työvoimaa. Osaavaa työvoimaa Libickin ym. mukaan on vaikea saada kohtuulliseen hintaan. Tämä johtuu korkean tason osaajien vähyydestä. (Libicki, Senty & Pollak, 2014). Kansainvälisesti kyberalan osaajapulan ennustetaan olevan 1,8 miljoonaa henkilöä vuonna 2022 (Blake, Nielsen & Wrozek, 2019).

Suomen kyberturvallisuusstrategiassa (Turvallisuuskomitea, 2013) kyberturvallisuuden visio on, että:

- *”Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan.*
- *Kansalaisilla, viranomaisilla ja yrityksillä on mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamiseen syntyvää osaamista sekä kansallisesti että kansainvälisesti.*
- *Vuonna 2016 Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa.”*

Valtiollisesta näkökulmasta strategian toteuttaminen pohjaa johtamiseen, lainsäädännön kehittämiseen, havainnointiin, osaamiseen sekä kansainväliseen yhteistyöhön. Valtiollisen kyberturvallisuuden lisäksi tarvitaan yksityistä kyberturva-alaa luomaan tuotteita, kehittämään osaamista, luomaan bisnesmahdollisuuksia sekä tuomaan laajuutta vahvistamaan suomalaista kyberomavaraisuutta. (Pelkonen ym., 2016). Suomi ei tavoitteista huolimatta ole noussut kärkimaiden joukkoon kyberturvallisuuden alalla, vaikka keikkuukin joissakin mittauksissa hyvillä sijoilla (ITU, 2017; Forbes, 2017). Kokonaisuutena kuitenkin jääme aivan kärkimaista (Halminen, 2017). Vastuiden jakoa eri osa-alueiden ja toimintojen mukaan on tehty. Lainsäädäntöä on uudistettu. (Eduskunta, 2019). Myös havainnointijärjestelmien kehitystä on jatkettu mm. kyberturvallisuuskeskuksen myötä (Kyberturvallisuuskeskus, 2018). Osaamistason turvaamisen toimenpiteet ovat epäselvempiä ja on vaikea yksiselitteisesti kuvata miten valtio edistää siltä osin kybertavoitteita.

2.3 Kyberalan työn jaottelu ja kompetenssit

2.3.1 Kompetenssin määritelmä

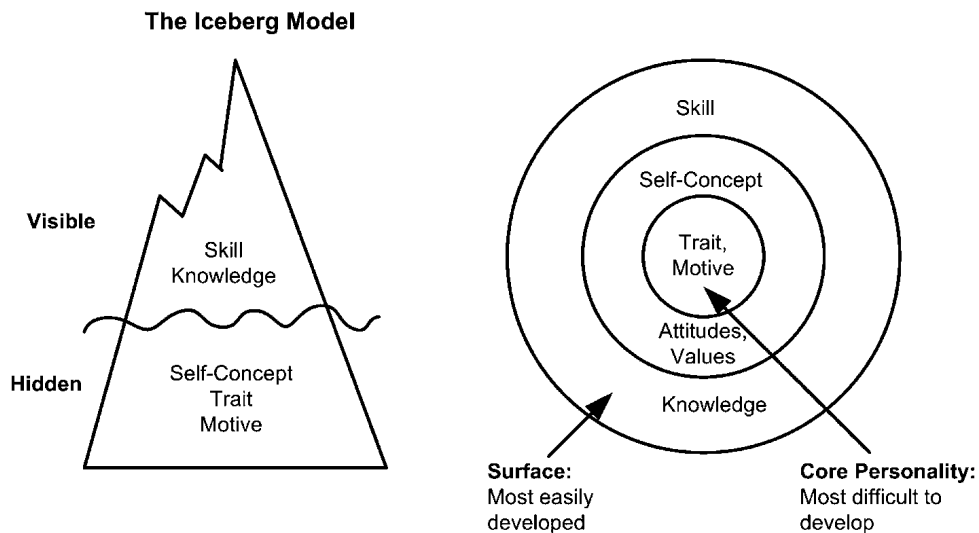
Kompetenssi-sanana synonyymina suomenkielessä on käytetty sanoja osaaminen, pätevyys ja valmius. Niillä viitataan kykyyn suorittaa velvoite tai tehtävä määritellyn kynnyksen ylittävällä tavalla. Siten kompetenssi sitoutuu enemmän

ammattillisiin kuin akateemisiin valmiuksiin. Kompetenssilla ei Niitamon (2003) mukaan tarkoiteta yleisälykkyyttä tai synnynnäisiä ominaisuuksia vaan merkitys on kääntynyt enemmän opittaviin valmiuksiin. Silti kompetenssi ei rajaudu vain opittuihin taitoihin vaan mukana on merkittävästi persoonallisuuteen ja motivaatioon sidonnaisia piirteitä. (Niitamo, 2003).

Kompetenssia tai osaamista on jaoteltu neljään luokkaan: tietoihin, taitoihin, kykyihin ja muihin persoonallisuustekijöihin ns. KSAO-kehyksessä (knowledge, skills, abilities, other personal factors). Siinä tiedolla tarkoitetaan lähinnä muodollisen koulutuksen tuomaa tietämystä. Taidot kehittyvät kokemuksen myötä ja niiden avulla pystytään suorittamaan tehtäviä tai toimintoja. Kyvyt ovat synnynnäisiä tai pääosin pysyviä ominaisuuksia, joita tarvitaan toimintojen suorittamiseen. Persoonallisuustekijät pitävät sisällään mm. motiivit, asenteet ja ajattelutavat. Mallin avulla jokainen yksittäinen osaaminen eritellään neljään KSAO-elementtiin. Elementin painoarvo yksittäisessä osaamisessa ohjaa toiminnan suorittamista. (Harvey, 1991).

Spencer ja Spencer (1993) kuvaavat jäävuorimallissaan kompetenssin ominaisuuksia ja niiden toimintaa, jotka yhdistyvät erinomaisessa suoriutumisessa. Ominaisuudet ovat taito, tieto, minäkuva, henkilökohtaiset ominaisuudet ja motiivit. Osa ominaisuuksista on ulkoisesti näkymättömiä ja osa voidaan havaita tai on mitattavissa. Mitä syvemmillä tai lähempänä sisäkehää ollaan, sitä vaikeampi niitä on havaita tai yksilön itse muuttaa. Jäävuoren pinnalla tai lähempänä ulkokehää olevia ominaisuuksia voidaan sen sijaan havaita ja kehittää helpommin. (Spencer & Spencer, 1993).

Kuviossa 2 on havainnollistettu ominaisuuksien jäävuorimalli.



KUVIO 2 The Iceberg Model of Competence (Spencer & Spencer, 1993, 11)

Blake ym. (2019) toteavat että kyberalan opiskelijan tulee kehittää STEM-kykyjä (Science, Technology, Engineering & Mathematics). STEM-termillä viitataan yleisesti koulutuspolitiikkaan tai opiskelijoiden koulutusvalintoihin, jolla ohjataan ja kannustetaan tieteen, teknologian, insinööritaitojen ja matematiikan

opiskeluun. Nämä taidot hallitsemalla voidaan toimia laajasti erilaisissa kyberturvallisuuden teknisissä rooleissa. Myös liiketoimintaymmärrys nousee esiin, jolla saavutetaan strateginen ja yhteistoiminnallinen havainnointikyky. Organisaatiot tarvitsevat kyberalan osaajilta molempia eli STEM-kykyjä ja liiketoimintaosaamista (Blake ym., 2019).

Organisaation kompetenssit ovat niitä ominaisuuksia, joilla organisaatio erottuu kilpailijoista ja menestyy. Organisaation ydinkompetenssit sitoutuvat sen työntekijöiden ominaisuuksiin, joilla se pystyy luomaan tuotteita tai palveluita. Siten organisaatiolle on tärkeää havaita omat kompetenssit ja rekrytoida tai kouluttaa niitä tukevia työntekijöitä. (Prahalad & Hamel, 1990). Wagnerin (2012) mukaan organisaation kompetenssi ei ole vain yksilöiden kompetenssien summa. Organisaation kompetenssi sisältää yksilöiden kompetenssit, jotka ovat yhdistetty organisaation kulttuuriin, rakenteeseen ja strategiaan. Siten soveltuvien henkilöiden saatavuus auttaa merkittävästi organisaatioita menestymään kilpailutilanteessa. (Wagner, 2012).

2.3.2 Kyberalan työtehtävien jaottelu ja työntekijöiden profilointi

Kyberalan työtehtävien jaotteluun on luotu kansainvälisesti käytetty National Cybersecurity Workforce Framework -viitekehys (NCWF). NCFW on taksonomia ja sanakirja, jolla voidaan kuvata kyberturvallisuusalan työtehtäviä. Sen tarkoituksena on helpottaa organisaatioita tunnistamaan kyberturvallisuusalan työtä. Tunnistamisen myötä henkilökunnan rekrytointi, koulutus, harjoittaminen ja kyvykkyyksien ylläpito voidaan organisoida. Samalla se antaa työntekijälle mahdollisuuden tunnistaa omat kyvykkyydet ja suunnitella omaa työuraa. (Newhouse, Keith, Scribner & Witte, 2017).

NCWF:issa on seitsemän kategoriaa:

- Turvallisuuden tarjoaminen (engl. Securely provision)
- Operointi ja ylläpito (engl. Operate and maintain)
- Valvonta ja hallinnointi (engl. Oversee and govern)
- Kerääminen ja operointi (engl. Collect and operate)
- Analysointi (engl. Analyze)
- Suojaaminen ja puolustus (engl. Protect and defend)
- Tutkinta (engl. Investigate)

Turvallisuuden tarjoaminen -kategoria käsitteellistää, suunnittelee ja rakentaa turvallisia IT-järjestelmiä. Operointi ja ylläpito -kategoria tukee ja ohjaa informaatioteknologian ylläpitoa. Valvonta ja hallinnointi -kategoria keskittyy kyberturvallisuusalan työn johtamiseen, hallinnointiin, ohjaukseen ja kehittämiseen. Kerääminen ja operointi -kategoria ohjaa kyberalueen tiedustelua sekä salaaminen ja harhauttaminen -toimintaa kybertoimintaympäristössä. Analysointi -kategoria tuottaa selontekoja ja arvioita kyberturvallisuustiedoista ja niiden käyttömahdollisuuksista. Suojaaminen ja puolustus -kategoria kohdistuu tietoturvaauhkien tunnistamiseen, analysointiin ja lieventämiseen. Tutkinta

-kategoria on kyberturvallisuustapahtumien sekä kyberrikosten tunnistamista ja tutkimista.

Näiden seitsemän kategorian tai yleistetyn erityisalan ryhmään on määritelty 33 tunnistettua kyberturvallisuusalan tehtävää (ks. taulukko 1). Näiden tunnistettujen ja ryhmiteltyjen tehtävien lisäksi NCWF huomioi 52 työroolia sekä niissä tarvittavat kompetenssit, joita kyberalan ammattilainen tarvitsee menestyäkseen. Siinä käytetään KSA-kehystä, jolla jokaisen tehtävä suoritusta voidaan arvioida tietojen, taitojen ja kykyjen suhteessa. (Newhouse ym., 2017).

TAULUKKO 1 NCWF työtehtävät (Newhouse ym., 2017).

Securely provision	Operate and maintain	Oversee and govern	Collect and operate	Analyze	Protect and defend	Investigate
Risk Management	Data Administration	Legal Advice and Advocacy	Collection Operations	Threat Analysis	Cyber Defense Analysis	Cyber Investigation
Software Development	Knowledge Management	Training, Education, and Awareness	Cyber Operational Planning	Exploitation Analysis	Cyber Defense	Digital Forensics
Systems Architecture	Customer Service and Technical Support	Cybersecurity Management	Cyber Operations	All-Source Analysis	Infrastructure Support	
R&D	Network Services	Strategic Planning and Policy		Targets Language Analysis	Incident Response	
Systems Requirements Planning	Systems Administration	Executive Cyber Leadership			Vulnerability Assessment and Management	
Test and Evaluation	Systems Analysis	Program/Project Management and Acquisition				
Systems Development						

NCWF kartoittaa kyberalan teknistä osaamista ja pilkkoo sen osiin. Viitekehys ei kuitenkaan huomioi työntekijän muita ominaisuuksia. Kybermaailma koostuu kolmesta tasosta: fyysisestä, loogisesta ja sosiaalisesta. Näistä NCWF kattaa vain kaksi ensimmäistä. Sosiaalinen taso jää huomioimatta, vaikka se on olennainen osa kyberturvallisuutta. Yksi suurimmista turvallisuusriskistä kybermaailmassa koostuu ihmisen toiminnasta ja siihen vaikuttamisesta. Esimerkkejä tästä ovat välinpitämättömyys tietoturvaohjeista tai phishingin kaltaiset tiedonhankintahyökkäykset. Dawson ja Thomson (2018) huomioivat, että kyberalan työvoimasta on erittäin vähän empiiristä informaatiota saatavilla. Kyberala on teknisesti orientoitunut ja homogeeninen ryhmä työntekijöitä. Dawson ja Thomson kuitenkin nostavat kuusi ominaisuutta, jotka tulevaisuuden menestyvällä kyberalan työntekijällä tulee olla: systemaattinen ajattelutapa, tiimipelaaaminen, tekniset ja sosiaaliset taidot, kansalaisvelvollisuuden tunto, jatkuva oppiminen sekä kommunikaatiotaidot. Kyberalan tulee siten keskittyä teknisten taitojen lisäksi muihin ominaisuuksiin, joiden kautta voidaan saavuttaa organisaatioissa tehokas kyberturvallisuustoiminta. (Dawson & Thomson, 2018).

Työntekijöiden profiloimista käytetään työvoiman tarkempien ominaisuuksien määrittelyyn. Työntekijä voi itse pitää kirjaa omista ominaisuuksista ja hyödyntää sitä työhaussa tai ammatillisessa kehittämisessä. Työntekijä sekä koulutuksen tarjoaja voivat myös kohdentaa tarvetta ja organisaationa kehittämistä profiloimista avulla. (Newhouse ym., 2017). NCWF painottaa teknisiä valmiuksia myös työntekijäprofiloinnissa. NCWF ottaa KSAO-kehuksesta mu-

kaan vain KSA-osat (Newhouse ym., 2017), jolloin O eli muut persoonallisuustekijät on jätetty tarkoituksellisesti pois.

Jyväskylän yliopisto tarjoaa yhden mallin työportfoliosta, jolla voi kartoittaa omaa kehitystä kahdeksassa kategoriassa: tutkinnot, opinnot, työkokemus, kansainvälistyminen, tieteellinen ja taiteellinen toiminta, kielitaito, osaaminen, muut kokemukset. Osaamisen kategoria tarjoaa seuraavat osiot, joilla kartoitetaan kompetenssin lisäksi muita kyvykkyyksiä: sosiaaliset taidot, kieli- ja viestintätaidot, opetus-, koulutus- ja ohjaustaidot, IT-osaaminen, ajattelu- ja ongelmanratkaisutaidot, itsesäätelytaidot, johtamis- ja organisointitaidot, kansainvälistymis- ja monikulttuurillisuustaidot, eettinen vastuullisuus, kyky toimia muutoksessa, ammatillinen osaaminen ja sen soveltaminen, taiteellinen osaaminen, tekninen osaaminen, liiketoiminta- ja yrittäjyysosaaminen. (JYU, 2018). Tässä mallissa myös persoonallisuustekijät ovat osittain mukana. Samoin huomioidaan myös luovuus. Luovuuden hyödyllisyyttä teknisessä ja sääntöjä noudattavassa työssä voi kritisoida, mutta toisaalta luova tai filosofinen laatikon ulkopuolinen ajattelu on mukana myös kyberalalla, mm. tuotekehityksessä tai kyberalan tutkinnassa tai tiedustelussa, kun tarvitaan tutkimustiedon lisäksi kykyä nähdä asiakkaan toiveita tai vastustajan ajatusmaailmaa. Eettinen puoli nostetaan portfoliossa esiin, mihin viittaa myös Dawsonin ja Thomsonin (2018) mainitsema kansallisvelvollisuuden tunto, joka oli yksi kyberturvallisuuden työntekijän ominaisuuksista (Dawson ym., 2018).

