Kyberosaaminen Suomessa – Liiketoiminta-analyysi

Suomalaisten tietoturvayritysten osaaminen ja kilpailukyky eSociety-palvelujen alueella

Cyberlab Oy

25.11.2015

Sisällysluettelo

1 Yleistä

Kaikkien palvelujen digitalisoituessa myös yhteiskunnan palvelut ja toiminnot ovat siirtymässä verkkoon. Tuloksena syntyy digitaalinen yhteiskunta eSociety, jossa kaikki mahdolliset yhteiskunnan toiminnot on siirretty digitaaliseen muotoon tietoverkkoihin.

Kun kansalaisten kannalta välttämättömät palvelut ja muu yhteiskunnan kriittinen infrastruktuuri siirtyvät verkkoon, on myös kyberturvallisuuden rooli erittäin tärkeä.

eSociety-palvelut ja niiden tietoturva ovat kehittymässä kaikkialla maailmassa. Kyse on kasvualasta, jossa kilpailukykyisillä yrityksillä on hyvät mahdollisuudet kasvaa markkinoiden mukana tai onnistuneella tuoteportfoliolla myös selkeästi markkinoita nopeammin.

Suomessa on paljon osaamista eSociety-palvelujen ja niiden tietoturvan alueella. Palvelut ovat Suomessa monilta osin kehittyneitä ja alalla on jo useita yrityksiä, joilla on kansainvälistä kilpailukykyä.

Tässä liiketoiminta-analyysissä tarkastellaan Suomessa toimivia tietoturvayrityksiä, joilla on osaamista eSociety-palvelujen kyberturvan alueella. Analyysissä kartoitetaan alan yritykset ja niiden osaaminen sekä arvioidaan kilpailukykyä Suomen markkinoilla ja vientimarkkinoilla.

Erityisesti vientimarkkinoiden osalta pyritään myös löytämään alueita, joilla tarjontaa ei vielä ole, mutta jolle panostamalla suomalaiset yritykset voisivat luoda uusia kilpailukykyistä tuotteita.

1.1 eSociety ja kyberturvallisuus

1.1.1 Tilanne Suomessa ja eSociety toimijat

Miksi Suomi on digitalisoitunut?

Miksi Suomessa on rakennettu yhteiskunnallisesti merkittäviä palveluita digitaalisesti vuosikymmeniä? Miksi Suomessa on kehittyneet eSociety palvelut tarjolla? Onko tämä sattumaa vai onko tämä kehitys ollut suunnitelmallista? Samalla kun yhteiskunnassa rakennetaan sähköisiä palveluita, joudutaan tarkastelemaan näiden palveluiden turvallisuutta sisällön ja palveluympäristöjen osalta. Onko Suomessa ollut riittävä tietoturva osaaminen palvelukehityksen tukena, onko tietoturva kehittynyt palveluiden rinnalla, ennen vai jälkeen?

