Kyberosaamistarpeet - esiselvitys

17.12.2020 Helsinki

Sisällys

Tiivistelmä

Esiselvitys Suomen kyberosaamistarpeista on tehty liikenne- ja viestintäministeriön toimeksiannosta osana kyberturvallisuuden kehittämisohjelman valmistelua. Esiselvityksen toteutti TkT Antti Sillanpää, Linkitin Oy. Selvityksessä esitetyt näkemykset ovat tekijän, eivätkä välttämättä edusta toimeksiantajan näkökantoja.

Esiselvityksen tärkeimpänä aineistona oli verkkokysely, jota jaettiin kyberturvallisuuden ja varautumisen toimijoille elinkeinoelämän, viranomaisten, koulutusorganisaatioiden ja kolmannen sektorin piirissä. Kyselyssä pyydettiin arvioimaan tilannetta nyt, osaamisvajeita noin kolmen vuoden päästä ja myöhempää kehitystä. Anonyymejä vastauksia analysoitiin 273. Tuloksia käsiteltiin vielä kahdessa työpajassa.

Tämä Kyberosaamistarpeet-esiselvitys vahvistaa jo aiemmin havaitun: Suomessa on merkittävä pula kyberturvallisuuden osaajista, ja se haittaa niin suomalaista turvallisuutta kuin hyvinvointiakin.

Pula osaajista on sekä laadullinen että määrällinen ongelma. Kyselyssä nousivat pahimmiksi ongelmiksi seuraavat alat: kaikki analysointitehtävät, järjestelmäarkkitehtuuri, kyberturvallisuuden hallinta, järjestelmien ja tietojen suojaustarpeiden analysointi, tapahtumiin vastaaminen ja haavoittuvuusarviointi ja -hallinta.

Edellä mainitut erikoistumisalat voidaan hahmottaa kahdeksi suureksi kokonaisuudeksi, jotka ovat: kyberturvallisuuden kokonaisuuden hallinta ja operatiivisempi järjestelmien suojaus sekä sitä tukeva analyysi. Tämä esiselvitys korostaa muita tutkimuksia enemmän kokonaisuuden hallintaan ja sen johtamiseen liittyviä tehtäviä.

Esiselvityksen perusteella organisaatiot rekrytoivat erityisesti kilpailijoiltaan. Työnantajien silmissä yliopiston maisteritaso on kannustettavin koulutustaso. Opintopolkujen houkuttelevuudessa on suuria eroja. Erityisesti julkiselle sektorille pääsee vain harvoja reittejä pitkin: toisesta organisaatiosta tai valmistuneena yliopistomaisterina.

Osaamisvajetta voidaan kuroa umpeen sekä nopeasti vaikuttavilla toimenpiteillä ja hitaammin toimivilla linjaratkaisuilla. Molemmat tarvitsevat resursseja julkiselta sektorilta mutta myös sitoutumista työnantajien puolelta. Työnantajien on oltava mukana määrittämässä koulutusaloja mutta myös hyödynnettävä laajasti erilaisia osaajia. Asiantuntijakeskustelujen perusteella summittaiseen tärkeysjärjestykseen on laitettu esimerkkejä keinoja osaamistarpeiden laventamiseksi:

- Kyberturvallisuus on nähtävä lukutaidon tapaisena kansalaistaitona. Osaamisongelman ratkaiseminen on aloitettava viimeistään peruskoulussa. Esiselvitys keskittyi kolmannen asteen opintojen ja erikoisosaajien rooliin, mutta näkökulma on liian kapea.
    - kyberopetuksen lisääminen laajasti eri oppiaineissa ja koulutustasoilla
- Oppilaitosten ja työnantajien yhteistyön parantaminen paikallisella tasolla, mihin liittyvät:
    - työn opinnollistaminen, joka edellyttää oppilaitosten hyväksyvän erilaisia tehtäviä opintosuorituksiksi ja yritysten halua lisätä tehtäviin opintoelementtejä
    - opiskelijoiden keskeyttämisprosentin vähentäminen
    - viestintä yrityksien suuntaan erilaisista opintopoluista ja niiden hyödynnettävyydestä
- Jatkotutkimuksen ja -selvitysten aiheiksi nousevat muun muassa:
    - mitkä tahot voisivat lisätä kyberopetusta huomioiden paikallistetut osaamisvajeet,
    - mitä muutoksia tämä tarkoittaa opetussuunnitelmiin ja
    - mitkä ovat käytännön työkalut ja parhaat käytännöt paikallisen yhteistyön parantamiseksi.

Arvio kyberosaajapulan merkityksestä

Osaamistarpeiden vaikutus kyselyn perusteella

Kyberosaajapula on sekä määrällinen että laadullinen ongelma, joka koskee koko vastaajakenttää. Tuloksia voidaan peilata muihin selvityksiin, jotka johdonmukaisesti – käytetystä menetelmästä riippumatta - osoittavat merkittävän resurssipulan. Tämän esiselvityksen vastaajista noin puolet oli yrityskentästä, vajaa puolet oli julkiselta sektorilta ja kolmannelta sektorilta 5% [1].

Kyselyssä tiedusteltiin (kysymys 5), kuinka merkittävä kyberturvallisuuden henkilöstölisäystarve on seuraavan 2-3 vuoden aikana. Vastausvaihtoehtojen vaihteluväli lähti liikkeelle tilanteesta, jossa ei ole lisäystarvetta ja päätyi siihen, että vaje vaarantaa toiminnan turvallisuuden tai kannattavuuden. Osalle se vaarantaa koko toiminnan, kun joillekin ongelma on hallittavissa. Useimmat vastaajat näkivät, että heillä on melko pieni tai melko suuri lisäystarve.

Kukaan ei vastannut, että lisähenkilöiden tarvetta ei ollut, mutta toisaalta 10 vastaajaa ilmoitti vajeen vaarantavan turvallisuuden tai kannattavuuden. Vaikka ongelma on vain harvoille toiminnan vaarantava, sen olemassaolo on kuitenkin hälyttävä.