3 TUTKIMUSMENETELMÄT

Tutkimuksen tavoitteena on kuvata ilmiötä, josta ei ole merkittävästi aiempaa tutkimusta. Siten tutkimus on luonteeltaan kvalitatiivinen tapaustutkimus. Laadullinen tutkimus pyrkii selittämään aihetta ja ilmiötä sen ympärillä, eikä pelkästään mittaamaan määrällistä aineistoa. Laadullisen tutkimuksen perinteessä tutkimus nojautuu fenomenologis-hermeneuttiseen perinteeseen. Fenomenologiassa korostuvat ihmisen kokemus ilmiöstä sekä ilmiön merkitys ihmiselle. Hermeneuttinen ulottuvuus tulee kokemuksen tulkinnan kautta. Siinä etsitään sääntöjä, joilla saavutetaan ymmärrys ilmiön merkityksestä. Ymmärrystä edeltää aina aiempi tieto ja esiymmärrys. (Tuomi & Sarajarvi, 2018).

Haastattelu ja kysely ovat yleisiä tutkimusmenetelmiä laadullisessa tutkimuksessa. Niiden avulla selvitetään mitä ihminen ajattelee tai mitä hänen toimintansa motiivit ovat. Haastattelun ja kyselyn käyttö tutkimuksessa on perusteltua, kun tarvitaan lisätietoa aiheesta, josta ei entuudestaan ole riittävästi tietoa. Siten vastauksia voidaan etsiä parhaiten aihetta tuntevia henkilöitä haastatteleamalla tai heille kohdistetulla kyselyllä. Teemahaastattelu eli puolistrukturoitu haastattelu on menetelmä, missä edetään ennakkoon valikoitujen teemojen mukaisesti. Kysymykset voidaan ilmoittaa haastateltaville etukäteen, jolloin heillä on mahdollisuus perehtyä teemoihin. Teemahaastattelussa noudatellaan valittua rakennetta, mutta haastattelijan on mahdollista soveltaa kysymysten järjestystä, esittää tarkentavia kysymyksiä, avata kysymyksiä ja tarkentaa niitä tarpeen mukaan. Siten voidaan varmistaa, että haastateltava on ymmärtänyt kysymyksenannon oikein ja vastaa siihen riittävällä tarkkuudella. Kirjallinen kysely on teemahaastattelun kaltainen. Se on kuitenkin joustamattomampi. Kyselyä tehtäessä tulee pohtia, että vastaajat ymmärtävät kysymyksenannon oikein ja vastaajilla on kyky sekä halu vastata kysymyksiin riittävällä tarkkuudella. (Tuomi ym., 2018).

Kirjallinen joukkotiedotemateriaali voi myös toimia tutkimuksen aineistona. Kirjallisen materiaalin käyttö keskittyy pitkälti aineiston keräys- ja analyysimenetelmiin. Aineistoa voidaan käyttää monin eri tavoin. (Tuomi ym., 2018).

Useammalla tutkimusmenetelmällä voidaan lisätä tutkimuksen kattavuutta ja saavuttaa teemoihin liittyvää varmennettavuutta. Mixed methods

-menetelmä täydentää, kehittää, laajentaa, vahvistaa tai varmentaa tutkimusta (Venkatesh, Brown & Bala, 2013). Metsämuuronen toteaa, että useampaa tutkimusmenetelmää käyttämällä lisätään havaintojen kattavuutta ja varmennettavuutta (Metsämuuronen, 2011, 266). Pelkästään useamman metodin käyttö ei kuitenkaan suoraan tee tutkimuksesta mixed methods tutkimusta (Tuomi ym., 2018). Jos tarkoituksena on luoda laadullinen varmentaminen eri lähteistä, ei niinkään yhdistää määrällistä ja laadullista tutkimusta, tutkimus vain sivuaa mixed methods -menetelmää.

Haastattelujen sekä kirjallisen materiaalin tutkimukseen soveltuu sisälönanalyysi. Teoriaohjaavassa sisälönanalyysissä käytetään tukena teoriaa, jota aiempi tieto ohjaa ja auttaa. Teoria ei kuitenkaan sido analyysia vaan avaa uusia ajattelun uria. Aineistolähtöisyys ja valmiit mallit vaihtelevat tutkimuksen ohjaavina tekijöinä. Päätelyn logiikka eli abduktiivinen päätely on tutkimuksen tekijän pohjana yhdisteltäessä eri ohjureita ja materiaaleja. (Tuomi ym., 2018, 109-110).

3.1 Tutkimuksen tavoitteet ja rajaus

Tutkimuskysymys tarkastelee, miten nykyinen työvoiman tarjonta vastaa työnantajan näkökulmasta kyberalan työvoiman tarvetta. Tutkimuskysymykseen vastataan teemahaastattelujen avulla. Pääkysymystä täydennetään apukysymyksellä, joka liittyy koulutuksen vastaavuuteen työnantajan näkökulmasta. Ensimmäinen apukysymys on: ”Miten kyberalan koulutusta tulisi mukauttaa vastaamaan paremmin työnantajan tarvetta?”. Edellä mainittuja kysymyksiä pohjustetaan toisella apukysymyksellä: ”Millaista työvoimaa kyberalalle haetaan nyt?”. Tähän kysymykseen vastaa tutkielmassa toteutettava työpaikkaseuranta.

Työn rajauksena ovat Suomessa sijaitsevat työpaikat ja työvoiman saatavuus kyberalalla. Työn ulkopuolelle rajataan varsinainen osaamiskartoitus ja keskitytään soveltuvan työvoiman saatavuuteen ja niihin ominaisuuksiin, joita rekrytoitavilta henkilöiltä odotetaan.

3.2 Tutkimusmenetelmien kuvaus

Teemahaastattelun avulla toteutettu tapaustutkimus sopii tutkimusmenetelmäksi, kun tietoa haetaan vähemmän tunnetusta asiasta (Tuomi ym., 2018). Kyberalan työvoimapula on kansainvälisesti havaittu (ISACA, 2018) ja Suomessa IT-alan työvoiman kehityksestä on tehty arvioita, jotka osoittavat työvoimapulan kasvavan seuraavien vuosien aikana (Mäntylä, 2017). Siitä huolimatta kyberalan osaavan työvoiman saatavuudesta ei ole tehty tutkimusta Suomessa. Siten tapaustutkimus haastattelemalla asiantuntevia rekrytoijia tuo arvokasta lisätietoa työmarkkinatilanteesta tällä hetkellä.

Teemahaastatteluun etsittiin haastateltavia organisaatioita kartoittamalla avoimia työpaikkoja sähköisistä rekrytointikanavista. Samalla työpaikkailmoituksista kerättiin tieto siitä, kuinka paljon työtehtäviä kyberalalla on avoinna. Työpaikkailmoituksista kerättiin myös tietoa millaista työvoimaa rekrytoivat organisaatiot työpaikkailmoitusten perusteella hakevat. Tästä kirjallisesta aineistosta saatiin haastatteluihin taustatietoa, joiden avulla voitiin tarkentaa ja varmentaa teemahaastatteluista saatuja aineistoa. Työpaikkailmoitusten aineisto kerättiin itse, koska aiemmin todetusti kyberalan työpaikkoja ei tilastoida erikseen sen määrittelemättömyyden ja laaja-alaisuuden vuoksi.

Kyberalalla osaaminen on merkittävässä asemassa uutta työvoimaa etsittäessä. Alalle on vaikea tulla ilman taustatietoja tekniikasta, turvallisuudesta, tiedustelusta tai muusta kyberalan erikoisalueesta. Siten kyberalan koulutus nousi mukaan voimakkaaksi teemaksi. Suomessa tarjottavaa koulutusta selvitetiin keräämällä kirjallisista julkaisuista aineistoa korkeakouluista ja muista koulutusta tarjoavista organisaatioista. Aineiston perusteella toimitettiin kirjallinen kysely valikoituihin korkeakouluihin tarkempien tietojen saamista varten sekä kartoittamaan kyberalaan keskittyneiden korkeakoulujen tulevaisuuden suuntauksia.

Kirjallinen kysely on tehokas tapa saavuttaa suurempi kohdejoukko kustannustehokkaasti. Kysely toteutettiin avoimilla kysymyksillä, jotka tukivat tutkimuksen teemaa. Avoimet kysymykset valikoituivat metodiksi kyselyn tarkoituksen ja kohdejoukon mukaan. Monivalintamenetelmällä ei olisi saatu riittävän kattavia ja monipuolisia vastauksia, joita tutkimuksessa haettiin. Lisäksi kohdejoukkona olivat korkeakoulut, joiden omaa toimintaa ja tulevaisuutta haluttiin selvittää. Kohdejoukolla voitiin katsoa olevan kyky ja halu vastata avoimiin kysymyksiin riittävällä tarkkuudella.

Usean tutkimusmenetelmän käyttö perustuu menetelmillä saatujen aineistojen muodostamaan jatkumoon. Siinä edetään kirjallisen aineiston tutkimisesta ja potentiaalisten haastateltavien organisaatioiden kartoituksesta teemahaastatteluihin. Teemahaastattelut ovat tutkimuksen ydin, jossa kartoitetaan työvoiman saatavuutta työnantajan näkökulmasta. Saatavuuden mahdollistajia, eli osaavan työvoiman muodostumista, etsittiin koulutuksen kautta, joita kartoitettiin kirjallisista materiaaleista ja kirjallisen kyselyn avulla.

3.3 Tutkimuksen kohdejoukko

Tutkimuksen kohdejoukkoja on kolme. Ensimmäisessä osiossa tutkitaan kirjallista joukkotiedotemateriaalia. Materiaali koostuu avoimista kyberalan työpaikkailmoituksista julkisissa rekrytointikanavissa. Tutkittaviksi rekrytointikanaviksi valikoituivat tunnetut sivustot, jotka internethakujen mukaan olivat yleisimmät rekrytointi-ilmoitusten julkaisualustat. Neljä rekrytointisivustoa koettiin riittäväksi antamaan kuva työmarkkinasta kyberalalla Suomessa valitun ajanjakson aikana.

Toisessa osiossa tutkitaan organisaatioiden rekrytoinneista vastaavien henkilöiden näkemyksiä teemahaastattelun avulla. Kohdejoukko muodostui ensimmäisen osion työpaikkailmoitusten pohjalta. Niistä valittiin organisaatioita, jotka toimivat kyberalan ydintehtävissä ja joilla oli avoimia työpaikkoja auki vuonna 2018 valituissa rekrytointikanavissa. Haastattelun tavoiteltu kohdejoukko oli 4-10 organisaatiota eri puolelta Suomea, minkä perusteella voidaan tehdä riittävä kartoitus kuvaamaan tilannetta tarvittavassa laajuudessa Suomessa tietyinä ajanjaksona. Tutkimuksessa tehtiin viisi haastattelua.

Kolmas kohdejoukko oli kyberalan opetusta tarjoavat korkeakoulut. Korkeakouluista tehtiin kartoitus opetustarjonnasta julkaistujen tietojen perusteella. Kartoituksen perusteella kerättiin tietoa kyberopetusta tarjoavista oppilaitoksista sekä niiden opetuksen laajuudesta. Kyberalan koulutusta tarjoaville oppilaitoksille lähetettiin kirjallinen kysely koulutuksen suuntauksista sekä laadusta. Kysely lähetettiin 13 valittuun oppilaitokseen. Vastukset saatiin 11:sta oppilaitoksesta.

3.4 Aineiston kerääminen ja analysointi

Aineistoa kerätään eri tavoin kohdejoukosta riippuen. Tässä tutkimuksessa aineistoa kerätään aluksi seuraamalla avoimia työpaikkoja valituista rekrytointikanavista valittuna ajanjaksona. Rekrytointikanavat ovat MOL.fi, Valtiolle.fi, Oikotie.fi ja Monster.fi. Työpaikkoja haetaan rekrytointikanavista hakusanoilla kyber ja cyber. Haun tuloksista rajataan pois selkeästi tässä kontekstissa virheelliset osumat. Aineiston keräämisen ajanjakso on 18.2.2018 - 20.5.2018. Työpaikkailmoitusten aineistoon pohjautuen haastatellaan rekrytoijia tarkempien määrittelyjen saamiseksi. Haastattelut toteutetaan puolistrukturoituina teema-haastatteluina.

Tutkimuksessa kerätyt työpaikkailmoitukset jaotellaan valitun viitekehyksen mukaisiin kategorioihin. Tutkimuksessa käytetään soveltaen NCWF-viitekehystä. NCWF kattaa seitsemän eri kategoriaa, jotka kuvaavat kyberalan osaamiskentän eri alueita. Tässä tutkimuksessa viitekehykseen on lisätty kahdeksas kategoria täydentämään kyberalaan liittyvien työpaikkojen jakoa. Kahdeksas kategoria on myyntiin, markkinointiin ja tukitoimiin liittyvät työtehtävät, joissa kyber- ja tietoturva-alan ymmärrys tai muu yleistietämys ovat osana työnantajan vaatimusta työntekijälle. Kahdeksanteen kategoriaan on laitettu myös työpaikkailmoitukset, jotka ovat verrattavissa opiskeluun. Näissä mukana on taloudellisesti tuettu työssäoppiminen tai työssäolojakso, mutta jotka eivät suoraan palkkaa työnhakijaa työtehtävään.

Työpaikkailmoituksista redusoidaan ylimääräinen informaatio pois. Tämän jälkeen aineisto klusteroidaan eli ryhmitellään työn nimikkeeseen, työn kuvauksen ja työn vaatimusten mukaan (ks. kuvio 3). Abstrahoinnissa eli käsitteellistämässä yhdistellään muodostuneita ryhmiä niin kauan, että ne mahtuvat laajennetun viitekehyksen kahdeksaan kategoriaan. Joissakin tapauksissa tehtävä sopii kahteen tai useampaan viitekehyksen kategoriaan. Niissä tapauk-

sisä käytetään työn nimikkeen, kuvauksen ja vaatimusten jälkeen työnantajaa ja työn alaa määrittelemään sopivin viitekehyksen ryhmä. Jokainen työpaikkailmoitus ilmoitetaan vain yhdessä viitekehyksen kategoriassa.

Jaottelu ilmaisee määrällisen tarpeen jokaiseen viitekehyksen luokkaan. Jaottelun jälkeen työpaikkailmoituksista poimitaan taulukoitavaa tietoa tekstianalyysin avulla. Siinä kerätystä aineistosta lasketaan informaatiota asetettujen kategorioiden mukaan (Metsämuuronen, 2011, 220). Taulukoitavaa tietoa ovat työn ala, työtehtävät sekä työnantajan vaatimukset. Taulukoitu tieto työnantajan vaatimuksista, KSAO-kehystä mukailen, luokitellaan profiileiksi. Profiilit kertovat millaista työvoimaa työpaikkailmoitusten perusteella haetaan töihin.

Puolistrukturoitua haastatteluja käytetään vastaamaan kysymyksiin soveltuvan työvoiman saatavuudesta sekä siinä mahdollisesti ilmenneistä puutteista. Kyberalalle haluttujen työntekijöiden profilointi ei suoraan kerro työvoiman saatavuudesta. Se kuvaa hyvin, millaista työvoimaa haetaan, mutta ei kerro suoraan sen löytymistä, puutetta tai laatua. Teemahaastattelulla selvitetään työnantajan kokemus työvoiman löytämisen helppoudesta ja haasteista. Se mahdollistaa myös tulevaisuuteen vievien johtopäätöksiä tekemisen. Teemahaastattelu soveltuu tutkimusmenetelmäksi, koska halutaan täsmentää annettuja vastauksia sekä muodostaa kuvaavia esimerkkejä muun aineiston pohjalta. Osittain tutkimus on myös haastateltavan yksilön kokemus aiheesta ja siihen voi liittyä emootio. (Metsämuuronen, 2011, 245). Emootion ylikorostumista haastattelussa pyritään välttämään, mutta rekrytoijan kokemus on arvokasta, koska kyberalan työvoimasta ei ole vielä tilastoja.

