Digi-baro-metri 2020

BUSINESS FINLAND
LIIKENNE- JA VIESTINTÄMINISTERIÖ
Elinkeinoelämän keskusliitto EK
Yrittäjät

Digibarometri 2020:

Kyberturvan tilannekuva Suomessa

Juri Mattila – Kalle Mäkäräinen – Mika Pajarinen –
Timo Seppälä – Jyrki Ali-Yrkkö – Elias Tervo

Etlatieto Oy
Kustantaja: Taloustieto Oy
Helsinki 2020

Julkaisijat
Business Finland
Liikenne- ja viestintäministeriö
Elinkeinoelämän keskusliitto EK
Suomen Yrittäjät

Toteutus
Etlatieto Oy

Kustantaja
Taloustieto Oy, Helsinki 2020

ISSN 2489-7159 (pdf)
ISBN 978-951-628-730-3 (pdf)

Suositeltava lähdeviittaus tähän vuosiraporttiin:
Mattila, Juri – Mäkäräinen, Kalle – Pajarinen, Mika – Seppälä, Timo –
Ali-Yrkkö, Jyrki – Tervo, Elias (2020).
Digibarometri 2020: Kyberturvan tilannekuva Suomessa Helsinki: Taloustieto Oy.

Digibarometri 2020

Esipuhe

Vuosina 2014–2019 julkaistut digibarometrit ovat kertoneet kansakunnan digitaalisen asennon sekä siinä tapahtuneet muutokset, myös suhteessa muihin maihin. Näin on jälleen tänäkin vuonna. Perinteisen digibarometrin tulokset ja havainnot löytyvät julkaisun alun tiivistelmästä ja liitteestä 3. Jo kolmatta kertaa muu osuus Digibarometri-julkaisusta rakentuu yhden pääteeman ympärille. Tänä vuonna teemaksi on valittu kyberturva ja tulevaisuuden digitaalinen luottamus.

Aiempien digibarometrien perusteella tiedämme, että heräämisensä jälkeen Suomi kiri itsensä vertailun kärkisijoille. Vuoden 2020 tuloksista on kuitenkin havaittavissa, että digitalisaation vaikutukset Suomalaisiin yrityksiin ovat jäämässä verrokkimaiden yrityksistä jälkeen.

Suomessa ollaan ottamassa vahvaa etukenoa ja investoimassa kvanttilaskentaan liittyvien kyberuhkien torjumiseen. Kvanttilaskennan laajempi soveltaminen vaatii toteutuakseen uuden salausalgoritmiikan ja standardoinnin. Toistaiseksi kvanttilaskentaan liittyvien salausalgoritmiikan ja sen eri teknologioiden osaaminen ovat maailmalla harvojen käsissä. Investoinnit tänään uusien salausalgoritmien ja kvanttiteknologioiden kehittämiseen mahdollistavat Suomelle vahvan roolin tulevaisuuden teknologioiden soveltajana. Kvanttilaskennan ja siihen liittyvien kyberuhkien kehittyminen tulisikin nostaa yrityksissä ja julkisella sektorilla nopeasti strategiseen tason seurantaan erityisesti Suomen huoltovarmuuteen liittyvillä kriittisillä teollisuudenaloilla.

Vuoden 2020 Digibarometri julkaistaan 11.6.2020 koronapandemian tähden verkkotilaisuudessa. Kiitos Etlatieto Oy:lle tutkimuksen ja julkaisun toteutuksesta.

Kirsi Kokko & Marko Heikkinen
Business Finland

Janne Hauta
Liikenne- ja viestintäministeriö

Leena Nyman & Mika Tuuliainen
Elinkeinoelämän keskusliitto EK

Joonas Mikkilä
Suomen Yrittäjät

Digibarometri 2020: Suomi hopealla

Suomi nostaa sijoitustaan yhden pykälän ollen hopealla kahden viime vuoden pronssitilojen jälkeen vuoden 2020 Digibarometrissä (22 maata, 36 muuttujaa). Tanska nousee toiselta tilalta vertailun kärkeen, ja Yhdysvallat tippuu niukasti kolmanneksi. Kolmen kärki on äärimmäisen tasainen mahtuen yhden indeksipisteen sisälle. Myös seuraava, edellisvuotiset sijoituksensa säilyttävä kolmikko – Alankomaat, Norja ja Ruotsi – hengittää tiukasti palkintopallisijoitusten tuntumassa (kuvio 1; täydelliset tulokset liitteessä 3).

Digibarometrissä mitataan *digitaalisuuden hyödyntämistä*. Mittaus tehdään *kolmella tasolla* (edellytykset, käyttö ja vaikutukset) ja *kolmella pääsektorilla* (yritykset, kansalaiset ja julkinen). Tasoittain tarkasteltuna Suomi menestyy parhaiten *edellytyksissä* (2., sijoitus ei muuttunut) ja *käytössä* (2., sijoitus nousi 3 sijaa). *Vaikutuksissa* (5.) sijoitumme heikommin, vaikka sijoituksemme nousikin yhden pykälän viime vuodesta (liitekuvio 39).

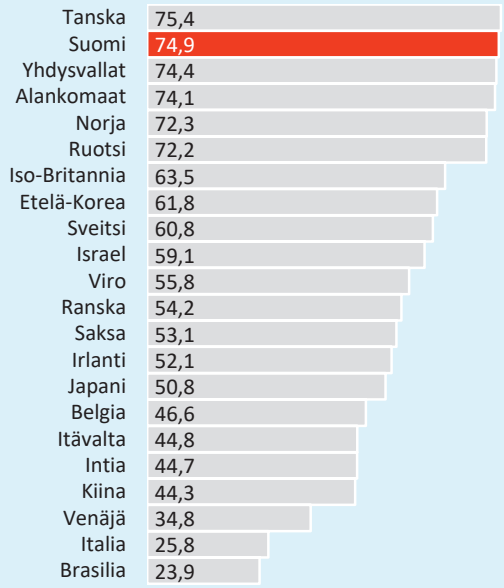
Sektoreittain tarkasteltuna Suomi on toinen *julkisen* sektorin (ei muutosta), kolmas *kansalaisten* (ei muutosta) ja seitsemäs *yritysten* (-3 sijaa)

Kuvio 1

Digibarometri: Kokonaisindeksi.

Tanska, Suomi ja Yhdysvallat ovat Digibarometrin kärkikolmikko. Alankomaat, Norja ja Ruotsi ovat tiiviisti kärkikolmikon imussa. Heikoiten menestyvät Brasilia, Italia ja Venäjä.

Lähde: Indeksin laskentatapa ja rakenne käyvät ilmi liitteen kuvauksesta. Tiedot ovat vuodelta 2019. Maa saa arvon 100 (arvon 1), jos se on paras (huonoin) kaikissa mukana olevissa osatekijöissä.



vertailussa. Yksityiskohtaisempien tasojen ja sektorien muodostamien solujen tarkastelussa sijoituksemme heikentyy eniten yritysten edellytyksissä (-6 sijaa). Viime vuoden barometriin verrattuna suomalaisten yritysten on ollut vaikeampaa rekrytoida osaavia ict-alan ammattilaisia. Myös nopeissa laajakaistayhteyksissä ja pilvipalveluiden valmiuksissa suomalaisten yritysten suhteellinen asema vertailumaiden joukossa on viime vuoteen verrattuna heikentynyt.

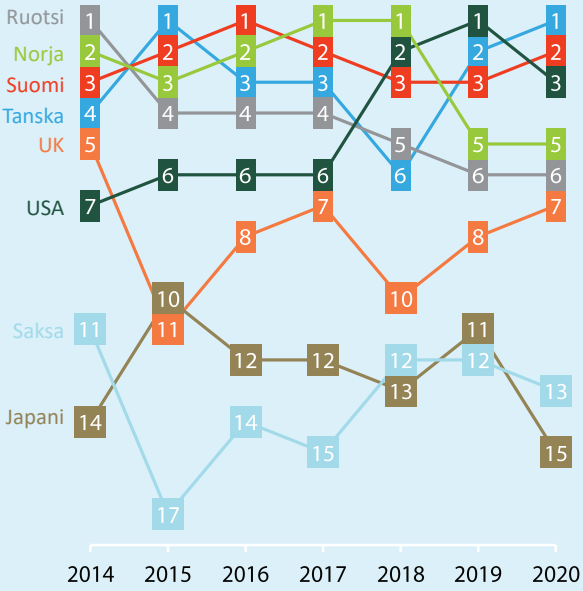
Suomi on ollut seitsemän vuoden ajan tasaisen varmasti Digibarometrin kolmen parhaan maan joukossa. Kuten kuviosta 2 havaitaan, useiden maiden historiaan mahtuu verrattain suuriakin vuosittaisia vaihteluita sijoituksissa. Digibarometrin historiassa eniten sijoitustaan on parantanut Yhdysvallat, joka oli vuoden 2014 vertailussa vasta sijalla seitsemän mutta nousi viime vuonna ykköseksi. Tänä vuonna tiukassa otannassa se kuitenkin tippui pari pykälää kolmanneksi. Toiseksi eniten vuoden 2014 vertailusta sijoitus on noussut Tanskalla (sijalta 4 tämän vuoden sijalle 1). Tanskalla sijoitusten vuosittainen hajonta on ollut verraten suurta sijoitusten vaihdellessa sijojen 1–6 välillä. Kärkimaista vuodesta 2014 vuoteen 2020 eniten asemaansa on puolestaan menettänyt Ruotsi, joka oli kärjessä vuonna 2014

Kuvio 2

Digibarometri: Eräiden vertailumaiden sijoitukset vuosina 2014–2020.

Suomi on ollut tasaisen varma suorittaja Digibarometrissa. Sijoitustaan on eniten nostanut vuodesta 2014 Yhdysvallat. Eniten asemiaan on menettänyt Ruotsi.

Lähde: Digibarometrit 2014–2020.



mutta on nyt sijalla 6. Norja oli barometrin alkuvuosina kärkikolmikossa ja jopa ykkösenä vuosina 2017 ja 2018, mutta on parina viime vuonna hiipunut sijalle 5. Isolla-Britannialla taivallus Digibarometrissa on ollut melkoista vuoristorataa. Se oli viides vuonna 2014, putosi seuraavana vuonna peräti sijalle 11, nousi sieltä parissa vuodessa sijalle seitsemän ja jälleen kahden heikommin sujuneen vuoden jälkeen löytyy nyt samalta sijalta seitsemän. Saksa ja Japani eivät ole vertailun perusteella digitalisaation kärkimaita. Japanin paras sijoitus on kymmenes sija vuodelta 2015 tänä vuonna sijoituksen ollessa 15. Saksan paras sijoitus on puolestaan 11. vuodelta 2014, tämän vuoden vertailussa se päätyy sijalle 13.

1. Suomi on yhä digitalisaation kärkikastia – mutta alkaako ote lipsua?

Kansa ja julkinen sektori pitävät pintansa – yritysten tilanne jatkaa laskuaan

Tämän vuoden Digibarometrissa suomalaisten yritysten sijoitus laski kolme sijaa yrityssektorin globaalissa kokonaisvertailussa. Kyseessä on Suomen osalta suurin yksittäinen pudotus moneen vuoteen Digibarometrin historiassa. Osatekijöiden tarkastelussa eniten suomalaisten yritysten sijoitus tippui digitaalisten edellytyksien (-6) ja vaikutusten (-2) osalta. Pientä nousua puolestaan tapahtui digitaalisten teknologioiden käyttöönotossa sekä käytön yleisyydessä (+2). Toisaalta julkinen sektori sekä kansalaiset pitävät pystyssä Suomen edelleen erinomaista sijoitusta Digibarometrissa.

Miksi suomalaisten yritysten sijoitus jatkaa laskemistaan jo toisena vuotena peräkkäin? Tähän kysymykseen kaivattaisiin pikaista vastausta. Mikäli negatiivinen kehitys edelleen jatkuu tulevina vuosina, voi suomalaisten yritysten kilpailukyky jo jatkossa vaarantua digitaalisten edellytyksien heikentymisen vuoksi.

Suomalaisten yritysten kokonaissijoitus tippui kolme sijaa. Se on suurin pudotus moneen vuoteen Digibarometrin historiassa.

Digitalisaatio ei pysähdy odottamaan Suomea. Sen kehitys kulkee vääjäämättä kohti tietojärjestelmien entistä vahvempaa yhteensulautumista. Kun informaatio liikkuu eri toimijoiden välillä uusin tavoin ja koko ajan nopeammalla vauhdilla, kehityskulku etenee kohti systeemisempää ja laaja-alaisempaa verkostoituneisuutta. Tässä muutoksessa digitaalisilla alustoilla on ollut keskeinen rooli. Se, kykenevätkö kotimaiset yritykset seuraamaan ja hyödyntämään tätä kehityskulkua nykyistä paremmin tulevina vuosina, on ratkaiseva tekijä Suomen tulevaisuuden kehityksen kannalta.

Kyberturvallisuuden teema ajankohtaisempi kuin koskaan

Kyberturvallisuuden merkitys digitalisaation keskeisenä tekijänä on korostunut viime vuosina. Kyberuhat aiheuttavat nykyisellään satojen miljardien

eurojen menetykset yksilöille, yrityksille ja julkisille sektoreille maailmassa vuosittain. Jo vuonna 2016 tietoturvayhtiö McAfee arvioi kyberrikollisuuden maailmanlaajuisiksi kustannuksiksi 600 miljardia euroa – eli karkeasti noin 0,8 % koko maailman vuotuisesta bruttokansantuotteesta. Sittemmin kyberuhkien kasvu ei ole hidastunut. (McAfee, 2018)

Ciscon tietoturvaohjelmistojen kirjaamien lokitietojen valossa kyberhavaintojen määrä nelinkertaistui maailmassa vuosina 2016–2017. Vastaavasti F-Securen taannoisten arvioiden mukaan kyberhyökkäysten määrä oli kaksinkertaistunut vuonna 2018 edellisvuoteen verrattuna. Sen lisäksi, että kyberriskien yleisyys sekä laaja-alaisuus ovat kasvaneet, niiden merkittävyys on myöskin viime vuosina lisääntynyt. Muun muassa Euroopassa GDPR-lainsäädännön mahdollistamat sanktiot yrityksille tietoturvan laiminlyönneistä ovat lisänneet taloudellisten seuraamusten uhkaa niin suurten kuin myöskin pienten yritysten näkökulmasta.

Alituisesti kasvava uhka liiketoiminnan vuosittaisista menetyksistä on vuosien saatossa ruokkinut globaalia kyberturvallisuusalan kasvua. Vuonna 2017 kyberturvayritysten vuosittaiseksi liikevaihdoksi arvioitiin jo yli 150 miljardia dollaria. Alan liikevaihdon on ennustettu kasvavan noin kymmenen prosentin vuosittaista vauhtia (Statista, 2018).

Kyberuhkien ja kyberturvallisuuden maailmassa eletään jatkuvaa kilpavarustelua hyökkääjien ja puolustajien välillä. Näin ollen, kyberturvallisuuteen liittyvillä teknologoilla ja työkaluilla on yleensä verrattain lyhyt elinkaari. Kyberturvallisuuden hallitseminen vaatiikin toimijoilta jatkuvaa ja yhä nopeampaa reagointia sekä uuden oppimista. Uudet, nopeasti muuttuvat teknologiat aiheuttavat osaamisvajetta yrityksissä. Toisaalta myös toimintaympäristön nopeat muutokset asettavat haasteita kyberturvan suhteen. Esimerkiksi COVID-19 -koronaviruspandemian yhteydessä on havaittu joidenkin tilannetietoja välittävien infopaneelisivustojen varastavan käyttäjiensä arkaluonteisia tietoja.

Kärki karkaamassa Suomelta myös kyberturvassa

Eurostat-tilastodatan pohjalta arvoituna Suomen kyberturvallisuuden tilanne on kohtuullisen hyvä muuhun Eurooppaan verrattuna. Useimmilla mittareilla Suomi sijoittuu selkeästi EU28-maiden keskiarvon paremmalle puolelle. Tilastojen valossa näyttää kuitenkin siltä, että Suomi on jäämässä kehityksessä terävimmän kärjen vauhdista. Niin ikään pohjoismaisessa vertailussa Ruotsi ja Tanska jättävät useimmilla mittareilla tarkasteltuna Suomen varjoonsa.

Suomessa kuitenkin panostetaan digitaitojen opetteluun selvästi muuta Eurooppaa ja myös muita Pohjoismaita enemmän. Vaikkakin taitojen opetteluun käytettyjen lisäpanostusten vaikutukset näkynevät viiveellä, herää tilastoista kysymys, kohdistuuko Suomessa tekeminen tässä suhteessa oikeisiin asioihin.

Data on monen suomalaisen yrityksen suurin yksittäinen tunnistamaton riskitekijä.

Huolestuttavana piirteenä Suomen tilanteessa vaikuttaa korostuvan erityisesti tietosuoja. Etenkin älylaitteiden kohdalla kuluttajien tietoturvakäyttäytymistä näyttää leimaavan jonkinlainen piittaamattomuus omien tietojen käytöstä, eikä niinkään tiedon ja osaamisen puute. Myös kotimaisissa yrityksissä tietovuodot näyttäytyivät erityisen korostuneessa roolissa, joskin niiden taustalla vaikuttavat tekijät jäävät epäselviksi.

Yrityskokovertailussa Suomessa parhaiten suoriutuivat pienyritykset. Niiden osalta lähes kaikilla mittareilla kyberturva-asioiden hoito oli Euroopan unionin keskitasoa paremmalla tolalla. Vaikkakin suuryrityksissä kyberturvallisuus oli selkeästi pienyrityksiä vahvempaa, EU-maiden vertailussa suomalaiset suuryritykset näyttäytyivät alisuoriutujina. Myös keskisuurten kotimaisten yritysten tilanne jättää paikoitellen toivomisen varaa erityisesti Ruotsin ja Tanskan vastinpareihin verrattuna.

Kyberturva näkyy heikosti suomalaisten yritysten viestinnässä

Tämän vuoden Digibarometrissa selvitettiin, miten hyvin sitoutuneisuus kyberturvallisuuden teemaan näkyy koko suomalaisen yrityskentän julkisessa viestinnässä. Tulosten perusteella suomalaisten yritysten liityntä kyberturvan teemaan yritysten omien verkkosivujen pohjalta näyttää varsin heikolta. Vainun yritystietokannasta tehtyjen hakujen perusteella suomalaisista yrityksistä noin 95 % ei maininnut kyberturvallisuuteen liittyviä hakutermejä lainkaan verkkosivuillaan.

Noin 20 000 yritystä, eli viitisen prosenttia Suomen yrityskentästä, toisaalta mainitsi vähintäänkin jonkin sovelletuista hakukriteereistä. Suuryritykset, nuoret yritykset sekä kaupan alan yritykset olivat hakuosumissa keskimääräistä useammin edustettuina. Ohjelmistoala ja tietopalvelutoimintayritykset näyttivät esimerkkiä, mutta niidenkin osalta osumaprosentti oli alhainen – vain hieman yli 14 %.

Tulisiko kyberturvallisuus entistä vahvemmin alkaa nähdä yrityksissä kilpailuetutekijänä?

Kertooko hakuosumien alhainen osuus huolestuttavaa tarinaa suomalaisten yritysten sitoutumattomuudesta kybervalmiuksien kehittämiseen? Suomalaisessa yrityskentässä tulisikin pohtia sitä, pitäisikö kyberturvallisuus aiempaa vahvemmin alkaa nähdä digitalisaation keskeisenä kilpailutekijänä. Vastaavasti on syytä pohtia, tulisiko kyberturva ottaa myös vahvemmin osaksi yritysten viestintästrategiaa?

Kyberturvaosaamisessa yhdistyvät tekninen ja strateginen kyvykkyys

Osana tämänkertaista Digibarometria haettiin myös näkymää siihen, millaisia tietoturvaosaajia eurooppalaisilla työmarkkinoilla tällä hetkellä ja lähitulevaisuudessa kaivataan. Vastausta kysymykseen etsittiin Concordian eurooppalaisia korkeakouluja, yrityksiä ja tutkimuslaitoksia yhteen kokoavan *Cyber Security Competence for Research and Innovation* -tutkimuksen pohjalta. Se listaa 200 erilaista tiedollista kyvykkyytä sekä 90 käytännön taitoihin liittyvää osaamisaluetta tulevaisuuden kyberasiantuntijalle.

Concordian tutkimuksessa noin viidesosa tulevaisuuden kyberturvakompetenssista muodostui teknisistä tiedoista ja taidoista. Lähes yhtä tärkeinä korostuivat niin ikään ylläpito- ja valvontaosaaminen sekä järjestelmäarkkitehtuurien tuntemus. Toisaalta kompetenssin osatekijöissä korostui myös suurten kokonaisuuksien hahmottaminen eli strategisen ymmärryksen sekä laajemman liiketoimintaosaamisen merkitys. (Concordia, 2020)

Kyberturvan tulevaisuuden huipputekijöiltä edellytetään lähes 300 eri kyvykkyyttä, mukaan lukien laajempaa liiketoiminnan ymmärrystä.

Toisena keskeisenä mielenkiinnon kohteena Digibarometri 2020 -tutkimuksessa selvitettiin tältä osin suomalaisen kyberturva-alan mahdollista osaamisvajetta. Kartoitus tehtiin Suomen kyberturva-alan edunvalvontajärjestö FISC:n keväällä 2020 tehdyn jäsenyritystutkimuksen pohjalta. Sen perusteella noin 60 % kotimaisista kyberturva-alan yrityksistä kokee pulaa alan osaajista. Työvoimapula koettiin myöskin yrityksissä haasteeksi kasvun

kannalta. Kaikkein kipeimmin jäsenyrityksissä kaivattiin digitaalisen identiteetin osaajia, pilviarkkitehtuurien osaamista, sekä tekijöitä, joilta löytyy liiketoimintaosaamista kyberturvaosaamisen rinnalle. Useimmiten näitä osaajia päädyttiin rekrytoimaan muualta Euroopasta ja Intiasta, koska Suomesta sopivaa osaamista ei välttämättä löytynyt – tai jos löytyikin, oli heille työmarkkinoilla erittäin kova kysyntä.

Digitaalinen huoltovarmuus vaatii digi-identiteetin kehitystä

Digitalisaation eteneminen kohti integroituneempia, systeemisempiä kokonaisuuksia asettaa kyberturvaan liittyviä haasteita myös digitaalisen identiteetin eri ilmentymille. Esimerkiksi Internetiin kytkettäville laitteille tullaan jatkossa tarvitsemaan henkilöiden tunnistautumisen kaltainen digitaalinen identiteetti. Vastaavasti tuotteille ja palveluille, sekä niitä tarjoaville yrityksille tullaan tarvitsemaan vastaavat tunnistautumisen käytänteet. Henkilöiden, laitteiden ja yritysten digitaaliset identiteetit ovat keskeisessä roolissa, kun mietimme tulevaisuuden kyberturvallisia digitaalisia yritys- ja yhteiskuntarakenteita.

Kuluttajien, tuotteiden sekä palveluiden kyberturvallisuuden on kehityttävä tasapainossa keskenään.

Suomen tulisikin luoda henkilöiden digitaalisen tunnistautumisen rinnalle, vastaavan kaltainen menetelmä yrityksille sekä niiden tuotteille ja palveluille. Digitaaliset identiteetit helpottavat uusien tiedonsiirron käytänteiden muodostumista. Kun digitaalinen luottamus paranee, vuorovaikutus digitaalisten järjestelmien välillä lisääntyy. Näin digitalisaation tiedonvälityksen uudet mahdollisuudet saadaan paremmin valjastettua hyötykäyttöön.

Kvanttilaskenta haastaa miettimään kyberturvakäytänteet uusiksi

Kvanttitietokoneiden kehityksessä saavutettiin viime vuonna yksi keskeinen virstanpylväs, kun Google ja Yhdysvaltain avaruushallinto NASA julkistivat saavuttaneensa ns. *kvanttiherruuden*. Mahtipontinen käsite viittaa tilanteeseen, jossa kvanttitietokone kykenee suoriutumaan jostakin sellaisesta tehtävästä, joka perinteiselle tietokoneelle olisi käytännöllisesti katsoen mahdoton ratkaistava. Koejärjestelyssä Googlen Sycamore-kvanttiproses-

sori suoriutui 200 sekunnissa laskutoimituksesta, johon maailman nopeimmalta supertietokoneelta olisi perinteisin menetelmin kulunut noin 10 000 vuotta.

Googlen edistysaskeleesta huolimatta, useimpien arvioiden mukaan laajamittaisia kvanttilaskennan käytännön sovelluksia saataneen odottaa vielä 15–20 vuotta. Kvanttilaskennan kyberuhat ovat kuitenkin jo nyt todellisia. Jos vaikkapa tänään salattavat arkaluonteiset tiedot joutuvat huomenna vääriin käsiin, ei tietojen paljastumista tulevina vuosikymmeninä voida enää estää. Lisäksi lienee myös todennäköistä, että valtiollisten intressien johdosta aivan pisimmälle ehtineestä kvanttilaskennan kehityksestä ei välttämättä valu tietoa julkisuuteen, ennen kuin suojautumisen näkökulmasta on jo liian myöhäistä.