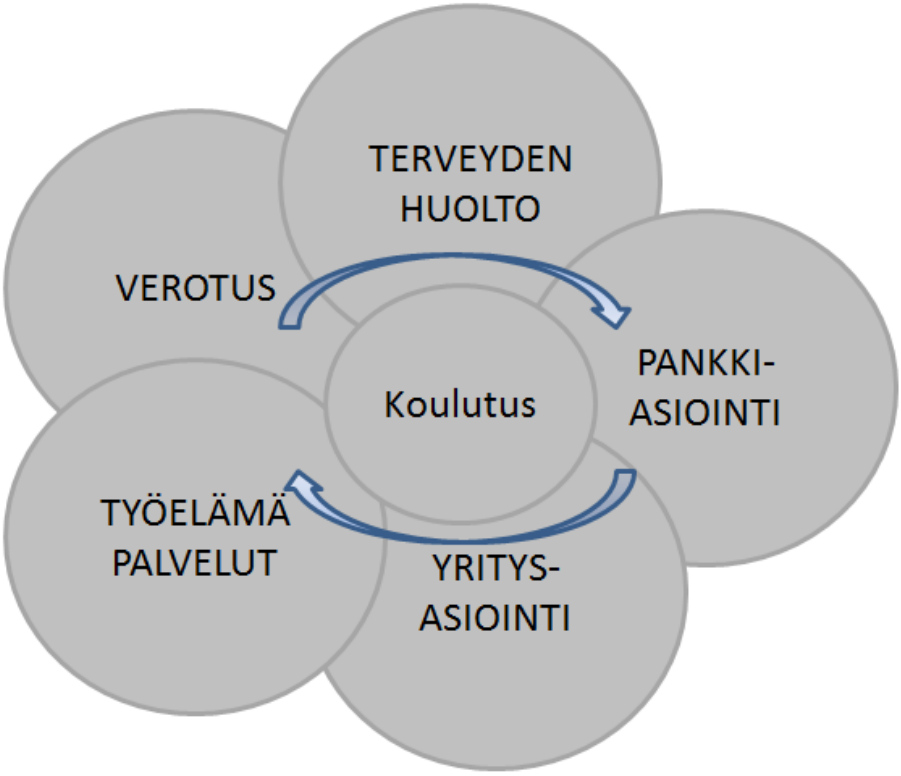
Yhteiskunnallisesti on kuitenkin tosiasia, että Suomesta löytyy paljon eSociety palveluita sekä julkisen kentän että yksityiskentän tuottamina. Suomi on ollut yksi edelläkävijä tällä saralla. Samalla Suomeen on varsin poikkeuksellisesti syntynyt lukuisia tietoturva- ja kyberturva-alan yrityksiä. Euroopassa on hyvin vähän maita joista löytyisi vastaavasti kansallista alkuperää olevia alan yrityksiä väestöpohjaan verrattuna yhtä paljon. Tämä perustuu FISC ry:n tietoturvakartoitukseen vuosina 2013 – 2014, alan puitteissa tehtyihin vierailuihin Euroopan maissa sekä jäsenistön kanssa käytyihin keskusteluihin. Toisaalta pääosa tieto- ja kyberturva-alan yrityksistä Suomessa ovat paikallisia ja pk-yrityksiä.

Muissa maissa, vastaava palvelutuotanto on amerikkalaisten ICT tai Kyberturva-alan tytäryritysten käsissä, ja tuotekehitystoiminta on kyseisen maan rajojen ulkopuolella. Suomalaisen yhteiskunnan kehittyminen on ollut tässä kehityksessä hyvin poikkeavaa. Toisaalta huomattavasti Suomea suuremmat panostukset tieto- ja kyberturva-alaan lukuisissa muissa Euroopan maissa sekä suurempien pääsijoitusmarkkinoiden saatavuus tulevat muuttamaan tätä asetelmaa lähivuosina erityisesti Snowdenin paljastuksista alkaneen boomin myötä.

Suomi on harvaan asuttu maa kuten Norja ja Ruotsi. Tämä on varmasti yksi luonnollinen syy mikä on johtanut palveluiden digitalisoimiseen. Työvoiman kustannusrakenteiden noustessa vuosien saatossa, työvoiman käyttäminen laajasti yhteiskunnan palveluiden tuottamiseen, ei yksinkertaisesti ollut mahdollista laajassa palvelupisteverkostossa. Näissä maissa on laajasti tuotettu digitaalisia palveluita yhteiskunnan toimesta.

Suomessa on myös ollut korkea elintaso ja Suomessa on laaja-alaisesti panostettu koulutukseen. Tämä on asettanut käyttäjien vaatimustason korkealle ja samalla myös yhteiskunnalla on ollut mahdollisuudet palveluiden kehittämiselle. Pohjoismaissa on kehitetty laaja-alaisesti verotuspohjaa, joka on ollut yksi syy digitalisoitumiselle. Laajakantaisen veropohjan perustana ovat olleet hyvät sähköiset rekisterit sekä tiedon keruun automatisointi.

Verotus on yksi tärkeimpiä palveluita, joita yhteiskunnallisesti halutaan kehittää. Ilman toimivaa verotusta ei yhteiskunnalla ole varaa tuottaa palveluita. Toisaalta verotietojen kerääminen ja niiden analysointi on paperisessa maailmassa ollut työlästä ja aikaa vievää, joten tässä on ollut huomattava tehostamisen paikka. Suomessa verottajan palvelupisteistä on karsittu lähes kaikki minimiin. Helsingissä veropalvelupisteitä oli joka kaupunginosassa vielä vuosituhannen alussa, nyt kaikki on keskitetty esimerkiksi pääkaupunkiseudulla yhteen palvelupisteeseen sekä muutamiin sivupalvelupisteisiin. Verottajan itsepalvelut ja sähköiset veroilmoituspalvelut on siirtänyt verkkoon yli 8 000 000 palvelutapahtumaa Suomessa kymmenen vuoden aikana. Samalla säästyy yhteiskunnallisesti rahaa ja kansalaisilta aikaa. Näiden palvelurakenteiden turvallisuus on ollut perusedellytys, että niitä on voitu siirtää verkkoon.