Haastattelupyynnö toimitettiin kahteentoista organisaatioon, joilla on toimintaa kyberalalla ja joilla oli työpaikkailmoituksia avoimena vuonna 2018. Kahdestatoista organisaatiosta haastattelu saatiin viideltä. Haastateltavat henkilöt ovat olleet rekrytoinnista vastanneita henkilöitä organisaatioissa, joilla on vuonna 2018 ollut työpaikkoja auki tutkituissa rekrytointikanavissa.

Haastateltavat organisaatiot tavoitettiin sähköpostilla, puhelimitse sekä osa rekrytointimessuilla paikan päällä. Haastattelun teemat ja kysymysten rungot toimitettiin haastateltaville etukäteen haastatteluun valmistautumista varten. Haastattelut toteutettiin kasvokkain organisaatioiden henkilöiden kanssa 6.11. - 7.12.2018 välisenä aikana Vantaalla, Helsingissä, Jyväskylässä ja Tampereella. Haastattelut tallennettiin digitaalisesti matkapuhelimella. Jokaisesta haastattelusta koottiin vastausten perusteella yhteenveto, joka toimitettiin haastatelluille tarkastettavaksi. Teemahaastattelussa oli 14 kysymystä sekä avoin osuus, missä haastateltavat saivat vapaasti kertoa aiheesta. Haastattelukysymykset koskivat kyberalan rekrytointia ja siinä ilmenneitä haasteita; hakijoiden soveltuvuutta ja ominaisuuksia sekä kyberalan koulutusta ja sen kehittämistä. Näin saatiin tuoreita näkemyksiä tämän hetken työvoimaa koskien, kuinka rekrytoinnissa mukana olleen yksilön mielestä hakijoiden määrä ja laatu vastaa organisaation asettamia tavoitteita. Rekrytointiin osallistuneet henkilöt ovat eturintamassa havainnoimassa työnhakijoiden soveltuvuutta, koulutusta, kokemusta ja osaamista.

Haastattelumateriaalin analysointi tehtiin aineistolähtöisesti teemoittamalla (ks. kuvio 4). Haastatteluvastaukset käytiin useaan kertaan läpi, ja niistä koottiin sisällönanalyysin avulla yhteenveto jokaisen haastatteluteeman osalta. Analyysi tehtiin kvalitatiivisuutta ja kvantitatiivisuutta yhdistellen. Sanallisista vastauksista prosessoitiin erot ja yhtenevyydet sekä numeraalisista vastauksista laskettiin keskiarvot ja hajonta.

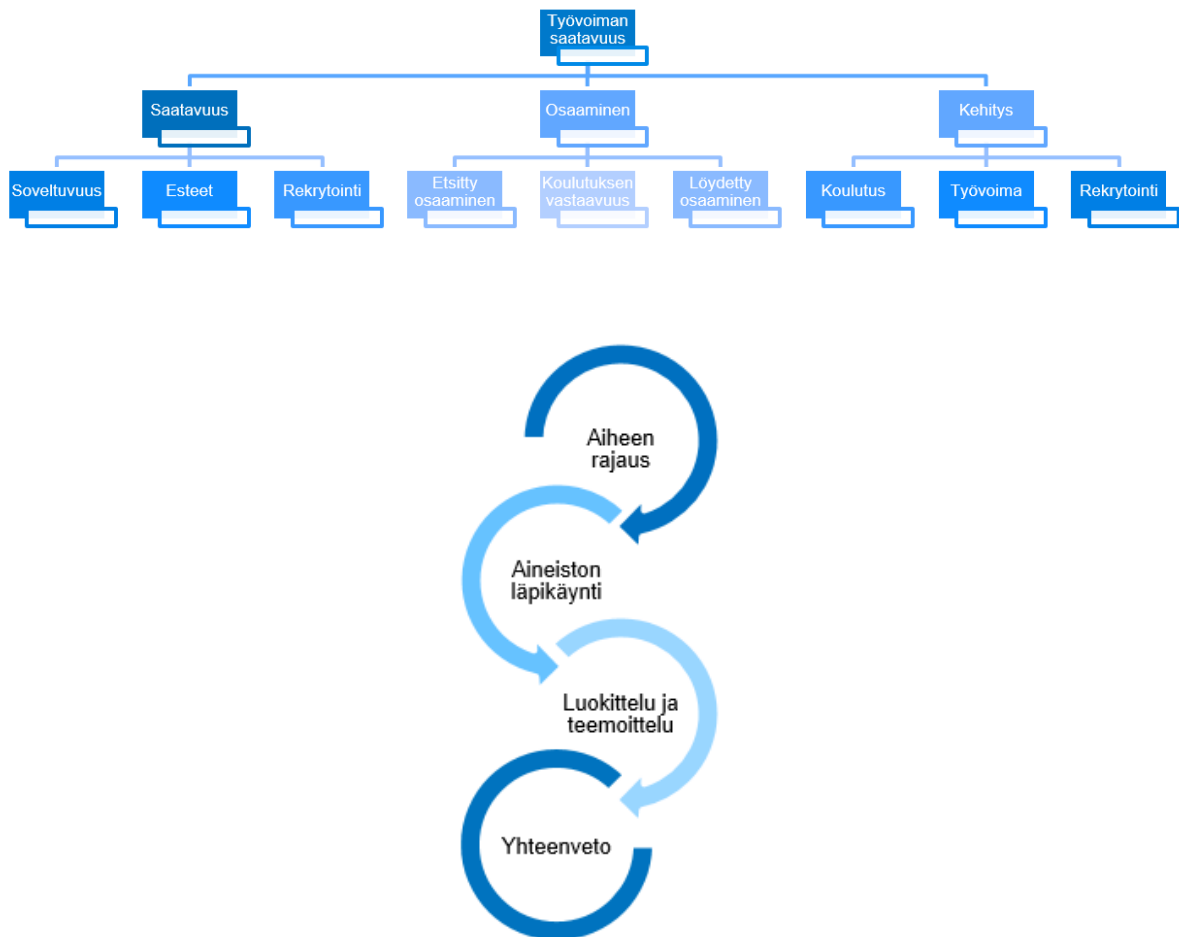
Koulutuksen nykytilaa selvitettiin tämän hetken opetustarjonnan kautta, eli millaista kyberalaaan liittyvää koulutusta Suomen korkeakouluissa on. Selvitys pohjautui korkeakoulujen sähköisesti julkaisemiin tietoihin opetustarjonnasta. Lisäksi valituille kyberalanopetusta tarjoaville korkeakouluille lähetettiin kirjallinen kysely. Siinä korkeakoulut tarkensivat omaa koulutustarjontaansa sekä tulevaisuuden suunnitelmia kyberalaaan liittyen, millaisia suunnitelmia heillä on muokata omaa kyberalan opetusta. Korkeakouluilta kysyttiin myös mielipidettä heidän oman koulutuksensa soveltuvuuteen työmarkkinoiden näkökulmasta. Kysely lähetettiin 13 korkeakouluun, joista 11 vastasi. Annetut vastaukset analysoitiin sisällön mukaan kysymyksittäin sekä oppilaitoksen kyberalan opetuksen laajuuden ja kypsyyden mukaan jaoteltuina. Vastauksista poimittiin yhteneväisyydet, eriäväisyydet sekä muut merkittävät huomiot. Kyberalan koulutuskartoitus kuvastaa rajatuilta osin kyberalan koulutussuuntauksia. Samalla se antaa viitteitä koulutuksen tuloksen ja työnantajien vaatimusten välisestä mahdollisesta kuilusta; kouluttavatko oppilaitokset riittävän osaavia työnhakijoita työnantajien tarpeisiin.

Kuviossa 3 on havainnollistettu työpaikkailmoitusten jaottelu ja niistä analysoitujen ominaisuuksien koostaminen kyberalan työntekijän profiiliksi.



KUVIO 3 Havainnekuva työpaikkailmoitusten perusteella tehtävästä jaottelusta

Kuviossa 4 on ilmaistu haastattelun teemat sekä havainnollistettu haastattelujen analysoinnin ketju.



KUVIO 4 Havainnekuva haastattelujen analysoinnista teemoittamalla

4 TULOKSET

Tutkimuksen kolme osiota kuvaavat millaista työvoimaa alalle haetaan nyt, millaiseksi työnantajat kokevat työvoiman rekrytoinnin tällä hetkellä ja miten oppilaitokset suuntaavat kyberalan opetusta. Tutkimus antaa vastauksia kyberalan työvoimapulan syvyydestä, työntajien vaatimista osaamisalueista, hakijoiden osaamistasosta ja soveltuvuudesta sekä opetuksen tarjonnasta. Kerätyt työpaikkailmoitukset jaettiin NCWF-viitekehyksen luokkiin ja selvitettiin määrällistä tarvetta eri luokkien työtehtäviin. Ilmoituksista kerättiin työtehtävät ja työnantajien vaatimukset luokittain. Vaatimuksista koostettiin kyberalan työntekijäprofiili. Työnantajien haastatteluilla kerättiin tietoa rekrytointikokemuksista kyberalalle. Selvitetiin, kuinka haastavaa työntekijöiden löytäminen alalle on nyt ja kuinka hyvin hakijoiden osaaminen ja koulutus vastaa työnantajan vaatimuksia. Kyberalan opetusta tarjoavilta oppilaitoksilta kerättiin kyselyn avulla tietoa koulutuksen suuntauksista ja opetuksen laadusta työmarkkinoiden näkökulmasta.

4.1 Työpaikkailmoitusten seuranta

Avoimien työpaikkojen seurannassa työpaikkailmoituksia oli kolmen kuukauden seurantajaksolla avoinna 159 kappaletta. Ilmoitukset ja niissä haetut avoimien työpaikkojen määrät (168) jakautuivat laajennetun NCWF-viitekehyksen kategorioihin seuraavasti:

NCWF-kategoria	Määrä
1. Turvallisuuden tarjoaminen (engl. Securely provision):	59
2. Operointi ja ylläpito (engl. Operate and maintain):	50
3. Valvonta ja hallinnointi (engl. Oversee and govern):	39
4. Kerääminen ja operointi (engl. Collect and operate):	0
5. Analysointi (engl. Analyze):	4
6. Suojaaminen ja puolustus (engl. Protect and defend):	6
7. Tutkinta (engl. Investigate):	10
Yhteensä:	168
8. Muut:	
a. <i>Sekalaiset</i>	16
b. <i>Myynti ja myynnin tuki</i>	5
c. <i>Kesätyö</i>	3
d. <i>Kyberalaan liittyvä koulutusohjelma</i>	9 tarjoajaa

Vertaamalla korkeakoulujen tietojenkäsittelyn ja tietoliikenteen aloilta vuosittain valmistuvien opiskelijoiden määrää ja kyberalan avointen rekrytointi-ilmoitusten määrää ei voi tehdä selkeitä johtopäätöksiä työvoiman riittävydestä. IT-ala on huomattavasti laajempi ja työvoiman tarve suurempi. Puhtaasti kyberalaan erikoistuneiden oppilaiden osuus valmistuvien opiskelijoiden määrästä on kuitenkin vain muutamia kymmeniä vuosittain. Siten on aiheellista nostaa huoli esiin kyberalan osaamisen määrällisestä riittämättömyydestä, kun kolmen kuukauden otanta tuo pitkälti toistasataa avointa työpaikkaa, joissa kyber on osana työntekijän hakuilmoitusta.

Työnantajien vaatimukset on koostettu kyberalantyöntekijän profiiliksi. Siinä nousevat esiin 1) tekninen osaaminen, 2) ammatillinen osaaminen ja sen soveltaminen, 3) työkokemus, 4) kielitaidot, 5) ajattelu- ja ongelmanratkaisutaidot, 6) sosiaaliset taidot, 7) koulutus. Kyberalan työtä tarkastellessa ei ole yllätys, että erityisesti tekninen osaaminen ja kokemus olivat eniten työnantajien toivelistoilla. Siis KSAO-kehityksen taito (engl. S-skills), joka syntyy työkokemuksen kautta. Sen sijaan formaali koulutus, eli tieto (engl. K-knowledge), ei noussut niin merkittäväksi tekijäksi työhakemuksissa ja se näkyi joissakin tapauksissa vain muodollisena vaatimuksena. Osaamista mitattiin korkeakoulutusta enemmän harrastuneisuuden, sertifikaattien tai muun näytön kautta. Suora hallinnollinen osaaminen jäi myös vähemmälle huomiolle. Projektiosaaminen sekä standardien, lakien ja asetusten tuntemus nousivat silti usein esiin. Opetus- ja tutkimustyöntekijöitäkin haettiin kohtuullisen runsaasti, mutta niiden tehtävien vaatimukset eivät nouse kokonaisuutena massasta esiin. Soveltuva ylempi korkeakoulu ja näyttö tutkimuksen tekemisestä oli ilmoitettu ehdoksi valinnalle.

Teknisen osaamisen ja kokemuksen lisäksi eniten arvostettiin persoonallisuustekijöitä (engl. O-other personal factors), missä korostuvat motiivit, asenteet ja ajattelutavat. Ne nousivat esiin kaikissa työpaikkaryhmissä ja laajasti ilmoituksissa, jotka tutkimuksessa oli mukana. Osittain ne menevät päällekkäin kykyjen kanssa (engl. A-abilities), jotka ovat pääosin muuttumattomia synnynäisiä ominaisuuksia, kuten sosiaaliset piirteet tai tilanteiden hahmotuskyky.

Neljä kyberalan työntekijän osaamisprofiilia tekstianalyysin avulla poimituna työpaikkailmoitusten vaatimuksista ja odotuksista:

- 1 Turvallisuuden tarjoaminen: *Ohjelmointi (Java, Perl, Python, C++), rajapinnat (API), palvelimet ja käyttöjärjestelmät (Linux, Android), Tietokannat (SQL), Security Information and Event Management (SIEM), ketterät projektimetodit, suomen ja englannin kieli, asiakasymmärrys, vuorovaikutustaidot, asenne, kokemus*
- 2 Operointi ja ylläpito: *Palvelimet ja käyttöjärjestelmät (Microsoft, Linux), tietoliikenne, palomuurit, tunkeutumisenestojärjestelmät, tietoturvan hallinnointi ja ylläpito, sertifikaatit (CISSP, CISA, CIPP/E), standardit/ohjeistukset/lait (ISO27001, Vahti, Katakri, GDPR), suomen ja englannin kieli, koulutus ja tutkinnot, joustavuus, vuorovaikutustaidot, projektointi*
- 3 Valvonta ja hallinnointi: *Security Information and Event Management (SIEM), pääsyn- ja riskien hallinta, suomen ja englannin kieli, koulutus, projektointi, johtaminen, kokemus, innovaatiot, tutkimus*
- 4: -
- 5 Analysointi, 6 Suojaaminen ja puolustus, 7 Tutkinta: *Tutkintaan liittyvä teknologia ja analysointi, kyberrikostorjunta, palomuurit, tunkeutumisenestojärjestelmät, haittaohjelmat, penetraatiotestaus, salausten purku, verkon valvonta, ohjelmointi, palvelimet, standardit/ohjeistukset/lait (ISO27001, Vahti, Katakri, GDPR), yhteistyökyky, oma-aloitteisuus, halu kehittyä, ongelmienratkaisukyky, koulutus, kokemus, johtaminen, suomen, ruotsin ja englannin kieli*

Yhdistettynä kyberalan työntekijän profiili muodostuu seuraavista ominaisuuksista:

- Tiedot: *matemaattisesti kyvykäs ja kielitaitoinen, ymmärtää liiketoiminnan vaatimukset, pystyy osoittamaan tiedonlähteen (koulutus, sertifikaatit, työhistoria)*
- Taidot: *ohjelmointitaitoinen sekä osaa tietojärjestelmien ja -verkkojen hallinnan sekä suojaamisen, valmis kouluttautumaan*
- Kyvyt: *oma-aloitteinen ja vuorovaikutustaitoinen*
- Muut persoonallisuustekijät: *motivoitunut sekä omaa analyttisen ja systemaattisen ajattelutavan*

4.2 Rekrytoijien haastattelut

Tutkimuksessa haastateltiin viisi henkilöä, jotka ovat olleet mukana vuonna 2018 kyberalan työvoiman rekrytointiprosessissa. Haastattelujen kautta muodostui kuva kyberalan työpaikkoja hakeneiden henkilöiden soveltuvuudesta työnantajan tehtävään; hakijoiden koulutuksen tasosta; rekrytoijien näkemys kyberalan koulutuksen tasosta ja muutostarpeesta; rekrytoinnin haastavuudesta tällä hetkellä sekä työnantajan mielestä tärkeimmistä työnhakijan ominaisuuksista, jotka alalle tulevalle tulisi olla. Viiden haastattelun otanta on riittävä

ja sen perusteella saadaan kartoitettua tutkittua aihetta. Haastattelujen aikana muodostui yhtenäinen kuva tutkittuun aiheeseen.