Kvanttilaskennan kyberuhat ovat jo todellisia. Erityisesti kriittisissä järjestelmissä niihin on syytä alkaa varautua jo tänään.

Vaikkakin kvanttitietokoneet ovat vielä pitkälti kehitysasteella, kvanttilaskennan uhkiin on syytä alkaa varautua jo nyt. Kvanttiturvallisia salausmenetelmiä onkin jo markkinoilla tarjolla, joskin huomattavan kalliiseen hintaan. Kvanttilaskennan aikaan valmistautumiseksi yhteiskunnan olisi kuitenkin syytä laatia suunnitelma siitä, millä aikataululla ja missä järjestyksessä yhteiskunnan kriittisiä järjestelmiä aletaan päivittää kvanttiturvallisen salauksen piiriin. Myös esimerkiksi aloilla, joilla laiteinvestointien elinkaaret ovat pitkiä, on kvanttisalauksen mahdollisuuteen syytä kiinnittää huomiota jo nyt tulevien järjestelmien suunnittelussa.

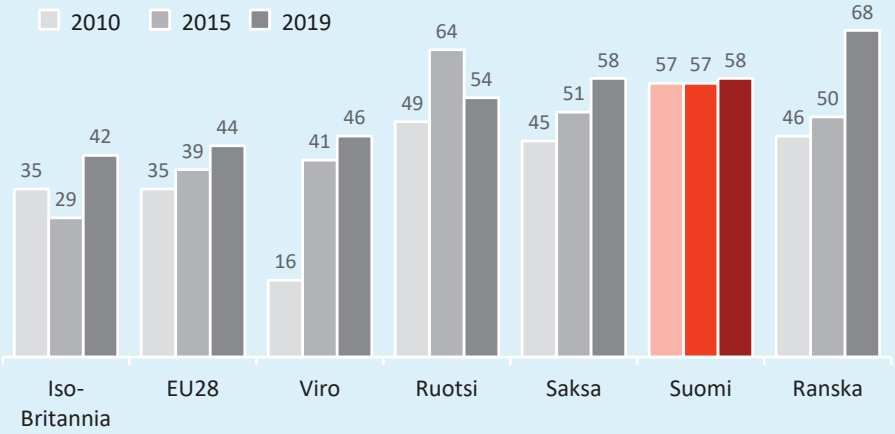
2. Kyberturvallisuuden tilannekuva Suomi vs. EU28

Yhä useampi jättää Euroopassa käyttämättä joitakin digitaalisia tuotteita tai palveluita kyberturvallisuuteen liittyvien huolien vuoksi. Kun vuonna 2010 noin kolmannes eurooppalaisista Internetin käyttäjistä oli rajannut käyttöään turvallisuushuolien vuoksi, oli vastaava osuus vuosikymmenen lopulle tultaessa kohonnut jo 44 prosenttiin. Erityisen suuret hyppäykset tässä suhteessa nähtiin mm. Virossa (16 % → 46 %) sekä Ranskassa (46 % → 68 %). Suomessa sen sijaan turvallisuushuolien vuoksi käytöstä pidättäytyneiden määrä säilyi tasaisella 57–58 %:n tasolla läpi koko vuosikymmenen.

Kansalaisten kokemat kyberturvaongelmat kohdentuvat eri tavoin monien eri luokittelujen suhteen. Vuonna 2019 koetut kyberturvaongelmat olivat esimerkiksi asteittain sitä yleisempiä, mitä urbaanimmasta ympäristöstä

Kuvio 3 **Internetin käyttäjät, jotka jättivät jonkin digitaalisen tuotteen tai palvelun käyttämättä turvallisuushuolien vuoksi (2019), %.**

Vuonna 2019 entistä useampi eurooppalainen Internetin käyttäjä jätti digitaalisia tuotteita tai palveluita käyttämättä kyberturvaan liittyvien huolien vuoksi. Erityisesti Virossa ja Ranskassa harppaukset ovat kuluneen vuosikymmenen aikana olleet huomattavia.



Lähde: Eurostat, Väestön tietotekniikan käyttö (ICT usage in households and by individuals).

oli kyse. Vastaavasti kyberturvaongelmia esiintyi korkeakoulutetuilla enemmän kuin matalasti koulutetuilla. Koettujen ongelmien yleisyys korreloi myös mm. tulotason suhteen: mitä suuremmat tulot, sitä enemmän kyberturva aiheuttaa päänvaivaa. Niin ikään sukupuoli oli selittävä tekijä, sillä miehillä kyberuhkiin törmääminen oli yleisempää kuin naisilla keskimäärin.

Mobiililaitteiden kyberturva – piittaamattomuutta dataliikenteessä?

Mobiililaitteiden käyttö verkkopalveluiden päätelaitteina lisääntyi niin yksityishenkilöillä kuin myös työelämässä läpi koko kuluneen vuosikymmenen. Sen seurauksena yleistyi myös erilaisten älypuhelinsovellusten käyttö.

Viime vuosina verkkopalveluiden käytössä on entistä enemmän siirrytty selainpohjaisista palveluista erilaisten älypuhelinsovellusten käyttöön. Yksityishenkilöiden tietoturvassa älypuhelinlaitteet ovatkin entistä enemmän nousemassa kyberturvallisuustarkastelun keskiöön.

> ”Tavanomainen älypuhelin lähettää päivän aikana dataa keskimäärin kymmeneen eri maahan 18 eri sovelluksen välityksellä.”
>
> *– Verizon 2020 Mobile Security Index.*

Sovellusten käyttäjistään keräämien tietojen laajuuteen onkin viime aikoina julkisessa keskustelussa herätty aiempaa paremmin. Siitä huolimatta Euroopassa huomattava osuus mobiilisovellusten käyttäjistä ei vuonna 2018 kertaakaan rajoittanut yhdenkään sovelluksen oikeutta kerätä tietoja itsestään. Kansalaisten mobiilikäytön valveutuneisuudessa on nähtävissä Euroopan unionin tasolla merkittäviä eroavaisuuksia jäsenvaltioiden välillä.

Varsin mielenkiintoisena poikkeamana datasta erottuu Avast-kyberturvayhtiön kotimaa Tšekki. Siellä nimittäin jopa kaksi kolmesta älypuhelimen käyttäjästä ei rajoittanut asentamiensa älypuhelinsovellusten käyttöoikeuksia lainkaan.

Kun sovellusten käyttöoikeuksien rajoittamattomuuden syitä tarkastellaan lähemmin, paljastuu motiiveista piirre, joka mm. Suomen kannalta on kenties huolestuttavampi kuin miltä tilanne äkkiseltään vaikuttaa. Esimerkiksi, kun Islannissa vuonna 2018 13 % älypuhelinten käyttäjistä ei rajoittanut käyttämiensä älypuhelinsovellusten käyttöoikeuksia, 12 % käyttäjistä ei

tiennyt rajoittamisen ylipäätään olevan mahdollista. Suomessa sen sijaan jopa 25 % mobiilisovellusten käyttäjistä ei milloinkaan rajoittanut asentamiensa sovellusten käyttöoikeuksia, mutta ainoastaan 4 % ei tiennyt rajoittamisen mahdollisuudesta. Toisin sanoen, yli viidesosa käyttäjistä jätti piittaamatta käyttämiensä sovellusten tiedonkeruuoikeuksista.

Yli viidesosa suomalaisista älylaitteiden käyttäjistä jätti sovellustensa käyttöoikeudet tietoisesti rajoittamatta.

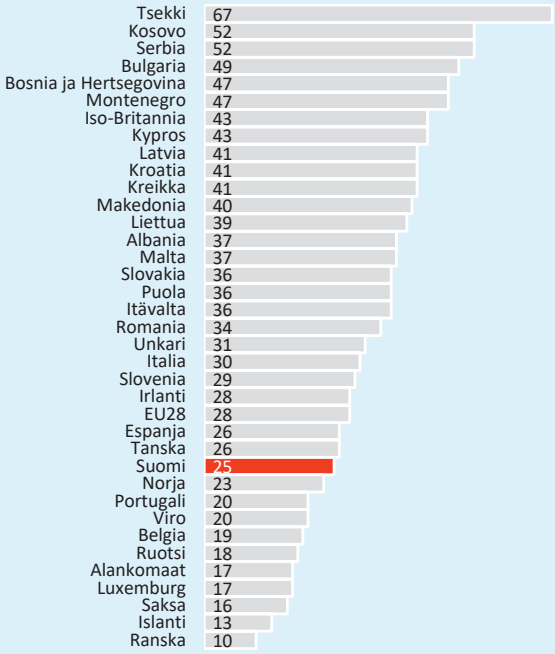
Länsinaapurissamme Ruotsissa eroavaisuus oli Suomea pienempi: käyttöoikeuksia ei rajoittanut 18 %, mutta 8 % ei tiennyt sen olevan mahdollista. Suomea jopa hälyttävämpi tilanne sen sijaan oli Isossa-Britanniassa. Saarivaltiossa jopa 43 % käyttäjistä jätti sovellusten käyttöoikeudet rajoittamatta, mutta vain 3 % käyttäjistä oli tietämätön moisesta mahdollisuudesta.

Kuvio 4

Mobiilikäyttäjät, jotka eivät rajoittaneet asentamiensa sovellusten käyttöoikeuksia (2018), %.

Huomattava osuus EU28-maiden älypuhelinten ja tablettien käyttäjistä ei lainkaan rajoittanut laitteisiin asennettujen sovellusten käyttöoikeuksia. Valtaosa heistä jätti rajoitukset asettamatta, vaikka tiesi sen olevan mahdollista.

Lähde: Eurostat, Väestön tietotekniikan käyttö (ICT usage in households and by individuals).



Niin ikään aiemmin mainitussa Tšekissä tiedon puute asiassa vaivasi ainoastaan 5 %:a vastaajista, vaikka käyttöoikeudet jätti rajoittamatta 67 %.

Älypuhelimiin erikseen jälkiasennettujen kyberturvaohjelmistojen yleisyydessä esiintyi niin ikään huomattavia eroja Euroopan unionin valtioiden välillä. Tilaston kärjessä paistatteli jälleen Avastin kotimaa Tšekki, jossa joka kolmannelta mobiilikäyttäjältä löytyi erillinen kyberturvaohjelmisto laitteestaan. Myös Suomi sijoittuu selkeästi EU28-keskitason paremmalle puolelle kärjen tuntumaan. Kun Euroopan unionissa keskimäärin 15 %:lla mobiilikäyttäjistä oli erillinen kyberturvaohjelmisto laitteessaan asennettuna, oli vastaava lukema Suomessa 23 %.

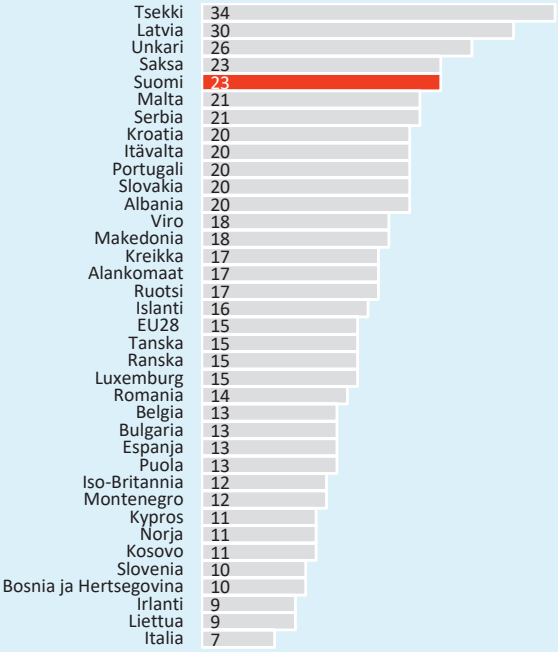
Tuloksellaan Suomi jättää jälkeensä myös muut Pohjoismaat. Vertailussa Ruotsi, Islanti ja Tanska sijoittuvat kaikki lähelle EU-maiden keskitasoa. Norja sen sijaan menestyy aavistuksen heikommin erikseen asennettujen tietoturvaohjelmistojen yleisyyden jäädessä 11 %:iin. Tuloksellaan Norja sijoittuukin tarkkailuasemiin mm. Romanian, Bulgarian, Montenegron sekä Kyproksen hännille.

Kuvio 5

Osuus mobiilikäyttäjistä, joiden älylaitteeseen oli asennettu erillinen kyberturvaohjelmisto (2018), %.

Älylaitteisiin asennettujen kyberturvaohjelmistojen yleisyydessä esiintyi merkittävää vaihtelua EU28-maiden välillä. Vaikka Suomessa ohjelmistot olivat keskimääräistä selvästi yleisempiä, silti niiden esiintyvyys jäi alle neljäsosaan käyttäjistä.

Lähde: Eurostat, Väestön tietotekniikan käyttö (ICT usage in households and by individuals).



Työn digitaalinen haastavuus lisääntyy myös matalasti koulutetuilla aloilla

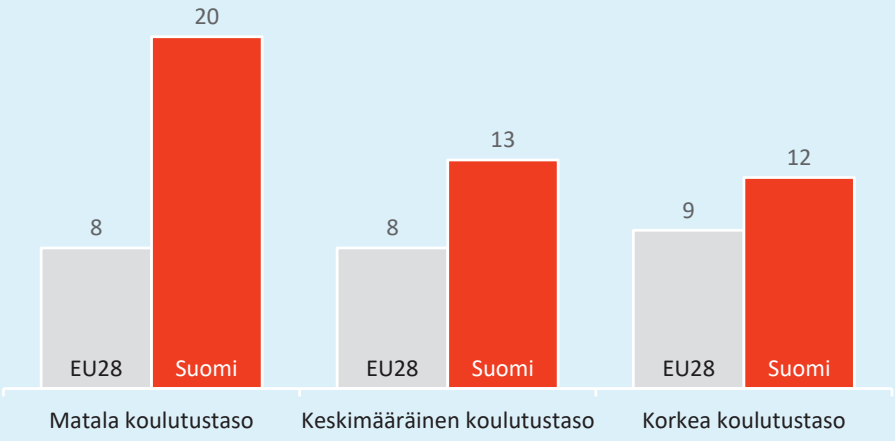
Kun henkilötason tarkastelu rajataan työvoiman muodostaviin yksilöihin, Suomen tilanne erottuu Euroopasta mielenkiintoisella tavalla. Vuonna 2018 Euroopan unionissa tietoteknistä lisäkoulutuksen tarvetta kokivat keskimäärin hieman enemmän korkeasti koulutetut kuin matalammin koulutetut. Suomessa sen sijaan tilanne vaikutti olevan täysin päinvastainen: tietoteknisen lisäkoulutuksen tarvetta kokivat selvästi eniten kaikkein matalimmin koulutetut yksilöt.

Toisin kuin Euroopassa keskimäärin, Suomessa tietoteknisen lisäkoulutuksen tarve oli suurin matalimmalla koulutustasolla.

Paradoksaalisesti kaikkein vähiten lisäkoulutustarvetta tietotekniikan, ohjelmistojen ja applikaatioiden käyttöön kaipasivat korkeakoulutetut – siis juuri ne, jotka tietoturvaongelmia kokivat kaikkein eniten. Mahdollista

Kuvio 6 **Tietoteknisen lisäkoulutuksen tarvetta kokevien osuus työvoimasta (2018), %.**

Toisin kuin Euroopan unionissa keskimäärin, Suomessa tietoteknisen lisäkoulutuksen tarvetta koettiin eniten kaikkein matalimmin koulutettujen keskuudessa.



Lähde: Eurostat, Väestön tietotekniikan käyttö (ICT usage in households and by individuals).

selitystä voidaan kenties hakea kyberuhkien kehittymisestä vaikeammin havaittaviksi, jolloin kyberhyökkäyksen kohteeksi joutumisen havaitseminen ylipäätään vaatii entistä korkeampaa taitotasoa.

Vaikka lisäkoulutuksen tarvetta koettiin Suomessa eurooppalaista keskiarvoa enemmän, toisaalta suomalaiset myös paransivat ICT-työtaitojaan muuta Eurooppaa selvästi hanakammin. Kun esimerkiksi Euroopan unionissa keskimäärin 9 % matalasti koulutetuista koki ajankäytön uusien tietoteknisten taitojen omaksumiseen lisääntyneen, Suomessa vastaava osuus oli jopa 33 %. Maiden välisessä vertailussa Suomi näyttääkin hallitsevan kärkisijoitusta täysin suvereenisti.

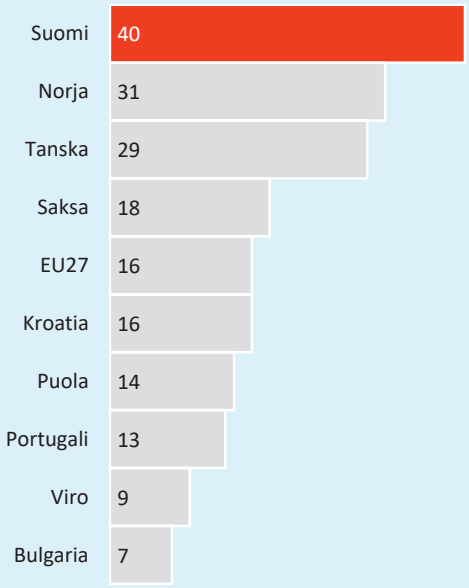
Ylipäätään Pohjoismaat erottuvat vertailussa selvästi edukseen. Suomi, Tanska ja Norja hallitsivat kukin koko työvoiman vertailussa kärkikolmikkosijoituksia yli 10 prosenttiyksikön etumatkan turvin muihin Euroopan maihin nähden. Sen sijaan esimerkiksi eteläinaapuri Viro sijoittui vertailun häntäpäähän, sillä virolaisista ajankäyttöään digitaitojen opetteluun oli lisännyt ainoastaan joka yhdestoista työntekijä.

Kuvio 7

Työntekijät, joilla tietoteknisten taitojen opetteluun käytetty aika lisääntynyt (2018), %.

Pohjoismaissa digitaalisten työtaitojen opetteluun käytetty aika lisääntyi muuta Eurooppaa nopeammin. Suomi hallitsi pohjoismaista kärkikolmikkoa suvereenisti yhdeksän prosenttiyksikön etumatkalla toiseksi sijoittuneeseen Norjaan.

Lähde: Eurostat, Väestön tietotekniikan käyttö (ICT usage in households and by individuals).



Kaiken kaikkiaan vaikuttaa siis siltä, että työn digitaalinen haastavuus lisääntyy kaikilla koulutustasoilla kaikkialla Euroopassa. Kehitys näyttää kuitenkin tässä suhteessa olevan Pohjoismaissa muuta Eurooppaa nopeampaa, ja kaikkein nopeimmalta muutostahti näyttää Suomessa.

Työn digitaalinen haastavuus kasvoi kaikilla koulutustasoilla. Pohjoismaissa uusien digitaitojen opettelu lisääntyi eniten.

Osaltaan tuloksia saattaa selittää se seikka, että pohjoismaalaiset ovat myöskin aktiivisia etätyön tekijöitä. Vuonna 2018 etätöitä vähintäänkin satunnaisesti teki Suomessa 42 % kokoaikaisista ja 29 % määräaikaisista työntekijöistä. Muuhun Eurooppaan nähden Suomi näyttäytyykin tässä suhteessa edelläkävijänä. EU28-maissa nimittäin keskimäärin vuonna 2018 etätöitä teki ainoastaan 23 % kokoaikaisista ja 16 % määräaikaisista työntekijöistä.

Suomalaisten yritysten tietoturva retuperällä

Kuten yksityishenkilöiden kohdalla, myös yrityskentässä kyberturvahaasteet kohdistuvat erilaisiin yrityksiin eri tavoin. Esimerkiksi vuonna 2019 kyberturvaongelmat olivat Euroopassa sitä yleisempiä mitä suuremmasta yrityksestä henkilöstömäärällä mitattuna oli kyse. Kun Suomessa pienistä, 10–50 henkilöä työllistävistä yrityksistä 16 % raportoi tarkastelujaksolla kokeneensa kyberturvaan liittyviä ongelmia, oli vastaava luku keskisuurten yritysten kohdalla 26 %, ja vähintään 250 henkilöä työllistävien suuryritysten sarjassa jopa 42 %.

Suomalaisten mikroyritysten kyberturvallisuudesta kaivataan tarkempaa dataa. Ruotsissa jopa neljäsosa mikroyrityksistä kohtasi kyberturvaan liittyviä ongelmia.

Alle kymmenen henkilöä työllistävien kotimaisten mikroyritysten tietoturvasta on dataa saatavissa varsin niukasti. Suomen osalta vertailukohtaa voitaneen kuitenkin hakea länsinaapurista Ruotsista. Vuonna 2019 ruotsalaisista yhden hengen mikroyrityksistä 12 % oli kohdannut kyberturvaan

liittyviä ongelmia. Kokoluokan kasvaessa myös kyberongelmat vaikuttavat lisääntyvän nopeasti: astetta suuremmista, 2–9 henkeä työllistävistä pienyrityksistä nimittäin Ruotsissa ilmoitti ongelmia kokeneensa jo 27 %.

Pienten yritysten kokemat kyberturvaongelmat olivat vuonna 2019 Suomessa jonkin verran Euroopan unionin keskitasoa yleisempiä. Sikäli kun EU28-maissa kyberturvaongelmia oli kokenut 11 % pienyrityksistä, oli Suomessa vastaava lukema 16 %. Kaikkein hankalin pienyritysten tilanne oli EU28-vertailumaista Ruotsissa, jossa ongelmia esiintyi jopa 32 %:ssa pienyrityksistä – siis kaksi kertaa yleisemmin kuin Suomessa ja jopa lähes kolminkertaisesti EU-maiden keskiarvoon verrattuna.

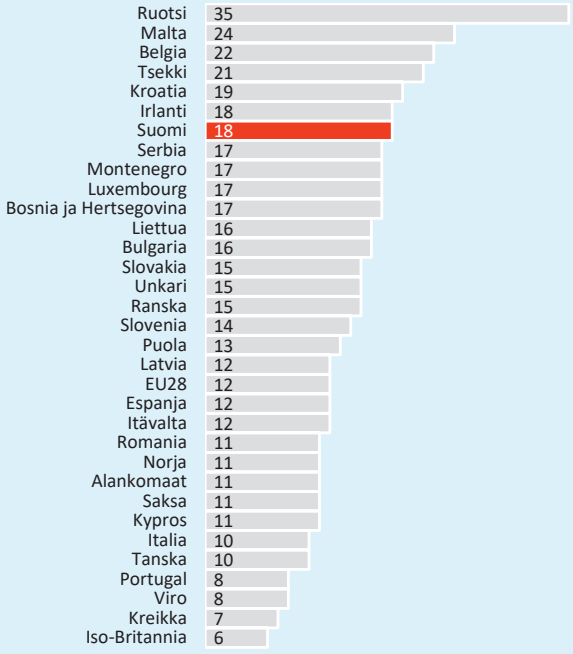
Kaikkein selvimmin pienyritysten kyberturvaongelmat liittyivät niin Suomessa kuin muuallakin Euroopassa palvelukatkoksiin esim. palvelunestohyökkäysten sekä kiristyshaittaohjelmien seurauksena. Toiseksi eniten ongelmia aiheutti tietojen tuhoutuminen esimerkiksi haittaohjelman takia tai ICT-laitteiden tuhoutumisesta tai varkaudesta johtuen.

Kuvio 8

Kyberturvaongelmia vähintään kerran tarkastelujaksolla kokeneet yritykset (2019), %.

Kyberturvaongelmien esiintyvyys vaihteli EU28-maiden välillä huomattavasti. Erityisenä poikkeamana massasta erottui Ruotsi, jossa esiintyvyys oli noin kolminkertainen keskitasoon verrattuna.

Lähde: Eurostat, Tietotekniikan käyttö yrityksissä (ICT usage and e-commerce in enterprises).

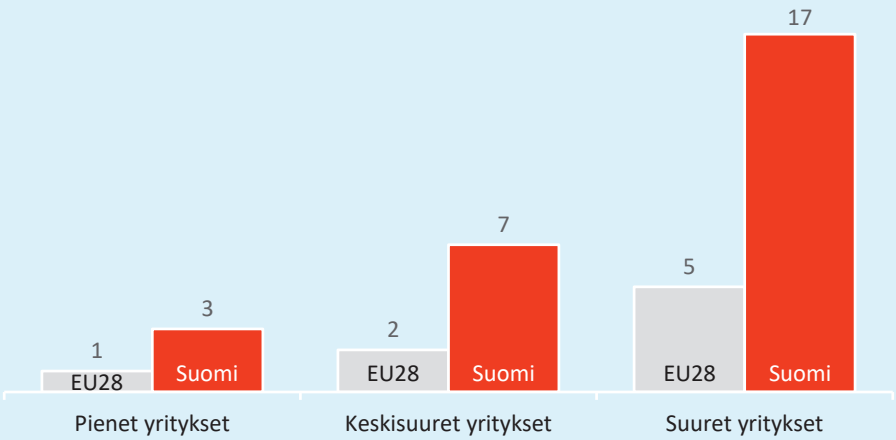


Keskisuurten yritysten tilanne oli Suomessa niin ikään selkeästi EU28-maiden keskiarvoa hankalampi. Kun Euroopan unionissa keskimäärin kyberturvaongelmia oli kyseisen kokoluokan yrityksistä kokenut 17 %, oli Suomessa ongelmia kokenut jo yli neljännes keskikokoisista yrityksistä. Vain Ruotsissa, Tšekissä, Belgiassa ja Montenegrossa tilanne oli tältä osin Suomea heikompi. Ruotsin osuus oli EU28-maiden vertailussa aivan omalla tasollaan, sillä lähes puolet ruotsalaisista keskikokoisista yrityksistä oli kokenut tarkastelujaksolla kyberturvaan liittyviä ongelmia.