Tekijäpulan merkitys vaihtelee vastaajien joukossa. **Julkisella sektorilla osaajien tarvetta koettiin hieman useammin. Yritykset olivat silti eniten kasvattamassa osaajiensa määrää.** Huomio on johdonmukainen Pöyhönen (2020) väitöskirjan huomion kanssa: (isoissa) yrityksissä on resursseja hyödyntää kyberturvallisuuden parhaita ratkaisuja ja palveluita, mutta julkiselle sektorilla tämä on haasteellista [2].

Kyselyyn vastanneet arvioivat organisaatioissaan perustettavien uusien kyberturvallisuustyöpaikkojen määrän (kysymys 6). Yleisin vastaus henkilöstölisäyksestä oli 0% ...20%:n vaihteluväli. Peräti 16 % prosenttia vastaajista oli vähintään kaksinkertaistamassa joukkoaan.

Muut selvitykset

Keväällä 2020 Kyberala (FISC) ry arvioi, että se työllistää Suomessa nyt 6500-7000 kyberturva-alan ammattilaista ja vuonna 2025 tarve olisi jopa 15 000:lle alan osaajalle. Jäsenet ovat lähinnä tieto- ja kyberturvatuotteita ja -palveluita tarjoavia yrityksiä ja organisaatioita. Kyselyn mukaan 60% vastaajista koki osaajapulaa [3]. Tässä esiselvityksessä luku oli suurempi, mitä voi selittää esimerkiksi se, että tähän osallistui enemmän muuta yrityskenttää ja viranomaisia.

---

[1] Yritysvastaajista 108 kpl, 40 % luokitteli itsensä kyberturvallisuuden käyttäjiksi, ja 44 kpl, 16% kyberturvallisuuden tuottajiksi. Valtiollisia julkisen sektorin toimijoita oli 77 kpl, 28%. Aluehallinnosta, kunnista ja kuntaliittymistä oli 36 kpl, 13%. Koulutusta ja tutkimusta edusti 19 kpl, 7%. Kolmatta sektoria edusti vastaajista 15 kpl, 5%. Näiden summa on yli 100%, koska oli mahdollista vastata useampaan.
Palveluita tai tuotteita myyvien yritysten tärkeimmät asiakkaat löytyivät kotimaisista yrityksistä, julkiselta sektorilta ja ulkomaalaisista yrityksistä. Anonyymin kyselyn luonteesta johtuen tuloksista ei voida tehdä tilastollisesti päteviä johtopäätöksiä. Johdonmukaisuus muiden selvitysten kanssa vahvistaa tulosten uskottavuutta.

[2] Jouni Pöyhönen (2020) ”Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa - systeemiajattelu”, Jyväskylän yliopisto.

[3] Arvio perustui jäsenkyselyn (2020) tuloksiin sekä mm. ENISA:n raporttiin ”Cybersecurity Skills development” (December 2019) ja ISC2 selvitykseen https://www.isc2.org/Research/Workforce-Study.

Teknologiateollisuuden arvion mukaan pelkästään sen jäsenyritykset tarvitsevat 11 400 ICT-ammattilaista. Teollisuuskyselyssä kartoitettiin laajemmin tietotekniikkaosaajien tilannetta, mutta vain yhden, erittäin suuren toimialan intresseistä. Teknologiateollisuuden yritykset vastaavat lähes puolesta Suomen t&k-investoinneista. Teollisuuskyselyn tarkastelujakso oli 2018-2021, mutta mikään ei osoita osaajavajeen kuroutumista. Tuohon työvoimatarvearvioon eivät sisälly muut yritykset tai julkinen sektori [4].

Kansainvälisen ISC työvoimakyselyn (2020) mukaan kyberammattilaisia tarvitaan globaalisti lähes 90% lisää nykytasoon verrattuna. Suomeen verrattavassa Alankomaissa kasvutarve oli 70%. Työvoimapulan vuoksi riskit olivat kohonneet 56%:lla ISC-kyselyyn vastanneista [5].

Osaamistarpeiden vaikutus - käsittely työpajoissa

Kaikki selvitykset osoittavat, että merkittäviä tappioita aiheuttava osaamisvaje ei ole hetkeen korjaantumassa. Työpajoissa nähtiin, että tarvekyselyt eivät huomioi kyberturvallisuuden piilevää kysyntää. Käydyssä keskustelussa pohdittiin, että yleensä tutkimuksiin osallistuvat henkilöt tuntevat jo ongelma-alueen. Esiselvityksen vastaajista puuttuvat muun muassa yritykset, jotka eivät vielä edes tiedä, että niiltä puuttuu osaamista. Asia voi nousta esiin, kun uutisoidaan kyberrikollisuudesta ja tietoturvaongelmista. Syksyllä 2020 paljastunut ongelma Valvomo-yrityksessä oli tästä esimerkki. Suurin työpaikkojen kasvu voi toteutua yrityksissä, joissa ei ole ennen havaittu kyberosaajatarvetta. Monissa pienissä ja keskisuurissa yrityksissä ei ole tiedostettu koko asiaa, todettiin erään osallistujan toimesta.

Osaamistarpeet ja erikoistumisalat kyselyn perusteella

Kyberturvallisuudessa osaamispulaa on lähes kaikista ammattiryhmistä. Osaamistarpeiden kartoituksessa käytettiin laajasti käytössä olevaa NCWF-viitekehikkoa [6]. Sen avulla voidaan kuvata kyberturvallisuuteen liittyviä kokonaisuuksia tai kategorioita ja sen alla olevia erityisosaamisaloja [7].

Peräti **joka toinen vastaaja (47%) ilmoitti, että heillä on osaajapulaa 2-3 vuoden kuluttua analysointikategorian eri erikoisosaamisalueissa** (Threat, Exploitation, All-Source, Target, Language Analysis). On huomattava, että syksyn 2020 Valvomo-tapaus tuli julkiseksi kyselyn aikana, mikä lisäsi yleisön huomiota uhkien ja tunkeutumisen analysointiin sekä tutkintaan.