Haastattelujen tulokset kertovat työvoiman saatavuuden vaikeudesta sekä hakijoiden osaamisesta ilmenevistä puutteista. Näkökulmasta riippuu, voidaanko puhua työvoimapulasta. Haastateltavat arvioivat työvoiman saatavuuden kokonaisuutena vaikeaksi (ka 2,2) asteikolla 1-5 (1 Erittäin vaikeaa - 2 Vaikeaa - 3 Melko helppoa - 4 Helppoa - 5 Erittäin helppoa). Seniortason osaajien rekrytointi nähtiin erittäin vaikeaksi ja siinä nousi esiin määrällinen puute. Juniortason osaajia oli määrällisesti selvästi paremmin saatavilla. Näidenkin osalta rekrytointitilanne nähtiin pääosin korkeintaan melko helppona. Juniortason osaajien perehdytys ja koulutus vaativat aikaa ja resursseja, jotta haluttu suoritustaso saadaan ulosmitattua. Silti lähes kaikki avoimet työpaikat saatiin täytettyä. Lisäksi organisaatioiden taloudelliset resurssit ja hakijoiden palkkatoiveet olivat yksi rekrytoimisen este organisaatioissa. Soveltuvia hakijoita oli, mutta liian korkeaan hintaan. Tämä vahvistaa haastatteluissa esiin tullutta havaintoa senior-tason osaajien määrällisestä pulasta, mikä nostaa työn hintaa. Siten rekrytointiongelma lienee täsmällisin termi kuvaamaan tämän hetken tilannetta työmarkkinoilla. Kaikki haastateltavat organisaatiot sanoivat avaavansa lisää työpaikkoja hakuun varmasti tai todennäköisesti haastattelua seuraavan 12 kuukauden aikana.

Osaajiahan Suomesta löytyy, mutta kaikki on työelämässä jo mukana. - - Jos me palkataan joku asiantuntija, se on joltakin toiselta yritykseltä pois.

Rekrytoivat yritykset kertoivat panostaneensa aiempaa enemmän hakuprosessiin ja siinä käytettäviin keinoihin, jotta soveltuvia hakijoita saatiin. Tämä väivannäkö tuotti myös tuloksia. Yritykset käyttivät suorien rekrytointimenetelmien lisäksi epäsuoria rekrytointimenetelmiä sekä erilaisia keinoja erottuakseen työmarkkinoilla. Perinteiset työpaikkailmoitukset olivat kaikkien yritysten pohja rekrytoinneissa. Eri hakukanavien käytöllä tehostettiin näkyvyyttä. Useissa eri kanavissa julkaisemisella sekä ostamalla näkyvyyttä rekrytointikanavissa haettiin suurempaa huomiota. Myös yhteistyö rekrytointikanavien kanssa, kuten erilaiset koulutuksen kautta työhön ohjelmat, olivat lisääntyneet. Suorahaku oli osalla käytössä, mutta sen ei laajasti koettu olevan ensisijainen menetelmä. Suorahakua tehtiin omilla resursseilla pääosin kohdistettuna ennalta tunnettuihin osaajiin. Osa haastatelluista oli käyttänyt tai harkitsi head hunting -yritysten käyttämistä. Sosiaalisen median käyttö oli jollakin tavalla osa kaikkien rekrytointiprosessia. Sosiaalinen media oli joko tärkeä osa kohderyhmän huomion hakemisessa tai ainakin yksi mainoskanava organisaatiolle. Sosiaalisen median tehoa tai vaikutusta rekrytointiprosessissa ei organisaatioissa kuitenkaan selkeästi pystytty osoittamaan tai mittaamaan. Silti sosiaalisessa mediassa näkyminen on imagon kannalta toivottavaa.

Koska näkyvyyttä ja sopivia hakijoita voi olla vaikea tavoittaa, on välillä tärkeä erottautua ja saada huomiota poikkeavilla hakemuksilla. Näitä voivat olla erottuva kielenkäyttö, kuten murteen hyödyntäminen tai kryptiset viestit, jotka aukeavat vain asiaan perehtyneille. Samoin catch the flag -tehtävät, jonka

ratkomalla pääsee suoraan tiettyyn pisteeseen rekrytointiprosessia. Kaksi haastateltua organisaatiota viidestä kertoi käyttäneensä viime aikoina näitä tai vastaavia keinoja erottuakseen työmarkkinoilla.

Epäsuorat rekrytointimenetelmät ovat olennainen osa kokonaisuutta. Rekrytointikilpailussa oman organisaation imagon ylläpito on tärkeää. Kun haluttu työnhakija on tilanteessa, missä hän voi valita työnantajan, mielikuva organisaatiosta ja mitä se edustaa, nousee tekijäksi, joka vaikuttaa suuresti päätöksentekoon. Imagon ylläpito on jatkuva prosessi, jossa sosiaalisella medially on haastattelujen perusteella selkeä roolinsa. Kaksi neljästä yksityisen sektorin organisaatiosta luottivat oman maineen olevan kilpailuvaltti kyberalan osaajamarkkinoilla. Myös potentiaalisten työntekijöiden kohtaamisella henkilökohtaisesti on osa positiivista näkyvyyttä. Kaksi viidestä haastatellusta nosti selkeästi esiin rekrytointimessujen roolin organisaation imagon luomisessa sekä yhtenä tärkeänä rekrytointikanavana. Haastatteluissa esille nousseet rekrytointitapahumat olivat oppilaitosten järjestämiä tai muuten nuorille suunnattuja. Siellä organisaatioilla on mahdollista saada näkyvyyttä tulevaisuuden osaajien parissa, kertoa omasta tekemisestä ja millaista osaamista heidän työssään tarvitaan. Siten organisaatiot voivat myös pieneltä osin ohjata opiskelijoiden opintoja kohdistumaan siihen osaamispulaan, mitä organisaatioilla on nyt ja lähitulevaisuudessa.

Haastatteluvastaukset tukevat ISACA:n esiin nostamaa teknistä tulokulmaa osaamisessa, mutta huomioivat muiden ominaisuuksien merkityksen työssä menestymiselle ja yrityksen arvolle. Dawsonin ja Thomsonin kybertyöntekijän ominaisuuksista kaikki vastaajat nostivat teknisen kyvykkyyden yhdeksi kolmesta tärkeimmästä ominaisuudesta. Se oli tärkein ominaisuus kuitenkin vain yhdellä vastaajista. Työnhakijoiden ihmissuhdetaitoja pidettiin korkeassa arvossa, mutta vastaukset jakautuivat tiimipelaamisen ja kommunikointitaitojen kesken, jotka molemmat koettiin välttämättömiksi organisaation omassa työyhteisössä sekä asiakaskohtaamisissa. Haastateltavat organisaatiot eivät nostaneet isänmaallisuuden tuntoa tai yrityksen arvopohjaa mitenkään merkittäväksi tekijäksi hakijoiden perusteena hakeutua töihin organisaatioon. Julkisella sektorilla ideologinen työpaikan valinta huomioitiin lähinnä työtehtävien kautta, joita yksityisellä sektorilla ei pääse toteuttamaan. Substanssiosaaminen oli kuitenkin kokonaisuutena kaikilla haastateltavilla erittäin suuressa roolissa, kun rekrytoidaan uutta henkilöä. Silti haastatteluvastauksissa todettiin, että pelkkä osaaminen ei nykyään riitä. Henkilökohtaiset ominaisuudet ovat tärkeä osa organisaation yhteistoimintaa ja asiakkaan kohtaamista. Organisaatiot etsivät ”hyvää tyyppiä”, jolla on kyky omaksua uutta tietoa.

Haastattelujen kautta saatua informaatiota verratessa NCWF-kehityksen seitsemään kategoriaan, ei voida selkeästi osoittaa, missä työvoimapula näkyisi eniten. Kaikissa kategorioissa voidaan havaita samat rekrytointiongelmat. Osaamis- ja kokemustason puutteet näkyvät haastattelujen kautta saadun informaation mukaan suurimmin Operointi ja ylläpito -kategoriassa, missä kaivataan ennen kaikkea seniortason hakijoita. Määrällisesti eniten vajetta on Turvallisuuden tarjoaminen -kategoriassa lähinnä laajemman ohjelmointiosaajien

puutteen vuoksi, joka heijastuu myös kyberalalle. Opetuksen puutteet näkyvät erikoisaloissa, joihin ei Suomessa ole suoraan pätevöittävää koulutusta. Näissä näkyvät Kerääminen ja operointi sekä Tutkinta -kategoriat. Vaikka haastateluissa todettiin mm. projektiosaamisen olevan kysyttyä, hallinnollisen työvoiman, eli Valvonta ja hallinnointi -kategorian, saatavuutta ei koettu laajemmin ongelmalliseksi. Ylemmän tason johtamisosaamista on saatavilla ja toteutustason työntekijöiden edellytetään olevan itseohjautuvia omassa työssään.

Tarkemmin eriteltynä haastateltujen organisaatioiden odotukset osaamisesta voidaan jakaa kolmeen ryhmään. Ensimmäisenä ohjelmistokehitys ja ohjelmointi, joissa erityisesti back end sekä reverse ohjelmointitaitoja ja rajapintojen osaamista tarvitaan. Toisena verkkoturvallisuus, kuten palomuurit ja SIEM-palvelut sekä palvelimien kovennus. Kolmantena verkkotekniikka, missä korostuvat uudet tekniikat sekä uusien ja vanhojen tekniikoiden yhdistäminen, esimerkiksi pilvipalvelut, IoT ja mobiiliverkot. Osaaminen vastasi melko hyvin (ka 3,1) asteikolla 1-5 (1 Erittäin huonosti - 2 Huonosti - 3 Melko hyvin - 4 Hyvin - 5 Erittäin hyvin) haastateltujen odotuksia. On merkittävää kuitenkin huomioida useamman haastateltavan maininta lasketusta odotustasosta.

Koulutuksen kehittämiseen liittyvä palaute tuo ilmi laadullisen puutteen; koulu ei valmista suoraan työelämään. Tämä yritysten kokemaa kuilu johtaa määrälliseen puutteeseen, koska osalta hakijoista puuttuu oleellisia kykyjä. Haastateltavat arvioivat koulutuksen vastaavan odotuksia melko hyvin (ka 3,0) asteikolla 1-5 (1 Erittäin huonosti - 2 Huonosti - 3 Melko hyvin - 4 Hyvin - 5 Erittäin hyvin). Vastaukset jakaantuivat tasaisesti 2-4 välille. Sen sijaan perustelut erosivat vastaajien kesken merkittävästi. Yhdessä ääripäässä todettiin, että soveltuvaa koulutusta ei Suomessa ole lainkaan, keskikastissa koettiin puutteita matemaattisten taitojen opetuksessa sekä koulutuksen hitaudessa tarpeeseen nähden ja toisessa ääripäässä koulutuksen tason koettiin olevan hyvä, mutta määrällisesti osaavia henkilöitä valmistuu liian vähän. Myös koulutuksen tason osalta haastateltavat olivat laskeneet odotuksia. Opiskelun jälkeen tulisi päästä työelämään kasvamaan kohti huippuasiantuntijuutta ja kouluttautua eteenpäin. Työnantajien tarve on voimakkaammin korkean asiantuntijuuden vaativissa, ns. seniortason, tehtävissä.

Me ei koulusta saada valmiita osaajia, me saadaan hyviä aihioita. - - Kouluttamalla tai sitten työelämässä oppimalla saadaan heistä sitten hyviä alan ammattilaisia.

Yleisesti koulutukseen liittyvä palaute oli yliopiston osalta puute käytännön osaamisesta. Teoreettinen lähestymistapa teknisessä ympäristössä rajoittaa työelämässä tarvittavien perustaitojen oppimista. Teoria pitäisi työelämässä pystyä linkittämään käytännön toimintaan. Ammattikorkeakoulujen osalta käytännön tekninen valmius nähtiin hyvänä. Lähtökohta työelämään, soveltuvan ammattikorkeakoulun käyneillä hakijoilla, on hyvä ja työssä oppimisen aloittaminen on saumattomampaa. Ammattikorkeakouluilta toivottiin pääosin nykyistä laaja-alaisempaa otetta opetukseen. Opetukselta yleisesti odotettiin korkeampaa ja tasaisempaa laatua. Samaan suuntaan viittaa myös Kyberalan osaaminen Suomessa -selvitys työvoiman tarpeesta, jonka mukaan nykyinen koulutus ei johda

riittävän laajaan tai edistyneeseen osaamiseen (Pelkonen ym., 2016). Haastateluista nousi esiin nopeasti muuttuvaan alaan liittyvä viive koulutuksen ja tarpeen välillä. Koulutus tulee myöhässä tarpeeseen nähden. Tähän on erittäin vaikea löytää helppoja ratkaisuja. Tiivis yhteistyö yritysmaailman kanssa voisi tuottaa tuloksia ja vähentää viivettä.

Korkeakoulujen ja kyberalan organisaatioiden yhteistyö nousi vahvasti esiin, kun mietitään opetuksen ja osaamistason kehittämistä. Rekrytoivilla organisaatioilla on tarve ja halu saada ääni kuuluvien opetuksessa ja tutkimusten tekemisessä. Vierailijaluennot ja kyberalan organisaatioiden osaamistarpeen huomioiminen opetustarjonnassa nähtiin tärkeäksi. Samalla tämä koettiin haastavaksi toteuttaa korkeakoulujen vaisun innostuksen vuoksi. Lopputöiden aiheita haastateltavat organisaatiot olivat tarjonneet ja olivat edelleen halukkaita tarjoamaan opiskelijoille. Samoin harjoittelupaikkoja ollaan valmiita tarjoamaan opiskelijoille mahdollisuuksien mukaan. Koska harjoittelupaikkojen tarjontaan liittyy osin varautuneisuus tai epävarmuus, oppilaitosten tulisi olla aktiivisia, avata kontakteja ja selventää harjoittelun toteuttamisen ehtoja. Tämä helpottaisi opiskelijoiden harjoittelupaikkojen saantia ja lieventäisi organisaatioiden kynnystä tarjota harjoittelupaikkoja.

Työnantajien tarpeeseen voi vastata useammalla tavalla. Oppilaitosten tulee suunnitella tarkkaan oma tarjonta ja varmistaa opetuksen laatu. Myös selkeä linjavalinta kyberalan opetuksen suunnassa ja sen markkinointi rekrytoivien organisaatioiden suuntaan toisi ryhtiä muuten epämääräiseksi jäävään kyberkoulutukseen; mitä taitoja juuri tästä oppilaitoksesta valmistuneella voidaan olettaa olevan. Samalla vahvempi ja aktiivisempi yhteistyö muiden oppilaitosten sekä yritysten kanssa parantaisi koko alan kehitystä. Vaivaton ja mahdollisimman pienellä byrokratialla toimiva malli työharjoitteluun edesauttaisi organisaatioiden innokkuutta tarjota harjoittelumahdollisuuksia.