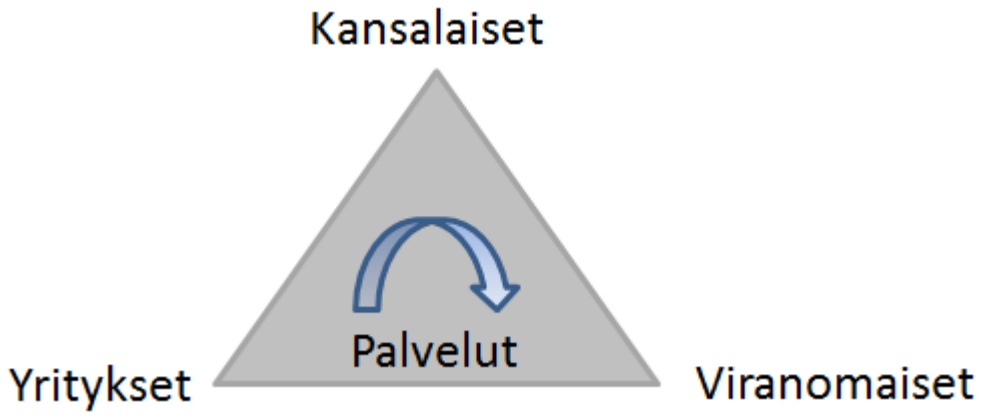
Palvelurakenteiden mallintamiseksi eSociety sektorilla on muitakin kriittisiä toimintoja. Näitä ovat terveydenhuolto, pankkiasiointi, joka toteutetaan pääosin yksityisen sektorin toimesta, yritysasiointi sekä työelämän palvelut. Lisäksi yhteiskunnallisesti koulutus on yksi keskeisimmistä palvelurakenteista. Koulutus edesauttaa palvelurakenteiden hyödyntämistä kattavan käyttöosaamisella. Suomessa digitaalisten palveluiden käyttöosaamisessa ollaan hyvin pitkällä mahdollistaen myös kehittyneempienkin sähköisten palveluiden tarjonnan.

Kaikkia sähköisiä palveluita yhdistää turvallisuus, kaikkien palveluiden on oltava turvallisesti tuotettuja. Jos näissä palveluissa asioidaan, on niihin kyettävä luottamaan.

Suomessa verottaja, työelämän palvelut (työ- ja elinkeinoministeriön) toimesta ovat olleet edelläkävijöitä yhteiskunnallisten digitalisten palveluiden tuottajina. Lisäksi terveydenhuollon ympärillä on ollut paljon palvelukehitystä, joiden onnistumisesta on erityyppisiä arvioita. Kuitenkin terveyden huollon keskiössä on ollut KELA ja etuisuuksien maksaminen, joiden siirto verkkoon on tehty varsin aikaisessa vaiheessa Suomessa.