Analyysitehtävien lisäksi suuria työvoimatarpeita oli muissakin kategorioissa, kuten turvallisessa tuotannossa, operoinnissa ja ylläpidossa, kokonaisuuden valvonnassa ja johtamisessa, suojaamisessa ja puolustuksessa sekä tutkinnassa. Nämä kokonaisuudet jakaantuvat omiin erikoisaloihinsa. Vähintään joka kolmas vastaajista näki, että seuraavien erikoisalojen ammattilaisia tullaan tarvitsemaan lisää seuraavien 2-3 vuoden aikana: järjestelmäarkkitehtuuri (Systems Architecture), kyberturvallisuuden hallinta (Cybersecurity Management), järjestelmien ja tietojen suojaustarpeiden analysointi (Cybersecurity Defence Analysis), tapahtumiin vastaaminen (Incident Response) ja haavoittuvuusarviointi ja -hallinta (Vulnerability Assesment and Management).

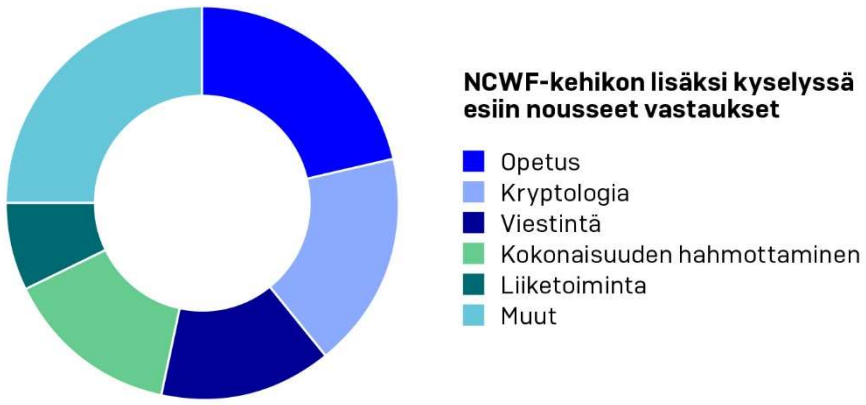
[4] 9 ratkaisua Suomelle - Teknologiateollisuuden Koulutus ja osaaminen -linjaus 2018 (2018).
[5] ISC2 (2020) Cybersecurity Workforce Study, 2020
[6] Viitekehikosta käytettiin kyselyssä nimeä NIST. Kyseessä on Yhdysvaltojen National Institute of Standards and Technologyn (NIST), National Initiative for Cybersecurity Education (NICE) -ohjelmaan liittyvä National Cybersecurity Workforce Framework (NCWF).
[7] Jukka Niemelä (2019), Kyberturvallisuusalan työvoiman kysyntä, saatavuus ja kehittäminen vastaamaan työvoiman tarvetta Suomessa, pro gradu, Jyväskylän yliopisto.

Vastauksista voidaan tiivistää kaksi suurempaa kokonaisuutta. Näitä ovat **kokonaisuuden hallinta** (mm. järjestelmäarkkitehtuuri, kyberturvallisuuden hallinta, strategiat sekä niitä hoitavat kyberturvallisuus- tai tietoturvajohtajat) ja operatiivisempi **järjestelmien suojaus sekä sitä tukeva analyysi** [8].

Kysely osoitti, että julkisella ja yksityisellä sektorilla on tarpeissaan painopiste-eroja. **Kun julkinen sektori hakee suhteellisesti enemmän hyvin laajasti katsovia johtaja- ja riskinhallintaosaajia, niin elinkeinoelämä hakee hallinta- ja arkkitehtuuriosaajia**[9].

Jos vastaajaluokkia pilkotaan pienemmiksi ryhmiksi, nähdyt osaamistarpeet eivät juurikaan muutu muutamia poikkeuksia huolimatta. Yritykset, jotka tuottavat **kyberturvallisuuden palveluita tai tuotteita tarvitsevat enemmän ohjelmistokehittämisen ja järjestelmäarkkitehtuurin ammattilaisia**. **Kuntasektorilla tarve oli muita pahempi asiakaspalvelussa ja teknisessä tuessa sekä projektinhallinnassa ja johtamisessa**. Viimeksi mainitut alat eivät olleet muiden sektoreiden vastauksissa yleisiä. **Kolmannen sektorin** toimijoita oli vastaajien joukossa vähän, mutta heille **datan hallinta ja analysointi** olivat erityisen tärkeitä erityisosaamisalueita.

Kyselyssä tarjotut vastausvaihtoehdot olivat NCWF-kehikosta. Tämän lisäksi annoimme vastaajille mahdollisuuden vastata vapaasti. Tässä esiin tulivat erityisesti kryptologia, viestintä, opetus sekä erilaiset maininnat kokonaisuuden hahmottamisesta.



[8]Joka neljäs vastaajista katsoi, että heillä on pulaa seuraavien erikoisalojen osaajista: riskinhallinta (Risk Management), ohjelmistokehitys (Software Development), järjestelmäarkkitehtuuri (Systems Architecture), arviointi ja testaus (Test and Evaluation), järjestelmäkehitys (Systems Development), datan hallinta (Data AdmiNCWFration), verkkoympäristön hallinta (Network Services), järjestelmäympäristön hallinta (Systems AdmiNCWFration), kyberturvallisuuden hallinta (Cybersecurity Management), strateginen suunnittelu ja linjaukset (Strategic Planning and Policy), kyberturvallisuus/tietoturvallisuusjohtaja (Executive Cybersecurity Leadership), järjestelmien ja tietojen suojaustarpeiden analysointi (Cybersecurity Defence Analysis), kyberturvallisuuden puolustusinfrastruktuuri (Cybersecurity Defense Infrastructure), tapahtumiin vastaaminen (Incident Response), haavoittuvuusarviointi ja -hallinta (Vulnerability Assesment and Management), analysointi kaikki mm. uhkien ja tunkeutumisen analysointi (Threat, Exploitation, All-Source, Target, Language Analysis), kyberturkinta (Cyber Investigation).