Kyberalan organisaatioiden tulisi olla aktiivisia omalta osaltaan oppilaitosten suuntaan ja esittää oma näkemyksensä, mihin suuntaan opetuksen tulisi kohdentua. Samalla organisaatioiden tulisi mahdollistaa nykyisellä työvoimalla mahdollisimman hyvät puitteet ja resurssit kouluttautua edelleen, jotta työntekijät voivat kehittyä vaativampiin tehtäviin. Uudelleen kouluttautuminen ja jatkokoulutus korkeakouluissa tai sertifikaattikoulutuksissa on välttämätöntä kybertyövoiman kehitykselle ja osaamisvajeen paikkaamiselle.

Opiskelijoiden itse tulisi suunnitella omat opinnot tarkemmin ja kohdentaa osaamistaan. Syvempi osaaminen jostakin kyberturvallisuuden osasta on työnantajien toiveena. Työnhakijoilta edellytetään haastattelujen perusteella ainakin yhden osa-alueen syvää asiantuntemusta sekä yhden tai useamman muun osa-alueen hyvää tietämystä. Tämä johtui pääosin kahdesta seikasta: työtehtävässä menestyminen edellyttää laajempaa tietämystä alasta sekä organisaatiolla ei ole resursseja tai halua palkata useampaa henkilöä hoitamaan määriteltyjä työtehtäviä.

Nykyisen työvoiman tulee jatkuvasti pysyä kehityksen mukana. Se vaatii paljon resursseja, joita työnantaja ei aina tarjoa. Eteneminen omalla uralla vaatii myös vapaa-ajan uhraamista uuden oppimiseen. Kaikki haastateltavat kokivat

työnhakijan oman aktiivisuuden, harrastuneisuuden ja alan seuraamisen oleelliseksi osaksi uuden työntekijän valintaa tehtäessä sekä tärkeänä osana oman olemassa olevan henkilökunnan kehitystä. Kaikki olivat myös valmiita tukemaan jollakin tavalla omien työntekijöiden ammatillista kehitystä tarjoamalla mm. aikaa tai oppimista tukevaa materiaalia.

Tällä alalla harrastuneisuus ei oo enää niin korkealla tasolla, kuin se oli aikaisemmin. Tästä on tullut mun näkökulmasta ihan tavallinen ammatti.

Haastateltavien vastaukset olivat pääosin melko yhtenäisiä. Niistä ei noussut selkeitä eroja esille. Vivahde-eroja sen sijaan löytyi työvoiman saatavuuteen liittyen. Tilanne työvoiman saatavuudessa itsessään ei kenelläkään vaikuttanut olevan sen parempi, mutta näkökulma ja organisaation taloudellinen valmius maksaa osaamisesta toivat eroja. Odotusarvo oli yksi tekijä, joka muodosti numeraalisiin vastauksiin eroavaisuutta. Osa koki todellisen saatavuuden huomommaksi, kuin arvosana osoittaa, koska arvosana oli suhteutettu aikaisempien kokemusten kautta hyvin matalalle tasolle. Madaltuneet odotukset käänsivät avosanan kahden vaihtoehdon välille ja siten nostivat annettua arvosanaa 0,5-1 verran. Toinen ero organisaatioiden välillä oli taloudelliset resurssit ja niiden käyttö. Osa sai hyviä hakijoita, mutta ei ollut valmis palkkaamaan heitä liian korkea hinnan vuoksi. Ne organisaatiot, jotka olivat valmiimpia maksamaan, olivat pääosin hieman tyytyväisempiä työvoiman saatavuuteen.

Työvoiman tarjonta vastaa työnantajien odotuksia huonosti. Seniortason työntekijät voivat valita työpaikkansa kovan kilpailun vuoksi ja palkkatoiveet ovat korkealla. Juniortason osaajia on hieman paremmin saatavilla. Heidän osaltaan työnantajat odottavat koulutuksen tuottavan valmiimpia osaajia. Nyt rekrytoinnin jälkeen tarvitaan perehdytystä ja pitkä työssäoppimisjakso. Yleisesti ottaen osaajia tarvitaan määrällisesti lisää.

TAULUKKO 2 Haastattelujen tulosten tiivistelmä tutkimuskysymysten osalta

Miten nykyinen työvoiman tarjonta vastaa työnantajan näkökulmasta kyberalan työvoiman tarvetta			
Aihe	Keskiarvo	Hajonta	Kooste kommentteista
Saatavuus vuonna 2018	2,2	0,5	Sattuman kautta on tullut hyviä hakijoita. Hakijoilla oli liian vähäinen osaaminen, tai palkkapyyntö oli liian suuri. Juniortason osaajia hyvin saatavilla. Seniortason osaajien saatavuus ja pitäminen firmassa on vaikeaa.
Saatavuus yleisesti	2,3	0,5	Osaajia on vähän ja he ovat sitoutuneita nykyiseen työhönsä. Ideologia ja raha ovat ainoat keinot houkutellessa vaihtamaan tehtävää. Pieni työmarkkina, mikä on tällä hetkellä kuuma.
Osaaminen	3,1	1,5	Melko hyvin, mutta johtuu lähinnä siitä, että odotukset eivät olleet korkealla. Huonosti. Vahvoja osaajia oli, mutta yleensä vain yksi osa-alue oli vahva. Hyvin saatu sopivia hakijoita, mutta tarjonta voisi olla vielä laajempaa. Melko hyvin, koska odotukset ovat olleet matalat tai aiempaa realistisemmat.
Koulutus	3,0	2,0	Ei ole alan täsmäkoulutusta Suomessa. Koulutus tulee tarpeen perässä. Sisältö vastaa tarvetta, mutta määrä ei ole riittävä.
Esteet työvoiman saatavuudessa			Koulutuksen laatu. Koulutusmäärä. Työvoima siirtyy tehtävästä toiseen vain korkeaa palkkaa vastaan.
Miten kyberalan koulutusta tulisi mukauttaa vastaamaan paremmin työnantajan tarvetta?			
Aihe	Kooste kommentteista		
Koulutuksen muutostarpeet	<p>Vahvistaa tekniikan perusosaamista ja ymmärrystä.</p> <p>Syventää käytännön osaamista.</p> <p>Kehittää IoT laitteiden tietoturvan koulutusta ja laitteiden penetraatiotestausta.</p> <p>Oppilaitosten tulisi olla trendien edelläkävijöitä, joiden kautta saadaan uutta osaamista.</p> <p>Pitäisi tehdä enemmän yhteistyötä mm. tarjota lopputöiden aiheita sekä pitää luentoja ja opetusta oppilaitoksissa.</p> <p>Lopputöiden tulisi olla laadukkaita ja tehty tarpeeseen/toimeksiannosta.</p> <p>Tietoturvan perusteita tulisi kouluttaa aktiivisesti, jonka kautta tulisi kiinnostus ja riittävä osaaminen/uskallus lähteä opiskelemaan lisää.</p> <p>Opetetaan muitakin kuin teknisiä taitoja, kuten liiketoiminnan ymmärrystä.</p> <p>Pääosin ohjelmistokehitys ongelmana, kuten turvallinen ohjelmointi.</p> <p>Virtualisointi, Linux -osaaminen ja tietoturva ovat osaamiskapeekoita.</p> <p>Verkostoituminen esim. YAMK koulutuksen kautta.</p>		
Millaista työvoimaa kyberalalle haetaan nyt?			
Aihe	Kooste kommentteista		
Hakijoiden kokemus, koulutus ja persoonallisuus	<p>Henkilöitä, joilla on valmiudet kouluttautua sekä tekninen tausta.</p> <p>Senior tason osaajia, joilla on tekninen tausta sekä kokemusta alalta.</p> <p>Senior- ja juniortason osaajia, joilla on tekniset taidot.</p> <p>Haetaan monen eri tason osaajia.</p> <p>Henkilöitä, jotka harrastuneisuudella osoittavat mielenkiintoa alaa kohtaan.</p>		
Hakijoiden tekninen osaaminen	<p>Ohjelmistokehitys, turvallinen ohjelmointi, back end ja reverse koodaus sekä rajapinnat.</p> <p>Verkkoturvallisuus, kuten palomuurit ja SIEM-palvelut sekä palvelimien kovennus.</p> <p>Verkkotekniikka, erityisesti uudet tekniikat sekä uusien ja vanhojen tekniikoiden yhdistäminen, pilvipalvelut, IoT ja mobiiliverkot.</p>		
Ominaisuudet Dawsonin & Thomsonin jaottelun mukaan	<p>Tekniset kyvyt *5</p> <p>Jatkuva opiskelu *3</p> <p>Tiimipelaaja *2</p> <p>Systemaattinen ajattelutapa *2</p> <p>Kommunikaatiotaidot *2</p> <p>Sosiaaliset kyvyt *1</p>		

4.3 Korkeakouluopetuksen selvitys ja kysely

Koulutuskyselyn kautta korkeakouluja pyydettiin antamaan tilannekuva heidän nykyisestä ja tulevasta kyberalan koulutuksesta. Sen lisäksi korkeakouluilta kysyttiin mielipidettä koulutuksen soveltavuuteen työmarkkinoiden näkökulmasta.

Kyselyn perusteella oppilasmäärät ovat pääsääntöisesti vakiintuneet tietylle tasolle. Aalto yliopisto, Helsingin yliopisto sekä Centria Ammattikorkeakoulu pyrkivät kasvattamaan sisään otettavien ja valmistuvien oppilaiden määrää. Turun yliopisto koki painetta kasvattaa kryptografiaan suuntautuvien oppilaiden määrää. Muilla oppilaitoksilla sisäänottomäärät pysyivät entisellään.

Kyberopetuksen opetustarjonta laajenee oppilaitosten vastausten perusteella alan kehityksen ja tarpeen mukaan. Yleisesti suuntaus on laajentaa opetusta muiden koulutusalojen kanssa tai suunnata koulutusta omille vahvuusalueille. Kyberala tulee kiinteäksi osaksi muuta IT-alan koulutusta sekä entistä vahvemmin sivuaineena muiden alojen opiskelijoille. Verkkokurssien määrä todennäköisesti tulee entisestään lisääntymään ja esimerkiksi Helsingin yliopiston kaikille avoimet verkkokurssit ovat olleet hyvin suosittuja.

Kyberalan opetuksen keskittäminen tietyille osa-alueille ei ole laajasti suunnitelmassa. Osa oppilaitoksista tarjoaa kyber- tai tietoturva-alan opetusta perustasolla kaikille opiskelijoille. Kyberalaan keskittyneet oppilaitokset pyrkivät tarjoamaan mahdollisimman laajan kirjon alan opetusta. Osa oppilaitoksista omaa vahvaa osaamista tietyiltä osa-alueilta ja se näkyy erikoistumisena, jota halutaan kehittää edelleen. Näistä esimerkkeinä Turun yliopiston kryptografia, Jyväskylän yliopiston laajeneva tiedusteluopetus sekä Aalto yliopiston hallinnollinen tietoturva sekä alkava liiketoimintaosaamisen yhteistyö Kauppakorkeakoulun kanssa.

Kyberalan koulutuksen ohjattuun keskittämiseen oppilaitokset suhtautuvat pääosin kielteisesti. Siitä huolimatta vastaukset osoittavat, että osaamiskeskittymiä on jo muodostunut ja niillä aloilla kilpailu Suomen kokoisessa markkinassa ei ole mielekästä. Yhteistyö ja yhdessä koordinointi toistuvat vastauksissa. Yhteistyön kautta oppilaitokset voivat yhdistää vahvuuksiaan ja siten luoda uusia innovaatioita ja tutkimusideoita poikkitieteellisesti. Osaamisen keskittäminen nähdään myös vahvuutena, jolla voidaan luoda parempaa opetusta ja korkeatasoisempaa tutkimusta. Vastauksissa näkyy kolme suuntausta: 1) Kyber on kaikkialla, joten opetusta tarvitaan kaikkialla. 2) Keskittäminen koetaan uhaksi omalle toiminnalle, erityisesti, jos oma kyberopetuksen suunta ja asema ei ole vielä vakiintunut. 3) Keskittäminen koetaan vahvuutena, jolloin isommissa yksiköissä saadaan tehtyä laadukkaampaa tutkimusta. Suuntaus korreloi oppilaitoksen tämän hetken asemaa kyberalan koulutuksen järjestäjänä. Vakiintuneet toimijat ovat myönteisempiä keskittämiseksi. Kyberalan suuntaa hakevat oppilaitokset ja uudet kyberopetusta tarjoavat tulokkaat suhtautuvat kielteemmin keskittämiseen.

Oppilaitosten mielestä koulutusta vastaa hyvin työmarkkinoiden tarpeita. Tästä todisteena oppilaitokset käyttävät yrityksistä saatua palautetta sekä valmistuneiden tai kesken opintojen työllistyneiden oppilaiden tilastoja. Oppilaitokset näkevät kuitenkin haasteena nopeasti muuttuvan ympäristön, johon on vaikea reagoida. Kyberala ja tekniikka kehittyy, joten muutoksen perässä on vaikea pysyä. Samalla tulisi pystyä tarjoamaan uusien ja nousevien tekniikoiden koulutusta, jota työnantajat toivovat. Opetuksen tulee olla joustavaa ja mukautua ajan myötä. Tutkimuksen ja kehityksen tulee suuntautua enenevässä määrin nouseviin trendeihin. Muina laadullisina huomioina nousivat esiin oppilaitoksien liian pienet resurssit ja koulutusmäärä sekä täydennyskoulutuksen tarve.

Vaikka opiskelijat työllistyvät hyvin, koulutuksen vastaavuus työmarkkinoiden vaatimukseen on silti laitettava tarkempaan tarkasteluun. Työmarkkinoilla on suuri pula alan osaajista ja koulutusta on ollut suhteellisen vähän aikaa tarjolla, joten työmarkkinat eivät ole kylläisiä. Tästä osoituksena voi ottaa vaikka kesken opiskelun töihin siirtyvien määrän. Työnantajat ottavat sen min-kä saavat, jopa kesken koulutuksen varmistukseksi edes tyydyttävän osaamistason rekrytointitilanteessa. Oppilaitosten ei siis tule tyytyä nykytilanteeseen vaan jatkuvasti pyrkiä mukautumaan ja kehittämään toimintaansa. Koulutuksen tasoa ja onnistumista tulisi työllistymisen sijaan mitata entistä enemmän työnantajapalautteista sekä käydä avointa keskustelua työnantajien kanssa.

4.3.1 Koulutuksen tulevaisuuden näkymät

Yhdistettäessä kaikki tulokset: työpaikkailmoitukset, työnantajien haastattelut sekä korkeakoulujen kyselyt nähdään, ettei nopeita ratkaisuja ole tiedossa. Työpaikkoja on melko runsaasti auki ja laajalti eri kyberalan sektoreilta. Työnantajan mielestä tarjonta on madaltuneista odotuksista huolimatta melko heikkoa tai korkeintaan melko hyvää. Oppilaitokset kuitenkin näkevät oman roolinsa vahvana vedoten mm. työllistymislukuihin. Ne eivät myöskään kyselyn mukaan laajasti ole lisäämässä koulutettavien määriä. Siten voidaan nähdä, että oppilaitokset ovat tyytyväisiä omaan toimintaansa, mutta eivät mittaa todellista suorituskykyä sen perusteella, miten oppilaiden osaaminen suhteutuu työnantajan vaatimukseen. Määrällisesti ne asettavat riman omien resurssien sekä opiskelemaan hakevien hakijoiden määrän mukaan. Ei ole oppilaitoksen näkökulmasta mielekästä laajentaa, jos aloituspaikkoja ei saada täytettyä riittävän laadukkailla hakijoilla ja omat panostukset resursseihin menisivät osin hukkaan.

Koulutettavia voi olla vaikea löytää, koska ikäluokat pienenevät ja IT-alalle ei ole suurta imua tällä hetkellä. Toisaalta kyberala vetää hakijoita määrällisesti hyvin. Tätä selittää osin jatkokoulutettavat henkilöt. Olevan työvoiman jatkokouluttaminen ei lisää määrällistä joukkoa, joka täyttäisi kyberalan avoimia työpaikkoja. Sen sijaan se lisää osaajien kykyä, jolloin heillä on mahdollista siirtyä vaativampiin tehtäviin, missä suurin pula työntekijäistä tällä hetkellä on. Jäljelle jää silti määrällinen tarve. Tähän tarpeeseen pitäisi kouluttaa työvoimaa muilta aloilta tai työttömistä työnhakijoista.