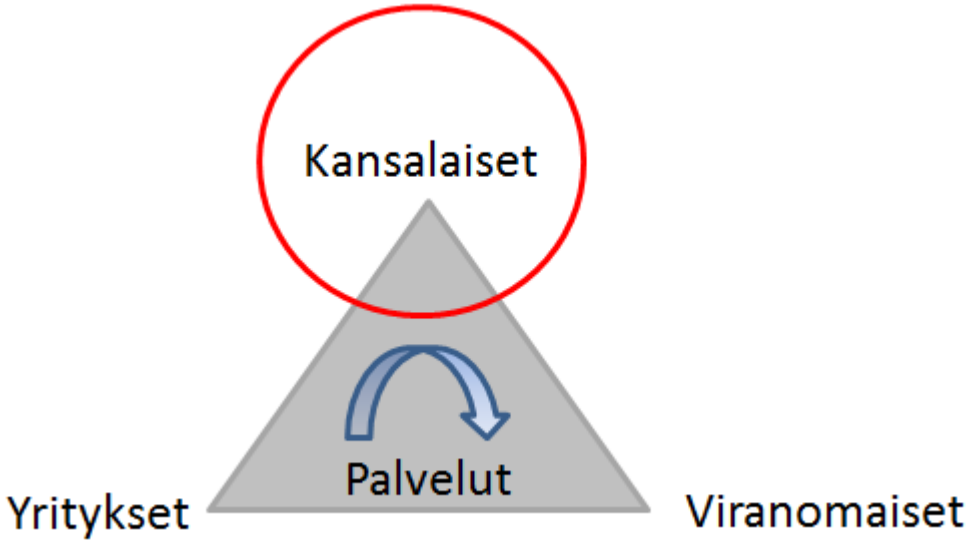
Käyttäjäryhmät

Mitkä asiat ovat eSociety palvelurakenteiden kannalta välttämättömiä peruspilareita palveluiden syntymiselle? Mikäli palveluita on kyettävä käyttämään kaikkialta, eikä vain itsepalveluna palvelua tuottavassa pisteessä, muuttuu palveluiden rakenne olennaisesti. Yhteiskunnallisesti digitaalisten palveluiden rakenne muodostuu aina eri sidosryhmien välille joita ovat kansalaiset, yritykset sekä viranomaiset. Näiden välille syntyy erityyppisiä palveluketjuja.



Näiden osapuolten on kyettävä toimimaan luotettavasti palveluissa. Luottamuksen on synnyttävä osapuolten välille sekä osapuolia yhdistäviin palveluihin. Luottamus syntyy joko asemaan tai toimijan esittämiin lisätietoihin perustuen sähköisessä maailmassa.

Kansalaiset



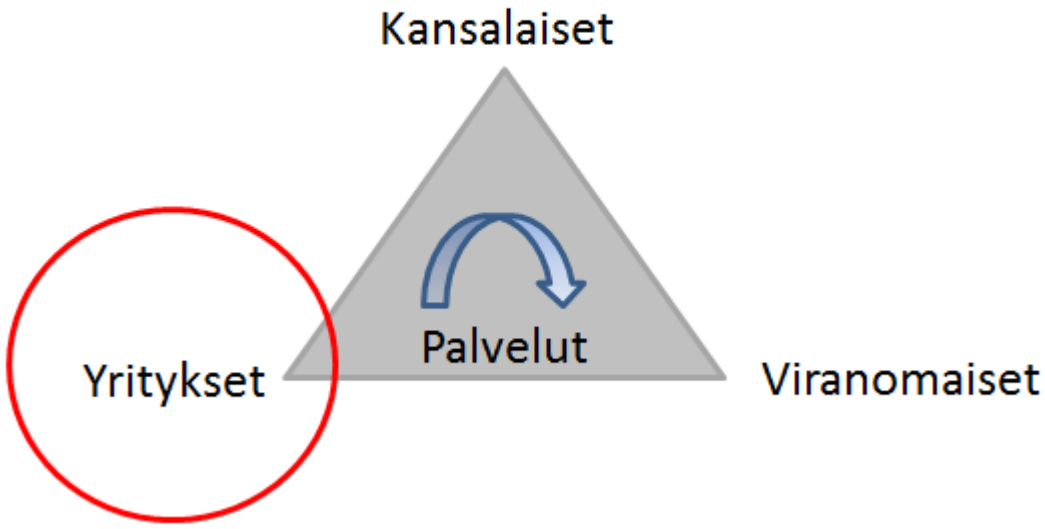
Kansalaisille suunnattavia palveluita on laajasti yhteiskunnissa tarjolla. Useimmissa maissa ei ole juuri sähköisiä palveluita kansalaisille tarjolla vaan ne hoidetaan paikan päällä. Palveluiden muodostumiselle on Suomessa ollut vahva perusta yhteiskunnan rakenteissa. Kansalaisten syntymätodistukset siirrettiin keskitettyyn väestörekisteriin 1969 ja rekisteri siirrettiin tietokoneelle 1971. Samassa yhteydessä luovuttiin työeläkekortin numerosta sekä muista henkilöllisyyteen viittaavista numeroista ja kansallinen sosiaaliturvatunnus tuli kansalaisten avaimeksi. Tämä onkin yksi yhteiskunnan tärkeimmistä numeroista, jolla kyettiin digitaalisessa maailmassa yksilöivästi yhdellä numerolla tunnistamaan ihminen.

Vuosien saatossa tämä yksilöivä numerosarja on ollut merkittävin asia keskitetyn väestötietojärjestelmän kanssa, jolla suomalaiset on voitu linkittää sähköisiin palveluihin. Vastaavan tunnisteen puuttuminen esimerkiksi Englannissa on johtanut

suuriin haasteisiin. Ihmisten ovat todistaneet kansalaisuuttaan tai asuinpaikkaa kaasu- ja sähkölaskuilla ja tämän on hidastanut palveluiden kehittämistä.