[9] Kyberturvallisuus-tietoturvajohtaja julkinen sektori 30%, elinkeinoelämä 26%; riskinhallinta julkinen sektori 36%, elinkeinoelämä 29%; kyberturvallisuuden hallinta julkinen sektori 37%, elinkeinoelämä 44%; datan hallinta julkinen sektori 33%, elinkeinoelämä 27%; järjestelmäarkkitehtuuri julkinen sektori 33%, elinkeinoelämä 44%.

Muut selvitykset

Kokonaisuuden hallinta ja järjestelmien suojaus sekä sitä tukeva analyysi ovat yhteneviä Huoltovarmuusorganisaation selvityksen kanssa, jossa tarkasteltiin huoltovarmuuden kannalta keskeisten toimialojen kyberturvallisuuden kypsyystasoa. Siinä havaittiin, että tärkeimmät yhtenevät kehityskohteet liiketoiminnan näkökulmasta olivat 1. Yrityksen kyberturvallisuusstrategia, 2. kyberturvallisuusarkkitehtuuri ja 3. tekninen jäljitettävyys[10].

Kyberala (FISC) ry:n jäsenkyselyn perusteella kyberturvallisuuden tuotteita ja palveluita tarjoavat vastaajat tarvitsivat osaajia seuraavilla alueilla: ohjelmisto-osaaminen, liiketoiminnallinen osaaminen, strateginen kyberturvallisuusosaaminen, kryptografia/kryptologia, tekninen kyberturvallisuus, ylläpidon ja valvonnan osaaminen sekä järjestelmäarkkitehtuurin osaaminen[11].

Teknologiateollisuuden osaaja- ja osaamisselvitys 2021 (2018) kysyi yrityksiltä ICT-osa-alueiden tärkeimpiä osaamistarpeita. Niitä olivat robotiikka ja automaatio, tuotteiden/palveluiden älykkyyden kehittäminen, toiminnanohjaus/tuotetietojärjestelmät, pilvipalvelut sekä data-analytiikka[12]. Kyberturvaaja-hankkeessa esille nousivat perustason kyberturvallisuusosaaminen koko henkilöstölle. Lisäksi tarvetta oli johdon osaamisen kehittämiseen, tiettyjen toimialaosaamisten tarpeisiin ja uusien teknologioiden käyttöön. Vastausten hajonta oli erittäin laaja [13].

Digibarometri 2020: Kyberturvan tilannekuva Suomessa -selvityksessä tarkasteltiin muun muassa kyberalan työpaikkailmoituksia[14]. Tarkasteluna ajankohtana etsittiin erityisesti järjestelmäarkkitehtuurin, alan liiketoiminnan, ohjelmistojen sekä ylläpidon ja valvonnan ammattilaisia. Niemelä (2019) löysi työpaikkailmoituksista eniten turvalliseen tuotantoon, operointiin ja ylläpitoon sekä valvontaan ja hallinnointiin liittyviä avoimia tehtäviä [15].

Globaalin ISC-kyselyn (2018) mukaan osaamispula on kriittinen seuraavilla aloilla: turvallisuusymmärrys (58%), riskiarviointi, analyysi ja johtaminen (58%), turvallisuusjohtaminen (53%), verkon valvonta (52%), havaintojen tutkinta ja vaste (52%), tunkeutumisen havaitseminen (52%), pilvipalvelut (51%) ja turvallisuussuunnittelu (51%) [16].

Osaamistarpeet ja erikoistumisalat - käsittely työpajoissa

Työpajoissa arvioitiin huolestuttavia kyselytuloksia. Asiantuntijoista 18 vahvisti kyselyn tulokset, mutta kaksi piti tilannetta vielä tätäkin pahempana. Kukaan ei pitänyt ongelmaa pienempänä.

Ensimmäisessä keskustelussa tiedusteltiin myös, milloin ongelmat saadaan ratkottua. Panelisteista kaksi optimistisinta arvioi, että ongelma saadaan kurottua yli viidessä vuodessa. Neljä näki, että ongelmaa ei saada hoidettua nykyisillä toimintatavoilla.

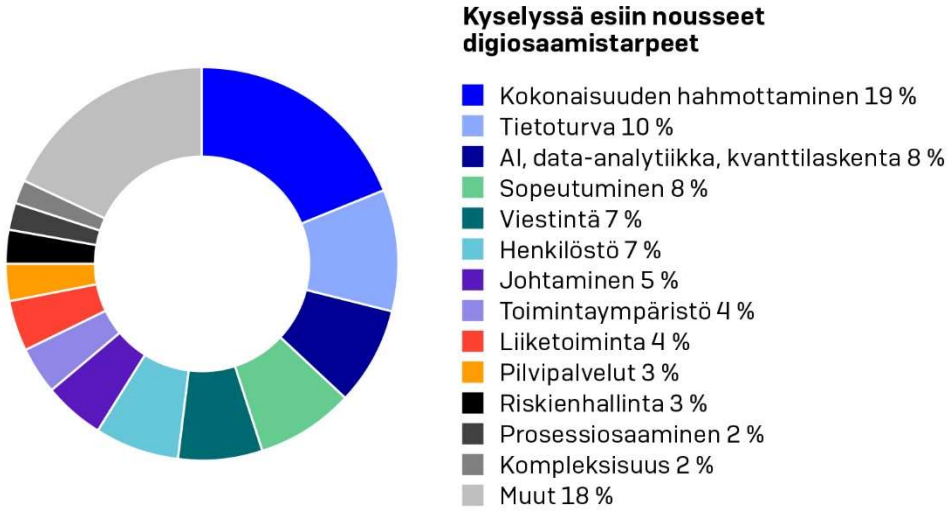
[10] Kyberturvallisuuden nykytila eri toimialoilla -kartoituksen keskeiset havainnot (2020), Huoltovarmuuskeskus.
[11] Kyberala (FISC) ry jäsenkysely 2020.
[12] 9 ratkaisua Suomelle - Teknologiateollisuuden Koulutus ja osaaminen -linjaus 2018 (2018).
[13] Kyberturvaaja-hanke - loppuraportti, tulokset, yhteenvedot ja tuotokset (2020), Metropolia ammattikorkeakoulu, Oulun yliopisto, Tampereen ammattikorkeakoulu, Tampereen korkeakoulusäätiö sr ja Turun ammattikorkeakoulu
[14] Digibarometri 2020: Kyberturvan tilannekuva Suomessa (2020), Taloustieto.
[15] Niemelä (2019)
[16] ISC2 (2018) Cybersecurity Workforce Study, 2018