Työnhakijoille uudelleen kouluttautuminen voi olla riski. Taloudellinen menetys nykyisestä työstä opiskelijaksi siirtymisessä tai työttömyystukien suhde opintotukeen voivat vaikuttaa halukkuuteen hakeutua koulutukseen. Joka tapauksessa työnhakijan tulee jatkuvasti pysyä ajan hermolla mihin maailma, tekniikka ja työvoiman tarve kehittyy sekä olla valmis uhraamaan omaa aikaa ja energiaa itsensä kouluttamiseen. Koulutuksen ei tarvitse olla tutkinto tai sertifikaatti, mutta työnhakijan tulee olla valmis omaksumaan uutta ja nähdä muutokset mahdollisuuksina.

5 JOHTOPÄÄTÖKSET

Tutkimus osoittaa selvästi soveltuvan työvoiman puutteen kyberalalla Suomessa. Työnantajien odotukset hakijoiden osaamisen tasosta eivät täyty. Lyhyellä aikavälillä tulisi keskittyä jatko- ja muuntokoulutukseen ja sen kautta uuden ja osaavamman työvoiman kehittämiseen alalle. Koulutusta tulee laajentaa kautta linjan ja lisätä alan houkuttelevuutta, että saadaan riittävästi hakijoita ja siten nostettua oppilaitosten koulutusmääriä. Siten voidaan vastata määrälliseen vaajeeseen pitkällä aikavälillä. Työnantajien tulee tarjota työntekijöille mahdollisuuksia lisätä osaamista tukemalla oppimista työpaikoilla.

Kyberalan koulutus elää edelleen kehittymisvaihetta. Opintotarjonta muuttuu jatkuvasti ja hakee omaa paikkaansa. Eri oppilaitosten suuntauksissa näkyvät voimakkaasti digitalisoitumisen vaikutukset ja tietotekniikan opetus tulee osaksi useita muita aloja. Koska tieto kulkee paljolti avoimen tietoverkon läpi, informaation turvaaminen on yhä kriittisempää. Siksi kyberturvallisuus on keskiössä joka alalla. Kyberturvallisuusalan tulee samaan aikaan yleistyä, erikoistua ja kasvaa. Se asettaa valtavan haasteen koulutukselle.

Samalla, kun koulutus hakee paikkaansa, työvoiman riittävyys on tutkimustuloksen perusteella pulma alalla. Tulokset tukevat ISACA:n kansainvälistä tutkimusta kyberalan työvoiman heikosta saatavuudesta (ISACA, 2018) sekä mediassa esiin nostettuja ennusteita kyberalan sekä koko IT-alan työvoimapuulasta (mm. Mäntylä, 2017; Tiihonen, 2018). Erityisesti pulaa on alan huippuosaamisesta sekä osaamisesta erikoisaloille, joille kyber laajentuu. Puutteita havaitaan perustason matemaattisessa osaamisessa ja ohjelmointitaidoissa sekä useilla eri osa-alueilla, joille kaivataan korkeampaa osaamista. Laadukasta teknologista osaamista tarvitaan voimakkaimmin pilvipalveluiden, turvallisen ohjelmoinnin ja rajapintojen tuntemuksessa sekä korkean turvatason palvelinympäristöjen osaamisessa. Työnantajat odottavat koulutuksen tuottavan valmiimpia osaajia. Erityisesti uusien tekniikoiden osalta oppilaitoksilta odotetaan edelläkävijyyttä. Perustietämys on hyvä, mutta rekrytoinnin jälkeen vaaditaan perehdytystä ja pitkä työssäoppimisjakso, että uusista työntekijöistä muodostuu osaava taloudellisesti tuottava resurssi. Lisäksi määrällinen puute on huomattava, mikä pakottaa työnantajat rekrytoimaan alan opiskelijoita jo ennen val-

mistumista. Työnantajat haluaisivat osallistua ja saada äänensä kuuluviin vahvemmin oppilaitosten suuntaa ja päästä vaikuttamaan alan opiskelijoiden kehitykseen jo ennen rekrytoimista.

Nykyinen osaava työvoima on töissä ja heitä voi olla vaikea saada vaihtamaan työpaikkaa ilman merkittävää taloudellista houkutusta. Huippuosaajia on määrällisesti liian vähän markkinoiden tarpeisiin nähden. Harrastuneisuus ja tiedon jatkuva päivitys nousee entistä suurempaan arvoon olevan työvoiman ja uusien hakijoiden osalta. Kyberalan työntekijöiden tulee olla aktiivisia ja pysyä mukana alan muutoksissa oma-aloitteisesti ja myös ilman työnantajan panosta. Kokonaisuutena työnantajat odottavat koulutukselta laadullisesti ja määrällisesti korkeampaa tasoa. Hakijoiden osaamistason odotusarvoa on laskettu, ja toiveena on jatkossa saada hakijoita, joilla on perusymmärrys kyberalasta sekä syväosaamista joltakin keskeiseltä kyberalan alueelta. Työvoiman tarjonta siten vastaa työnantajien odotuksia huonosti.

Kyberalan opiskelijoiden ja työelämässä olevan työvoiman tulisi kohdentaa omaa osaamista ja erikoistua. Tässä auttaa koulutuksen aikainen suunnittelu sekä urapolun luominen itselle. Tekniset taidot tulisi olla keskiössä suurimmalla osalla, vaikka kysyntää on myös hallinnollisessa tekemisessäkin, kuten projektinnissa ja johtamisessa. Tutkimus-, kehitys- ja opetustyö näkyy myös avoimissa työpaikoissa kohtuullisena määränä. Näiden tehtävien merkitys on työpaikkojen määriä merkittävämmän alan kokonaiskuvassa, koska tutkimus-, kehitys- ja opetustyön kautta saadaan uutta tietoa ja uusia innovaatioita. Nämä ovat välttämättömiä Suomen kilpailukyvyyn ja kyberturvallisuuden jatkuvan kehityksen takaajana. Oman suuntautumisen lisäksi tulee hallita sosiaaliset taidot, erityisesti ryhmätyöskentelytaidot, sekä kehittää analysointi- ja ongelmanratkaisukykyjä, joiden avulla voi tehdä oma-aloitteisesti töitä.

Erikoistumiseen tähtäävää kyberturvallisuuden opetusta tarjoavat opintosuunnitelmien mukaan lähinnä Jyväskylän yliopisto (kyberturvallisuuden suunnittelu ja tietoturvariskien hallinta sekä kokonaisturvallisuus ja strateginen tiedustelu) (JY, 2018), Turun yliopisto (informaation hallinta sekä tiedon suojaaminen ja kryptografia) (TY, 2018), Jyväskylän ammattikorkeakoulu (tietoturva-avaavoittuvuudet sekä tunkeutumis- ja puolustautumismenetelmät) (JAMK, 2018) ja Kaakkois-Suomen ammattikorkeakoulu (tietoturva-avaavoittuvuudet sekä tunkeutumis- ja puolustautumismenetelmät) (XAMK, 2018). Korkeakoulutettavien opiskelijoiden määrä tulee saada nousemaan, koska ennuste osaajatarpeesta koko IT-alalla on suuri. Tämä ilmenee mm. Yle-uutisten julkaisemasta ennusteesta osaamisvajeen kehityksestä (Mäntylä, 2017). Muutoksen tarpeellisuuteen on herätty ja koulutusmäärien nostamista on ehdotettu elinkeinoministerille mm. vuonna 2018 Jyväskylän yliopiston informaatioteknologian tiedekunnan toimesta (Hartio, 2018).

Koulutuksen lisäämisen ja olevan työvoiman sertifikaattikoulutusten lisäksi tulisi tarjota vielä laajemmin erikoistumiseen suuntaavaa jatko-opetusta. Muunto- ja jatkokoulutusmahdollisuuksien kehittäminen tulee olla keskiössä tulevaisuudessa. Koko IT-alalle on tarve saada lisää työvoimaa, mutta perusopiskelijamäärät eivät ole kasvussa, pikemminkin päinvastoin. Kybermaailma

muuttuu niin nopeasti, että IT-alan nykyisen työvoiman osaaminen ei kaikilta osin vastaa työnantajien tämän hetkisiä vaatimuksia. Osittain siitä kertoo rekrytointivaikeudet ja samanaikainen IT-alan työttömyys. Jatkokoulutuksen tarpeeseen vastaa mm. Jyväskylän yliopiston kyberturvallisuuden maisteriohjelma (JY, 2018) sekä Jyväskylän ja Kaakkois-Suomen ammattikorkeakoulujen kyberturvallisuuden YAMK-tutkinnot (JAMK, 2018; XAMK, 2018). Samalla monet yritykset ovat ottaneet aloitteen, osin pakon edessä, ja lähteneet tarjoamaan pika-koulutuksen kautta uraa IT-alalle.

Tutkielma on otanta työnantajien mielipiteistä, jolla kartoitetaan kyberalan työvoiman tarvetta Suomessa. Tutkimus antaa selvän indikaation soveltuvan työvoiman puutteesta. Työvoimaa on tarjolla, mutta sen osaamistaso jää alle työnantajien odotusten. Vaikka tutkimuksen otos on työmarkkinoiden kokoon nähden pieni, se kuvaa tämän hetken tilannetta hyvin. Tulokset on yleistettävissä kuvaamaan koko kyberalan rekrytoinnin toimivuutta.

6 POHDINTA

Kyberala kehittyy tekniikan, digitalisoitumisen, uusien verkkojen sekä koko maailman muutosten mukana. Kehitys vaatii mukautumista niin opetuksen, työvoiman ja rekrytoinnin osalta. Tarvitaan tutkimusta, joka tukee muutosta, jolla taataan riittävä koulutus laadullisesti ja määrällisesti tuottamaan riittävästi työvoimaa. Lisäksi tarvitaan suomalaista osaamisen kehitystä joka tasolla, jolla tuetaan kansallisen kybertavoitteiden savuttamista laajasti.

Jatkotutkimusideoita:

- Taloudellinen menetys Suomelle, jos kyberalan osaajia ei saada täyttämään työpaikkoja.
 - Koko talouden kehitys jää jälkeen, jos työvoimaa ei saada tekemään väistämättömiä yhteiskunnallisia digitalisaatioon liittyviä muutoksia.
- Kansallinen turvallisuusuhka, jos kyberalan osaajia ei saada täyttämään työpaikkoja.
 - Suomella tulee olla riittävät resurssit vastata sisäisiin kyberuhkiin.
 - Suomella tulee olla riittävän laaja ja tasokas kyky vastata valtiollisen tason uhkiin kybermaailmassa.
 - Suomen tulee omata riittävä resilienssi yhteiskunnan kaikilla tasoilla kyberturvallisuuden ja informaatiovaikuttamisen uhkiin.
- Alan kiinnostavuuden kasvattaminen Suomessa.
 - IT-alan nostaminen nousevaksi trendiksi takaamaan riittävän laajan ja kyvykkään opiskelijatason korkeakouluissa.
- Suomen kiinnostavuuden lisääminen kansainvälisillä työmarkkinoilla.
 - Suomikuvan parantaminen ja esteiden madaltaminen ulkomaisen työvoiman näkökulmasta, jolla voimme kilpailla globaaleilla työmarkkinoilla.
- Kyberalan työvoiman kognitiivisten ominaisuuksien (trade) tutkiminen.

- o Millainen on tulevaisuuden kyberalan työntekijän profiili, jota tarvitaan? Vastaako se nykyistä kysyntää vai nouseeko esiin uusia ominaisuuksia, joita työnhakijalla tulee olla menestyäkseen tulevaisuudessa kyberalalla?

Koulutukseen tulee kehittää riittävän korkea taso takaamaan kaikille työvoiman tarvitsijoille soveltuva osaaminen. Kuinka valtion tulisi edistää oppimista kaikilla tasoilla? Oppimista tulee kehittää alkaen yleistietämyksen levittämistä kaikille kansalaisille, peruskoulutuksen kehityksestä takaamaan reitti korkeakoulutukseen sekä korkeakoulutuksen resurssien varmistamisesta kehittämään laaja pohja osaajia sekä huippuosaajien kärki viemään Suomea eteenpäin, kohti tavoitteeksi asetettua edelläkävijyyttä.

Yleisesti perustason kansalaistietämys lisää resilienssiä laajasti koko Suomessa yksittäisestä kansalaisesta alkaen. Tietämys kybermaailman riskeistä ja niiltä suojautumisesta tuo yleistä turvaa ja helpottaa vaikutusyrityksiin puuttumista. Laaja-alainen kybermaailman ymmärrys, kyberjohtamisen kehittäminen, kansainvälinen yhteistyön lisääminen sekä tutkimustoiminnan keskittäminen suuremiksi kokonaisuuksiksi mahdollistaa kyberosaamisen säilymisen ja kehittämisen Suomessa. Pitkälle viety erikoisosaaminen ja sen koulutuksen kehitys auttaa suomalaisten yritysten menestysmahdollisuuksia kansainvälisessä kilpailussa sekä valtiota omavaraisuuden lisäämisessä sisäisessä turvallisuudessa mm. rikollisuutta vastaan sekä kyberpuolustuksessa ulkoisia vaikutteita vastaan.

LÄHTEET

- Aalto yliopisto (2018). Koulutus. Haettu osoitteesta <http://www.aalto.fi/fi/studies/education/>.
- Aalto yliopisto (2018). Tutkimus. Haettu osoitteesta <http://comnet.aalto.fi/en/research/>.
- Academic Work (2018). Academic Work Academy - Avoimet koulutusohjelmat. Haettu osoitteesta <https://www.academy.fi/open/avoimet-ohjelmat>.
- Alasuutari P. (2011). *Laadullinen tutkimus 2.0*. Tampere: Osuuskunta Vastapaino.
- Alertum (2018). Tietosuojakortti. Haettu osoitteesta <https://www.alertum.fi/koulutukset/muut-turvallisuuskoulutukset/tietosuojakoulutus>.
- Ammattibarometri (2019). Työllistymisen näkymät eri ammateissa. Haettu osoitteesta <https://www.ammattibarometri.fi/>.
- Blanke S., Nielsen P. & Wrozek B. (2018). *How Can a Cybersecurity Student Become a Cybersecurity Professional and Succeed in a Cybersecurity Career?* Teoksessa Christiansen B. & Piekarz A., *Global Cyber Security Labor Shortage and International Business Risk* (s. 111-128). IGI Global.
- Centria ammattikorkeakoulu (2018). Koulutus. Haettu osoitteesta https://soleops.cou.fi/opsnet/disp/fi/ops_KoulOhjOps/tab/tab/sea?ryhma_id=5303193&koulohj_id=2003952&valkiel=en&stack=push.
- Centria ammattikorkeakoulu (2018). Tutkimus. Haettu osoitteesta <https://tki.centria.fi/hankkeet/digitalisaatio>.
- CyberLab Oy (1.2.2016). Kyberosaaminen Suomessa - Liiketoimintanalyysi. Haettu osoitteesta http://www.kyberosaaminen.fi/materials/Cyberlab%20liiketoiminta_analyysi_final_251115.pdf.
- Danske Bank (2018). Taloutesi työkalut. Haettu osoitteesta <https://danskebank.fi/sinulle/tyokalut>.
- Dawson J., & Thomson R. (12.6.2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology*, June 2018, Volume 9.