Suomalaisten keskisuurten yritysten kokemissa kyberturvaongelmissa korostuvat erityisesti luottamuksellisten tietojen päätyminen vääriin käsiin, esimerkiksi tietojärjestelmämurroista, tietojen kalastelusta sekä työntekijöiden virheellisestä menettelystä johtuen. Kun vuonna 2019 Euroopassa keskimäärin 2 % keskikokoisista yrityksistä raportoi joutuneensa tietovuodon kohteeksi, oli vastaava luku Suomessa jopa 7 %. Suomen osuus on varsin huomattava, sillä lukema oli selvästi EU28-maiden korkein. Lähimmäksi keskikokoisten yritysten tietovuotojen yleisyydessä sijoittuvat Viro ja Montenegro viiden prosentin osuudella kumpainenkin.

Kuvio 9 **Tietovuodon kohteeksi joutuneet yritykset kokoluokittain (2019), %.**

Keskisuurten sekä suurten yritysten tietovuodot olivat Suomessa yli kolme kertaa yleisempiä kuin Euroopassa keskimäärin. Vuonna 2019 joka kuudes suomalainen suuryritys oli joutunut tietovuodon kohteeksi.



Lähde: Eurostat, Tietotekniikan käyttö yrityksissä (ICT usage and e-commerce in enterprises).

Tietovuodot olivat suomalaisissa yrityksissä yli kolme kertaa yleisempiä kuin Euroopassa keskimäärin. Joka kuudes suomalainen suuryritys oli joutunut tietovuodon kohteeksi.

Suuryritysten kentässä sekä Suomi (42 %) että Ruotsi (64 %) sijoittuivat molemmat kyberturvallisuuteen liittyvien ongelmien esiintyvyydessä selkeästi EU:n keskitason (23 %) yläpuolelle vuonna 2019. Ongelmien syyt näyttävät kuitenkin pohjoismaisilla naapureilla poikenneen merkittävästi toisistaan. Ruotsissa suuryritysten kyberongelmat näyttävät liittyneen pääasiassa palvelukatkoksiin johtuen mm. palvelunestohyökkäyksistä, kiristyshaittaohjelmista sekä muista vastaavista ohjelmistojen vikaantumisista.

Suomessa suurten yritysten kyberturvallisuuden haasteissa korostuivat sen sijaan keskisuurten yritysten tavoin erityisesti tietovuodot. Kun esimerkiksi Ruotsissa tietovuotoihin liittyvien kyberturvallisuusongelmien esiintyvyys (8 %) oli lähellä EU-maiden keskitasoa (5 %), oli Suomen suuryrityksissä niiden esiintyvyys (17 %) yli kaksinkertainen Ruotsiin ja jopa yli kolminkertainen EU-maiden keskitasoon verrattuna. Ainoa toinen yli kymmenen prosentin osuuteen yltänyt EU28-maa tässä suhteessa oli Tanska. Siellä tietovuodon kohteeksi oli vuonna 2019 joutunut 12 % maan suuryrityksistä.

Valppaus ja varautuminen kohentuneet, mutta Suomi jää kärjestä

Kyberturvavakuutusten yleisyydessä Suomi sijoittuu kaikkien yritysten tarkastelussa Euroopan unionin keskitasoa paremmin, mutta häviää selvästi pohjoismaisille kilpakumppaneilleen Ruotsille, Norjalle ja Tanskalle. Kun vuonna 2019 Suomessa kyberturvavakuutusta sovelsi 28 % koko yrityskentästä, oli vastaava osuus Ruotsissa 39 % ja Tanskassa jopa 56 %. Myös Norja kiritti vertailussa Suomen edelle 33 %:n osuudellaan.

Kun asiaa tarkastellaan yrityskokoluokittain, erityisesti suurten yritysten tilanne näytti Suomen kohdalla heikolta. Niin Ruotsissa, Tanskassa kuin Norjassakin kyberturvavakuutusten hyödyntäminen suuryrityksissä oli vähintäänkin EU28-maiden keskitasolla (40 %). Suomessa sen sijaan suuryrityksistä kyberturvavakuutuksia toiminnassaan sovelsi ainoastaan noin kolmasosa lukeman jäädessä selkeästi Euroopan unionin keskiarvon alapuolelle.

Kyberturvavakuutukset olivat Suomen pienyrityksissä EU:n keskitasoa yleisempiä, mutta suuryrityksissä sitä harvinaisempia. Pohjoismaille Suomi kuitenkin häviää kaikissa yrityskokoluokissa.

Keskisuurten yritysten joukossa kyberturvavakuutusten esiintyvyys puolestaan heijasteli Suomessa EU28-maiden keskitasoa.

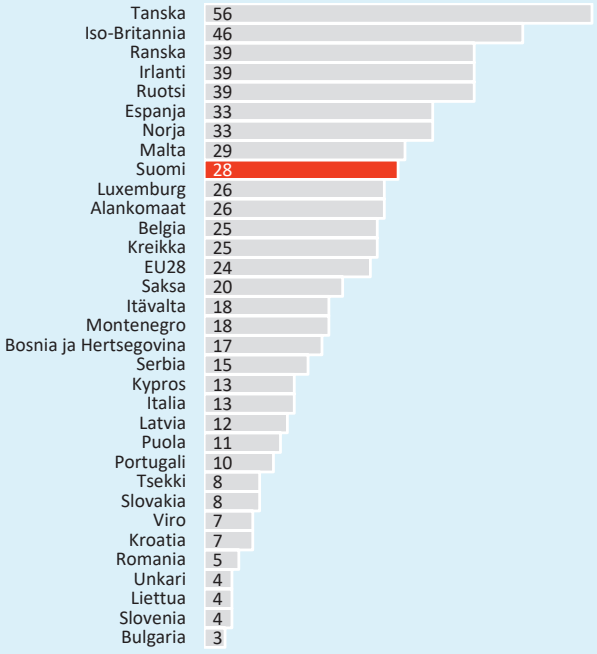
Pohjoismaiden välisessä mittelössä Suomi jää takamatkalle kaikissa yrityskokoluokissa. Vaikka pienten yritysten tarkastelussa Suomi pärjääkin koko Euroopan unionin keskitasoon (22 %) nähden hyvin, on Suomen takamatka tältäkin osin naapureihinsa verrattuna varsin huomattava. Siinä, kun kotimaisista pienyrityksistä hieman yli neljäsosalla (27 %) oli käytössään kyber-

Kuvio 10

Yritykset, joilla käytössä kyberturvavakuutus (2019), %.

Kyberturvavakuutusten yleisyydessä Pohjoismaiden tilanne oli EU28-vertailumaiden keskitasoa parempi. Myös Länsi-Euroopassa tilanne näytti pääosin keskimääräistä valoisammalta.

Lähde: Eurostat, Tietotekniikan käyttö yrityksissä (ICT usage and e-commerce in enterprises).



turvavakuutus, löytyi vastaava vakuutus Norjassa kolmasosalta Ruotsissa lukeman ollen vielä sitäkin suurempi, tarkalleen ottaen 38 %. Pienyritysten osalta koko Euroopan paras tilanne oli kuitenkin Tanskassa, jossa jopa 57 % kyseisen kokoluokan yrityksistä sovelsi kyberturvavakuutusta toiminnassaan. Virossa puolestaan tilanne näytti tässä suhteessa poikkeuksellisen heikolta. Virolaisista pienyrityksistä nimittäin ainoastaan 5 % ilmoitti ottaneensa kybervahingot kattavan vakuutuksen.

Vuoden 2019 tarkastelussa yritysten dokumentoitujen tietoturvakäytänteiden ajantasaisuus oli selvästi kohentunut muutaman vuoden takaisesta tilanteesta. Kehitys viittaa siihen, että kyberturvallisuuden teemaan on ylipäätään eurooppalaisissa yrityksissä viime aikoina havahduttu aiempaa paremmin.

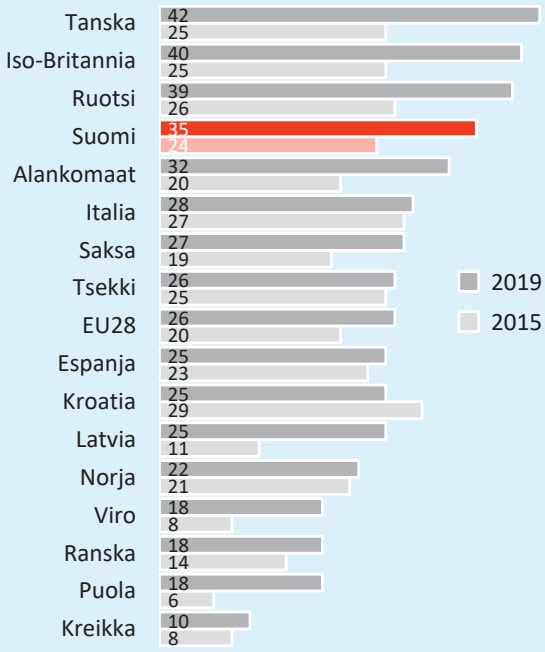
Pohjoismaista Tanskassa, Ruotsissa ja Suomessa taso oli parantunut kautta linjan, mutta Tanska ja Ruotsi ottivat tässä suhteessa Suomea suuremman harppauksen. Myös Iso-Britannia kiri tuoreessa vertailussa Suomen edelle.

Kuvio 11

Yritykset, joiden tietoturvakäytänteet päivitetty viimeisten 12 kk aikana, %.

Tietoturvakäytänteiden ajantasaisuus on parantunut Euroopassa selvästi viimeisten viiden vuoden aikana. Muun muassa Latviassa, Virossa ja Puolassa kehitys on ollut erityisen nopeaa.

Lähde: Eurostat, Tietotekniikan käyttö yrityksissä (ICT usage and e-commerce in enterprises).

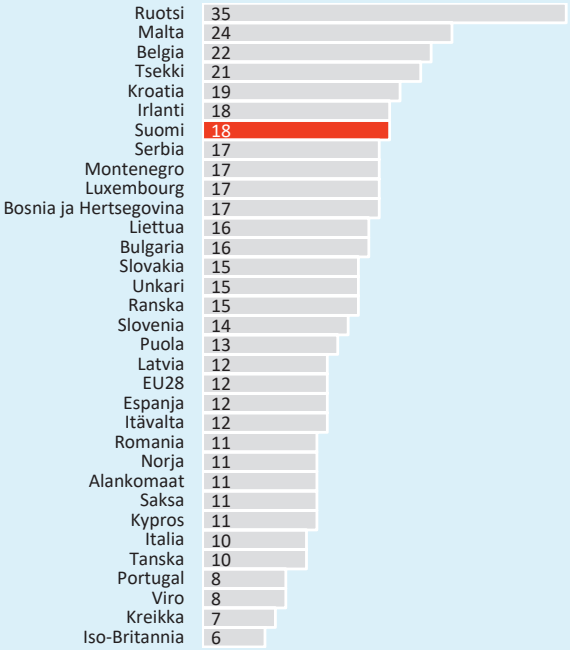


Kuvio 12

Yritykset, joilla säännöllisenä käytäntönä tietojärjestelmän turvallisuustestaus (2019), %.

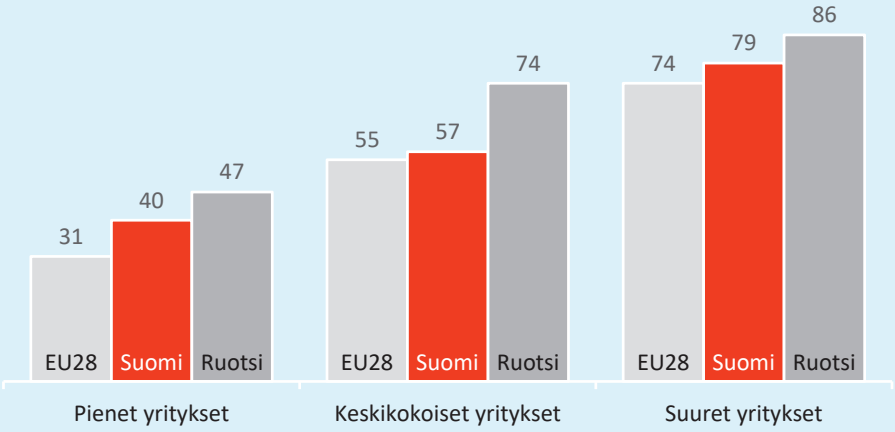
Säännöllisesti tietojärjestelmiensä turvallisuustestausta suoritti Euroopassa reilu kolmasosa yrityksistä. Suomi sijoittui EU28-maiden keskitasoa paremmin, mutta jäi jälkeen mm. Ruotsista ja Tanskasta.

Lähde: Eurostat, Tietotekniikan käyttö yrityksissä (ICT usage and e-commerce in enterprises).



Kuvio 13 **Yritykset, joilla säännöllisenä käytäntönä tietojärjestelmän turvallisuustestaus (2019), %.**

Tietojärjestelmien turvallisuustestaus oli sitä yleisempää, mitä suuremmasta yrityksestä oli kyse. Vaikka Suomen tilanne oli kautta linjan EU28-maiden keskiarvoa parempi, jäi Suomi jälkeen Ruotsista kaikissa yrityskokoluokissa.



Lähde: Eurostat, Tietotekniikan käyttö yrityksissä (ICT usage and e-commerce in enterprises).

Sen sijaan esimerkiksi Kroatiassa, Italiassa, Norjassa ja Tšekissä kehityskulku jäi tältä osin suutariksi Kroatian ottaessa jopa hieman takapakkia vuoden 2015 tasoon verrattuna.

Suhteellisesti kaikkein mittavimman harppauksen ottivat perässähiihtäjät Puola, Latvia sekä Viro. Kun vuonna 2015 puolalaisista yrityksistä ainoastaan 6 % oli alle vuosi sitten päivittänyt tietoturvakäytänteensä, oli vuonna 2019 vastaava osuus Puolassa jo 18 %, eli kolminkertainen aiempaan ajankohtaan verrattuna. Myös Latviassa yritykset paransivat osuuttaan reilusti yli kaksinkertaiseksi ohittaen samalla vertailussa muun muassa Ranskan sekä pahoin kompuroineen Norjan.

Vuonna 2019 säännöllistä tietojärjestelmien turvallisuustestausta harjoitti Euroopan unionissa noin kolmasosa yrityksistä. Maiden välisessä vertailussa toistuu Suomen kohdalla sama tarina kuin monilla muillakin mittareilla tarkasteltuna: Suomi (44 %) sijoittui EU28-maiden keskitason (36 %) paremmalle puolelle mutta jälleen kerran jäi jälkeen pohjoismaisista verrokeistaan Ruotsista (52 %) ja Tanskasta (49 %).

Yrityskokoluokkakohtaisessa tarkastelussa Suomessa parhaiten suoriutuivat pienet yritykset. Kun Euroopan unionissa keskimäärin 31 % pienyrityksistä suoritti tietojärjestelmänsä säännöllisiä turvallisuustestauksia, oli vastaava lukema Suomessa 40 %. Suomen hyvä suoritus ei kuitenkaan jatku yrityskoon kasvaessa. Keskisuurista yrityksistä Suomessa turvallisuustestausta harjoitti säännöllisesti nimittäin 57 %, mikä käytännössä katsoen edusti Euroopan unionin keskitasoa. Keskikokoisten yritysten sarjassa Ruotsin ylivoima Suomeen nähden olikin murskaava. Ruotsin keskisuurissa yrityksissä turvallisuustestaus oli yhtä yleistä (74 %) kuin Euroopan unionin suuryrityksissä keskimäärin. Suuryritysten luokassa Suomi (79 %) sijoittui EU28-maiden keskitasoa paremmin, muttei kuitenkaan Ruotsin (86 %) tai Tanskan (84 %) veroisesti, eikä etenkään Irlannin (90 %) hallitseman kärjen tuntumaan.

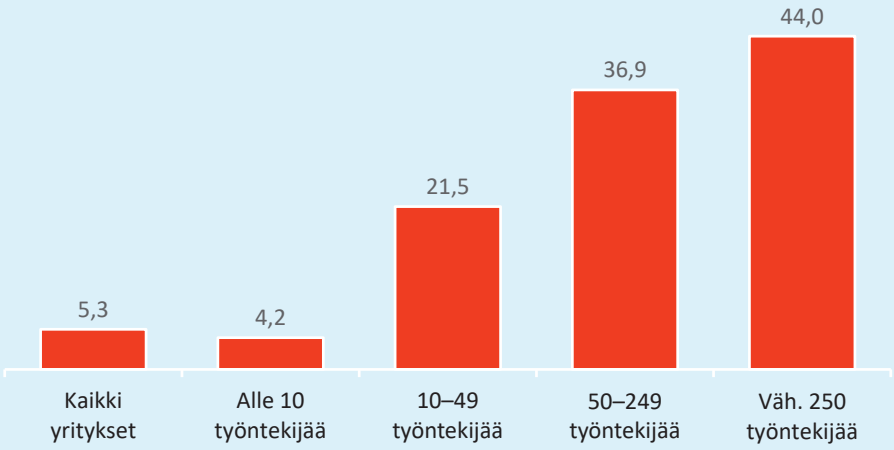
3. Kyberturvaa painottavat suomalaiset yritykset

Analyysin tarkoituksena oli selvittää, kuinka paljon Suomessa on kyberturvallisuutta painottavia yrityksiä. Kaiken todennäköisyyden mukaan tällaiset yritykset mainitsevat siitä omilla www-sivuillaan. Tästä syystä aineistona käytettiin Vainu.io:n tietokantaa. Se sisältää erilaisia digitalisaatioon liittyviä indikaattoreita. Aineisto kattaa käytännössä kaikki Suomen yritykset, joilla oli www-sivut joulukuussa 2019.

Työn aluksi määritettiin kyberturvallisuutta koskevat hakusanat[1]. Nämä hakusanat perustuivat Suomessa käytössä olevan kyberturvallisuuden sanastoon[2]. On syytä huomioida, että hakukriteereiden määrän ollessa suurempi yrityksen on helpompi päätyä kyberturvallisuutta painottavaksi yritykseksi. Vainu.io:n aineistosta saadut tiedot yhdistettiin Tilastokeskuksen yritysrekisteriin. Näin pystyttiin saamaan tarkempia tietoja kyberturvalli-

Kuvio 14 **Kyberturvallisuutta painottavien yritysten osuus kokoluokittain, %.**

Kyberturvallisuusasiat nostetaan sitä useammin esiin, mitä suurempi yritys on.



Lähde: Kirjoittajien laskelmat perustuen Vainu.ion tietokantaan ja Tilastokeskuksen yritysrekisteriin.

suutta painottavista yrityksistä. Lisätiedot koskivat yritysten kokoa, ikää ja toimialaa.

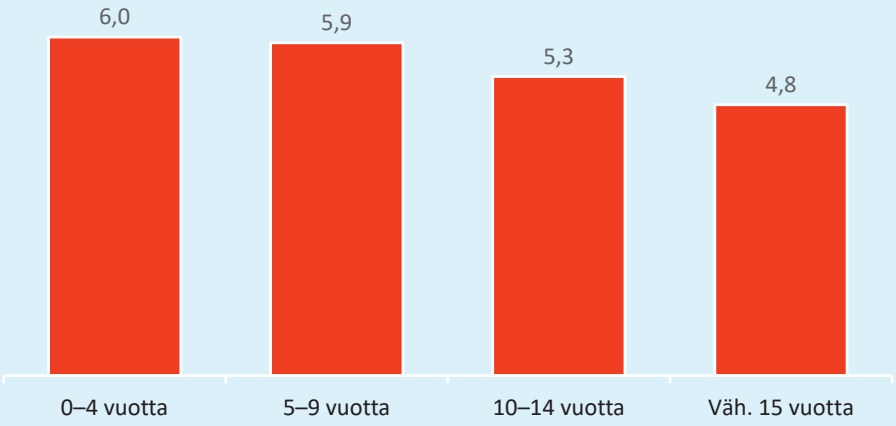
Hakusanoihin perustuva luokittelu tuotti tulokseksi 19 239 yritystä. Tämä vastaa 5,3 % Vainu.io:n koko tietokannan yrityksistä. Vähintään kymmenen henkilöä työllistävistä yrityksistä jonkin kyberturvallisuuteen liittyvän termin mainitsi www-sivuillaan 4 659 yritystä eli 24,6 %.

Yritysten kokoluokittainen tarkastelu tuottaa kiinnostavan havainnon. Kyberturvallisuusasioita mainitaan www-sivuilla sitä useammin, mitä suuremmasta yrityksestä on kyse (kuvio 14).

Vain 4,2 % alle 10 työntekijän yrityksistä mainitsee www-sivuillaan jonkin kyberturvallisuutta koskevan termin (kuvio 14). Tätä isommissa yrityksissä osuudet nousevat korkeammiksi. 10–49 työntekijää työllistävissä yrityksissä osuus on 21,5 %. Keskisuurissa yrityksissä osuus yltää jo 37 %:iin ja peräti 44 % vähintään 250 työntekijää yrityksistä mainitsee jonkin kyberturvallisuustermin sivuillaan.

Kuvio 15 **Kyberturvallisuutta painottavien yritysten osuus ikäluokittain, %.**

Nuoret yritykset nostavat kyberturvallisuusasiat esiin useammin kuin vanhemmat yritykset. Erot ikäryhmien välillä eivät kuitenkaan ole kovin suuria.



Lähde: Kirjoittajien laskelmat perustuen Vainu.ion tietokantaan ja Tilastokeskuksen yritysrekisteriin.

On kuitenkin mahdollista, että kyse ei ole pelkästään yritysten koosta. Myös yritysten ikä voi vaikuttaa siihen, miten kyberturvallisuusasioita tuodaan esiin. Tästä syystä kuviossa 15 tarkastellaan kyberturvallisuusasioiden esilletuomista suhteessa yrityksen ikään.

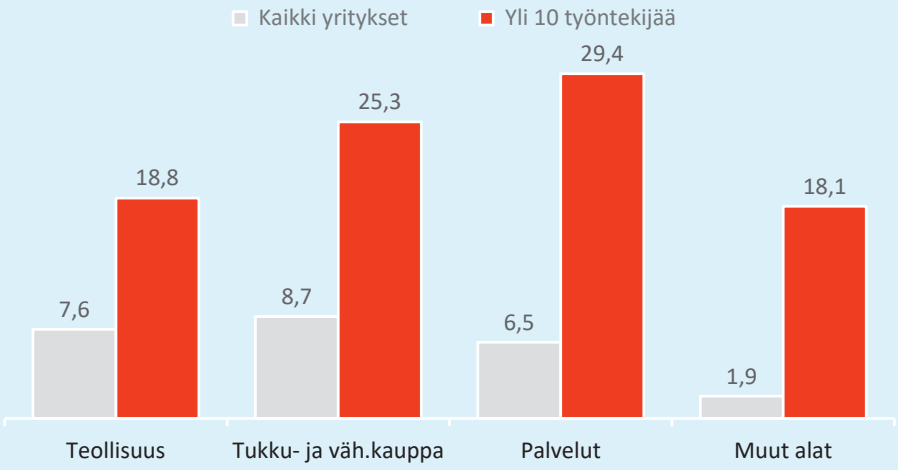
Yrityksen ikäluokittainen tarkastelu osoittaa, että erot eri ikäluokkien välillä jäävät melko pieniksi (kuvio 15). Tästä huolimatta jonkinlainen vaikutus yrityksen iällä näyttää olevan. Nuoremmat yritykset mainitsevat kyberturvallisuusasioita www-sivuillaan useammin kuin vanhemmat yritykset.

Alle 5-vuotiaista yrityksistä noin 6 % mainitsee jonkin kyberturvallisuutta koskevan termin internet-sivuillaan. Sen sijaan vähintään 15 vuotta vanhoissa yrityksissä vastaava osuus jää 4,8 %:iin. Näiden ääripäiden väliin jäävissä yrityksissä osuudet ovat 5,9 % (5–9-vuotiaat yritykset) ja 5,3 % (10–14-vuotiaat yritykset).

Yrityskoon ja -iän lisäksi myös toimialalla on todennäköisesti merkitystä siinä, mikä rooli kyberturvallisuudella on. Kuviossa 16 tarkastellaan yhtä aikaa sekä toimialaa että yrityskokoa.

Kuvio 16 **Kyberturvallisuutta painottavien yritysten osuus toimialoittain, %.**

Mikroyritykset (0–10 työntekijää) mainitsevat kyberturvallisuusasioista sivuillaan selvästi harvemmin kuin tätä suuremmat yritykset. Vaikka eroja on eri toimialojen välillä, yrityskoon merkitys säilyy kaikilla aloilla.