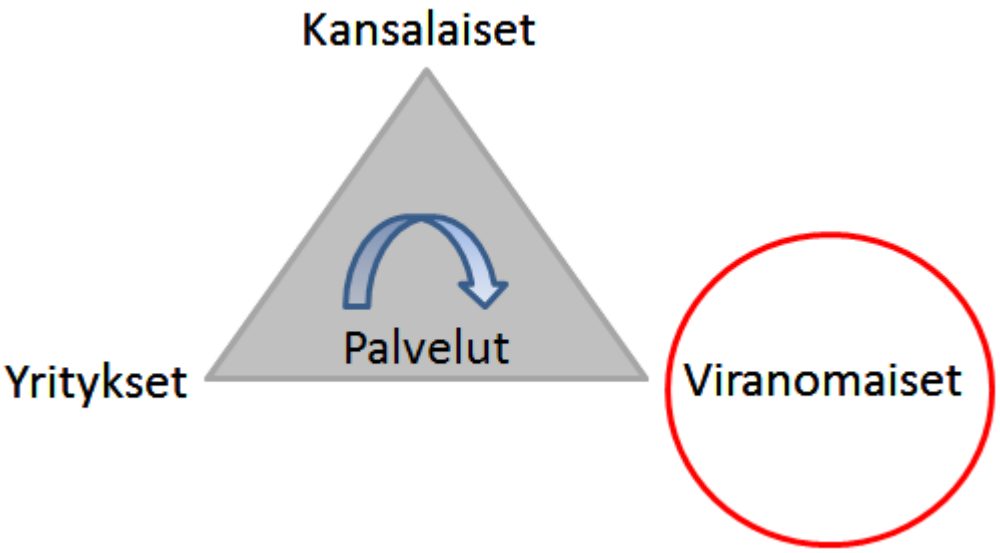
Kansalaisten ympärille on muodostunut palvelurakenteita kuten verotus, kansalliset etuisuudet, terveys sekä työelämään liittyvät palvelut, joiden keskeinen asema on aktivoinut kansalaisia käyttämään yhteiskunnassa tarjolla olevia palveluita myös digitaalisesti. Vaikka palvelut eivät ole kaikilta osin olleet helppokäyttöisiä, on niiden opettelu säästänyt huomattavasti jonotusaikaa ja vaivaa palvelupisteissä.

Yritykset



Yritysten rekisteröinti on toteutettu useissa eri tasoissa. Kunnallisesti Maistraatit huolehtivat osin yritysten ja yhteisöjen rekisteröinnistä. Palvelukehityksen kannalta yritysten rekisteröinti on vaatinut keskittämistä. Suomessa Kaupparekisteri on huolehtinut varsin tehokkaasti yritysten ja yhteisöjen rekisteröinnin 1990-luvulta keskitetysti. Suomessa yritysten rekisteröinti on ollut vuoden 2014 huhtikuusta mahdollista toteuttaa täysin verkossa, ilman fyysisiä dokumentteja tai käyntejä virastoissa. Yritysten rekisterinumerot (Y-tunnukset) ovat mahdollistaneet yritysten yksilöinnin sähköisiin palveluihin ja YTJ-rekisterin avaaminen sähköisesti automatisoidut palvelut.