Esiselvitykseen liittyneessä asiantuntijatyöpajassa nousi esille, että insinöörikoulutuksessa oppimisen esteet eivät ole kyberiin liittyvässä teknologiassa vaan kompleksisuuden ymmärtämisessä. Kompleksisuus tarkoittaa tässä mm. monia vuorovaikutteisia elementtejä, joiden yhteistoiminta vaikuttaa kyberturvallisuuteen. Tämäntyyppinen ongelman hahmotus voi selittää miksi vastaajat – erityisesti julkisella sektorilla – nostivat keskeiseksi osaamistarpeeksi kokonaiskuvan hallinnan.

Keskusteluissa todettiin myös, että tutkintoon johtavassa koulutusvaatimukset ovat jo nyt laajat. Keskittyminen oppiaineiden erikoistumisvaiheisiin tai muihin aiheisiin voi jättää perusosaamisen heikoksi. Olisikin päästävä useammin tilanteeseen, jossa esimerkiksi hyvä ohjelmoija tekee asiat kyberturvallisesti, oli hän kyberin erikoisosaaja tai ei. **Turvallisuus on eräs laadun mittari.**

Mitä uusia osaamisia tarvitaan jatkossa?

Kyselyn perusteella tulevien digiosaamistarpeiden suunta on jo nähtävissä. Osaamistarpeiden tarkkaa muutosta on vaikea tietää, mutta vastaajat olettavat **digiosaamistarpeiden kehityksen etenevän saman suuntaisena myös lähivuosien jälkeen**. Kyselyssä pyydettiin vastaajia vapaamuotoisesti kertomaan, mitkä ovat digitaalisen työelämän tärkeimmät osaamistarpeet seuraavan kymmenen vuoden kuluessa. Vastaajien kirjoitukset (165 kpl) ryhmiteltiin ja esiin useimmiten seuraaviin ryhmiin kuuluvia termejä: **1. Kokonaisuuden hallinta, 2. tietoturva, 3. sopeutuminen jatkuvaan muutokseen ja 4. uusin teknologia**, jota kuvaavat tekoäly, data-analytiikka, kvanttilaskenta ja robotiikka. Viestintään, henkilöstöosaamiseen ja johtamiseen liittyvät termit olivat myös varsin yleisiä vastauksia.



Vastauksista ei ilmennyt mitään uutta nousevaa trendiä tai teknologiaa, josta ei olisi jo laajemmin puhuttu. Käänteentekevät muutokset tulevat aina jonkinlaisina yllätyksinä. Eräässä Digibarometri 2020 -haastattelussa mainittiin, että yritykset eivät välttämättä osaa arvioida, millaisia tietoturvan osaajia ne muutaman vuoden päästä tarvitsevat.

Työpajat eivät keskittyneet yksittäisten erikoisalojen tilanteeseen. Keskusteluissa todettiin, että liian jäykät ja yksityiskohtaiset suunnitelmat eivät huomioi teknologioiden kehitystä tai paikallisten työnantajien tilannetta. Kielteisenä esimerkkinä nostettiin lyhyeksi jäänyt Symbian-osaajien koulutus, joka palveli vain paria toimijaa.

Keskusteluissa pohdittiin, tuleeko kyberturvallisuuskoulutuksen painopisteitä muuttaa. Eniten kannatusta sai asioiden kehittäminen paikallisesti yhteistyössä eri toimijoiden kanssa. Toisaalta lähes yhtä paljon nähtiin, että isoja muutoksia ei tarvita, vaan se toteutuu askeleittain kysynnän ja tarjonnan mukaan. Keskeinen havainto on, että yritysten ja oppilaitosten **vuoropuhelun merkitys on erittäin suuri.**

Osaajien löytäminen

Kyberosaajien rekrytointi ja osaamisen ylläpito kyselyn perusteella

Kyberturvallisuustoimijat hakevat rekrytoinnissaan ensisijaisesti valmiita ammattilaisia (kysymys 7). Osaajat löytyvät ylivoimaisesti useimmiten muiden työnantajien palkkalistoilta. Lähes ¾ vastasi, että valmiit ammattilaiset ovat ensisijainen keino saada osaajia. **Töissä perehdyttäminen ja yliopistomaisterit** ovat myös kohtuullisen suosittuja tapoja saada osaajia sekä yritys- että julkissektorille.

Edellä mainittujen reittien jälkeen julkiselle sektorille pääsi seuraavia opintopolkuja pitkin: YAMK, työntekijän täsmäkoulutus, AMK ja yliopisto (kandidaattitaso) ja muut kanavat. Nämä olivat kuitenkin selvästi vähemmän suosittuja. Mahdollisuus osallistua tutkintoon valmistavaan koulutukseen näyttää hajottavan mielipiteitä: joidenkin vastaajien työantajat hyödyntävät sitä, kun osa julkisen sektorin organisaatioista ei käytä sitä lainkaan.

Yritykset löysivät ammattilaisensa useampaa eri reittiä. Moninaisuudesta huolimatta on nähtävissä, mitä taustoja arvostettiin. Tyypillisen vastaajan suosituimmuuslista oli seuraava: valmiiden ammattilaisten rekrytointi, yliopisto (maisteritaso), AMK, töissä perehdyttäminen ja ulkomailta palkkaaminen. Yliopisto (kandidaattitaso) ja YAMK tulivat näiden jälkeen.

Kansainvälinen rekrytointi jakaa vahvasti yrityskenttää. Tulosten perusteella osa yrityksistä kelpuuttavat mielellään ulkomaalaisosaajan samalla kuin osa pitää keinoa vähiten suosittuna tapana saada osaajia. Laaja hajonta voi selittyä asiakkaiden erilaisilla vaatimuksilla.