- Eduskunta (2019). Tiedustelulait. Haettu osoitteesta https://www.eduskunta.fi/FI/tietoeduskunnasta/kirjasto/aineistot/kohtainen_oikeus/LATI/tiedustelulait/Sivut/default.aspx.
- Elisa Santa Monica (2018). Elisa Santa Monica Career Kickstart. Haettu osoitteesta <https://hub.elisa.fi/career-kickstart-reittina-tietoverkko-ja-kyberturvaosaamisen-ytimeen/>.
- EUGDPR (2018). GDPR timeline. Haettu osoitteesta <https://www.eugdpr.org/gdpr-timeline.html>.
- Forbes (2017). Cyber Security: The World's Best And Worst Presented With A Well-Designed Infographic. Haettu osoitteesta <https://www.forbes.com/sites/kevinmurnane/2017/05/04/cyber-security-the-worlds-best-and-worst-presented-with-a-well-designed-infographic/#486e3e424416>.
- Hakola E. (20.4.2018). Työn perässä muuttaminen ei kiinnosta suomalaisia, kertoo tutkimus – seurauksena työvoimapulaa ja rakenteellista työttömyyttä. Haettu osoitteesta <https://www.talouselama.fi/uutiset/tyon-perassa-muuttaminen-ei-kiinnosta-suomalaisia-kertoo-tutkimus-seurauksena-tyovoimapulaa-ja-rakenteellista-tyottomyytta/a77c4abb-7cf9-349c-b62a-f53d8e38bfdf>.
- Halminen L. (17.2.2018). Raportti antaa suomalaisesta kyberturvallisuudesta synkän kuvan - nyt Suomi varustautuu verkkosodankäyntiin. Helsingin sanomat. Haettu osoitteesta <https://www.hs.fi/kotimaa/art-2000005093202.html>.
- Halminen L. (17.2.2018). Raportti: Kaikkia elintärkeitä toimintoja ei ole turvattu kyberhyökkäyksen varalta – poliittinen sitoutuminen puuttuu. Haettu osoitteesta <https://www.hs.fi/kotimaa/art-2000005091782.html>.
- Hartio I. (17.9.2018). Jyväskylän yliopisto haluaa lisätä ict-alan koulutusta. Haettu osoitteesta <https://www.ksml.fi/kotimaa/Jyv%C3%A4skyl%C3%A4n-yliopisto-haluaa-lis%C3%A4t%C3%A4-ict-alan-koulutusta/1257983>.
- Harvey R. (1991). *The handbook of industrial and organizational psychology*. Palo Alto, CA: Consulting Psychologist Press.
- Helsingin yliopisto (2018). Koulutus. Haettu osoitteesta <https://www.helsinki.fi/fi/koulutustarjonta>.
- Helsingin yliopisto (2018). Tutkimus. Haettu osoitteesta <https://www.helsinki.fi/fi/tietojenkasittelytiede/tutkimus>.

- Hirsjärvi S., Remes P. & Sajavaara P. (2009). *Tutki ja kirjoita*. (15. uud. painos). Helsinki: Tammi.
- Hirsjärvi S. & Hurme H. (2015). Tutkimushaastattelu - Teemahaastattelun teoria ja käytäntö: e-kirja Gaudeamus.
- International Telecommunication Union (ITU) (2017). Global Cybersecurity Index (GCI) 2017. Haettu osoitteesta https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.
- ISACA (2018). State of Cybersecurity 2018, Part 1: Workforce Development. Haettu osoitteesta http://www.isaca.org/Knowledge-Center/Research/Documents/cyber/state-of-cybersecurity-2018-part-1_res_eng_0418.PDF?regnum=466324.
- Itä-Suomen yliopisto (2018). Tietojenkäsittelytieteiden laitos. Koulutus. Haettu osoitteesta <http://www.uef.fi/fi/web/cs/cs> .
- Itä-Suomen yliopisto (2018). Tietojenkäsittelytieteiden laitos. Tutkimus. Haettu osoitteesta <http://www.uef.fi/web/cs/tutkimus>.
- Jyväskylän ammattikorkeakoulu (2018). Insinööri, tieto- ja viestintäteknikka. Koulutus. Haettu osoitteesta <https://www.jamk.fi/fi/Koulutus/tekniikan-ala/insinööri-tieto-ja-viestintäteknikka/>.
- Jyväskylän ammattikorkeakoulu (2018). Tutkimus. Haettu osoitteesta <https://www.jamk.fi/fi/Tutkimus-ja-kehitys/vahvuusalat/Kyberturvallisuus/>.
- Jyväskylän yliopisto (2018). Koulutus. Haettu osoitteesta <https://www.jyu.fi/it/fi>.
- Jyväskylän yliopisto (2018). Tutkimus. Haettu osoitteesta <https://www.jyu.fi/it/en/research>.
- Jyväskylän yliopisto (2018). Tutkimus, kyberturvallisuus. Haettu osoitteesta <https://www.jyu.fi/it/en/research/research-areas/cyber-security>.
- Kaakkois-Suomen ammattikorkeakoulu (2018). Cybersecurity – kyberturvallisuus, ylempi AMK. Koulutus YAMK. Haettu osoitteesta <https://www.xamk.fi/koulutukset/insinööri-ylempi-amk-tieto-ja-viestintäteknikka/>.
- Kaakkois-Suomen ammattikorkeakoulu (2018). Koulutus AMK. Haettu osoitteesta <https://www.xamk.fi/koulutus/tutkinto-amk/>.

- Kaakkois-Suomen ammattikorkeakoulu (2018). Koulutus YAMK. Haettu osoitteesta <https://www.xamk.fi/koulutus/tutkinto-yamk/>.
- Kaakkois-Suomen ammattikorkeakoulu (2018). Tutkimus. Haettu osoitteesta <https://www.xamk.fi/digitaalisen-talouden-osaamiskarjet/>.
- Kaijala M. (2016). *Rekrytointi*. Helsinki: Alma
- Kansalaisopistot.fi (2018). Kurssit. Haettu osoitteesta <http://kansalaisopistot.fi/kurssit/>.
- Kinnunen P. & Neittaanmäki P. (2016). *Työttömyys IT-alalla koko Suomessa ja maakunnissa 2006-2015*. Informaatioteknologian tiedekunnan julkaisuja No. 23/2016.
- Koistinen P. (2014). *Työ, työvoima & politiikka*. Tampere: Osuuskunta Vastapaino.
- KPMG (2018). Tietoja KPMG:stä. Haettu osoitteesta <https://home.kpmg/fi/fi/home/tietoa-kpmgsta.html>.
- KPMG (2018). KPMG Trainee Program. Haettu osoitteesta <https://trainee.kpmg.fi/home>.
- KPMG (2018). #KPMGTechGuru. Haettu 11.5.2018 osoitteesta <https://home.kpmg.com/fi/fi/home/tyopaikat/kpmgtechguru.html>.
- Kyberturvallisuuskeskus (2018). Havainnointi ja avunanto. Haettu osoitteesta <https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto>.
- Laitinen J. (2017). Kodin kyberopas. Haettu osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2017/04/Kodin_kyberopas_TK_2017_verkkojulkaisu.pdf.
- Lappeenrannan yliopisto (2018). Koulutus. Haettu osoitteesta <https://www.lut.fi/opiskelu/kandidaattiohjelmat/tietotekniikka>.
- Lappeenrannan yliopisto (2018). Tutkimus. Haettu osoitteesta <https://www.lut.fi/web/en/research>.
- Laurea ammattikorkeakoulu (2018). Koulutus. Haettu osoitteesta <https://www.laurea.fi/opiskelu-ja-hakeminen/amk-tutkinnot/tietojenkäsittely>.
- Laurea ammattikorkeakoulu (2018). Tutkimus. Haettu osoitteesta <https://www.laurea.fi/tutkimus-kehitys-ja-innovaatiot/tki-toiminta-laureassa/yhtenäinen-turvallisuus>.

- Lehto M. & Kähkönen A. (2015). Kyberturvallisuuden kansallinen osaaminen Informaatioteknologian tiedekunnan julkaisuja No. 20/2015
- Lehto M., Limnell J., Innola E., Pöyhönen J., Rusi T. & Salminen M. (17.2.2018). Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Haettu osoitteesta http://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213?version=1.0.
- Libicki M. C., Senty D. & Pollak J. (2014). *H4cker5 wanted: An examination of the cybersecurity labor market*. [Santa Monica, California]: RAND Corporation.
- Luukka T. (16.1.2018). Moni työ jää ilman tekijää. *Helsingin sanomat*, s. 26-28
- Lönnqvist I. & Moilanen P. (2017). *Kyberin taskutieto*. Jyväskylä/Rauma.
- Maanpuolustuskorkeakoulu (2018). Haettu osoitteesta <http://maanpuolustuskorkeakoulu.fi/opiskelu>.
- Maanpuolustuskoulutusyhdistys, MPK (2018). Kyberturvallisuus. Haettu osoitteesta <https://www.mpk.fi/Kyberturvallisuus>.
- Metsämuuronen, J. (2011). *Tutkimuksen tekemisen perusteet ihmistieteissä*: e-kirja opiskelijalaitos. Helsinki: International Methelp, Booky.fi 2011.
- Mäntylä J-M (20.10.2017). Digiosaajien puute uhkaa kansantaloutta – "koulutusmäärät kaksinkertaistettava". Haettu osoitteesta <https://yle.fi/uutiset/3-9894310>.
- Niitamo P. (2003). *Henkilöarviomenetelmät työelämässä*. Jyväskylä: Gummerrus Kirjapaino Oy
- Nordea (20.4.2018). Lehdistötiedote: Tutkimus: Suomalaiset eivät halua muuttaa työn perässä, vaikka työvoiman liikkuvuutta tarvittaisiin. Haettu osoitteesta <https://www.nordea.com/fi/media/uutiset-ja-lehdistotiedotteet/press-releases/2018/04-20-07h00-tutkimus-suomalaiset-eivat-halua-muuttaa-tyon-perassa-vaikka-tyovoiman-liikkuvuutta-tarvittaisiin.html>.
- Nordea (2018). Verkko- ja mobiilipalvelut. Haettu osoitteesta <https://www.nordea.fi/henkiloasiakkaat/palvelumme/verkko-mobiilipalvelut/helppo-asioida.html>.
- Newhouse W., Keith S., Scribner B. & Witte G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Haettu osoitteesta

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf>.

Newell Brown J. (2011). *The Complete Guide to Recruitment: A Step-By-Step Approach to Selecting, Assessing and Hiring the Right People*. London: Kogan Page Limited 2011.

Opetushallitus (2014). Perusopetuksen opintosuunnitelma. Haettu osoitteesta https://www.oph.fi/download/163777_perusopetuksen_opetussuunnitelman_perusteet_2014.pdf.

Opetushallitus (2015). Lukion opetussuunnitelman perusteet. Haettu osoitteesta https://www.oph.fi/download/172124_lukion_opetussuunnitelman_perusteet_2015.pdf.

Opetushallinnon tilastopalvelu (2017). Ammattikorkeakouluissa suoritettut tutkinnot 2017. Haettu osoitteesta https://vipunen.fi/fi/fi/_layouts/15/xlviewer.aspx?id=/fi-fi/Raportit/Ammattikorkeakoulujen%20tutkinnot%20%20koulutusala.xlsb.

Opetushallinnon tilastopalvelu (2017). Yliopistoissa suoritettut tutkinnot 2017. Haettu osoitteesta https://vipunen.fi/fi/fi/_layouts/15/xlviewer.aspx?id=/fi-fi/Raportit/Yliopistokoulutuksen%20tutkinnot-n%C3%A4k%C3%B6kulma-koulutusala.xlsb.

Oulun yliopisto (2018). Koulutus. Haettu osoitteesta <http://www oulu.fi/yliopisto/hakijalle/kandidaatti-ja-maisterikoulutus>.

Oulun yliopisto (2018). Tutkimus. Haettu osoitteesta <http://www oulu.fi/tst/yksiköt>.

Oulun yliopisto (2018). Tutkimus. Haettu osoitteesta <http://www oulu.fi/matematiikka/tutkimus>.

Oulun ammattikorkeakoulu (2018). Koulutus. Haettu osoitteesta <http://www.oamk.fi/opinto-opas/opintojen-sisalto/opetussuunnitelmat>.

Oulun ammattikorkeakoulu (2018). Tutkimus. Haettu osoitteesta <https://www.oamk.fi/fi/tutkimus-ja-kehitys/hankkeet/>.

Pelkonen A., Ahlqvist T., Leinonen A., Nieminen M., Salonen, J. Savola R., Savolainen P., Suominen A., Toivanen, H., Kyheröinen J. & Remes J. (2016). *Kyberosaaminen Suomessa - Nykytila ja tiekartta tulevaisuuteen*. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2016.

- Poliisi (2018). Keskusrikospoliisi. Haettu osoitteesta.
<https://www.poliisi.fi/keskusrikospoliisi>.
- Poliisiammattikorkeakoulu (2018). Koulutus. Haettu osoitteesta
https://www.polamk.fi/amk/koulutus_ja_opiskelu.
- Poliisiammattikorkeakoulu (2018). Tutkimus. Haettu osoitteesta
<https://www.polamk.fi/tki/tutkimus>.
- Prahalad CK. & Hamel G. (1990). The core competence of the corporation.
Harward Business Review, May-June, 79-91.
- Puolustusministeriö (2019). Laki sotilastiedustelusta. Kysymyksiä ja vastauksia.
Haettu osoitteesta
https://www.defmin.fi/files/4543/Q_A_sotilastiedustelu110319.pdf.
- Rekrytointikoulutus (2018). Cyber Security Academy. Haettu osoitteesta
<http://www.rekrytointikoulutus.fi/cyber-security-academy/>.
- Raunio M. (2002). Suomi globaalitalouden osajien valintojen kentällä. Haettu osoitteesta
https://www.researchgate.net/publication/260781978_SUOMI_GLOBAALITALOUDEN_OSAAJIEN_VALINTOJEN_KENTALLA_Ulkomaalaisten_huippuosajien_mielikuvat_ja_todellisuudet_suomalaisessa_työ-ja_kaupunkiymparistossa.
- Saaranen-Kauppinen, A. & Puusniekka, A. (2006.) KvaliMOTV – Menetelmäopetuksen tietovaranto [verkkójulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto [ylläpitäjä ja tuottaja]. Haettu osoitteesta <http://www.fsd.uta.fi/menetelmaopetus/>.
- Sanastokeskus TSK ry (2018). *Kyberturvallisuuden sanasto*. Helsinki: Huoltovarmuuskeskus & Sanastokeskus TSK ry. Haettu osoitteesta http://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf.
- Saranen Consulting (2018). Rekrytoiva koulutus työnhakijoille. Haettu osoitteesta <https://www.saranen.fi/rekrytoiva-koulutus-tyonhakijoille/>.
- Sinko P. & Vihriälä V. (2007). *Rekrytointiongelmat, työvoiman tarjonta ja liikkuvuus*. Valtioneuvoston kanslian julkaisusarja 5/2007.
- Sisäministeriö (2018). Tiedustelulainsäädäntö. Haettu osoitteesta
<http://intermin.fi/tiedustelu>.
- Sivistysvantaa (2018). Kansalaisopiston kurssit. Haettu osoitteesta
http://www.sivistysvantaa.fi/material/attachments/pZtWW4Dna/vantaaan_aikuisopiston_opinto-ohjelma_kevat2018.pdf.