Viranomaiset



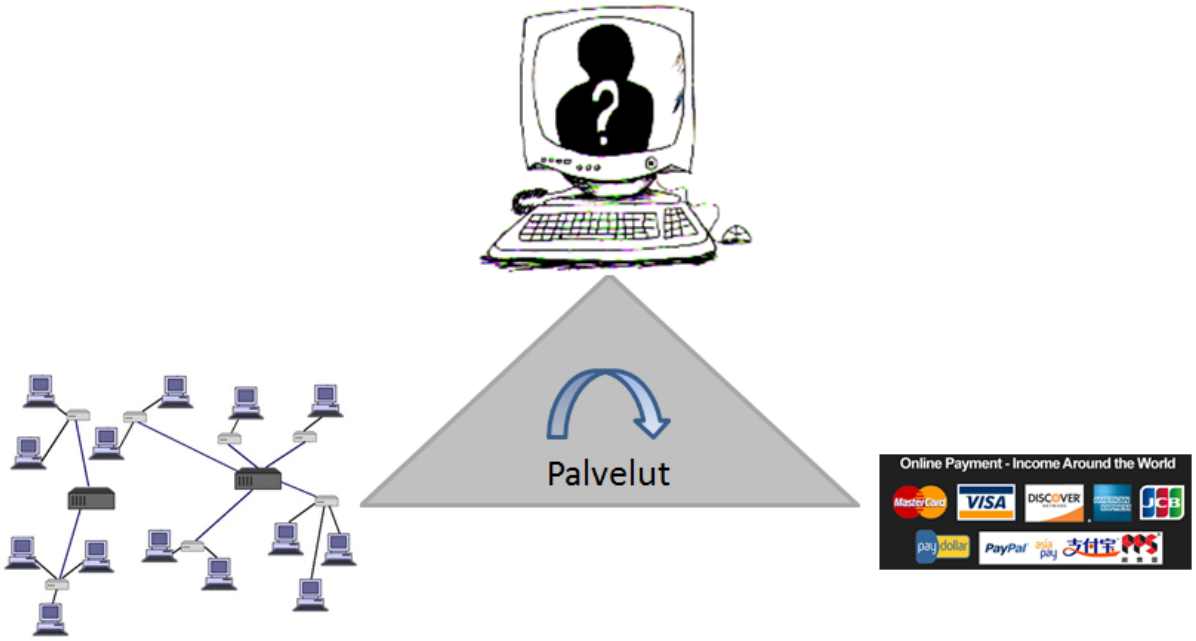
Viranomaiset tuottavat julkiset palvelut muille sidosryhmille ja toisaalta käyttävät muiden viranomaisten tuottamia palveluita. Suomessa perusedellytykset palvelujen tuottamiselle ovat olemassa, mutta muutamia kehityskohteita löytyy.

Palveluiden tuottamiseksi tarvitaan usein joko yhden tai useamman viranomaisen rekistereitä. Nämä rekisterit ovat Suomessa olleet hajallaan, jokaisen viranomaisen itse toteuttamina. Tämä hajanaisuus on vaikeuttanut sähköisten palvelujen toteuttamista. Yhteisen kansallisen palveluväylän odotetaan ratkaisevan tämän ongelman. Palveluväylän toteuttaminen on jo käynnissä.

Roolien rakentaminen niin yritysten kuin viranomaisten aseman toteamiseksi tai asemavaltuuksien hallitsemiseksi on myös yksi palveluiden kehittymisen edellytys. Verottajan Katso-palvelussa on olemassa kattava roolienhallinta, joka on mahdollistanut Suomessa yritysten ja organisaatioiden palvelemisen verkossa. Kansalaisten rooli- ja valtuushallinnan toteuttaminen on käynnissä Rova-hankkeessa.

1.1.2 eSociety:n Peruspilarit

Mitkä ovat eSociety-palvelurakenteiden kannalta välttämättömiä perustoiminnallisuuksia? Osapuolten on kyettävä tunnistautumaan toisilleen, osapuolilla on oltava luotettavat verkkoyhteydet toimintansa turvaamiseksi ja osapuolten on kyettävä maksamaan luotettavasti toisilleen palveluissa. Lisäksi yhteiskunnan merkittävien rekistereiden tiedot on oltava käytössä sähköisesti. Myös kansalaisten, yritysten ja viranomaisten roolien ja asemavaltuuksien tarjoaminen sähköisten palvelujen käyttöön helpottaa huomattavasti palvelujen toteuttamista.



Verkkoyhteydet

Kattavat ja luotettavat verkkoyhteydet ovat kaikkien digitaalisten palvelujen perusedellytys. Suomi on pinta-alaltaan laaja, mutta harvaan asuttu maa. Siitä huolimatta perusinfrastruktuuri, kuten luotettavat sähköverkot ovat lähes kaikkialla saatavilla.

Tietoliikenteen vapauttaminen Suomessa 1990-luvulla käynnisti nopean tietoverkkojen kehityksen Suomessa ja Suomi olikin 2000-luvun alkuun asti edelläkävijä Internet-penetraatiossa ja erityisesti langattomassa viestinnässä. Myös eSociety-palvelut lähtivät Suomessa nopeasti kehittymään kehittyneiden tietoverkkojen ansiosta ja toisaalta laman aiheuttamien kustannussäästöpaineiden ansiosta.

Tällä hetkelläkin verkkoyhteydet ovat Suomessa hyvällä tasolla ja mahdollistavat käytännössä kaikille kansalaisille ja yrityksille luotettavan asioinnin verkossa.