Esiselvityksen vastaajien mielestä **rekrytoinnit ovat melko onnistuneita.** Vastausten keskiarvo oli 6 asteikolla 0 .. 10 niin julkisella sektorilla kuin yritysten joukossa.

Kyselyssä haettiin vastauksia myös osaamisen ylläpitoon. Tärkeimmäksi tavaksi nousi töissä perehdyttäminen. Julkinen sektori kannusti lisäksi omaehtoiseen opiskeluun ja täsmäkoulutukseen. Yritykset suosivat perehdyttämisen lisäksi myös kurssi- ja messumatkoja sekä täsmäkoulutusta.

Kyberosaajien rekrytointi tulevaisuudessa kyselyn perusteella

Näyttönsä jo antaneista työntekijöistä kilpaillaan entistäkin enemmän jatkossa. Tämä selvisi kysyttäessä, kuinka toimijat haluavat saada ammattilaisensa lähivuosina (kysymys 9). Vastaajat laittoivat järjestykseen, mistä aikovat tulevaisuudessa rekrytoida.

Eteenpäin suuntaava kysymys toistaa hyvin pitkälle nykytilannetta. Noin **80% vastaajista näki, että myös jatkossa ensisijaisesti etsitään valmiita ammattilaisia. Yliopisto (maisteritaso) pysyy seuraavaksi suosituimpana taustana niin julkisella sektorilla kuin yrityksissäkin**.

Julkiselle sektorille kolmanneksi suosituin tapa lisätä osaajia oli töissä perehdyttäminen. Sektori näyttää tulevaisuudessa olevan aiempaa valmiimpi järjestämään työntekijälle mahdollisuuden osallistua tutkintoon valmistavaan koulutukseen. YAMK ja täsmäkoulutus nousevat myös esille.

Yritysvastaajat näkivät, että seuraavaksi yleisimmät tavat saada ammattiosaajia olivat töissä perehdyttäminen, ulkomaalaisten rekrytointi, työntekijän täsmäkoulutus, YAMK ja yliopistokandidaatit. AMK-valmistuneiden asema näyttää hieman heikentyvän suhteessa nykytilaan.

Esiselvityksessä kartoitettiin (kysymys 10), kuinka paljon oppilaitoksista tulee uusia kandidaatteja, maistereita ja tohtoreita. Kymmenen henkilöä kertoi, kuinka monta henkilöä opiskeli kyberturvallisuutta vastaajien yliopistoissa. Vuonna 2019 valmistui 334 opiskelijaa. Koulutusohjelmissa oli 3057 kandidaatti- maisteri tai tohtoriopiskelijaa.

Koulutustasolla on selkeä suhde työllistymiseen, mikä on havaittu aiemmissa tutkimuksissa. Epäsuhta eri opintopolkujen suosion välillä voi pysyä pinnan alla niin kauan kuin osaamisvajetta ei saada täytettyä. Yhteistyö oppilaitosten ja työnantajien välillä parantaisi tilannetta.

Muut selvitykset

Vaikka kyselyn tulokset eivät korostaneet täsmäkoulutuksen merkitystä, niin muut selvitykset ovat osoittaneet sen potentiaalin. Viiden korkeakoulun Kyberturvaaja-hankkeessa kysyttiin tarkemmin koulutuksista ja havaittiin yritysten toivovan lyhyitä, käytännönläheisiä ja mahdollisimman lähellä pidettäviä koulutuksia, joissa päästään myös tekemään harjoitus[17]. Tulosten ero voi selittyä sillä, että tässä esiselvityksessä vastaajat laittoivat rekrytointireitit suosituimmuusjärjestykseen, kun Kyberturvaaja-hankkeessa aktivoitiin vastaajat jo pohtimaan tämän tyyppisiä koulutuksia.

Digibarometri 2020 -selvityksessä haastatellut suuremmat yritykset mainitsivat käyttävänsä Euroopan ja Aasian laajuisia suorahakuja. Kansainväliset rekrytoinnit voivat tuoda jopa kilpailuetuja, mainitsi eräs Digibarometrin haastateltava.

Suomessa suositaan selvästi enemmän rekrytointeja muilta työnantajilta kuin mitä maailmalla tehdään. Kansainvälisen ISC työvoimakyselyssä (2020) Euroopassa suosituinta oli käyttää konsultteja työvoimatarpeen täydentäjinä. Globaalisti vastavalmistuneet olivat suosituin rekrytoinnin lähde [18].

Niemelän (2019) tutkielmassa haastatellut työhonottajat näkivät koulutuksessa laadullisia puutteita. Syinä oli muun muassa koulutuksen jälkeenjääneisyys ja käytännön osaamisen puutteet [19].

Eurooppalaisessa tutkimuksessa nähtiin, että työnantajat haluavat uusien työntekijöidensä osaavan välittömästi kaiken tarpeellisen. Mutta dynaamisessa ympäristössä osaaminen voi vanhentuakin nopeasti. Oppilaitosten on siksi haettava tasapaino opiskelijoidensa houkuttelevuuden ja vankan osaamisperustan tarjoamisen välillä, arvioi ENISA. Eurooppalaisessa kontekstissa osaamispulan merkittävimmät syyt ovat opettajapula, huono yhteistyö teollisuuden kanssa, heikko ymmärrys työmarkkinoista, huonot oppimisalustat ja jälkeenjääneisyys [20].