Lähde: Kirjoittajien laskelmat perustuen Vainu.ion tietokantaan ja Tilastokeskuksen yritysrekisteriin.

Yrityskoon merkitys säilyy, vaikka otetaan huomioon toimiala. Kaikilla toimialoilla toistuu sama ilmiö, jossa yli 10 työntekijän yritykset nostavat kyberturvallisuusasiat selvästi useammin esiin kuin tätä pienemmät yritykset.

Kaikista teollisuusyrityksistä vajaa 8 % mainitsi kyberturvallisuusasioista Internet-sivuillaan (kuvio 16). Yli 10 hengen yrityksissä vastaava osuus oli yli kaksinkertainen (18,8 %). Tukku- ja vähittäiskaupassa ero repesi jo kolminkertaiseksi ja palvelualoilla vielä tätäkin suuremmaksi. Yhteenvetona voidaan todeta, että kyberturvallisuusasioiden esiin nostaminen ei riipu vain koosta vaan toimialakin on samanaikaisesti otettava huomioon.

Lopuksi tarkastellaan vielä ohjelmisto- ja tietopalvelualaa omana kokonaisuutenaan (taulukko 1). Osa tämän alan yrityksistä keskittyy kyberturvallisuustuotteiden tai -palvelujen myyntiin. Näiden ydinyritysten lisäksi kyberturvallisuus koskettaa niitä tyypillisesti useammin kuin muita aloja.

Käytetty aineisto sisälsi tiedot vajaan 7 400 ohjelmisto- ja tietopalvelualan yrityksen Internet-sivujen sisällöstä. Näistä hieman yli 14 % mainitsi jonkin kyberturvallisuuteen liittyvän sanan sivuillaan. Osuutta voi pitää yllättävän pienenä. Onhan kyberturvallisuudesta huolehtiminen oleellista kaikille tällä alalla toimiville yrityksille.

Yrityskoko vaikutti jälleen siihen, kuinka usein kyberturvallisuus oli Internet-sivuilla mainittu. Vähintään 10 työntekijän ohjelmisto- ja tietopalveluyrityksistä lähes kolmasosa mainitsi jotain kyberturvallisuudesta sivuillaan.

Edellä olevat tarkastelut ovat perustuneet kyberturvallisuutta koskevien hakusanojen määrittelyyn ja niiden löytymiseen www-sivuilta. Tarkastelutapa on sinänsä perusteltu, mutta jää varsin karkealle tasolle. Tästä syystä teimme syväsukelluksen pienempään yritysjoukkoon.

Taulukko 1 **Ohjelmisto- ja tietopalvelualan yritykset ja kyberturvallisuus.**

	Yritysten määrä	Niiden osuus, jotka mainitsivat kyberturvallisuuden, %
Kaikki yritykset	7 364	14,1
Vähintään 10 työntekijää	822	31,5

Lähde: Kirjoittajien laskelmat perustuen Vainu.io:n tietokantaan.

Kuten aiemmin mainittiin, kaikkiaan 19 239 yritystä mainitsi sivuillaan jonkin kyberturvallisuutta koskevan termin. Valitsimme tästä joukosta satunnaisesti 100 yritystä tarkempaan jatkotarkasteluun. Kävimme jokaisen sadan yrityksen www-sivut yksityiskohtaisesti läpi. Tarkoitus oli saada käsitys siitä, mikä rooli kyberturvallisuudella näille yrityksille on. Näistä sadasta yrityksestä seitsemällä kyberturvallisuus liittyi suoraan niiden tarjontaan koskien siis joko niiden myymiä fyysisiä tuotteita tai palveluita. Ylivoimaisesti valtaosalla (93 yritystä) kyberturvallisuus oli muulla tavalla osa niiden normaalia liiketoimintaa.

4. Osaaminen ja osaamisvaje suomalaisissa kyberyrityksissä

Keväällä 2020 FISC (engl. *"Finnish Information Security Cluster"*) teki kyselyn jäsenyrityksilleen. Kyselyssä havaittiin, että noin 60 % prosenttia tutkimukseen osallistuneista yrityksestä koki tietoturvan osaajista ja osaamisesta pulaa yrityksessään. Osaamisvaje nähtiin suurimmaksi haasteeksi yritysten kasvun kannalta. Osaavaa työvoimaa koettiin tarvittavan erityisesti seuraavilla tietoturvan osa-alueilla: 1) ohjelmisto-osaaminen, 2) liiketoiminnallinen osaaminen, 3) strateginen kyberturvallisuusosaaminen, 4) kryptografia/kryptologia, 5) tekninen kyberturvallisuus, 6) ylläpidon ja valvonnan osaaminen ja 6) järjestelmäarkkitehtuurin osaaminen.

Osana tämän vuoden Digibarometria kartoitimme FISC:n tulosten pohjalta vastaavia osaamisalueita Oikotie.fi -työnhakuportaalin työpaikkailmoituksista vuosien 2019–2020 ajalta. Valitsimme tarkasteluun FISC-järjestön jäsenyritykset sekä joitakin Vainun yritystietokannasta satunnaisotannalla valittuja yrityksiä. Vainun satunnaisotannalla mukaan valitut yritykset edustivat henkilöstömääriltään eri kokoisia yrityksiä ja eri toimialoja (ks. liite 4).

Avainsanoina tässä haussa käytimme tietoturvaan liittyviä sanoja (katso luvussa 3 kuvatut hakusanat). Mikäli jokin näistä avainsanoista tai osa siitä löytyi yrityksen työpaikkailmoituksen työtehtävän tittelistä, kävimme ilmoituksen läpi tarkemmin. Löysimme 24 avainsanoja vastaavaa työpaikkailmoitusta. Näiden työpaikkailmoitusten avulla arvioimme, mihin tietoturvan osa-alueeseen osaamisvajeet yrityksissä liittyivät.

Suurimmalla osalla 24 työpaikkailmoituksesta etsittiin teknisen kyberturvallisuuden osaajia (18 työpaikkailmoituksessa). Järjestelmäarkkitehtuuriin, alan liiketoimintaan, ohjelmistoihin sekä ylläpitoon ja valvontaan liittyviä vaatimuksia havaittiin ilmoituksissa kategorioina miltei yhtä paljon kutakin. Strategiseen kyberturvallisuuteen liittyvää osaamista etsittiin sen sijaan selvästi vähemmän (8 työpaikkailmoituksessa). Vain yhdessä työpaikkailmoituksessa etsittiin suoraan kryptografian tai kryptologian osaajaa.

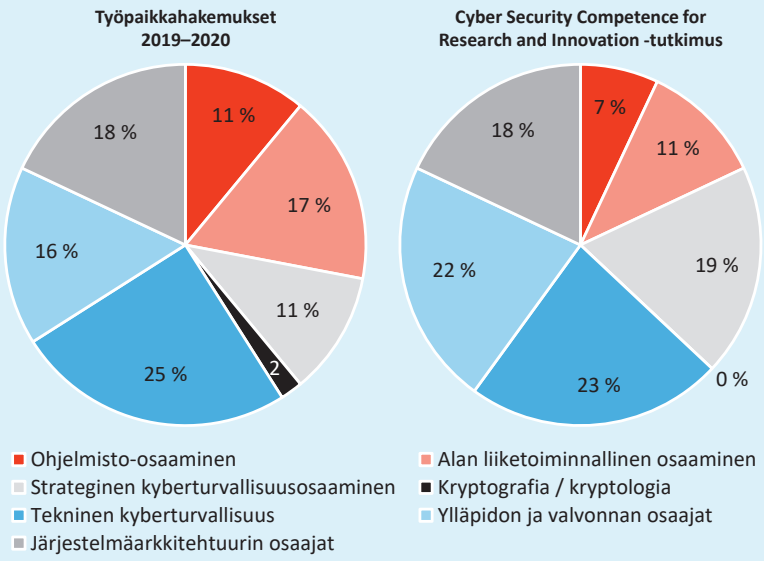
Osassa työpaikkailmoituksista tietoturvaan liittyvä vaadittava osaaminen ilmaistiin varsin ympäripyöreästi. Tämä voi kuvastaa sitä, etteivät kaikki yritykset välttämättä itsekään tienneet, millaista tietoturvaosaajaa ne tarkalleen ottaen etsivät. Toinen näkemys tähän on FISC-järjestön kartoituksessa

ilmennyt vallitseva osaavan työvoiman pula. Tällöin työpaikkailmoitusten osaamisvaatimukset jätetään tarkoituksella laveaksi, jotta osaamisvaatimukset eivät estäisi hakemista tehtävään. Vertailtaessa FISC-järjestön jäsenistön osaamispulan osa-alueita ja keskeisiä ominaisuuksia työpaikkailmoituksissa oli erikoista huomata muun muassa kryptografian ja kryptologian vähäisyys.

Tutustuimme myös eurooppalaisia korkeakouluja, yrityksiä ja tutkimuslaitoksia yhteen kokoavan Concordian *Cyber Security Competence for Research and Innovation* -tutkimukseen. Sen tarkoituksena on luoda profiilia eurooppalaisilla työmarkkinoilla halutuista tietoturvaosaajista. Concordia on yhteistyössä Twenten yliopiston kanssa luonut tätä tarkoitusta varten kyselyn ja koonnut sen pohjalta tietopankin eri osaamiskyvykkyyksistä.

Concordian tietopankki määrittelee 200 erilaista tiedollista kyvykkyytä sekä 90 käytännön taitoihin liittyvää osaamisaluetta, joita tulevaisuuden kyberasiantuntijalta voidaan ennakoida odotettavan. Nämä osaamisalueet eroavat erittäin paljon toisistaan muodostaen laajan skaalan erilaisia

Kuvio 17 **Kyberturva-asiantuntijan osaamisen jakauma, %.**



Lähde: Oikotie, Cyber Security Competence for Research and Innovation -tutkimus, Etlan laskelmat.

kompetensseja. Osa kyvykkyyksistä liittyy laajoihin käsitteisiin (esimerkiksi *”knowledge of information technology architectural concepts and frameworks”*) ja osa taas yksityiskohtaisempiin aihealueisiin (esimerkiksi *”knowledge of query languages such as SQL”*).

Kävimme selvityksessämme Concordian listaamat 290 eri osaamisaluetta läpi. Käytimme analysoinnissa hyväksi FISC:n jäsenyritysten esiintuomia tietoturvan osaamisvajeen osa-alueita. Lisäksi saatoimme verrata Concordian osaamisalueiden listausta jo aiemmin tutkimiemme työpaikkailmoitusten osaamisvaatimuksiin.

Concordian tutkimuksen osaamisalueita ja Oikotie.fi-sivuston tietoturvaan liittyviä työpaikkailmoituksia verrattaessa voidaan havaita, että muun muassa liiketoimintaosaamista ja ohjelmisto-osaamista on painotettu hieman enemmän työpaikkailmoituksissa. Strateginen kyberturvaosaaminen sekä ylläpito- ja valvontaosaaminen taas puolestaan korostuvat enemmän tutkimuksen puolella. Suhteellisten osuuksien erot ovat kuitenkin Concordian ja Oikotie.fi-sivuston välillä tässä suhteessa marginaalisia. Näin ollen tutkimusta ja työpaikkailmoituksia voitaneen pitää melko yhteneväisinä toisiinsa nähden.

Kyberturvan tulevaisuuden osaajalta edellytetään lähes 300 eri kompetenssia, joissa yhdistyy tekninen ja strateginen osaaminen.

Lähestyimme lisäksi tietoturvan parissa työskentelevää viittä suurempaa yritystä. Kysyimme yrityksiltä seuraavat viisi kysymystä: 1) Kuinka suuri osa toimialanne rekrytoinneista toteutetaan suorahaulla? 2) Tekeekö yrityksenne paljon rekrytointeja/suorahakuja Euroopasta tai muualta ulkomailta? 3) Tehdäänkö julkisista työpaikkailmoituksista tarkoituksella kuvauksiltaan laveita, jotta ne eivät sulje hakijoita pois? 4) Kuinka tärkeää kryptologian tuntemus on kyberturvan asiantuntijoille? 5) Kuinka suureksi olette kokeneet yleisesti alan rekrytointien haastavuuden, ja mitä kautta saadaan parhaiten rekrytoitua tietoturvan osaajia?

Haastateltujen yritysten edustajat ilmoittivat hyödyntävänsä vahvasti Euroopan tai Aasian laajuisia suorahakuja rekrytoinnissa, sillä avoimien työpaikkailmoitusten avulla osaajien löytäminen koettiin erittäin vaikeaksi.

Ulkomailta tehtävien rekrytointien luonne vaihtelee kuitenkin yrityksittäin sen suhteen, millaiseen osaajaan ja mihin maailman kolkkaan hakuja kohdistetaan. Eräs haastateltu mainitsi ulkomaisten rekrytointien tarjoavan kilpailuetua yritykselleen.

Kyberturvallisuuden ammattilaiset joudutaan hakemaan yhä useammin Euroopan tai Intian rekrytointimarkkinoilta.

Osa haastatteluista mainitsi tekevänsä työpaikkailmoituksistaan tarkoituksellisesti laveita, jotta potentiaalisia osaajia löytyisi enemmän. Toisaalta näissäkin tapauksissa nähtiin, että tarkempi työpaikkailmoitus on kuitenkin parempi. Näin saadaan hakijoita, jotka vastaavat paremmin haluttua osaamista.

Eräs haastateltu toi esiin oman näkemyksensä pienten yritysten käyttämistä todella laveista työpaikkailmoituksista. Haastateltavan mukaan niissä etsitään monipuolista osaajaa, joka omaa paljon osaamista monelta eri osaalueelta ja pystyy tekemään ”kaikkea”. Näkökulman esiin tuoneen haastatellun mukaan näitä osaajia on kuitenkin käytännössä mahdotonta löytää.

Kryptologian osaaminen ei haastateltujen mukaan ollut tarkoituksella etsittävä merkittävä taito. Haastatellut kyllä mainitsivat kryptologian perusteiden osaamisen tai jonkinlaisen ymmärryksen sen luonteesta olevan eduksi. Syvällistä kryptologian osaamista ei kuitenkaan toistaiseksi nähty tarpeelliseksi.

Kryptologia nähtiin joka tapauksessa tulevaisuudessa tärkeäksi esimerkiksi kvanttilaskennassa ja sen teknologian tietoturvakysymyksissä. Haastatteluista ilmeni, kuinka kyseisessä teknologiassa ei ole vielä kehitetty vaadittavia kryptologiaan pohjautuvia tietoturvan komponentteja.

Yksi haastatelluista huomautti, että teknologian nopean kehittymisen vuoksi yritykset eivät välttämättä osaa arvioida, millaisia tietoturvan osaajia ne muutaman vuoden päästä tarvitsevat. Hänen näkemyksensä mukaan yleisesti teknologia-alan isot toimijat (kuten Google ja Microsoft) ovat edelläkävijöitä tietoturvateknologioissa ja niihin liittyvien tietoturvatarpeiden ja osaamisen tunnistamisessa.

5. Digitaalinen luottamus vaatii identiteettien kehitystä

Digitalisaatio etenee vääjäämättä kohti integroituneempia ja systeemisempiä kokonaisuuksia. Kun tietojärjestelmät linkittyvät entistä laajemmin toisiinsa, mahdollistaa integraatiokehitys aivan uusia tapoja synnyttää arvoa ja luoda hyvinvointia. Samalla, kun kehitys tarjoaa mahdollisuuksia, synnyttää se myöskin kyberturvaan liittyviä haasteita. Yksi keskeinen haaste tässä suhteessa liittyy digitaalisen luottamuksen säilyttämiseen integraatiokehityksen keskellä. Yhteiskunnan digitaalinen luotettavuus tuleekin jatkossa edellyttämään kehittyneempiä ja moniulotteisempia digitaalisen identiteetin muotoja.

Digitaalinen luottamus koostuu monen eri tekijän yhdistelmästä. Kun haluamme kytkeytyä eri laitteisiin ja palveluihin, meidän on kyettävä luottamaan siihen, että tuotteet ja palvelut ovat suojattuja datan väärinkäytöltä ja haittaohjelmilta. Toiseksi, meidän on kyettävä tunnistamaan vuorovaikutuksessa olevat laitteet ja palvelut sekä niihin kytkeytyvät osapuolet. Kolmantena asiana meidän tulee pystyä varmistumaan siitä, että eri osapuolet kunnioittavat annettuja lupauksiaan. Annettuja sitoumuksia tulee pystyä valvomaan sopimusoikeudellisin keinoin.

Henkilöllisyyden todentamisen rinnalle tarvitaan tunnistautumismenetelmät laitteille, palveluille ja yrityksille kaikilla eri järjestelmien riskitasoilla.

Digitaalinen luottamus koostuu toisin sanoen kolmesta tekijästä: turvallisuudesta, tunnistettavuudesta ja jäljitettävyydestä. Matalimman kynnyksen lähestymistavassa yritykset ja/tai valtio voivat ottaa roolin, jossa ne toimivat digitaalisen luottamuksen ja turvallisuuden välittäjinä yhteiskunnassa. Digitaalinen tunnistautuminen on yksi tapa, jolla voidaan toteuttaa välittäjän roolia luottamuksen ja turvallisuuden luomiseen ja jäljitettävyyden mahdollistamiseksi. Digitaalinen henkilöiden tunnistautuminen ei kuitenkaan jatkossa ole riittävä keino yksinään. Vastaavaa tunnistautumisme-

kanismia tulisikin miettiä laitteille ja palveluille, sekä yrityksille ja julkisille toimijoille.

Digitaalinen identiteetti (eIDAS-tunnistautuminen) synnytti ajatuksen, jota voitaisiin hyödyntää vastaavasti laitteiden ja palveluiden sekä yritysten digitaalisen identiteettikonseptin kehittämisessä. Digitaalisen identiteetin eri tasot kuvastavat tunnistautumisen luotettavuutta eri henkilötunnistautumisen tasoilla ja eri riskitason järjestelmiin. Asian selkeyttämiseksi kuvaamme kuusitasoisen konseptualisoinnin taulukossa 2. Konseptoidut luottamuksen kuusi eri tasoa mahdollistavat myös tapauskohtaisesti mm. korkealaatuisen datan hallinnan käytänteet eri järjestelmän riskitasojen välillä.

Tulevaisuudessa tuote, palvelu ja yritys tulevat sisältämään sekä fyysisen ulottuvuuden, että digitaalisen kaksosen (ulottuvuuden). Digitaalinen ulottuvuus toimii monella eri tapaa käyttöliittymänä ihmisten ja Internetiin linkitettyjen tuotteiden, palveluiden ja yritysten välillä. Tällä hetkellä niin digitaalisen identiteetin kuin digitaalisten kaksostenkin järjestelmiä mietitään varsin yrityskeskeisesti.

Tarvitaan kyberfyysisten järjestelmien eurooppalaiset standardit tietojenkäsittelylle, verkottumiselle sekä fyysisten prosessien ja kyberturvan integroinnille kaikilla eri sovellusten riskitasoilla.

Ilman digitaalista identiteettiä internetiin kytkettyihin laitteisiin, palveluihin ja yrityksiin on vaikea luottaa. Laajemmin ajateltuna järjestelmissä tarvitaan tulevaisuudessa niin sanottu laite- ja palveluidentiteetin varmistaja (allekirjoittaja). Käytännössä sillä tarkoitetaan seuraavaa porrasta, joka ns. hyväksyy ja varmentaa Internetiin kytketyt uudet laitteet, palvelut ja yritykset.

Sen sijaan, että yhteiskunnassa tyydyttäisiin vain synnyttämään käytäntöjä ja vahvistamaan yksittäisten henkilöiden ja laitteiden kyberturvallisuutta, Euroopan komission tulisi laatia teknologianeutraalit standardit digitaaliselle tunnistautumiselle ajatellen laajempaa järjestelmien kokonaisuutta. Myös kvanttilaskenta ja uusi salausalgoritmiikka tulisi huomioida osana tätä laajempaa standardikehitystä.

Taulukko 2 **Henkilöiden, tuotteiden, palveluiden ja yritysten tunnistautumisen eri tasot ja digitaalinen identiteetti**

Riskitaso	Käyttökohde	Henkilötunnistautumisen tekniset toimintatavat	Identiteetin varmistaja	Sääntelytaso tunnistautumiselle	Laitetunnistautumisen tekninen tapa ja identiteetin varmistaja
0 Ei tunnistautumista	Pimeä verkko (engl. dark web)	Ei tunnistautumista	Ei varmistajaa	Ei määritelmää	Julkinen tunnistin (sisältää IP:n, MAC osoitteen)
1 Minimaalinen	Ei-kaupallinen sovellus (esim. sosiaalinen media ja sähköposti)	Syntymäpäivä, nimi	Facebook, Google jne.	Itsemääritelty	(Julkinen) tunnistin käyttäjän identiteetillä
2 Matala	Kaupallinen sovellus (esim. verkkokauppa)	Ajokortti, digitaalinen identiteetti	Amazon, WeChat, Google	Itsemääritelty	Valmistajan hyväksymä tunnistus / tuote tunnistetiedot
3 Merkittävä	Pankki-, finanssi- ja terveyspalvelut, energiajärjestelmät	Tupas-varmennepalvelu, passi	Pankki, puhelinyhtiö, kaukolämpöyhtiö, sähköyhtiö	Verkko-operaattorin hyväksymä	Verkko-operaattorin hyväksymä
4 Korkea	Ihmisten liikkuminen maarajojen yli	Passi	Valtio	Valtion määrittämä	Valtion hyväksymä
5 Korkea+	Turvallisuuden erikoistapaukset, kuten ydinvoimala ja puolustusvoimat	Turvatarkastus	Supo, Puolustusvoimat	Valtion määrittämä	Verkon tai valtion hyväksymä

Lähde: Timo Seppälä, Etla. Kehitetty yhteistyössä Aalto-yliopiston tutkijoiden Juuso Autiosalon, Kari Hiekkasen ja Jari Juhangon kanssa.

6. Kvanttilaskenta tulee – kestääkö kyberturva?

Vuonna 1980 yhdysvaltalainen fyysikko Paul Benioff julkaisi teoreettisen mallin laitteesta, joka kykenisi suorittamaan matemaattisia laskutoimituksia kvanttimekaniikan ilmiöitä hyödyntäen (Benioff, 1980). Konsepti oli lähtölaukaus kvanttitietokoneen kehitykselle. Nyt, 40 vuotta myöhemmin, kvanttilaskennan unelma on lähempänä todellisuutta kuin koskaan. Vuoden 2019 lopulla Google ja Yhdysvaltain ilmailu- ja avaruushallintovirasto NASA julkistivat Sycamore-kvanttitietokoneen suorittaneen muutamassa minuutissa laskutoimituksen, joka nopeimmallekin tavalliselle tietokoneelle olisi käytännössä katsoen mahdoton ratkaista (Arute ym., 2019).

Vaikkakin Googlen haastaja IBM riensi nopeasti kritisoimaan koejärjestelyä ja kiistämään tulosten merkittävyyden, edustaa Sycamoren saavutus keskeistä merkkipaalua kvanttilaskennan kehityksessä. Aikakausi, jossa kvanttitietokoneet suoriutuvat asioista, joihin tavalliset tietokoneet eivät kykene, ns. kvanttiherruus, on saavutettu – tai ainakin se on hyvin lähellä.

Vuonna 2019 Googlen kvanttitietokone suoritti 200 sekunnissa laskutoimituksen, johon maailman nopeimmalta supertietokoneelta olisi kulunut 10 000 vuotta.

Kvanttitietokoneiden hyötypotentiaali on valtava. On arvioitu, että kvanttilaskennan vaikutukset tulevat koskettamaan laaja-alaisesti koko yhteiskuntaa ja sen kaikkia osa-alueita. Vaikka laajamittaisia käytännön sovelluksia saataneen vielä odottaa vähintäänkin 2030-luvulle saakka, jo nyt on kuitenkin syytä pohtia, millaisia vaikutuksia kvanttilaskennan mullistuksella tulee olemaan kyberturvallisuuteen, ja miten uuteen aikakauteen tulisi valmistautua.

Perinteisiin tietokoneisiin verrattuna kvanttitietokone on täysin omanlaisensa peto. Sen tehokkuus ei perustu tavanomaisten tietokoneiden tavoin yksittäisten perättäisten laskutoimitusten nopeuteen ja suureen määrään, eikä nopeakaan kvanttitietokone siten ole tavallisen tietokoneen korvike.

Kvanttilaskenta mahdollistaa sen sijaan täysin erilaisen tavan lähestyä ja ratkaista tietyn tyyppisiä laskennallisia ongelmia, jotka tavallisille tietokoneille ovat erityisen hankalia.

Kvanttifysiikan lainalaisuuksia hyödyntämällä kvanttitietokoneella voidaan suorittaa valtava määrä eri laskutoimituksia yhtä aikaa. Kun ratkaistava ongelma muotoillaan siten, että ei-kiinnostavien laskutoimitusten tulokset kumoavat toisensa, voidaan valtavasta samanaikaisten laskutoimitusten merestä myös nopeasti löytää juuri ne oikeat kaivatut vastaukset.