Tunnistaminen

Pankit joutuivat myös kilpailun vapauduttua tehostamaan liiketoimintojaan ja se siirsi vähitellen ihmiset asioimaan verkkopankkeihin. Verkkopankit tarvitsivat turvallisen tavan tunnistaa käyttäjänsä, ja koska suomalaiset pankit olivat edelläkävijöitä verkkopankkien kehittämisessä, ne joutuivat itse luomaan myös tunnistamisen protokollat ja välineet. Tunnistamisstandardiksi Suomessa muodostui kansallinen TUPAS (= Tunnistuspalvelustrandardi). TUPAS-tunnistamisella on Suomessa ylivoimainen markkinaosuus. TUPAS-tunnistuksen leviämistä on myös helpottanut Suomen kattava pankkikonttorien verkosto, jota kautta ensitunnistaminen on saatu hoidettua. Pankit ovat myös ajoissa avanneet tunnistamisrajapinnan muille toimijoille, jolloin TUPAS-tunnistusta käyttäviä palveluja on syntynyt nopeasti. Lisäksi lainsäädäntö, sopimukset ja pankkien ja niiden asiakkaiden välinen luottamus ovat luoneet luotettavan verkkoasioinnin ja tunnistamisen ympäristön.

Valtion puolesta on myös pyritty kehittämään kansalaisten tunnistamisvälineitä. Sähköinen henkilökortti oli edelläkävijä turvallisuuden ja teknologian osalta, mutta ei pystynyt horjuttamaan TUPAS -tunnistuksen asemaa. Sähköinen henkilökortti vaatii erillisen lukijan, jota kansalaiset eivät ole valmiita hankkimaan, koska heillä on jo käytössään toimiva pankkien TUPAS-tunnistus. Sähköisellä henkilökortilla ei myöskään pysty tunnistautumaan pankkipalveluihin, jotka ovat käytetyimmät palvelut verkossa.

Virossa vastaava valtion sähköinen henkilökortti on laajasti käytössä sekä pankkiasioinnissa, että muussa eSociety-palveluissa. Sen leviämisen ovat mahdollistaneet toisaalta se, että markkinoilla ei ollut muita vaihtoehtoja ja toisaalta kattavat sähköisellä henkilökortilla tavoitettavat palvelut mm. pankkipalvelut.

Maksaminen

Luotettavat maksamisen välineet ovat myös eSociety-palvelujen kannalta välttämättömät.

TUPAS-tunnistamisen suosion yksi syy on varmasti sen yhteydessä tarjottava verkkomaksutapa, maksunappi. Maksunappi mahdollistaa asiakkaan kirjautumisen TUPAS-tunnuksilla verkkopankkiin ja tilisiirron tekemisen maksun vastaanottajalle. Lisäksi se välittää maksun vastaanottajalle pankin kuittauksen maksun tekemisestä.

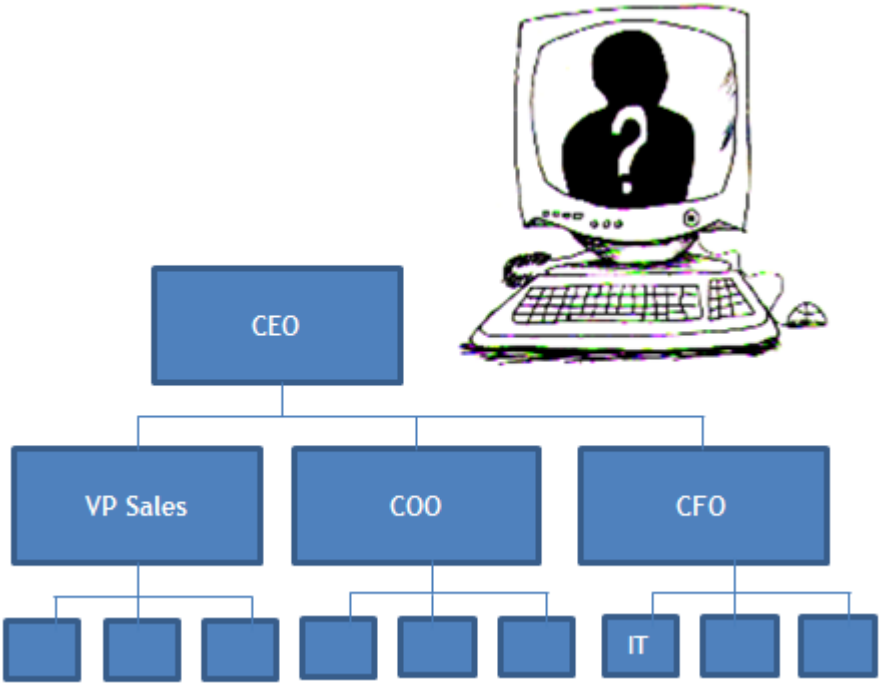
Muita tarjolla olevia maksutapoja ovat eri liikkeellelaskijoiden luotto- ja käteiskortit.