[17] Kyberturvaaja-hanke - loppuraportti, tulokset, yhteenvedot ja tuotokset (2020),
[18] ISC2 (2020) Cybersecurity Workforce Study, 2020
[19] Niemelä (2019)
[20] ENISA Report - Cybersecurity Skills Development in the EU (December 2019)

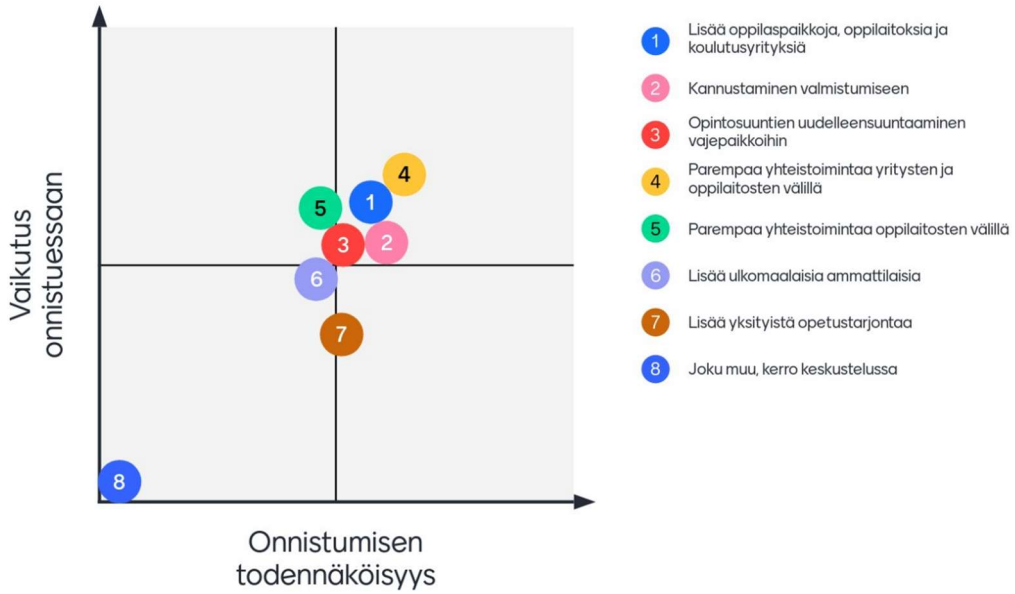
Koulutuksen tarjoajia on Suomessa merkittävä määrä sekä julkisella, yksityisellä että kolmannella sektorilla. Kyberalan koulutus Suomessa -tutkimuksessa kartoitettiin 7 yliopiston ja 9 ammattikorkeakoulun koulutustarjonta. Tämän lisäksi koulutusta tuottivat muun muassa puolustusvoimat varusmiehille ja Maanpuolustuskoulutusyhdistys sekä useita yrityksiä. Osa koulutuksista keskittyy kyberturvallisuuteen mutta useimmissa ohjelmissa kyberturvallisuuden opetus on integroitu osaksi eri koulutusohjelmiin. [21]

Kyberosaajien rekrytointi – käsittely työpajoissa

Vaikka yleisesti julkisella sektorilla koettiin kovempaa pulaa osaajista, niin yritykset olisivat todellisuudessa palkkaamassa useampia kyberosaajia. Eräässä vastauksessa nähtiin, että erityisesti julkisella sektorilla rahapulan vuoksi koko kysely – ja siten ratkaisuyritykset - ovat ”irti todellisuudesta”. Asiantuntijakeskustelun osallistujista suuri enemmistö koki, että ongelmat eivät tule ratkeamaan nykyisillä menettelytavoilla. Tilanteen on siis muututtava.

Ensimmäisessä työpajassa pohdittiin, kuinka kyberosaamiseen liittyvät ongelmavyyhti lähtisi purkautumaan. Osallistujat kirjoittivat näkemyksensä, joista useimmat liittyivät yritysyhteistyöhön, lisäresursseihin, eri opiskelumuotojen kehittämiseen (ml. joustavuus, työn opinnollistaminen) sekä opetussuunnitelmien ja koulutusohjelmien merkitykseen.

Keskustelijat arvioivat myös eri toimenpiteiden onnistumismahdollisuuksia, ja saman toimenpiteen onnistumisen vaikutusta. Kahdessa keskustelussa tulokset olivat hyvin samankaltaisia. **Yritysyhteistyö** ja **oppilaspaikkojen lisääminen** olivat sekä helpoimmat toteuttaa, ja tuottivat onnistuessaan parhaat tulokset.



[21] Lehto & Niemelä (2018) Kyberalan tutkimus ja koulutus Suomessa 2019, Jyväskylän yliopisto.

Oppilaspaikkojen lisääminen kustannustehokkaasti edellyttää myös **parempaa yhteistyötä oppilaitosten sisällä ja niiden kesken**. Resurssikamppailut vaikeuttavat järkevää työnjakoa, ja tällaisista ongelmista on raportoitu niin oppilaitosten kesken kuin sisälläkin. Keskusteluissa arvioitiin oppilaitosten keskinäisen yhteistyön onnistumisen mahdollisuudet keskinkertaista huonommiksi.

Keskustelussa nostettiin esille, että hyvätasoisten valmistuneiden lukumäärää vähentää opiskelijoiden 50-60 prosenttiin kipuavat **keskeyttämiset**. Ratkaisukeinona tarjottiin, että **valmistumiseen on luotava riittävästi houkuttimia**. Opintovaatimusten vähentäminen ei ole sellainen, mutta erilaisten näyttöjen hyväksyminen opintosuorituksiksi voi sitä olla. Tällainen työn opinnollistaminen vaatii joustavuutta ja yhteistoimintahalua kaikilta osapuolilta. Valmistumiseen tai sertifikaattien hankkimiseen kannustaminen edellyttää myös monelta työnantajalta uusia toimintatapoja. Kulttuurin kehittäminen ei välttämättä synny itsestään, vaan työnantajiinkin on vaikutettava viestinnällisesti ja markkinoinninkin keinoin. Moninaisten opintopolkujen toteutuminen edellyttää hyvää paikallista vuoropuhelua. **Yhteistyön parantaminen työnantajien ja oppilaitosten välillä vähentää keskeyttämisiä ja tuottaa parempia valmistuneita oppilaitoksista.**