Aalto-yliopiston kvanttilaskennan professori Mikko Möttösen toteamusta mukaillen, kvanttitietokoneella voi ikään kuin yhdellä vilkaisulla löytää neulan heinäsuovasta. Monet erilaiset optimointiongelmat soveltuvatkin kvanttitietokoneen pureskeltaviksi erinomaisesti. Esimerkiksi ennustemallien herkkyysanalyysit ilmastotieteessä, reitinhakualgoritmit älyliikenteessä, sekä esimerkiksi molekyylirakenteiden mallintaminen lääketieteellisen biokemian saralla ovat osa-alueita, joissa kvanttitietokoneella voidaan mitä luultavimmin tulevaisuudessa ottaa suuria edistysaskeleita.

”Kvanttitietokone on kybersodan vetypommi.”

– Elina Hiltunen, futuristi

Kuten teknologioilla on tapana, on myös kvanttitietokoneilla kuitenkin synkempi varjopuolensa. Kyberturvan maailmassa kvanttilaskennan edellä kuvattu kyky paikantaa neula heinäsuovasta nimittäin tarjoaa yleisavaimen, jolla suurin osa nykyisen tietoyhteiskunnan lukoista aukeaa käden käänteessä. Nykyisessä tietoyhteiskunnassa käytettävät tiedonsalaus- ja tunnistautumismenetelmät perustuvat näet pitkälti juurikin siihen edellä mainittuun seikkaan, että jotkin laskutoimitukset ovat tavanomaisille tietokoneille epäsymmetrisesti hankalia. Toisin sanoen, vaikka oikeaa ratkaisua on vaikea löytää, löydetyn ratkaisun tarkistaminen käy nopeasti. Kvanttitietokoneella sen sijaan vaikeasti löydettävät, mutta helposti tarkistettavat salausavaimet selviävät yhdellä vilkaisulla, sillä kvanttitietokone kykenee laskemaan ongelman myös takaperin.

Toistaiseksi kvanttitietokoneiden käytännön sovelluksiin liittyy vielä suuria haasteita, mm. kvanttimaailman epävarmuuksista kumpuavaan epä-

luotettavuuteen liittyen. Mitä luultavimmin kvanttilaskennan käytännön sovelluksia saataneenkin odotella vielä tovi, useimpien arvioiden mukaan noin 15–20 vuotta. On kuitenkin syytä pitää mielessä, että kvanttilaskennan mahtiin liittyy myös valtiollisia intressejä, jotka eivät välttämättä ole kehityskaarensa osalta julkisia. Topcoder-yrityksen toimitusjohtaja Michael Morris onkin osuvasti todennut, ettei kvanttilaskennan pisimmälle ehtineestä käytännön kehityksestä välttämättä valu tietoa julkisuuteen, ennen kuin kvanttitietokonetta lopulta on jo käytetty kybersodankäynnin välineenä salausmenetelmien murtamiseen.

Vaikka kvanttiteknologian voidaan siis ennakoida aiheuttavan kyberturvallisuudelle valtavia haasteita, tarjoaa se samalla mahdollisiin ongelmiin myös potentiaalisia ratkaisuja. Yhdysvaltain kauppaministeriön alainen National Institute of Standards and Technology (NIST) on vuodesta 2016 lähtien työskennellyt standardien sekä käyttöönotto-ohjeistuksen luomiseksi kvanttiturvalliselle salaukselle. Vaikka erilaisia salausmenetelmiä on vertailussa arvioitu kymmeniä, ei kvanttiturvalliseen salaukseen ole selvityksessä toistaiseksi löydetty yhtäkään tapaa, joka suoraan sopisi nykyisten salausmenetelmien korvaajaksi (Barker ym., 2020). Näyttääkin siltä, että kvanttiturvallinen salaus tulee edellyttämään ainakin jossakin määrin myös fyysisten laitteistojen ja nykyisten tietojärjestelmien korvaamista.

Kvanttilaskennan kyberuhat ovat jo todellisia. Kriittisissä toiminnoissa ne on viimeistään nyt alettava ottaa vakavasti.

Kvanttisalausavainten vaihtoon kykeneviä kaupallisia järjestelmiä on jo nyt markkinoilla kaupan. Nykyisellään kvanttisuojattujen yhteyksien hinnat liikkuvat kuitenkin sadoissa tuhansissa euroissa, joten laajempia käytännön sovelluksia saataneen vielä odottaa pitkään. Kvanttisalausavainten vaihtoon kykenevät järjestelmät eivät myöskään skaalaudu tehokkaasti eivätkä ne siten välttämättä koskaan yleisty kuluttajien käyttöön. Ensimmäisiä valokuitu- ja satelliittiyhteyksiin perustuvia kvanttisuojattuja verkostoja on kuitenkin alettu jo rakentaa niin Kiinassa, Euroopassa kuin Yhdysvalloissakin (Korolov & Drinkwater, 2019; Möttönen, 2020).

Kvanttiajan kyberuhkiin valmistautumiseksi yhteiskunnan tulisi pikimmiten laatia suunnitelma siitä, missä järjestyksessä yhteiskunnan tietojärjestel-

miä ja niissä käytettäviä salausmenetelmiä aletaan uusia kvanttiturvallisiksi kriittisimmistä järjestelmistä alkaen. Myös aloilla, joissa tietoteknisten laitteistojen investointisyklit ovat pitkiä, on jo nyt syytä huomioida kvanttisalauksen yhteensopivuus laitteiden ja järjestelmien koko tulevan elinkaaren aikana (Barker ym., 2020).

Niin ikään joitakin kyberturvamenettelyitä on kvanttilaskennan aikakauden kynnyksellä mietittävä uusiksi. Jo nyt on esimerkiksi syytä pohtia, miltä tänään salattavat tiedot näyttävät tulevaisuudessa, mikäli ne 15 vuoden kuluttua tulevatkin yllättäen julkisiksi. Mikäli tänään salatut arkaluonteiset tiedot päätyvät huomenna vääriin käsiin, ei niiden murtamista tulevina vuosina voida enää mitenkään estää (Barker ym., 2020).

Esimerkiksi Wikileaksin julkaisemat arkaluonteiset asiakirjat, kuten diplomaattisähkeet, ovat viime vuosina osoittaneet, millaisia vaikutuksia vielä vuosienkin päästä voi aiheutua, jos arkaluonteiset asiakirjat vuotavat julkisuuteen. Julkisuudessa on taannoin uumoiltu esimerkiksi Yhdysvaltain kansallisen turvallisuusvirasto NSA:n Utahiin perustetun valtavan datakeskuksen palvelevan juurikin tätä tarkoitusta. Kaikki haltuun saadut salatut tiedot säilötään talteen odottamaan eri murtamismenetelmien kehittymistä tulevina vuosina (Bamford, 2012).

Mikäli nykyiset salausmenetelmät murtuvat, vaarantuu niin ikään myös nykymuotoisen sähköisen allekirjoituksen luotettavuus. Jos esimerkiksi sopimuksia laaditaan nykypäivänä pelkän sähköisen allekirjoituksen varassa, on hyvä kysymys, miten tulevina vuosikymmeninä tullaan varmistumaan nykyajassa tehtyjen sähköisten allekirjoitusten todenperäisyydestä.

Kaikkia kvanttilaskennan mahdollisuuksia ei myöskään vielä täysin ymmärretä. On mahdollista, että esimerkiksi jokin tulevaisuudessa kehitettävä kvanttilaskenta-algoritmi kykeneekin murtamaan jonkin nykyisin kvanttiturvallisena pidetyn salausmenetelmän. Siksi kvanttiturvallisen salauksenkaan suomaan turvaan, kuten kryptografisiin menetelmiin ylipäätään, ei pidä jatkossakaan luottaa täysin sokeasti. Lisäksi on syytä muistaa, että oli sitten kyseessä kvanttiturvallinen järjestelmä tai ei, luultavasti jatkossakin sen helpoin murtokohta on edelleen sen erehtyväisin elementti: järjestelmää käyttävä henkilö. Sen heikkouksiin eivät kvanttiturvalliset salausmenetelmätkään auta.

Liite 1: Digibarometrin muuttujat

Tässä liitteessä kuvataan Digibarometrin yksittäiset muuttujat. Edellisen vuoden muuttujiin verrattuna tämän vuoden barometrissa on 5 uutta muuttujaa. Muutokset johtuvat siitä, että aiemmista tilastolähteistä ei ollut saatavissa päivitettyä aineistoa tai että maajoukon kattavuus paranee. Lisäksi mukana on 9 edellisen vuoden muuttujaa, joista ei ole saatavissa tämän vuoden osalta päivitystä. Ne haluttiin siitä huolimatta sisällyttää barometriin, koska vastaavan kaltaisia tekijöitä mittaavia vaihtoehtoisia muuttujia ei löydetty.

Yritysten edellytykset

1. Yritysten laajakaistakäyttö. Muuttuja on laskettu prosenttiosuutena vähintään 10 henkeä työllistävistä yrityksistä, joilla on käytössään nopeudeltaan vähintään 100 Mbit/s laajakaistainen Internet-yhteys. Lähteenä on OECD:n tietokanta ”ICT Access and Usage by Businesses”. Tiedot ovat vuodelta 2019.

2. Tekniset valmiudet pilvipalvelujen hyödyntämiseen. Maa saa arvon 100 (arvon 1), jos se on vertailumaiden paras (huonoin) kaikissa kuudessa osatekijässä. Osatekijät ovat tiedon siirtonopeus verkkopalvelimelta päätelaitteelle (*download*) ja toisinpäin (*upload*) sekä tiedon siirtopyynnön saantiviipymä (*latency*). Nämä kolme tekijää on mitattu sekä kiinteiden että langattomien verkkojen osalta. Lähteenä on Cisco Systemsin (2020, v.gd/778NsI) kartoitus. Tiedot koskevat maaliskuun 11. päivän tilannetta vuonna 2020.

3. ICT-alan rekrytoinnissa ei vaikeuksia. Muuttuja on laskettu prosenttiosuutena vähintään 10 henkilöä työllistävistä yrityksistä, joilla ei ollut vaikeuksia löytää ammattitaitoisia ICT-alan asiantuntijoita. Lähteenä on Eurostatin *Information society statistics* -tietokanta (muuttujakoodi isoc_ske_itrcrn2). Tiedot ovat vuodelta 2019.

4. IPv6-valmius www-sivuilla. Mittari kuvaa osuutta Googlen käyttäjien vierailemista www-sivuista, joilla on IPv6-kattavuus nimipalvelintietueissa. Käytännössä tämä tarkoittaa sitä, että käyttäjä, jolla on IPv6-yhteys, saa avattua haluamansa www-sivun. Lähteenä ovat Googlen julkaisemat tilastotiedot (haettu 11.3.2020), https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

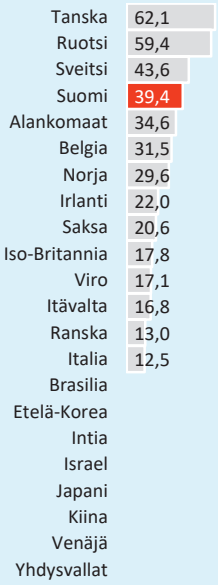
Yritysten edellytykset

Liitekuvio 1

Yritysten laajakaistakäyttö.

%-osuus yrityksistä, joilla käytössään nopeudeltaan vähintään 100 Mbit/s laajakaistainen Internet-yhteys.

Lähde: OECD. Tiedot ovat vuodelta 2019.

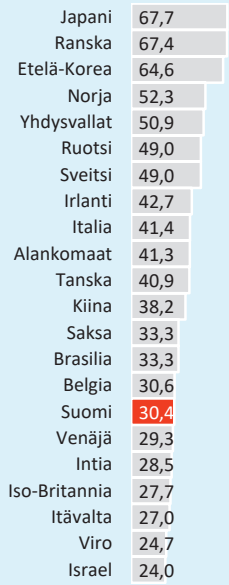


Liitekuvio 2

Tekniset valmiudet pilvipalvelujen hyödyntämiseen.

Maa saa arvon 100 (arvon 1), jos se on vertailumaiden paras (huonoin) kaikissa kuudessa osatekijässä.

Lähde. Cisco Systems (2020, http://v.gd/778NsI). Tiedot ovat vuodelta 2020.

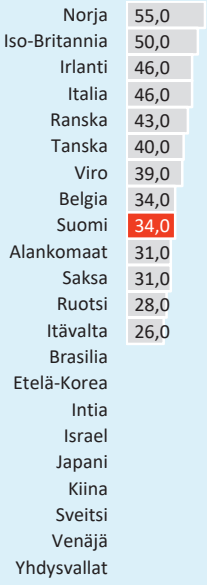


Liitekuvio 3

ICT-alan rekrytoinnissa ei vaikeuksia.

%-osuus rekrytoivista yrityksistä, joilla ei ollut vaikeuksia löytää ICT-alan asiantuntijoita.

Lähde. Eurostat Information society statistics. Tiedot ovat vuodelta 2019.

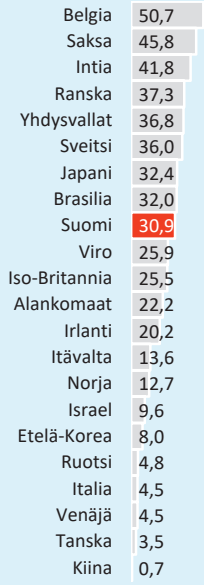


Liitekuvio 4

IPv6-valmius www-sivuilla.

%-osuus Googlen käyttäjien vierailemista www-sivuista, joilla on IPv6-kattavuus nimipalvelintietueissa.

Lähde. Google. Tiedot ovat vuodelta 2020.



Yritysten käyttö

5. ICT:n käyttö B-to-B -transaktioissa. Vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa, että ICT:tä hyödynnetään enemmän yritysten välisessä liiketoiminnassa. Lähteenä on WEF Executive Opinion Survey 2017 ja 2018. Tiedot ovat vuodelta 2018.

6. Big datan hyödyntäminen liiketoiminnassa. Maa saa arvon 10 (arvon 0), jos kyselyyn vastaajien mielestä maassa toimivat yritykset hyödyntävät big dataa ja siihen liittyvää analytiikkaa liiketoiminnassaan erittäin hyvin (erittäin huonosti). Lähteenä on IMD:n kilpailukykyvertailun yrityskysely, ja muuttuja on raportoitu IMD:n vuoden 2019 World Competitiveness Yearbookissa, muuttujan koodi 3.4.07. Tiedot koskevat vuotta 2019.

7. Tietoverkkojen turvallisuuden huomioiminen. Maa saa arvon 10 (arvon 0), jos kyselyyn vastaajat katsovat yritysten panostavan tietoverkkojensa turvallisuuteen erinomaisesti (erittäin huonosti). Lähteenä on IMD:n kilpailukykyvertailun yrityskysely, ja muuttuja on raportoitu IMD:n vuoden 2019 World Competitiveness Yearbookissa, muuttujan koodi 4.2.18. Tiedot koskevat vuotta 2019.

8. Sosiaalisen median käyttö liiketoiminnassa. Muuttuja mittaa osuutta yrityksistä, jotka käyttävät liiketoiminnassaan jotain sosiaalisen median tyyppiä, kuten yhteisöpalveluja, blogeja, multimedian jakamista tai wiki-pohjaisia tiedon jakamisen työkaluja. Lähteenä on Eurostat Information society statistics. Muuttujan tiedot koskevat vuotta 2019.

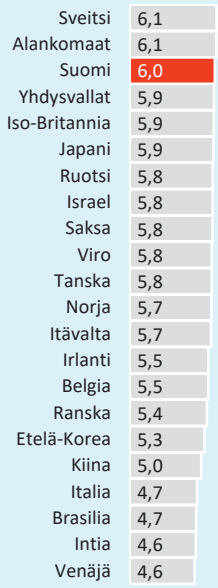
Yritysten käyttö

Liitekuvio 5

ICT:n käyttö B-to-B -transaktioissa.

Vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa, että ICT:tä hyödynnetään enemmän yritysten välisessä liiketoiminnassa.

Lähde: WEF Executive Opinion Survey 2017 ja 2018. Tiedot ovat vuodelta 2018.

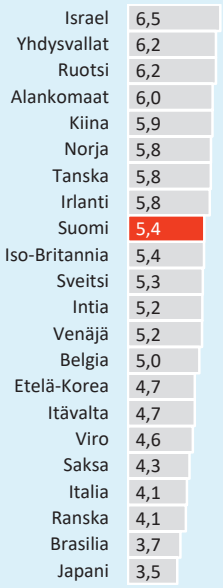


Liitekuvio 6

Big datan hyödyntäminen liiketoiminnassa.

Maa saa arvon 10 (arvon 0), jos kyselyyn vastaajien mielestä yritykset hyödyntävät big dataa liiketoiminnassaan erittäin hyvin (erittäin huonosti).

Lähde: IMD (2019, muuttuja 3.4.07). Tiedot ovat vuodelta 2019.

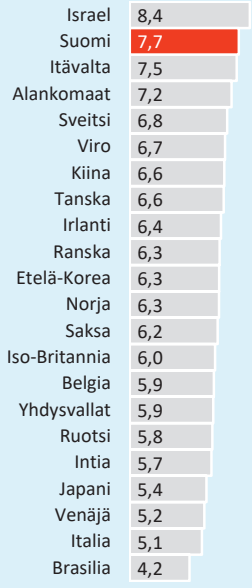


Liitekuvio 7

Tietoverkkojen turvallisuuden huomioiminen.

Maa saa arvon 10 (arvon 0), jos kyselyyn vastaajat katsovat yritysten panostavan tietoverkkojensa turvallisuuteen erinomaisesti (erittäin huonosti).

Lähde: IMD (2019, muuttuja 4.2.18). Tiedot ovat vuodelta 2019.

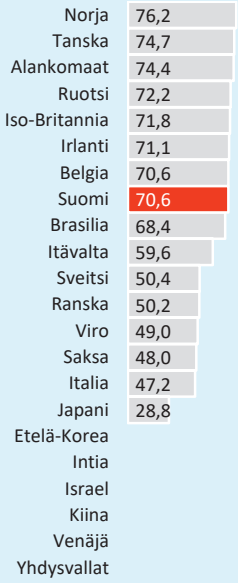


Liitekuvio 8

Sosiaalisen median käyttö liiketoiminnassa.

%-osuus yrityksistä, jotka käyttävät liiketoiminnassaan jotain sosiaalisen median tyyppiä, kuten yhteisöpalveluja, blogeja, multimedian jakamista tai wiki-pohjaisten tiedon jakamisen työkaluja.

Lähde: Eurostat Information society statistics. Tiedot ovat vuodelta 2019.



Yritysten vaikutukset

9. Viestintäteknologia täyttää yritysten tarpeet. Muuttujassa maa saa arvon 10 (arvon 0), jos kyselyyn vastanneet henkilöt katsovat maassa tarjotun tai sovelletun viestintäteknologian täyttävän yritysten tarpeet erinomaisesti (erittäin huonosti). Lähteenä on IMD:n kilpailukykyvertailun yrityskysely, ja muuttuja on raportoitu IMD:n vuoden 2019 World Competitiveness Yearbookissa, muuttujan koodi 4.2.04. Tiedot koskevat vuotta 2019.

10. ICT:n vaikutus yritysten kilpailukykyyn. Vastaajien keskimääräinen arvo asteikolla yhdestä kymmeneen. Korkeampi arvo tarkoittaa, että ICT:llä on suurempi vaikutus yritysten kilpailukykyyn. Lähteenä on IMD:n kilpailukykyvertailun yrityskysely, ja muuttuja on raportoitu IMD:n vuoden 2019 World Competitiveness Yearbookissa, muuttujan koodi 3.1.10. Tiedot ovat vuodelta 2019. Muuttuja korvaa edellisen vuoden WEF:n yrityskyselyyn perustuvan muuttujan ”ICT:n vaikutus uusiin liiketoimintamalleihin”, koska siitä ei ollut saatavissa päivitystä.

11. ICT-pääoman kasvukontribuutio. Mittari kuvaa ICT-pääoman keskimääräistä vaikutusta bruttokansantuotteen kasvuun aikavälillä 2008–2018. Lähteenä on Conference Board Total Economy Database, April 2019, www.conference-board.org/data/economydatabase/.

12. Yritysten sähköiset hankinnat. Mittari on laskettu osuutena vähintään 10 henkeä työllistävistä yrityksistä, jotka käyttävät sähköistä tietoverkkoa ostoissaan. Tähän sisältyvät www-sivujen, EDI-järjestelmien ja vastaavien kautta tapahtuva sähköinen tiedonsiirto, mutta siihen eivät kuulu käsin kirjoitetut sähköpostiviestit. Lähteenä on Eurostatin Information society statistics -tietokantaan sisältyvä yrityskysely Community survey on ICT usage and eCommerce in Enterprises. Luvut koskevat vuotta 2018.

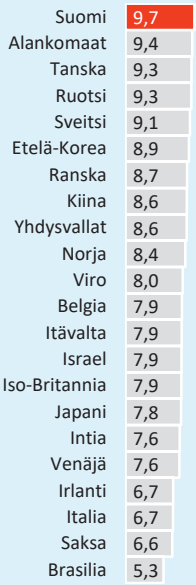
Yritysten vaikutukset

Liitekuvio 9

Viestintäteknologia täyttää yritysten tarpeet.

Maa saa arvon 10 (arvon 0), jos kyselyyn vastaajat katsovat maassa tarjotun/sovelletun viestintäteknologian täyttävän yritysten tarpeet erinomaisesti (erittäin huonosti).

Lähde: IMD (2019, muuttuja 4.2.04). Tiedot ovat vuodelta 2019.

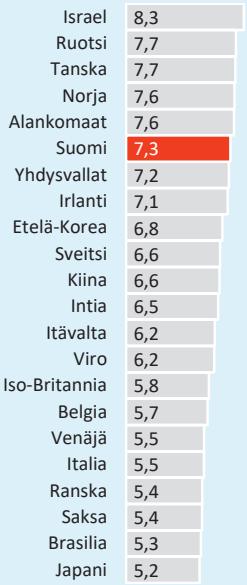


Liitekuvio 10

ICT:n vaikutus yritysten kilpailukykyyn.

Maa saa arvon 10 (arvon 0), jos kyselyyn vastaajat katsovat ICT:llä olevan suuri vaikutus yritysten kilpailukykyyn (pieni vaikutus).

Lähde: IMD (2019, muuttuja 3.1.10). Tiedot ovat vuodelta 2019.

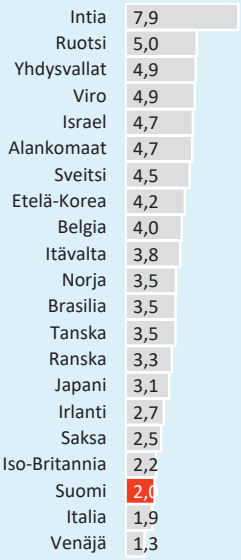


Liitekuvio 11

ICT-pääoman kasvukontribuutio.

Keskimäärin promillea vuodessa aikavälillä 2008–2018.

Lähde: The Conference Board Total Economy Database, April 2019, http://www.conference-board.org/data/economydatabase/. Tiedot ovat vuodelta 2018.



Liitekuvio 12

Yritysten sähköiset hankinnat.

%-osuus yrityksistä, jotka käyttävät sähköistä tietoverkkoa ostoissaan.

Lähde: Eurostat Information society statistics. Tiedot ovat vuodelta 2018.

Kansalaisten edellytykset

13. Nopean (väh. 2 Mbit/s) laajakaistan yleisyys. Mittari kuvaa kiinteiden (ts. sijaintipaikkaan sidoksissa olevien langallisten ja langattomien) laajakaistaliittymien tilaajien määrää suhteessa väestön määrään (jaettuna sadalla). Nopeus on luokiteltu myyntiesitteessä ilmoitettuna keskimääräisenä siirtonopeutena Internetistä liittymään päin, eikä siten välttämättä vastaa todellista siirtonopeutta. Väestön määrä on mitattu vuosikeskiarvona. Luvut koskevat vuotta 2018. Lähteenä on ITU World Telecommunication/ICT Indicators Database.

14. Aktiivisten mobiililaajakaistakäyttäjien osuus. Muuttuja kuvaa aktiivisten mobiilien laajakaistatilausten määrää suhteessa väestön määrään (jaettuna sadalla). Mobiileihin laajakaistatilauksiin sisältyvät sekä matkapuhelinten että erillislaitteiden langattomat liikkuvat laajakaistayhteydet. Aktiivisuus on laskettu laajakaistatilausten perusteella eikä siis sellaisten päätelaitteiden perusteella, joissa on mahdollisuus käyttää laajakaistayhteyksiä. Väestön määrä on mitattu vuosikeskiarvona. Luvut koskevat vuotta 2018. Lähteenä on ITU World Telecommunication/ICT Indicators Database.

15. Kansalaisten digitaidot. Vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa, että kansalaiset omaavat paremmat digitaaliset taidot liittyen esimerkiksi tietokoneiden käyttöön, ohjelmointiin ja multimedian käyttöön. Lähteenä on WEF Executive Opinion Survey 2018 ja 2019. Tiedot koskevat vuotta 2019. Tämä muuttuja korvaa edellisen vuoden WEF-kyselymuuttujan Internetin hyödyntäminen opetuksessa.