- Spencer, L. M., & Spencer, P. S. M. (1993). Competence at work: Models for superior performance. John Wiley & Sons Inc.
- Suihkonen R. (13.3.2018). Puolustusvoimat rekrytoi jo vaivihkaa tiedustelijoita. Haettu osoitteesta <https://www.ksml.fi/kotimaa/Puolustusvoimat-rekrytoi-jo-vaivihkaa-tiedustelijoita-%E2%80%93-P%C3%A4%C3%A4esikunta-vaikenee-yksityiskohdista/1122040>.
- Suojelupoliisi (2019). 10 kysymystä tiedustelulaista. Haettu osoitteesta https://www.supo.fi/tietoa_suposta/tiedustelulaki.
- Tampereen ammattikorkeakoulu (2018). Tieto- ja viestintätekniiikan koulutus. Haettu osoitteesta <http://opinto-opas-ops.tamk.fi/index.php/fi/167/fi/49583>.
- Tampereen ammattikorkeakoulu (2018). Tietojenkäsittelyn koulutus. Haettu osoitteesta <http://opinto-opas-ops.tamk.fi/index.php/fi/167/fi/49535>.
- Tampereen teknillinen yliopisto (2018). Koulutus. Haettu osoitteesta <http://www.tut.fi/fi/tietoa-yliopistosta/tiedekunnat/index.htm>.
- Tampereen teknillinen yliopisto (2018). Tutkimus. Haettu osoitteesta <http://www.tut.fi/fi/tutkimus/tutkimusalat/tietotekniikka/tietoturva/index.htm>.
- Tampereen yliopisto (2018). Koulutus. Haettu osoitteesta <https://www10.uta.fi/opas/opetusohjelma/index.htm>.
- Tampereen yliopisto (2018). Tutkimus. Haettu osoitteesta <http://www.uta.fi/sis/cis/index.html>.
- Tampereen yliopisto (14.12.2017). Tampereen uusi korkeakouluyhteisö syntyy vuoden 2019 alussa. Haettu osoitteesta <http://www2.uta.fi/ajankohtaista/uutinen/tampereen-uusi-korkeakouluyhteiso-syntyy-vuoden-2019-alussa>.
- Telia Company (2018). About the company. Haettu osoitteesta <https://www.teliacompany.com/en/about-the-company/>.
- Telia Cygate Oy (2019). Lyhyesti. Haettu osoitteesta <https://www.teliacygate.fi/fi/lyhyesti>.
- The International Information System Security Certification Consortium (ISC)². Certifications. Haettu osoitteesta <https://www.isc2.org/>.
- The National Cybersecurity Workforce Framework. (2013). National Initiative for Cybersecurity Education. Haettu osoitteesta <https://csrc.nist.gov/CSRC/media/Presentations/The-21st-Century->

[Cybersecurity-Workforce-Framework/images-media/fissea-conference-2012_maxson_workforce-framework.pdf](https://www.sans.org/images-media/fissea-conference-2012_maxson_workforce-framework.pdf).

The SANS Institute (2018). SANS information security training. Haettu osoitteesta <https://www.sans.org/>.

The Department of Defense (2018). The DoD Cyber Workforce Framework (DCWF). Haettu osoitteesta <https://dodcio.defense.gov/Cyber-Workforce.aspx>.

Tietoturvallisuuskortti (2018). Tietoturvallisuuskortti. Haettu osoitteesta <http://www.tietoturvallisuuskortti.fi/>.

Tiihonen I. (8.1.2018). Osaajapula vaarantaisi pahimmillaan turvallisuuden. *Keskisuomalainen*, s. 9

Tilastokeskus (2018). Käsitteet. Haettu osoitteesta <http://www.stat.fi/meta/kas/tyovoima.html>.

Tilastokeskus (2018). Työvoimatutkimuksen keskeiset käsitteet ja määritelmät. Haettu osoitteesta http://www.stat.fi/til/tyti/2017/13/tyti_2017_13_2018-04-12_kat_006_fi.html#_ga=2.214905812.2110726230.1524336673-302107004.1524336673.

Tilastokeskus (2018). ICT-sektori. Haettu osoitteesta https://www.stat.fi/meta/kas/ict_sektori.html.

Tilastokeskus (24.4.2018). Työttömyysaste. Haettu osoitteesta <https://findikaattori.fi/fi/34>.

Tilastokeskus (2018). Työvoimatutkimus 2018, syyskuu. Työttömyysaste. Haettu osoitteesta https://www.stat.fi/til/tyti/2018/09/tyti_2018_09_2018-10-23_tie_001_fi.html.

Tilastokeskus (2018). Työvoimatutkimus 2018, syyskuu. Työlliset toimialoittain. Haettu osoitteesta https://www.stat.fi/til/tyti/2018/09/tyti_2018_09_2018-10-23_tau_028_fi.html.

Tilastokeskus (2018). Tietotekniikka-ammattilainen. Haettu osoitteesta <https://www.stat.fi/meta/kas/tietotekniikka.html>.

Tilastokeskus (29.11.2016). Tutkintotavoitteisen koulutuksen opiskelijamäärä 1,27 miljoonaa. Haettu osoitteesta https://www.stat.fi/til/opiskt/2015/opiskt_2015_2016-11-29_tie_001_fi.html.

Tilastokeskus (6.2.2018). Palkansaaajien ansiot nousivat 0,2 prosenttia. Haettu osoitteesta

https://www.tilastokeskus.fi/til/ati/2017/04/ati_2017_04_2018-02-06_tie_001_fi.html.

Turku AMK (2018). Haettu osoitteesta

https://ops.turkuamk.fi/opsnet/disp/fi/ops_PuuHierValOpas/tab/nop/clr?menuid=2.

Tuomi, J. & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi*. Helsinki: Tammi.

Turku AMK (2018). Koulutus. Haettu osoitteesta

https://ops.turkuamk.fi/opsnet/disp/fi/ops_PuuHierValOpas/tab/nop/clr?menuid=2.

Turku AMK (2018). Tutkimus. Haettu osoitteesta

<https://www.turkuamk.fi/fi/tutkimus-kehitys-ja-innovaatiot/tutkimusryhmat/tietoliikenne-ja-tietosuoja/>.

Turun yliopisto (2018). Koulutus. Haettu osoitteesta

<http://www.utu.fi/fi/yksikot/sci/opiskelu/koulutustarjonta/ohjelmat/Sivut/home.aspx>.

Turun yliopisto (2018). Tutkimus. Haettu osoitteesta

<https://tech.utu.fi/en/information-security-and-cryptography/>.

Turvallisuuskomitea (2013) Suomen kyberturvallisuusstrategia Haettu osoitteesta

<https://www.turvallisuuskomitea.fi/index.php/fi/component/k2/14-suomen-kyberturvallisuusstrategia>.

Turvallisuuskomitea (2017) Suomen kyberturvallisuusstrategian toimenpano-ohjelma 2017-2020. Haettu osoitteesta

<https://www.turvallisuuskomitea.fi/index.php/fi/mcdc/126-suomen-kyberturvallisuusstrategian-toimeenpano-ohjelma-2017-2020>.

Vaasan yliopisto (2018). Koulutus. Haettu osoitteesta

<https://www.univaasa.fi/fi/for/student/materials/handbooks/technology/>.

Vaasan yliopisto (2018). Tutkimus. Haettu osoitteesta

<https://www.univaasa.fi/fi/research/>.

Valtiovarainministeriö (17.1.2018). 19 kysymystä ja vastausta Suomen työmarkkinoista ja työvoimakapeikoista. Haettu osoitteesta

<https://vm.fi/dms-portlet/document/0/534720>.

- Valtiovarainministeriö (2018). Digitalisaatio. Haettu osoitteesta <https://vm.fi/digitalisaatio>.
- Varusmies (2018). Puolustusvoimat, palvelustehtävät, kybervarusmies. Haettu osoitteesta <http://varusmies.fi/palvelustehtavat-ja-paikat/-/services/506>.
- Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative - quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS quarterly*, 37(1), 21-54.
- Wagner, R. (2012). Organizational competence in project management - new perspectives on assessing and developing organizations. *Journal of Project, Program & Portfolio Management*, 3(1), 45-57.
- Wilson, A., & Wilson, C. (2011). THE EFFECTS OF U.S. GOVERNMENT SECURITY REGULATIONS ON THE CYBERSECURITY PROFESSIONAL. *Allied Academies International Conference: Proceedings Of The Academy Of Legal, Ethical & Regulatory Issues (ALERI)*, 15(2) , 5-12.
- Åbo Akademi (2018). Koulutus. Haettu osoitteesta <https://www.abo.fi/studera-hos-oss/vara-utbildningar/>.
- Åbo Akademi (2018). Tutkimus. Haettu osoitteesta <https://www.abo.fi/fi/tutki-kanssamme/>.

LIITE 1 TUTKIMUSHAASTATTELUN KYSYMYKSET

Kerro omasta työtehtävästäsi sekä organisaatiostasi kyberalan näkökulmasta. Millaista toimintaa teillä on alalla? Kuinka paljon teillä on alan työntekijöitä?

1. Kuinka helppoa tai vaikeaa soveltuvan henkilön löytäminen oli avoimiin kyberturvallisuusalaa koskeviin työpaikkoihin, jotka yrityksellenne oli avoinna vuonna 2018? Arvioi asteikolla yhdestä viiteen (1 - 5). Kuvaile tarkemmin hakijoiden soveltuvuutta.

1 Erittäin vaikeaa - - - 2 Vaikeaa - - - 3 Melko helppoa - - - 4 Helppoa - - - 5 Erittäin helppoa

2. Kuinka helppoa tai vaikeaa mielestänne työvoiman löytäminen kyberturvallisuusosalalla on yleisesti (1 - 5) ja perustele vastauksesi?

1 Erittäin vaikeaa - - - 2 Vaikeaa - - - 3 Melko helppoa - - - 4 Helppoa - - - 5 Erittäin helppoa

3. Mitkä seikat mielestänne ovat suurimmat esteet soveltuvan työvoiman saantiin kyberturvallisuusosalalla?

4. Millaisia osaajia ensisijaisesti etsitte?

5. Millaisia rekrytointimenetelmiä olette käyttäneet ja harkitsetteko uusia metodeja? Käyttäisittekö palvelua, missä työvoimaa voisi hakea työntekijäpoolista?

6. Mitkä seuraavista seitsemästä ominaisuudesta, ovat mielestänne kolme tärkeintä kyberturvallisuusalan työntekijälle? Perustele lyhyesti valintasi.

- Systemaattinen ajattelutapa
- Tiimipelaaja
- Tekniset kyvyt
- Sosiaaliset kyvyt
- Kansalaisvelvollisuuden tunto tai yrityksen arvomaailma
- Jatkuva opiskelu
- Kommunikointitaidot

7. Miten kyberturvallisuusalan työnhakijoiden osaaminen vuonna 2018 vastasi yrityksenne toiveita tai odotuksia (1 - 5) sekä kuvaile tarkemmin, mitkä osaamisalueet olivat hyvin ja mitkä huonosti hakijoiden hallussa?

1 Erittäin huonosti - - - 2 Huonosti - - - 3 Melko hyvin - - - 4 Hyvin - - - 5 Erittäin hyvin

8. Miten yleisesti ajatellen kyberturvallisuusalan koulutus vastaa teidän yrityksenne ja koko alan osaamistarvetta (1 - 5) ja perustele vastauksesi?

1 Erittäin huonosti - - - 2 Huonosti - - - 3 Melko hyvin - - - 4 Hyvin - - - 5 Erittäin hyvin

9. Kuinka kyberturvallisuusalan koulutusta teidän mielestänne tulisi kehittää, että se vastaisi paremmin teidän yrityksenne/koko alan tarvetta?

10. Miten koulutatte omia kyberturvallisuusalan työntekijöitänne? Huomio olevan työvoiman koulutus sekä uusien henkilöiden perehdytys.

11. Tulisiko mielestänne työntekijöiden aktiivisesti kouluttautua itsenäisesti ja pysyä kehityksen mukana ilman työnantajan panosta?

12. Tulisiko kyberalan koulutusta ja tutkimusta keskittää tai jakaa oppilaitosten kesken siten, että se palvelisi Suomen kokonaisturvallisuutta tai kilpailukykyä? Perustele vastauksesi.

13. Palkkaisitteko enemmän kyberturvallisuusalan työntekijöitä, jos soveltuvia osaajia olisi helpommin saatavilla?

14. Oletteko valmiita palkkaamaan tai palkanneet kyberalan työvoimaa ulkomailta? Mitkä ovat suurimmat syyt tähän?

Haluaisitko kertoa muuta kyberalaan liittyvää, mikä mielestäsi olisi syytä nostaa esiin työvoimasta ja koulutuksesta keskusteltaessa?

LIITE 2 TUTKIMUSHAASTATTELUUN OSALLISTUNEET ORGANISAATIOT

Cygate Oy

Cygate on osa Telia Companya ja yrityksen nimi muuttui 1.1.2019 Telia Cygate Oy:ksi. Se toimii omana tytäryhtiönä. Cygate tarjoaa tietoturvallisia ICT-ratkaisuja ja -palveluita B2B asiakkaille. Cygatella on henkilökuntaa yli 300 henkilöä ympäri Suomea. (Telia Cygate Oy, 2019). Kyberturvallisuuden yhtä ydintekemisen osa-aluetta Cygatessa edustaa SOC-toiminnot. Näissä tiimeissä työskentelee noin 39 henkilöä projekteissa, kehitystyössä, analyytikkona sekä tietoturva- ja verkkoasiantuntijana.

Insta DefSec Oy

Insta Group Oy on suomalainen perheyritys, joka koostuu neljästä osasta. Insta Automation Oy on erikoistunut teollisuusautomaatioon. Insta ILS Oy tuottaa elinkaaripalveluja ilmailualalle. Insta DefSec Oy kehittää tietoturvaratkaisuja sekä - palveluita. Marraskuussa 2018 ostettu Intopalo Digital Oy tarjoaa turvallista digitalisointia. Insta Group työllistää noin 1000 henkilöä. Näistä noin 250 henkilöä Insta Def Sec Oy:ssä. Heistä noin 70 henkilöä työskentelee kyberalan tehtävissä sekä marraskuussa ostetussa Intopalossa toiset 70 henkilöä. Iso osa on myös ohjelmistokehitys, missä työskentelee noin 350 henkilöä. Kyberalan työ Insta DefSecissä keskittyy turvallisuuskriittisten järjestelmien tarjoamiseen B2B (business to business) asiakkaille. Asiakaskunta koostuu suurelta osin valtiohallinnon toimijoista.

Keskusrikospoliisi

"Keskusrikospoliisi (KRP) on Suomen poliisin valtakunnallinen yksikkö, jonka toimialueena on koko Suomi." (Poliisi, 2018). Yhteensä KRP työllistää noin 300 henkilöä. Kyberosa-alueella toimintaa Suomen poliisissa harjoittaa mm. kyberkeskus ja rikostekninen laboratorio. Kyberkeskus koostuu noin 70 henkilöstä. Rikostekniikassa laboratoriossa työskentelee noin 100 henkilöä, joista kyberalaa edustavan digitaalisen forensiikan parissa työskentelee noin 10 henkilöä.

KPMG Suomi

KPMG on kansainvälinen asiantuntijapalveluita tarjoava yritys, jonka päätoimialoja ovat mm. tilintarkastus, vero- ja lakipalvelut, neuvontapalvelu sekä konsultointi. Yrityksellä on noin 207 000 työntekijää 154 maassa. Suomessa työntekijöitä on noin 1400 henkilöä. Kyberalalla KPMG tarjoaa asiantuntijapalveluita ratkaisemaan asiakkaidensa tietoturvakysymyksiä mm. suojaratkaisujen

suunnittelussa, muutostilanteiden läpiviemisessä, tietomurtojen varautumisessa sekä tietoturva-auditoinneissa. (KPMG, 2018).

Telia Finland Oyj

Telia Company on kansainvälinen suuryritys, jonka päätoimiala on tietoliikennepalveluiden tarjoaminen kuluttaja- ja yritysasiakkaille. Yritys työllistää yhteensä noin 19 632 henkilöä, joista noin 2 788 on Suomessa. (Telia Company, 2018). Kyberturvallisuuden osalta Telia Finland tarjoaa laajasti tietoturvapalveluita itse ja tytäryhtiöidensä kautta. Telian Finlandin CERT-toimintojen vahvuus on noin 20 henkilöä.

LIITE 3 OPPILAITOSKYSELYN KYSYMYKSET

1. Mihin suuntaan kyberalan opetus teidän oppilaitoksessanne on kehittymässä?
 - a. Oppilasmäärät
 - b. Opetustarjonta
 - c. Erikoistuminen tiettyyn kyberturvallisuuden osa-alueeseen tai sen linkittäminen toiseen alaan

2. Tulisiko kyberalan opetusta Suomen mittakaavassa keskittää tai jakaa ohjautusti?

3. Miten hyvin kyberturvallisuuden koulutus mielestänne valmistaa oppilaita työmarkkinoiden tarpeisiin?