Toisessa työpajassa keskustelijat (15) laittoivat myös tärkeysjärjestykseen, mihin julkisen vallan rajalliset panostukset osaamisongelmassa tulisi laittaa. Vaihtoehto ”Kyberopintoja useammin osaksi muuta korkean asteen koulutusta” oli selkeä ykkönen, jota seurasi ”Kyberkoulutusta vauvasta vaariin”, muiden vaihtoehtojen seuratessa myöhemmin. Tärkeysjärjestys osoittaa toiveen, että valtakunnan tasolta tulevien ohjeiden ja rahoituksen avulla viedään kybertaidot osaksi muuta opetusta ja kaikille kansalaisille. Keskusteluissa todettiin, että lähes kaikissa ammateissa kyberturvallisuus on osa uuden työelämän perustaa, kuten taito kirjoittaa tietokoneella, ei salaperäinen tai erillinen erikseen opiskeltava osa. Tämän lisäksi tarvitaan kyberkursseja ja jopa kybertutkintoja. Näiden vaikuttavuus riippuu vahvasti yhteistyöstä paikallisten toimijoiden kanssa.
Kun tarkennettiin, kuinka yhteistyötä tulisi lisätä työnantajien ja koulutuslaitosten välillä, niin vastaukset olivat hyvin selkeitä. ”Työsuoritusten laajempi hyväksilukeminen opintosuorituksiksi” sekä ”Yhteistyön tiivistäminen paikallisella tasolla” koettiin kohtuullisen helpoiksi saavuttaa ja vaikuttaviksi onnistuessaan. Valtakunnallisia portaaleja esimerkiksi opinto-ohjelmista, opinnäyte/harjoittelutiedoista pidettiin kyllä melko helppoina toteuttaa, mutta niiden vaikutukset koettiin edellä mainittuja pienemmiksi.

Johtopäätökset

Esiselvitys osaamistarpeista keskittyi seuraaviin kysymyksiin: millaiset ovat koulutus- ja rekrytointitarpeet, kuinka hyvin nykyinen kyberturvallisuuskoulutus vastaa kysyntään, ja miten yritysten ja julkisen sektorin kysyntään osaajista voidaan vastata.

Vastausten perusteella Suomessa on merkittävä vaje henkilöistä, jotka pystyvät hallitsemaan kyberturvallisuuteen liittyviä kokonaisuuksia. Tämä pitää paikkansa niin 2-3 vuoden kuluttua kuin kymmenen vuoden päästä. Toinen kokonaisuus on operatiivisempi kyberpuolustus, mutta siinä ennustehorisontti näyttää ulottuvan vain muutaman vuoden päähän.

Kyberosaamisen isot teemat jakaantuvat pienempiin osaamisalueisiin, joista lähes kaikista oli Suomessa pulaa. Ankarin vaje oli analyysiosaamisessa, josta ilmoitti joka toinen vastaaja. Lisäksi viiden muun erikoisalan osaajia tarvittiin joka kolmannessa organisaatiossa.

Tekijäpulan merkitys vaihtelee vastaajien joukossa. Ongelma on joillekin toimijoille jopa toiminnan vaarantava. Useimmat työnantajat pystyvät silti sopeutumaan työvoimavajeeseen, mikä ei poista yhteiskunnallisia – talouteen ja turvallisuuteen liittyviä - menetyksiä. Investointi koulutuspaikkojen ja laajemminkin aihepiirin integroimiseen muuhun koulutukseen näyttää tuottavalta panostukselta.

Tarjolla on merkittävä määrä työpaikkoja, vienti- ja verotuloja, jos tarjonta saataisiin sujuvasti vastaamaan kysyntää.

Rekrytoinnissa työnantajat keskittyvät etsimään ammattilaisia ensisijaisesti muilta toimijoilta. Työnantajat löytävät tekijänsä myös muilla keinoin. Yliopistomaisterit ja ehkä töissä perehdyttäminen nousevat seuraaville sijoille. Muiden reittien suosio on merkittävästi pienempi.

Ankara rekrytointikilpailu jo näyttönsä antaneista ammattilaisista ei vielä lisää uusien osaajien määrää tai paranna vastavalmistuneiden mahdollisuuksia. Koulutusta olisi lisättävä tehokkaasti siten, että työnantajat arvostaisivat uusiakin osaajia. Nopeammin suunniteltavat ja toteutettavat koulutukset helpottavat myös teknologisen kehityksen mukana pysymistä.

Erikoistumisalueen pätevyyden tuottavat ja osoittavat koulutusohjelmat ovat osa ratkaisua. Esimerkiksi Kyberturvaaja-hankkeessa kehitettiin olemassa olevista tutkintokoulutusten osista lyhyitä työelämäkoulutuksia, mitkä voivat nopeasti laventaa osaamistarpeita. Yksityinen sektori tarjoaa erityisesti eri sertifikaatteihin liittyvää täsmäkoulutusta.

Olisi hyvä, jos oppilaitokset pystyisivät hyväksymään erilaisia töissä tehtäviä suorituksia. Työn opinnollistaminen edellyttää joustavuutta, mutta ei laadun laskemista. On myös työnantajien etu, että työntekijät saavat opintonsa valmiiksi.

Tämäkin esiselvitys vahvistaa huomioita, että työnantajat eivät vahvasti luota vastavalmistuneiden osaamiseen. Muunto- ja lisäkoulutukset, jotka osoittaisivat uusien erikoistumisalojen pätevyyttä, eivät ole myöskään ottaneet sitä roolia, minkä voisivat. Uusia opintopolkuja on markkinoitava myös työnantajille.

Käytännönläheistä, ajassa elävää kyberkoulutusta on lisättävä. On myös kerrottava työnantajille, että näiden kannattaa olla mukana osaamisen vahvistamisessa. Kaksisuuntainen viestintä auttaa kysynnän ja tarjonnan kohtaamisessa vaikuttamalla työnantajien asenteisiin ja koulutuksen sisältöön.

Kyberturvallisuus on osa digitalisoituvaa arkea, ja siksi osaamista tarvitsee jokainen. Kyberturvallisuuden erikoisosaajien on ymmärrettävä laajempi kokonaisuus. Mutta toisaalta lähes kaikissa ammateissa kyberturvallisuus on osa uuden työelämän perustaa. Ymmärrys kyberturvallisesta toimintatavasta olisi upotettava osaksi kaikkia opintoja. Kyberturvallisuus on yksi läpileikkaava teema, ja vain harvoille se tärkein. Perustaitojen hallinta luo paremman perustan kaikille. Sen päälle on turvallisempaa rakentaa.