16. Internet-osaamisen saatavuus. Maa saa arvon 10 (arvon 0), jos kyselyyn vastaajat katsovat ICT-osaajien tarjonnan olevan erinomaista (erittäin huonoa). Lähteenä on IMD:n kilpailukykyvertailun yrityskysely, ja muuttuja on raportoitu IMD:n vuoden 2019 World Competitiveness Yearbookissa, muuttujan koodi 4.2.10. Tiedot koskevat vuotta 2019.

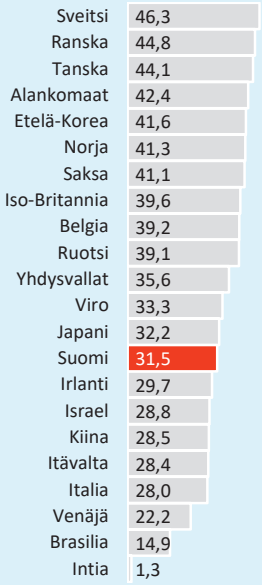
Kansalaisten edellytykset

Liitekuvio 13

Nopean laajakaistan yleisyys.

Tilaajien määrä suhteessa väestöön, %:a.

Lähde: ITU World Telecommunication/ICT Indicators. Tiedot ovat vuodelta 2018.

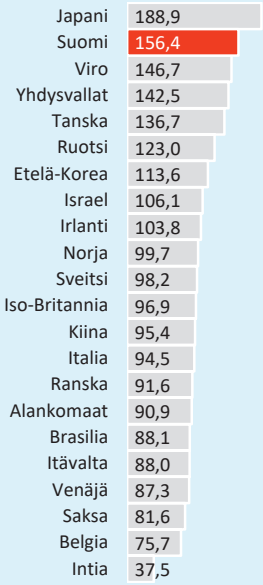


Liitekuvio 14

Aktiivisten mobiililaajakaistakäyttäjien osuus.

%:a väestöstä.

Lähde: ITU World Telecommunication/ICT Indicators. Tiedot ovat vuodelta 2018.

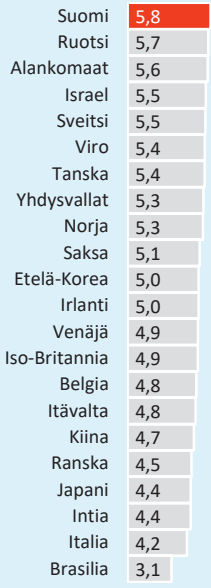


Liitekuvio 15

Kansalaisten digitaidot.

Vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa, että kansalaiset omaavat paremmat digitaaliset taidot.

Lähde: WEF Executive Opinion Survey 2018 ja 2019. Tiedot ovat vuodelta 2019.

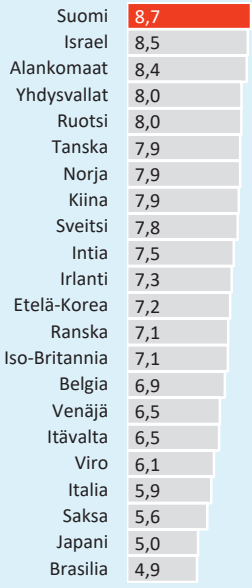


Liitekuvio 16

Internet-osaamisen saatavuus.

Maa saa arvon 10 (arvon 0), jos kyselyyn vastaajat katsovat ICT-osaajien tarjonnan olevan erinomaista (erittäin huonoa).

Lähde: IMD (2019, muuttuja 4.2.10). Tiedot ovat vuodelta 2019.



Kansalaisten käyttö

17. Internetin käyttäjien osuus väestöstä. Internetin käyttäjien lukumäärä 10 henkeä kohden. Lähteenä on WEF:n 2019 kilpailukykyvertailun muuttuja *netuserpct*, joka pohjautuu ITU World Telecommunication/ ICT Indicators Database:n tietoihin. Tiedot koskevat vuotta 2018.

18. Aktiivisuus sosiaalisessa mediassa. Vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa, että sosiaalista mediaa käytetään väestön keskuudessa enemmän. Muuttuja on vaihdettu edellisen vuoden Eurostatin tietoihin perustuvasta muuttujasta laajemman maajakauman takia. Lähteenä on WEF Executive Opinion Survey 2017 ja 2018. Tiedot koskevat vuotta 2018.

19. Ostanut tuotteita tai palveluita Internetistä. Mittari on laskettu osuutena kuluttajista, jotka ovat ostaneet tavaroita tai palveluja muuhun kuin työkäyttöön Internetin välityksellä. Aikakriteerinä on ollut, että Internetin kautta on tehty ostoksia kyselyä edeltävän vuoden aikana. Lähteenä on OECD:n tietokanta ”ICT Access and Usage by Households and Individuals”. Luvut ovat vuodelta 2019.

20. Myynyt tuotteita tai palveluita Internetissä. Mittari on laskettu osuutena kuluttajista, jotka ovat myyneet tavaroita tai palveluja Internetin välityksellä viimeisen kolmen kuukauden aikana. Lähteenä on OECD:n tietokanta ”ICT Access and Usage by Households and Individuals”. Luvut ovat vuodelta 2019.

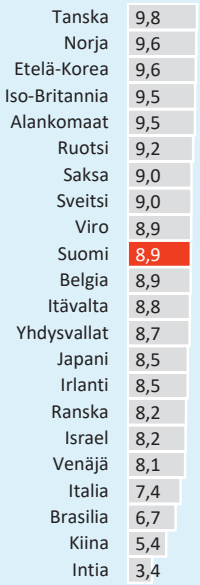
Kansalaisten käyttö

Liitekuvio 17

Internetin käyttäjien osuus väestöstä.

Internetiä käyttävien osuus väestöstä 10 henkeä kohden.

Lähde: ITU World Telecommunication/ICT Indicators. Tiedot ovat vuodelta 2018.

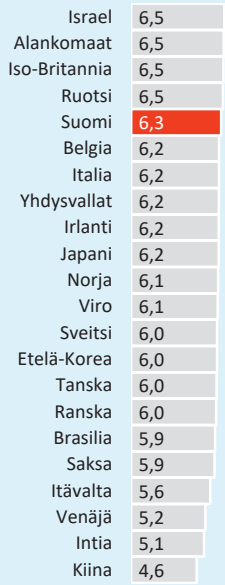


Liitekuvio 18

Aktiivisuus sosiaalisessa mediassa.

Vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa, että sosiaalista mediaa käytetään enemmän.

Lähde: WEF Executive Opinion Survey 2017 ja 2018. Tiedot ovat vuodelta 2018.

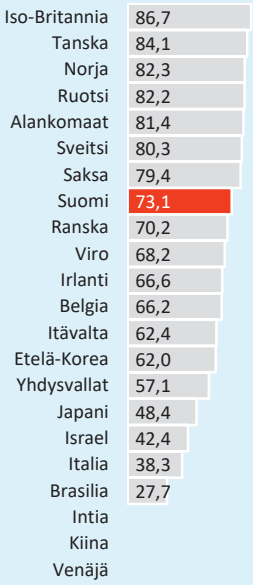


Liitekuvio 19

Ostanut tuotteita tai palveluita Internetistä.

%-osuus kuluttajista, jotka ovat ostaneet tuotteita tai palveluita Internetin välityksellä vuoden aikana.

Lähde: OECD, ICT Access and Usage by Households and Individuals. Tiedot ovat vuodelta 2019.

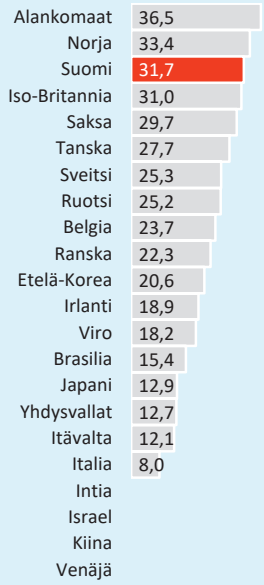


Liitekuvio 20

Myynyt tuotteita tai palveluita Internetissä.

%-osuus kuluttajista, jotka ovat myyneet tuotteita tai palveluita Internetin välityksellä vuoden aikana.

Lähde: OECD, ICT Access and Usage by Households and Individuals. Tiedot ovat vuodelta 2019.



Kansalaisten vaikutukset

21. ICT:n vaikutus työmarkkinoihin. %-osuus 25–44-vuotiaista työssäkäyvistä henkilöistä, joiden pääasialliset työtehtävät ovat muuttuneet viimeisen vuoden aikana uuden tietokoneohjelmiston tai tietokoneohjatun laitteiston käyttöönoton seurauksena. Lähteenä on Eurostatin tietokanta ”ICT usage in households and by individuals” ja sen tietokantataulu ”Impact of ICT on tasks and skills (isoc_iw_imp)”. Tiedot koskevat vuotta 2018. Muuttuja korvaa edellisen vuoden Maailmanpankin tietoihin perustuvan muuttujan, koska siitä ei ole ollut saatavissa päivitettyjä tietoja.

22. Internet-vähittäiskaupan arvo dollareina 10 miljoonaa henkeä kohden. Lähteenä on IMD:n vuoden 2019 digitaalisen kilpailukykyvertailun muuttuja 3.1.2, jonka aineistolähteenä puolestaan on Euromonitor International. Tiedot koskevat vuotta 2018.

23. Peruspalvelujen parempi saavutettavuus ICT:n myötä. Kilpailukykykyselyn vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa, että ICT:llä on ollut merkittävämpi vaikutus palvelujen saavutettavuudessa. Peruspalveluilla tarkoitetaan mm. sosiaali- ja terveyspalveluita, koulutusta ja pankki- ja vakuutuspalveluita. Lähteenä on WEF Executive Opinion Survey 2017 ja 2018. Tiedot koskevat vuotta 2018.

24. ICT:tä hyödyntävä yhteiskunnallinen osallistuminen (E-participation). Muuttuja on indeksiarvo nollasta sataan, jossa korkeampi arvo kuvaa maan laajempaa hyödyntämistä. Muuttaja pyrkii huomioimaan sekä julkisen sektorin tarjoamat erilaiset kannustimet ja pyrkimykset sähköisten palvelujen lisääntyvälle käytölle että kansalaisten halun ja kyvyn osallistua yhteiskunnalliseen toimintaan ICT:tä hyödyntäen. Lähteenä on YK:n E-Government Survey 2018, ja luvut koskevat vuotta 2018.

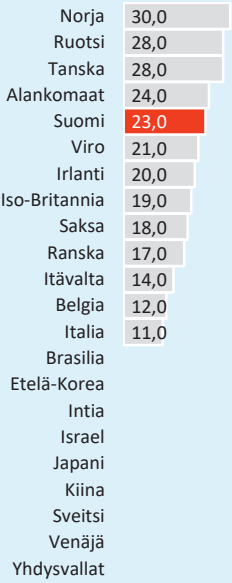
Kansalaisten vaikutukset

Liitekuvio 21

ICT:n vaikutus työmarkkinoihin.

%-osuus työllisistä, joiden pääasialliset työtehtävät ovat muuttuneet ICT:n seurauksena.

Lähde: Eurostat, ICT usage in households and by individuals. Tiedot ovat vuodelta 2018.

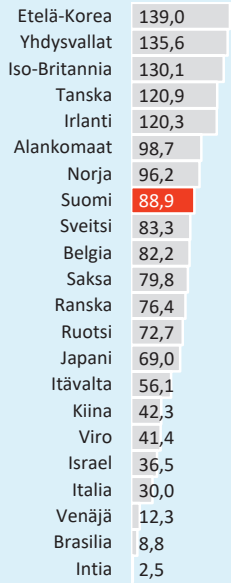


Liitekuvio 22

Internet-vähittäiskaupan arvo.

Dollareina 10 miljoonaa henkeä kohden.

Lähde: IMD:n digitaalinen kilpailukykyvertailu, muuttuja 3.2.1. Tiedot ovat vuodelta 2018.

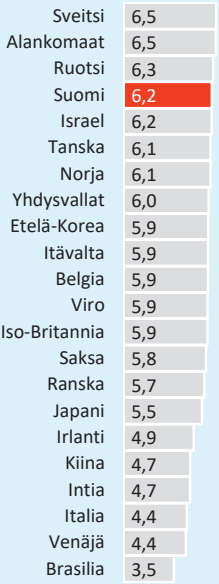


Liitekuvio 23

Peruspalvelujen parempi saavutettavuus ICT:n myötä.

Vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa, että ICT:llä on ollut merkittävämpi vaikutus palvelujen saavutettavuudessa.

Lähde: WEF Executive Opinion Survey 2017 ja 2018. Tiedot ovat vuodelta 2018.

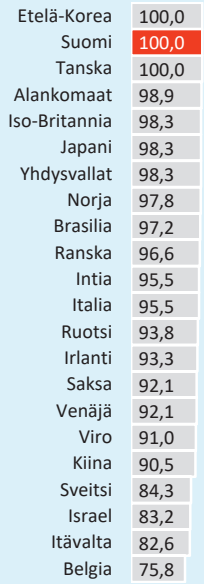


Liitekuvio 24

ICT:tä hyödyntävä yhteiskunnallinen osallistuminen.

Indeksiarvo nollasta sataan, jossa korkeampi arvo kuvaa maan laajempaa hyödyntämistä.

Lähde: United Nations E-Government Survey 2018. Tiedot ovat vuodelta 2018.



Julkisen sektorin edellytykset

25. Tietoturvahuolet eivät estä kansalaisten viranomaisasiointia Internetissä. %-osuus 16–74-vuotiaista Internetiä viimeisten 12 kuukauden aikana käyttäneistä henkilöistä, joiden mielestä tietoturvahuolet eivät ole haitanneet heidän asiointiaan viranomaistahojen kanssa Internetissä. Lähteenä on Eurostatin Information society statistics -tietokantaan sisältyvä kysely ICT usage in households and by individuals, ja tiedot koskevat vuotta 2019.

26. Oikeudellinen toimintaympäristö tukee uuden teknologian kehittämistä ja soveltamista. Maa saa arvon 10 (arvon 0), jos kyselyyn vastaajat katsovat maan oikeudellisen toimintaympäristön tukevan yritystoiminnan kehittämistä ja innovaatiotoimintaa erinomaisesti (erittäin huonosti). Lähteenä on IMD:n kilpailukykyraportti vuodelta 2019, muuttujan koodi 4.2.13. Tiedot ovat vuodelta 2019.

27. ICT:tä sivuavan lainsäädännön edistyksellisyys. Kilpailukykykyselyn vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa parempaa lainsäädäntöä ICT:n käyttöön liittyen (esim. sähköinen kaupankäynti, digitaaliset varmenteet, kuluttajansuoja). Lähteenä on WEF Executive Opinion Survey 2017 ja 2018. Tiedot ovat vuodelta 2018.

28. Teknologian kehittämisen rahoituksen saatavuus. Vastaajien keskimääräinen arvo asteikolla yhdestä kymmeneen. Korkeampi arvo tarkoittaa, että teknologian kehittämiseen on saatavissa hyvin rahoitusta. Lähteenä on IMD:n kilpailukykyvertailun yrityskysely, ja muuttuja on raportoitu IMD:n vuoden 2019 World Competitiveness Yearbookissa, muuttujan koodi 4.2.14. Tiedot ovat vuodelta 2019. Muuttaja korvaa edellisen vuoden WEF:n yrityskyselyn muuttujan ”ICT:n hyödyntäminen julkisessa tiedottamisessa”, koska siitä ei ollut saatavissa päivitystä.

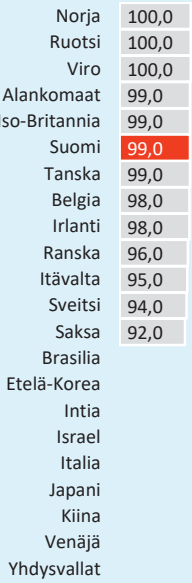
Julkisen sektorin edellytykset

Liitekuvio 25

Tietoturvahuolet eivät estä kansalaisten viranomaisasiointia Internetissä.

%-osuus 16–74-vuotiaista henkilöistä, jotka ovat käyttäneet Internetiä viimeisten 12 kuukauden aikana.

Lähde: Eurostat Information society statistics. Tiedot ovat vuodelta 2019.

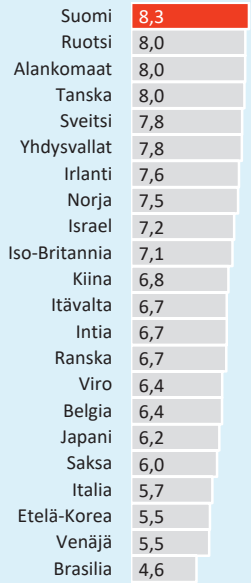


Liitekuvio 26

Oikeudellinen toimintaympäristö tukee uuden teknologian kehittämistä ja soveltamista.

Maa saa arvon 10 (arvon 0), jos kyselyyn vastaajat katsovat maan oikeudellisen toimintaympäristön tukevan yritystoiminnan kehittämistä ja innovaatiotoimintaa erinomaisesti (erittäin huonosti).

Lähde: IMD (2019, muuttuja 4.2.13). Tiedot ovat vuodelta 2019.

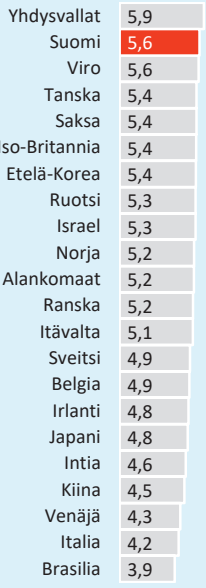


Liitekuvio 27

ICT:tä sivuavan lainsäädännön edistyksellisyys.

Vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa parempaa lainsäädäntöä.

Lähde: WEF Executive Opinion Survey 2017 ja 2018. Tiedot ovat vuodelta 2018.

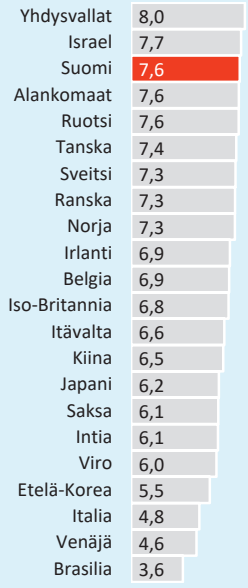


Liitekuvio 28

Teknologian kehittämisen rahoituksen saatavuus.

Vastaajien keskimääräinen arvo asteikolla yhdestä kymmeneen. Korkeampi arvo tarkoittaa, että teknologian kehittämiseen on saatavissa hyvin rahoitusta.

Lähde: IMD (2019, muuttuja 4.2.14). Tiedot ovat vuodelta 2019.



Julkisen sektorin käyttö

29. Kansalaisten sähköinen viranomaisasiointi. Muuttuja kuvaa osuutta 16–74 vuotta vanhoista kansalaisista, jotka ovat hakeneet viranomaistietoa Internetin välityksellä viimeisen 12 kuukauden aikana pois lukien Sveitsin, jonka osalta tieto kattaa kaikki 14 vuotta täyttäneet henkilöt. Lähteenä OECD:n tietokanta ”ICT Access and Usage by Households and Individuals”. Tiedot koskevat vuotta 2019.

30. Julkisen datan avoimuus. Indeksiarvo nollasta sataan, jossa korkeampi arvo kuvaa julkisen datan suurempaa avoimuutta. Lähteenä on Open Knowledge Network. http://index.okfn.org/place/. Tiedot koskevat vuotta 2017.

31. Julkiset teknologiatuotteiden hankinnat. Vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa, että julkisin hankinnoin edistetään enemmän korkean teknologian kehittämistä ja käyttöä. Lähteenä on WEF Executive Opinion Survey 2017 ja 2018. Tiedot ovat vuodelta 2018.

32. Julkisten online-palvelujen laajuus ja laatu. Indeksiarvo nollasta sataan, jossa korkeampi arvo kuvaa maan julkisten online-palvelujen parempaa laajuutta tai laatua. Lähteenä on United Nations E-Government Survey 2018, muuttuja Online Service Index.

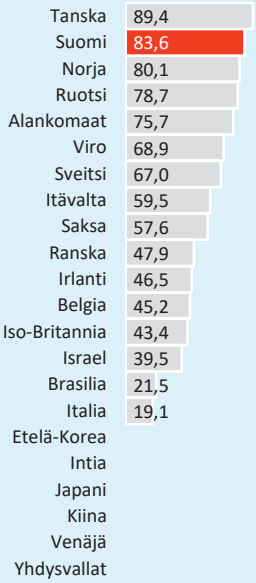
Julkisen sektorin käyttö

Liitekuvio 29

Kansalaisten sähköinen viranomaisasiointi.

%-osuus kansalaisista, jotka hakevat viranomaistietoa Internetin välityksellä.

Lähde: OECD, ICT Access and Usage by Households and Individuals. Tiedot ovat vuodelta 2019.

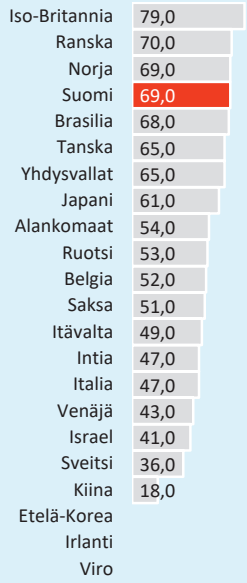


Liitekuvio 30

Julkisen datan avoimuus.

Indeksiarvo nollasta sataan, jossa korkeampi arvo kuvaa julkisen datan suurempaa avoimuutta.

Lähde: Open Knowledge Network. http://index.okfn.org/place/. Tiedot ovat vuodelta 2017.

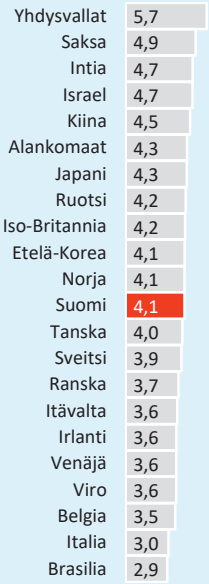


Liitekuvio 31

Julkiset teknologiatuotteiden hankinnat.

Vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa, että julkisin hankinnoin edistetään korkean teknologian kehittämistä ja käyttöä.

Lähde: WEF Executive Opinion Survey 2017 ja 2018. Tiedot ovat vuodelta 2018.

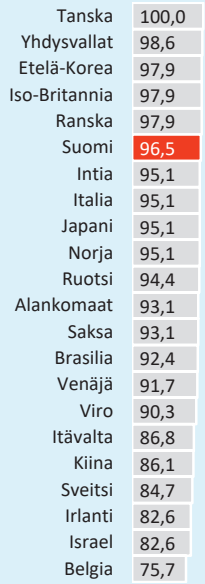


Liitekuvio 32

Julkisten onlinepalvelujen laajuus ja laatu.

Indeksiarvo nollasta sataan, jossa korkeampi arvo kuvaa maan parempaa laajuutta/laatua.

Lähde: United Nations E-Government Survey 2018. Tiedot ovat vuodelta 2018.



Julkisen sektorin vaikutukset

33. ICT parantaa julkisten palvelujen tuottavuutta. Kilpailukykykyselyssä vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa ICT:n suurempaa vaikutusta esimerkiksi palveluiden nopeampaan saatavuuteen, virheiden vähenemiseen, läpinäkyvyyden parantumiseen ja uusien online-palvelujen luomiseen. Lähteenä on WEF Executive Opinion Survey 2017 ja 2018. Tiedot koskevat vuotta 2018.

34. Julkiset toimet ICT:n hyödyntämisen edistämiseksi. Kilpailukykykyselyssä vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa, että julkisin toimin edistetään johdonmukaisesti ICT:n hyödyntämistä maan kilpailukyvyn parantamisessa. Lähteenä on WEF Executive Opinion Survey 2017 ja 2018. Tiedot koskevat vuotta 2018.

35. Julkisen sektorin sopeutumiskyky digitaalisten liiketoimintamallien tarpeisiin. Vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa, että julkinen sektori pystyy sopeuttamaan toimintatapojaan nopeammin digitaalisten liiketoimintamallien, kuten verkkokaupan, jakamistalouden, fintechin yms. vaatimuksia vastaaviksi. Lähteenä on WEF Executive Opinion Survey 2018 ja 2019. Tiedot ovat vuodelta 2019. Muuttuja korvaa edellisen vuoden saman aineistolähteen muuttujan ”Julkisten ICT-toimien vaikuttavuus taloudessa”, koska siitä ei ollut saatavissa päivettyjä tietoja.

36. Viestintäpalvelujen kilpailullisuus. Vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa, että ala on kilpailullisempi. Lähteenä on WEF Executive Opinion Survey 2018 ja 2019. Tiedot koskevat vuotta 2019.

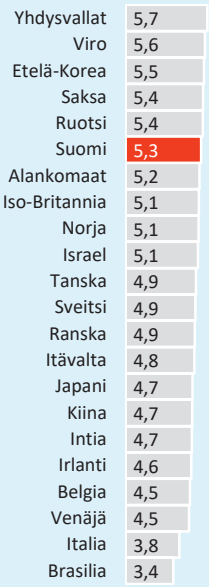
Julkisen sektorin vaikutukset

Liitekuvio 33

ICT parantaa julkisten palvelujen tuottavuutta.

Vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa ICT:n suurempaa vaikutusta.

Lähde: WEF Executive Opinion Survey 2017 ja 2018. Tiedot ovat vuodelta 2018.

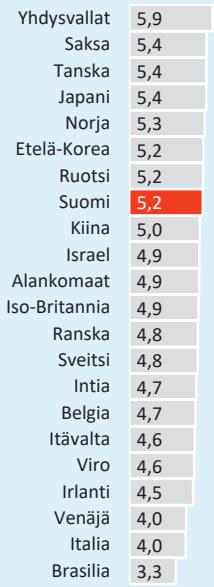


Liitekuvio 34

Julkiset toimet ICT:n hyödyntämisen edistämiseksi.

Vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa, että julkisin toimin edistetään johdonmukaisesti ICT:n hyödyntämistä maan kilpailukyvyn parantamisessa.

Lähde: WEF Executive Opinion Survey 2017 ja 2018. Tiedot ovat vuodelta 2018.

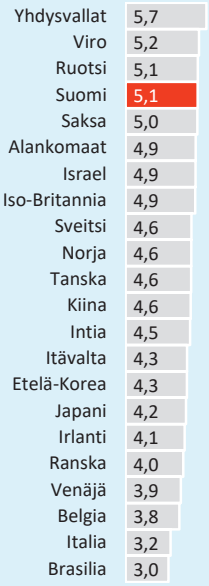


Liitekuvio 35

Julkisen sektorin sopeutumiskyky digitaalisten liiketoimintamallien tarpeisiin.

Vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa, että julkinen sektori pystyy sopeuttamaan toimintatapojaan nopeammin digitaalisten liiketoimintamallien vaatimuksia vastaaviksi.

Lähde: WEF Executive Opinion Survey 2018 ja 2019. Tiedot ovat vuodelta 2019.

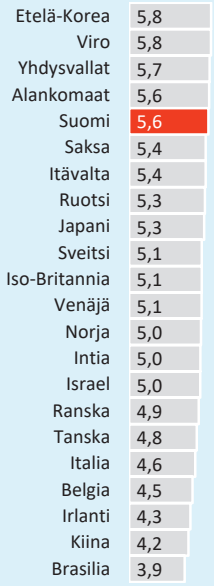


Liitekuvio 36

Viestintäpalvelujen kilpailullisuus.

Vastaajien keskimääräinen arvo asteikolla 1:stä 7:ään. Korkeampi arvo tarkoittaa, että ala on kilpailullisempi.

Lähde: WEF Executive Opinion Survey 2018 ja 2019. Tiedot ovat vuodelta 2019.



Liite 2: Digibarometrin toteutus

Viimevuotiseen tapaan Digibarometri on tehty soveltaen mm. IMD:n kilpailukykymittauksille sukua olevaa lähestymistapaa, jossa maita laitetaan paremmuusjärjestykseen indeksillä ja joka perustuu vakioitujen tilastoja muiden muuttujien yhdistelyyn. Barometri mittaa digitaalisuuden laajaa yhteiskunnallista hyödyntämistä, eikä sijoituksiin siten suoraan vaikuta esim. maan rooli digitaalisten tuotteiden ja palveluiden tarjonnassa.

Viitekehys

Toteuttamistapa on käytännössä sama kuin vuosi sitten julkaistussa Digibarometrissä, joskin aineistot on pyritty päivittämään kautta linjan. Joitain yksittäisiä muuttujia on jouduttu vaihtamaan, koska täsmälleen sama muuttuja ei enää ollut saatavilla (muuttujista liitteessä 1).

Barometri mittaa yhteiskunnan digitaalisia ulottuvuuksia kolmella toisiinsa kytkeytyvällä tasolla – *edellytyksissä*, *käyt*össä ja *vaikutuksissa* – sekä kolmella pääsektorilla – *yrityksissä*, *kansalaisten* keskuudessa ja *julkisella* sektorilla. Kolme tasoa ja kolme sektoria yhdistämällä syntyy yhdeksän solun matriisi, joka toimii *Digibarometrin* viitekehyksenä (liitekuvio 37).

Liitekuvio 37 **Digibarometrin viitekehys**

Digibarometrissa kansainvälinen vertailu toteutetaan kilpailukykyindekseistä (IMD, WEF) tutulla tavalla, ja käytännössä se perustuu maatasolla mitattujen muuttujien vakiointiin ja yhdistelyyn. Digibarometrin muuttujat on valittu yleisesti saatavilla olevista tilasto- ja muista lähteistä. Muuttujat on esitetty liitekuviossa 38 ja tarkemmin liitteessä 1.

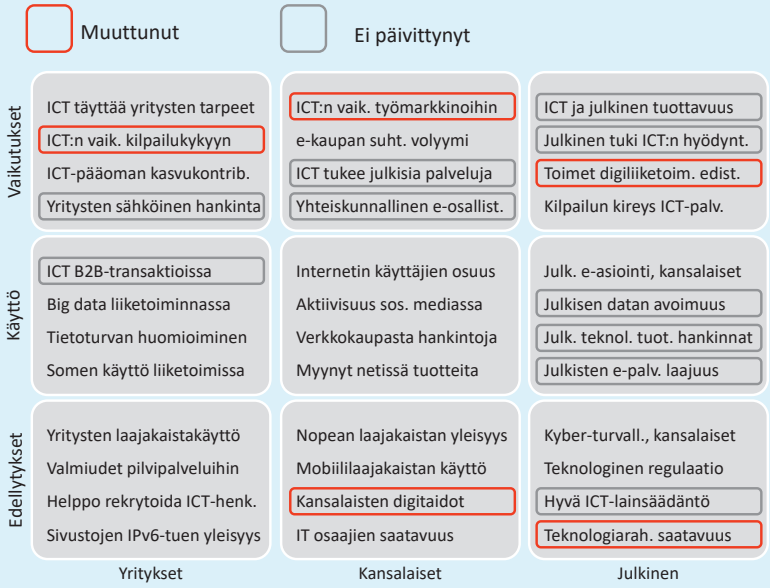
Muuttujien valinta

Indeksin laskentaan käytetyt muuttujat on valittu siten, että ne kuvaavat suoraan eri digitaalisia ulottuvuuksia mutta eivät itse ICT-alaa tai koulutustason kaltaisia yleisiä edellytyksiä. Mukaan on valittu nimenomaan Suomea ja lähimpiä kilpailijamaita, kuten Ruotsia, erottelevia muuttujia.

Viitekehysmatriisin kuhunkin yhdeksään soluun on valittu neljä muuttujaa, jotka tuovat esiin erilaisia ulottuvuuksia solun aihepiiristä. Koska digitaalisuuteen liittyvät ulottuvuudet ovat usein voimakkaasti korreloituneita, laajemman muuttujajoukon ei katsottu tarjoavan olennaista etua.

Rahamääräisiä muuttujia (esim. laajakaistaliittymien kuukausi- tai puhelujen minuuttihinnat) vältettiin, koska ne ovat ehdollisia maan yleiselle kustannustasolle ja regulaatioympäristölle sekä vallitsevalle kysynnän ja tarjonnan luonteelle ja rakenteelle. Lisäksi eri valuuttojen yhteismitallistami-

Liitekuvio 38 **Digibarometrin muuttujat**



selle ei ole yksiselitteisesti oikeaa tapaa (sekä käyvillä että ostovoimapariteettipohjaisilla valuuttakursseilla on omat etunsa ja haittansa).

Myöskään investointitietoja ei käytetty. Rahamääräisten suureiden jo mainittujen ongelmien lisäksi ne ovat ehdollisia vallitsevalle suhdannetilanteelle ja maan talouden kehitysvaiheelle sekä vaihtoehtoisille investoinneille (esim. kiinteän *versus* mobiilin verkon investoinnit). Lisäksi tehtyjen investointien määrä ei suoraan kerro niiden hyvästä kohdentumisesta tai onnistuneesta toteutuksesta.

Maiden valinta

Vertailussa on 22 maata, joiden pääasiallisina valintakriteereinä ovat olleet, että ne ovat Suomen kaltaisia pieniä korkean tulotason maita (esim. Alankomaat, Sveitsi, Tanska) tai Suomen lähinaapureita (Norja, Ruotsi, Venäjä, Viro). Lisäksi mukana on verrokkeina neljä suurinta EU-maata (Iso-Britannia, Italia, Ranska, Saksa), vakiintuneita teollistuneita digiteknologiaa kehittäviä maita (Etelä-Korea, Japani, Yhdysvallat) ja nopeasti digitaalisuudessakin kehittyvät BRIC-taloudet.

Indeksin laskenta

Kustakin mukana olevasta muuttujasta käytetään viimeistä saatavilla olevaa tietoa. Muuttujien yhteismitallistaminen on tehty yleisesti käytetyllä *z-score* -menetelmällä siten, että positiivisten ja negatiivisten ääriarvojen ylisuuri vaikutus eliminoidaan.

Laskettaessa *z-scorea* otetaan ensin erotus kunkin maan tietyn muuttujan arvosta ja kaikkien maiden keskiarvosta kyseisessä muuttujassa ja sitten jaetaan kyseinen muuttuja kaikkien maiden välisellä keskihajonnalla:

$$z\text{-}score = \frac{\text{Maan arvo muuttujassa } y - \ y\text{: n keskiarvo}}{y\text{: n keskihajonta}}$$

Ongelmana *z-scoressa* on se, että hyvin suuret tai pienet arvot voivat vaikuttaa merkittävästi lopputuloksiin. *Digibarometria* laskettaessa haluttiin, että maa kyllä saa ruusuja tai risuja erittäin korkeasta tai matalasta arvosta mutta siten, ettei yksittäinen muuttuja pääse dominoimaan maan kokonais-, taso-, sektori- tai solusijoitusta eikä laajemminkaan pääse hämärtämään maiden välisiä suhteita.

Niinpä meneteltiin niin, että kertaalleen lasketun *z-scoren* perusteella jakauman äärimmäisiä positiivisia (ja negatiivisia) arvoja tasoitettiin korkealle mutta kohtuulliselle positiiviselle (tai negatiiviselle) tasolle alla kuvattavalla tavalla.

Z-scoren kaava tuottaa muuttujan, jonka keskiarvo yli maiden on nolla ja keskihajonta yksi. Niinpä normaalijakautuneen muuttujan tapauksessa vakioitujen muuttuja-arvojen -2:n ja +2:n väliin jää 95 % havainnoista sekä jakauman positiiviseen ja negatiiviseen häntään yhteensä 5 %. Näihin häntiin jääviä arvoja muokattiin siten, että ne laitettiin vastaamaan jakauman keskimmäisen 95 % ylä- tai alalaitaa (käytännössä alle -2 suuruiset arvot saivat arvon -2 ja yli +2 suuriset arvon +2). Menetelmää kutsutaan *winsoroinniksi*. Koska alkuperäisen *z-scoren* laskennassa ääriarvot vaikuttivat ko. jakaumaan mahdollisesti tuloksia harhauttavalla tavalla, *winsoroinnin* jälkeen *z-scoret* laskettiin uudelleen muokkauksen jälkeisistä arvoista.

Kokonais-, taso-, sektori- ja soluindeksien arvot ovat yksinkertaisesti mukaan tulevien yllä kuvatulla tavalla vakioitujen muuttujien ei-puuttuvien havaintojen summia. Jotta indekseillä olisi intuitiivisempi tulkinta ja niiden tulosten hahmottaminen olisi helpompaa, ääriarvokorjatut ja uudelleen vakioidut *z-score*-summat rajattiin vaihtelemaan välillä 1:stä 100:aan.

Maa saa arvon 1, jos se määrittää ko maajoukon huonoimman arvon *kaikissa mukaan tulevissa muuttujissa* ja vastaavasti 100, jos se on *paras kaikissa muuttujissa*. Olennainen välivaihe tähän pääsemisessä on seuraava: otetaan ensin erotus maan muuttujasummasta ja muuttujien matalimpien arvojen summista (saivatpa nämä mikä maa tahansa), ja sitten jaetaan erotuksella muuttujien korkeimpien ja matalimpien arvojen summista. Kaavan muut osat liittyvät halutun ylä- ja alarajan määräämiseen. Indeksiarvo lasketaan kaavasta:

$$\text{Maan indeksi} = 99 \times \frac{\text{Maan oikea summa} - \text{Minimien summa}}{\text{Maksimien summa} - \text{Minimien summa}} + 1$$

Kuten yllä olevasta kaavasta havaitaan, tapauksessa, jossa maa on paras kaikissa mukaan tulevissa muuttujissa, jakolaskun osoittaja ja nimittäjä ovat sama luku, jolloin maan indeksiarvoksi tulee 100. Vastaavasti kaikissa muuttujissa heikoin maa saa arvon 1.

Liite 3: Digibarometrin tulokset

Suomi toinen Digibarometrin *kokonaisindeksissä*

Suomi nousee Digibarometrin kokonaissijoituksessa toiselle sijalla viime vuoden kolmannelta sijalta. Tanska kirii toiselta sijalta koko vertailun kärkeen. Yhdysvallat tippuu ykköspallilta pronssitilalle. Kärkikolmikko on äärimmäisen tasainen vain yhden indeksipisteen erottaessa ykkös- ja kolmossijoja. Myös seuraava, edellisvuotiset sijoituksensa säilyttävä kolmikko – Alankomaat, Norja ja Ruotsi – on erittäin lähellä palkintopallille yltäneitä maita. Heikoiten menestyvät Brasilia, Italia ja Venäjä.

Alatasoista *edellytykset – käyttö – vaikutukset* sijoituksemme edellytyksissä ei muutu, sen sijaan vaikutuksissa sijoituksemme kohentuu yhden pykälän ja käytössä jopa 3 sijaa. Näissä dimensioissa sijoituksemme ovat parhaat edellytyksissä ja käytössä (sijat 2) ja huonoin vaikutuksissa (sija 5). Sektoreittain kansalaisten (sija 3) ja julkisen sektorin (sija 2) vertailuissa asemamme eivät muutu viime vuoteen verrattuna. Sen sijaan yritysten alaindeksissä kehitys on negatiivista (-3 sijaa) sijoituksemme ollessa tänä vuonna seitsemäs. Tasojen ja sektorien muodostamia soluja tarkasteltaessa sijoituksemme heikentyy eniten yritysten edellytyksissä (-6 sijaa). Soluittain sijoituksemme parantuu eniten julkisissa vaikutuksissa (+4 sijaa).

Liitekuvio 39

Suomen kokonais-, taso-, sektori- ja solukohtaiset sijoitukset Digibarometrissä.

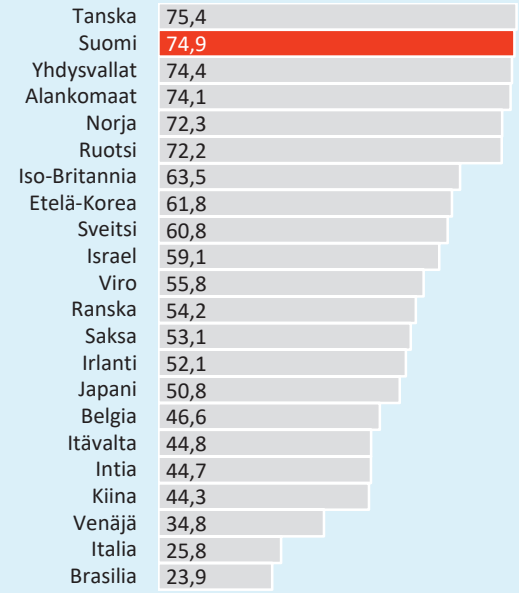
Suomi sijoittuu toiseksi Digibarometrin kokonaisindeksissä. Suomi menestyy parhaiten edellytyksissä ja käytössä sekä julkisessa sektorissa. Sijoitusten muutos viimevuotiseen verrattuna kursiivilla. Suomen merkittävin parannus on tapahtunut julkisissa vaikutuksissa. Suurin pudotus liittyy yritysten edellytyksiin.

Liitekuvio 40

Digibarometri: Kokonaisindeksi.

Tanska, Suomi ja Yhdysvallat ovat Digibarometrin kärkikolmikko. Alankomaat, Norja ja Ruotsi ovat tiiviisti kärkikolmikon imussa. Heikoiten menestyvät Brasilia, Italia ja Venäjä.

Lähde: Indeksin laskentatapa ja rakenne käyvät ilmi liitteen kuvauksesta. Tiedot ovat vuodelta 2019. Maa saa arvon 100 (arvon 1), jos se on paras (huonoin) kaikissa mukana olevissa osatekijöissä.

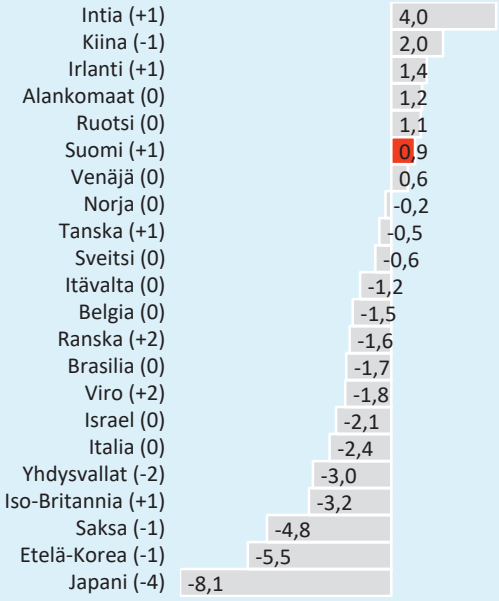


Liitekuvio 41

Digibarometri: Kokonaisindeksin muutokset edelliseen barometriin verrattuna.

Intia ja Kiina ovat parantaneet ja Japani sekä Etelä-Korea heikentäneet indeksiarvoaan eniten viime vuoden Digibarometriin verrattuna. Sijoitustaan ovat nostaneet eniten Ranska ja Viro, ja sijoitus on heikentynyt eniten Japanilla.

Lähde: Indeksin laskentatapa ja rakenne käyvät ilmi liitteen kuvauksesta. Tiedot ovat vuosilta 2018 ja 2019. Vaakapylväissä on raportoitu indeksilukujen muutokset. Maan perässä suluissa on puolestaan sijaluvun muutos.

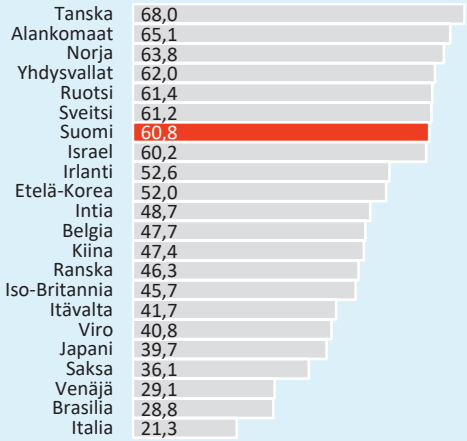


Liitekuvio 42

Digibarometri: Yritykset (3 ulottuvuutta).

Suomi on seitsemäs *yritysten* vertailussa Tanskan, Alankomaiden ja Norjan ollessa kärkikolmikko. Italia, Brasilia ja Venäjä löytyvät vertailun häntäpäästä.

Lähde: Indeksin laskentatapa ja rakenne käyvät ilmi liitteen kuvauksesta. Tiedot ovat vuodelta 2019. Maa saa arvon 100 (arvon 1), jos se on paras (huonoin) kaikissa mukana olevissa osatekijöissä.

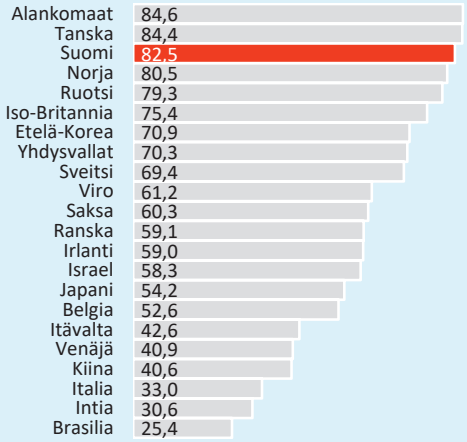


Liitekuvio 43

Digibarometri: Kansalaiset (3 ulottuvuutta).

Kansalaisten vertailussa Suomi on kolmas Alankomaiden ja Tanskan perässä. Brasilia ja Intia pitävä perää.

Lähde: Indeksin laskentatapa ja rakenne käyvät ilmi liitteen kuvauksesta. Tiedot ovat vuodelta 2019. Maa saa arvon 100 (arvon 1), jos se on paras (huonoin) kaikissa mukana olevissa osatekijöissä.

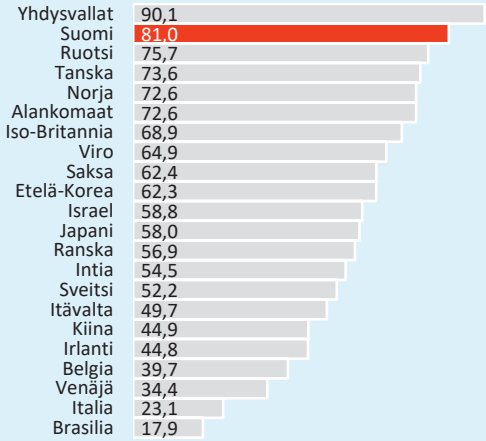


Liitekuvio 44

Digibarometri: Julkinen (3 ulottuvuutta).

Vain Yhdysvallat on Suomen edellä *julkisen* sektorin vertailussa. Brasilia ja Italia menestyvät heikoiten.

Lähde: Indeksin laskentatapa ja rakenne käyvät ilmi liitteen kuvauksesta. Tiedot ovat vuodelta 2019. Maa saa arvon 100 (arvon 1), jos se on paras (huonoin) kaikissa mukana olevissa osatekijöissä.

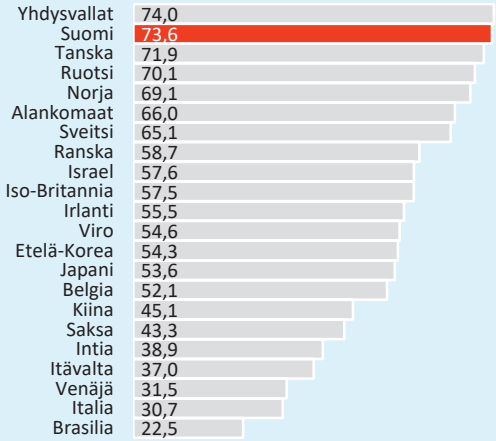


Liitekuvio 45

Digibarometri: Edellytykset (kaikki sektorit).

Yhdysvalloilla on Suomea paremmat *edellytykset* digitaalisuuden hyödyntämiseen. Muut Pohjoismaat hengittävät tiukasti Suomen kannoilla.

Lähde: Indeksin laskentatapa ja rakenne käyvät ilmi liitteen kuvauksesta. Tiedot ovat vuodelta 2019. Maa saa arvon 100 (arvon 1), jos se on paras (huonoin) kaikissa mukana olevissa osatekijöissä.

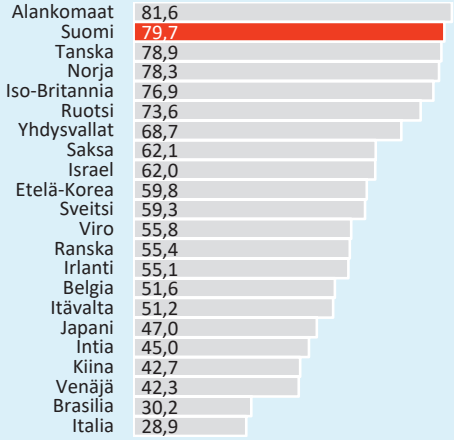


Liitekuvio 46

Digibarometri: Käyttö (kaikki sektorit).

Suomi menestyy Yhdysvaltoja paremmin digin *käytössä* huonommista *edellytyksistä* huolimatta.

Lähde: Indeksin laskentatapa ja rakenne käyvät ilmi liitteen kuvauksesta. Tiedot ovat vuodelta 2019. Maa saa arvon 100 (arvon 1), jos se on paras (huonoin) kaikissa mukana olevissa osatekijöissä.

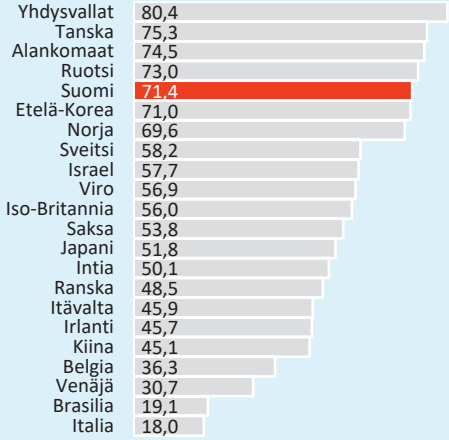


Liitekuvio 47

Digibarometri: Vaikutukset (kaikki sektorit).

Digin *vaikutuksissa* Suomi on viides Yhdysvaltojen, Tanskan, Alankomaiden ja Ruotsin jälkeen. Italia, Brasilia ja Venäjä ovat peränpitäjinä.

Lähde: Indeksin laskentatapa ja rakenne käyvät ilmi liitteen kuvauksesta. Tiedot ovat vuodelta 2019. Maa saa arvon 100 (arvon 1), jos se on paras (huonoin) kaikissa mukana olevissa osatekijöissä.

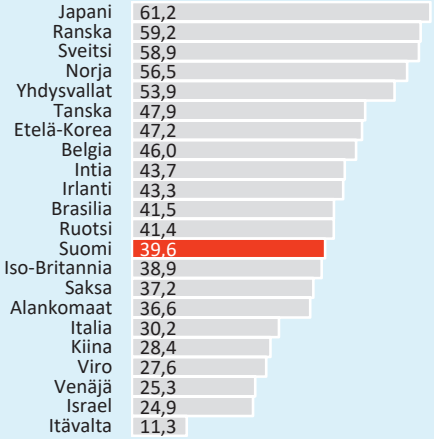


Liitekuvio 48

Digibarometri: Yritysten edellytykset.

Japanilla on parhaat *yritysten edellytykset*. Suomi sijoittuu alempaan keskikastiin sijalle kolmetoista.

Lähde: Indeksin laskentatapa ja rakenne käyvät ilmi liitteen kuvauksesta. Tiedot ovat vuodelta 2019. Maa saa arvon 100 (arvon 1), jos se on paras (huonoin) kaikissa mukana olevissa osatekijöissä.

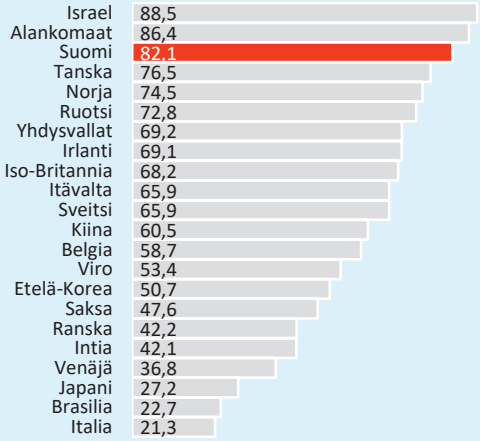


Liitekuvio 49

Digibarometri: Yritysten käyttö.

Suomi sijoittuu *yritysten käytössä* kolmanneksi lyöden mm. Ruotsin ja Yhdysvallat. Italia ja Brasilia sijoittuvat heikoiten.

Lähde: Indeksin laskentatapa ja rakenne käyvät ilmi liitteen kuvauksesta. Tiedot ovat vuodelta 2019. Maa saa arvon 100 (arvon 1), jos se on paras (huonoin) kaikissa mukana olevissa osatekijöissä.

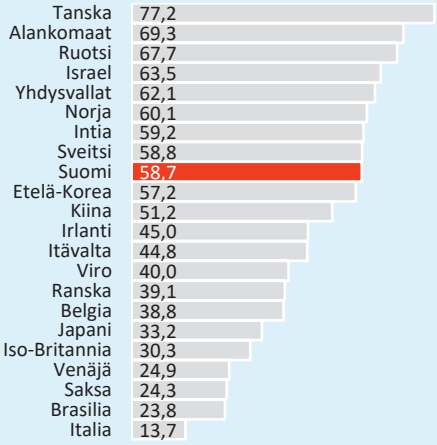


Liitekuvio 50

Digibarometri: Yritysvaikutukset.

Suomi on *yritysvaikutuksissa* keskikastissa sijalla yhdeksän. Suomen takana ovat mm. Etelä-Korea, Japani ja Saksa.

Lähde: Indeksin laskentatapa ja rakenne käyvät ilmi liitteen kuvauksesta. Tiedot ovat vuodelta 2019. Maa saa arvon 100 (arvon 1), jos se on paras (huonoin) kaikissa mukana olevissa osatekijöissä.

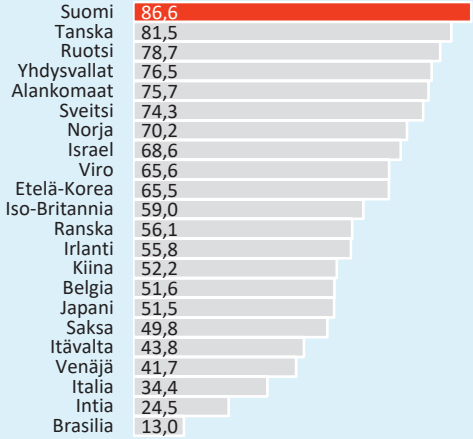


Liitekuvio 51

Digibarometri: Kansalaisten edellytykset.

Suomessa on vertailumaiden parhaat *kansalaisten edellytykset* digitaalisuuden hyödyntämiseen ennen Tanskaa ja Ruotsia.

Lähde: Indeksin laskentatapa ja rakenne käyvät ilmi liitteen kuvauksesta. Tiedot ovat vuodelta 2019. Maa saa arvon 100 (arvon 1), jos se on paras (huonoin) kaikissa mukana olevissa osatekijöissä.

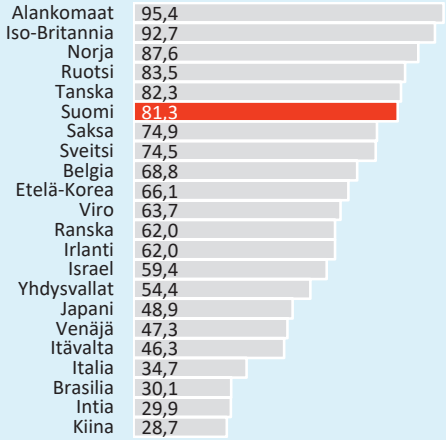


Liitekuvio 52

Digibarometri: Kansalaisten käyttö.

Hyvistä edellytyksistä huolimatta *kansalaisten käytössä* Suomi sijoittuu vasta kuudenneksi.

Lähde: Indeksin laskentatapa ja rakenne käyvät ilmi liitteen kuvauksesta. Tiedot ovat vuodelta 2019. Maa saa arvon 100 (arvon 1), jos se on paras (huonoin) kaikissa mukana olevissa osatekijöissä.

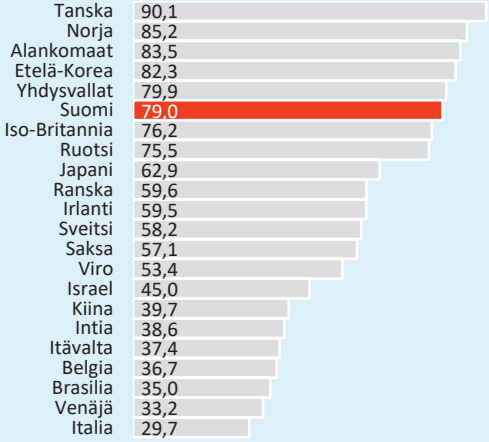


Liitekuvio 53

Digibarometri: Kansalaisvaikutukset.

Digin *vaikutuksissa kansalaisiin* Suomi on kuudes niukasti Yhdysvaltojen jäljessä mutta Ison-Britannian edellä. Tanska ja Norja ovat vertailun parhaat ja Italia sekä Venäjä heikoimmat.

Lähde: Indeksin laskentatapa ja rakenne käyvät ilmi liitteen kuvauksesta. Tiedot ovat vuodelta 2019. Maa saa arvon 100 (arvon 1), jos se on paras (huonoin) kaikissa mukana olevissa osatekijöissä.

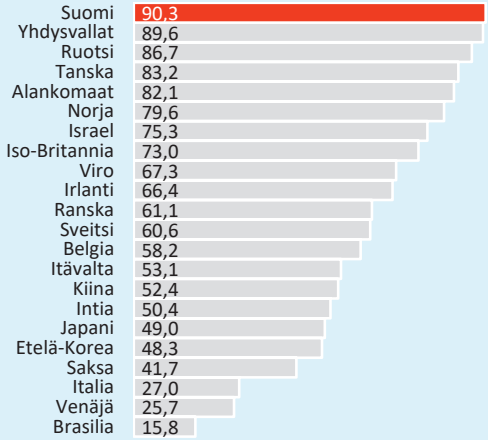


Liitekuvio 54

Digibarometri: Julkisen sektorin edellytykset.

Suomella ovat vertailumaiden parhaat *julkisen sektorin edellytykset* digin hyödyntämiseen ennen Yhdysvaltoja ja Ruotsia. Brasilialla, Venäjällä ja Italialla edellytykset ovat heikoimmat.

Lähde: Indeksin laskentatapa ja rakenne käyvät ilmi liitteen kuvauksesta. Tiedot ovat vuodelta 2019. Maa saa arvon 100 (arvon 1), jos se on paras (huonoin) kaikissa mukana olevissa osatekijöissä.

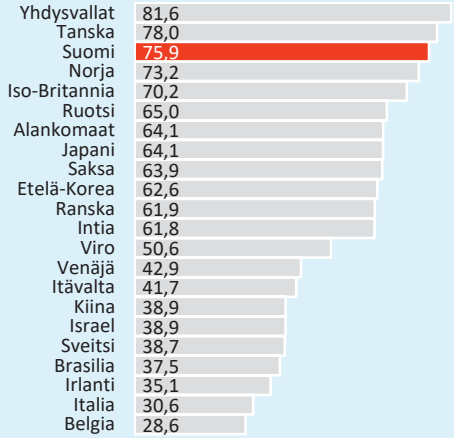


Liitekuvio 55

Digibarometri: Julkisen sektorin käyttö.

Julkisen sektorin käytössä Yhdysvallat on kärjessä ennen Tanskaa, Suomea ja Norjaa.

Lähde: Indeksin laskentatapa ja rakenne käyvät ilmi liitteen kuvauksesta. Tiedot ovat vuodelta 2019. Maa saa arvon 100 (arvon 1), jos se on paras (huonoin) kaikissa mukana olevissa osatekijöissä.

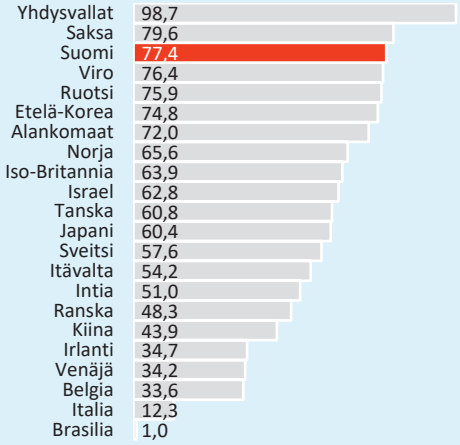


Liitekuvio 56

Digibarometri: Julkiset vaikutukset.

Julkisten vaikutusten indeksissä Yhdysvallat on paras maa ennen Saksaa ja Suomea. Heikoiten menestyvät Brasilia ja Italia.

Lähde: Indeksin laskentatapa ja rakenne käyvät ilmi liitteen kuvauksesta. Tiedot ovat vuodelta 2019. Maa saa arvon 100 (arvon 1), jos se on paras (huonoin) kaikissa mukana olevissa osatekijöissä.



Liite 4: Osaaminen ja osaamisvaje -haun toteutus

Kyberturvaan liittyviä yritysten työpaikkailmoituksia Suomessa kartoitimme hyödyntäen Vainun yritystietokantaa, josta poimimme satunnaisotannalla 100 yritystä mukaan. Satunnaisotantaan mukaan otettuja yrityksiä erottivat toisistaan yrityksen henkilöstön määrä ja yrityksen toimiala. Halusimme eri kokoisia yrityksiä eri toimialoilta, jotta saisimme yleisellä tasolla mahdollisimman kattavan kuvan siitä, millaisia kyberturvaan liittyviä työpaikkailmoituksia Suomessa on tehty.

Tämän lisäksi otimme kartoitukseen mukaan myös suomalaiseen FISC-järjestöön (engl. Finnish Information Security Cluster) kuuluvia jäsenyrityksiä. Kyseinen järjestö toimii Suomessa kyberturvallisuusalan edunvalvojana, joten odotimme löytävämme järjestön jäsenyrityksistä useita kyberturvallisuuteen liittyviä työpaikkailmoituksia (https://www.fisc.fi/organisaatio/).

Kartoituksen toteutimme siten, että päätimme etsiä Oikotie.fi -työpaikkasivustolta mukaan valittujen yritysten avoimia ja päättyneitä työpaikkailmoituksia. Päättyneet työpaikkailmoitukset katsoimme vuoden 2019 alkuun asti. Kartoituksessa kävimme lävitse jokaisen yrityksen alasivun Oikotie.fi, jossa oli koottuna listaan kaikki yrityksen työpaikkailmoitukset työnimikkeen ja ilmoituksen julkaisuajankohdan perusteella. Työpaikkailmoituslistan kohdalla katsottiin ensin työpaikkailmoituksessa ilmoitettu työnimike. Mikäli työnimike oli kyberturvallisuuteen tai sen avainsanoihin viittaava, avattiin kyseisen työpaikkailmoituksen alasivu ja kerättiin sieltä talteen työnimike, työssä työntekijältä toivotut ja vaadittavat ominaisuudet ja ilmoituksen julkaisupäivämäärä. Jos työnimikkeessä ei ollut mitään kyberturvaan viittaavaa tai työpaikkailmoitus oli julkaistu ennen vuotta 2019, emme tarkemmin perehtyneet tähän ilmoitukseen avaamalle sen omaa sivua.

Prosessin nopeuttamiseksi teimme PyCharm-ohjelman, ja sen sisällä olevan Python-kielen, avulla ohjelmoinnit, jotka automatisoivat kartoitusprosessia. Ensimmäisessä vaiheessa halusimme saada selville jokaisen kartoituksessa mukana olevan yrityksen työpaikkailmoitussivun URL-osoitteen Oikotie.fi -sivustolla. Näin pääsimme suoraan kyseisen yrityksen työpaikkailmoitussivulle, ilman että meidän tarvitsi manuaalisesti etsiä yritys Oikotie.fi -sivustolta ja klikkailla moneen otteeseen, jotta pääsisimme

valitun yrityksen työpaikkojen ilmoitussivulle. Nämä URL-tiedot jokaisen yrityksen Oikotie.fi -alasivusta saimme ohjelmoimalla PyCharmin hakemaan Google-hakukoneesta haun ”yrityksen nimi” + ”Oikotie avoimet työpaikat”. PyCharmiin oltiin aluksi syötetty yritysten nimilista, josta PyCharm poimi yksi kerrallaan kyseisen yrityksen nimen ja lisäsi tuon ”Oikotie avoimet työpaikat” yrityksen nimen perään Google-hakua varten. Google-hausta PyCharm poimi hakukoneen ensimmäisen löydön URL-osoitteen ja tallensi sen omaksi riviksi URL-osoitteita varten luodulle uudelle listalle. Näin saimme suurimman osan yritysten suorista Oikotie.fi -työpaikkailmoitussivujen URL-osoitteista. Muutaman kohdalla Google-haku ei onnistunut johtuen joko siitä, ettei ensimmäinen hakutulos ollut Oikotie.fi -sivustolla, tai siitä, ettei yrityksellä ollut omia alasivuja Oikotie.fi -sivustolla.

Kun olimme keränneet URL-osoitteet talteen, teimme PyCharmilla toisen ohjelmoinnin. Tässä ohjelmoinnissa PyCharm kävi lävitse jokaisen yrityksen URL-osoitteen ja tutki kyseisen URL-osoitteen avoimesta HTML-kielestä tunnisteen ”job-title”. Mikäli tämä ”job-title” löytyi, tarkoitti se kyseisen yrityksen Oikotie.fi -alasivulla olevan avoimia tai suljettuja työpaikkailmoituksia. Tämän tunnisteen avulla PyCharm poimi sivulta kaikki työnimikkeet talteen omaan uuteen tiedostoon tallentaen samalla myös kyseisen sivun URL-osoitteen. Näin saimme jokaisen yrityksen kohdalta tietää, millaisia työnimikkeitä niiden työpaikkailmoituksissa on ollut. Mikäli URL-osoitteessa ei ollut tunnistetta ”job-title”, PyCharm tallensi siitä URL-osoitteen ja tyhjän rivin, joka toi ilmi, ettei sivulla ole ollut avoimia tai suljettuja työpaikkailmoituksia.

Tästä listasta kävimme lävitse jokaisen yrityksen työpaikkailmoituksen työnimikkeet. Jos työnimike viittasi kyberturvaan tai siihen liittyviin avainsanoihin, katsottiin kyseinen työpaikkailmoitus Oikotie.fi -sivustolta ja tallennettiin sieltä ylös halutut tiedot.

Digibarometer 2020: Finland in the second place

Executive Summary

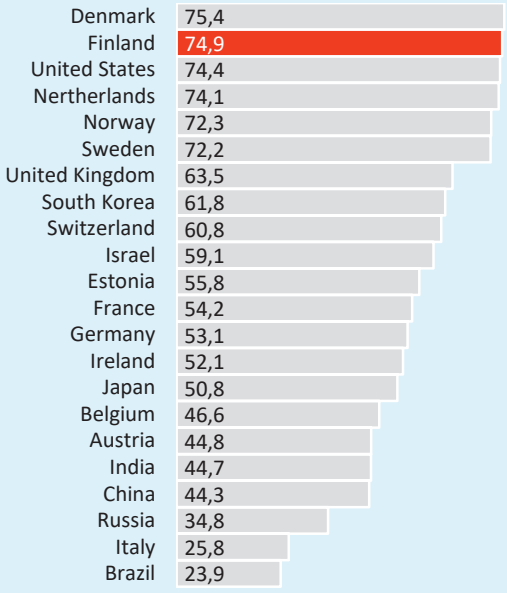
Finland ranks second in Digibarometer 2020, which compares 22 countries with a composite index consisting of 36 variables. The ranking goes up one place from the last year. Denmark rises from its last year's second place to the first place. The United States leaps from the first position to third place. The Netherland remains at fourth, Norway at fifth and Sweden at sixth position. The bottom of the list is once again occupied by Brazil, Italy, and Russia.

Digibarometer is a study which evaluates how well individual countries utilize digitalization and how they compare to one another in this respect. It measures the utilization of digital capabilities. In other words, general fac-

Digibarometer: Overall ranking.

Denmark, Finland and the United States are the best performers in this year's Digibarometer. The bottom of the list is occupied by Brazil, Italy and Russia.

Source: Digibarometer 2020. The study includes 22 countries and 36 variables. A country scores 100(1) if it is the best(worst) in the each nine sub-indices of the barometer.



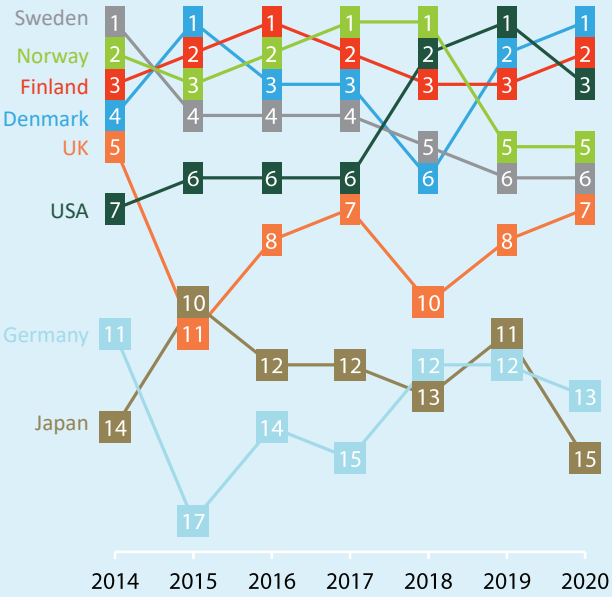
tors such as educational levels or a country's role as a producer of ICT, for example, do not affect the scoring. The measurement is done on three levels (capabilities, utilization, and implications) and across three sectors (company, civic, and public). Each sector is examined on each level, thus forming a scoring matrix of nine cells for each country.

Finland has been among the three best countries in the Digibarometer during the seven years it has been carried out. It has even held the lead once, in 2016. Finland's high placement is explained by its even performance across various indicators. Finland's capabilities to utilize digitalization as well as the actual utilization are the second best in the world. Regarding implications (5th), however, Finland scores lower. Earlier on, the company sector has been Finland's leading digital sector. Now the position of the Finnish companies is slightly waning in the international comparison (7th this year). Simultaneously, the public sector (2nd) maintains its good position, thus assuming the role of the new cornerstone of Finland's placement. In the civic sector, Finland ranks also well and is now in the third place.

Digibarometer: Rankings of the selected countries in 2014–2020.

Finland has been among the top3 countries in each year in the Digibarometer. From 2014 the ranking has been improved the most in the United States and decreased the most in Sweden.

Source: Digibarometers 2014–2020.



Viitteet

[1] tietoturva; tietoturvallisuus; information security; data security; henkilötietosuoja; tietosuoja; privacy protection; confidentiality of personal information; data protection; tietoturvavalvomo; security operations centre; tietoturvaloukkaus; security breach; security violation; identiteetinhallinta; identity management; sähköinen henkilöllisyys; sähköinen identiteetti; digitaalinen identiteetti; sähköinen henkilötunnistetieto; electronic identity; electronic ID; digital identity; digital ID; kyber-; cyber-; kybertoimintaympäristö; kyberympäristö; cyber environment; cyberspace; kyberturvallisuus; cyber security; cybersecurity; kyberpuolustus; cyber defence; tietoverkkovalvonta; verkkovalvonta; network surveillance; tietoturvauhka; data security threat; information security threat; kyberuhka; cyber threat; hakkeri; hacker; hybridivaikuttaminen; informaatiovaikuttaminen; tietoverkkohyökkäys; verkkohyökkäys; kyberhyökkäys; network attack; cyber attack; haittaohjelma; haittakoodi; malicious software; malware; malicious program;

[2] Kyberturvallisuuden sanasto, https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/ (tieto haettu 10.1.2020)

Lähteet

Arute, F., Arya, K., Babbush, R. ym. (2019). Quantum supremacy using a programmable superconducting processor. Nature 574, 505–510. https://doi.org/10.1038/s41586-019-1666-5.

Bamford, J. (2012). The NSA Is Building the Country's Biggest Spy Center. [Verkkouutinen]. Saatavilla: https://www.wired.com/2012/03/ff-nsadatacenter/ [Viitattu 4.6.2020].

Barker, W., Polk, W. & Souppaya, M. (2020). Getting Ready for Post-Quantum Cryptography. NIST Cybersecurity White Paper (Draft), 26.5.2020. Gaithersburg, MD, USA.

Benioff, P. (1980). The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. J Stat Phys 22, 563–591. https://doi.org/10.1007/BF01011339.

Concordia (2020). Participate in the definition of the European Cybersecurity Consultant profile. https://www.concordia-h2020.eu/news/participate-in-the-definition-of-the-european-cybersecurity-consultant-profile/ [Viitattu 25.5.2020].

Korolov, M. & Drinkwater, D. (2019). What is quantum cryptography? It's no silver bullet, but could improve security. https://www.csoonline.com/article/3235970/what-is-quantum-cryptography-it-s-no-silver-bullet-but-could-improve-security.htm [Viitattu 4.6.2020].

McAfee (2018). The Economic Impact of Cybercrime – No Slowing Down https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf [Viitattu 9.6.2020].

Möttönen, M. (2020). Kvantit pannaan töihin. Helsingin Sanomat, 30.3.2015. Saatavilla: https://www.hs.fi/tiede/art-2000002812223.html [Viitattu 8.6.2020].

Statista (2018). Size of the cyber security market worldwide, from 2017 to 2023. https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/ [Viitattu 9.6.2020].

Digibarometri 2020

Business Finlandin, Liikenne- ja viestintäministeriön, Elinkeinoelämän keskusliiton ja Suomen Yrittäjien **Digibarometri** julkaistaan nyt seitsemättä kertaa. Aiempien tilaisuuksien videot ja materiaalit ovat saatavissa osoitteessa

http://www.digibarometri.fi/

Aika: torstai 11.6.2020 klo 10.30–11.30

Osallistuminen: Microsoft Teams -etäyhteyden kautta

Koronakevät on nostanut digitalisaation uuteen arvoon: parhaiten pärjäävät ne yhteiskunnat, jotka osaavat hyödyntää edelläkävijän tavoin digiteknologiaa, -viestintää ja -palveluita. Digibarometri kertoo, mikä on Suomen pärjäämisen taso vuonna 2020. Lisäksi pureudutaan syvällisemmin tämän vuoden erikoisteemaan kyberturvallisuuteen.

Ohjelma

Tilaisuuden avaus
Johtaja Taina Susiluoto, Elinkeinoelämän keskusliitto EK

Suomen digitalisaatio – miten pärjäämme, kuinka kirimme?
Liikenne- ja viestintäministeri Timo Harakka,
Liikenne- ja viestintäministeriö

Digibarometri 2020 tulokset – kuinka Suomi sijoittui ja miksi?
Johtava tutkija Timo Seppälä, Etla

Kommenttipuheenvuorot sektorikohtaisista tuloksista

Kansalaiset:
Asiantuntija Virva Viljanen, Suomen nuorisoalan kattojärjestö Allianssi ry

Julkinen sektori:
Ylijohtaja Anna-Maija Karjalainen, Valtiovarainministeriö

Yritykset:
Smartum Oy:n perustaja ja The Orange Company Oy:n hallituksen puheenjohtaja Jarmo Hyökyvaara

Johtopäätökset

Johtaja Taina Susiluoto, Elinkeinoelämän keskusliitto EK

BUSINESS FINLAND · LIIKENNE- JA VIESTINTÄMINISTERIÖ · Elinkeinoelämän keskusliitto EK · Yrittäjät