Luottokorttimaksamisen perusinfrastruktuuri syntyi fyysisessä maailmassa samoilla perusrakenteilla, ihmisten siirtyessä käteisestä sähköiseen maksamiseen, oli maksajan kyettävä vahvistamaan maksutapahtuma. Tämä perustui perinteisessä korttimaksamisessa henkilötodistukseen ja allekirjoitukseen, joka korvautui myöhemmin PIN-koodilla. Silti PIN-koodin lisäksi suuremmissa maksutapahtumissa käytetään lisäturvavarmistuksia, joilla maksaja voidaan turvallisemmin liittää maksutapahtumaan ja -välineeseen. Luottamus maksutapoihin ja turvallisuus maksamiseen liittyy vastaavasti maksuvälineen tarjoajaan. Alkuvaiheessa maksuvälineen tarjoajina ovat olleet Suomessa pankit, myöhemmin vaihtoehtoja on syntynyt operaattoreiden ja muiden toimijoiden toimesta.

Yhteiskunnan perusrekisterit

Yksilöivän henkilötunnistamisen taustalla oli kuitenkin kansallinen tapa identifioida kansalaiset, Henkilöturvatunnus. Tämä on ollut avain ihmisiin, jolla voidaan erotella saman nimiset henkilöt toisistaan.

Roolit ja valtuutukset



Toisaalta pankit eivät pystyneet ratkaisemaan toista kansallista haastetta, asiakkaan asemaa yhteiskunnassa.

Perusinfrastruktuurin kehittämiseksi toteutettiin henkilökortti josta eriteltiin myöhemmin roolirakenne, eli viranomaisen asema. Virkamieskortti kuvastaa erityisoikeuksia ammatillisesti kuten lääkärin toimintaoikeuksia, viranomaisen oikeuksia sekä viranomaisen asemaa toimia omassa organisaatiossaan. Vastaavia yleisimmin käyttöön sopivia tunnistusvälineitä ei ole maahan syntynyt. Yrityksien tunnistamisen ja siellä nimettyihin asemavaltuuksiin on olemassa patentti- ja rekisterihallituksen kaupparekisteri, jossa ylläpidetään yritysten ja muiden rekisteröityjen organisaatioiden virallisia nimikirjoittajia sekä luottamusasemia. Tämä on ollutkin haaste jonka yritykset ovat joutuneet itse ratkaisemaan palvelutasolla synnyttäen hyvin erityyppisiä asiakkuuden rekisteröinti ja luomisprosesseja. Samalla on myös rakennettu järjestelmäkokonaisuuksia hallinnoimaan organisaatioiden sisäisiä valtuuksia.

Kokonaisuudessaan Suomi on rakentanut viimeisen kahdenkymmenen vuoden aikana osin sattumalta ja osin järjestelmällisesti yhteiskunnalliset eSociety toiminnalliset pääperuspilarit kuntoon.

1.1.3 Palveluiden elinkaari ja evoluutiotasot

Palveluiden kehittäminen etenee vaiheissa. Palveluiden sähköistäminen tasot mitataan palvelumahdollisuuksilla.

Vietnamissa Ministry of Communication (työpaja 9.4.2015) määritteli yhteiskunnallisten e-palveluiden evoluutioportaat seuraavasti:

1. taso: lomakkeet verkossa
a. manuaalinen lähetys
b. sähköinen lähetys
2. taso: lomakkeet kaksisuuntainen palvelu
a. lomakkeet lähetetään sähköisesti
b. viranomainen vastaa manuaalisesti
c. viranomainen vastaa sähköisesti (esim. email)
3. automaattinen palvelu
a. tiedon järjestelmään suoraan syöttö ja perustietojen tausta käsittely
4. Reaaliaikainen automaattinen palvelu
5. Alueellinen ja keskitetty asiointi toimii dynaamisesti

Tätä Vietnamin valtion soveltamaa arviointitapaa (joka pohjautuu osin Aasian kehityspankin tapaa arvioida yhteiskuntien digitalisoitumista) käytetään myöhemmin tässä selvityksen vertailukaavioissa pisteytykseen, jotta maiden palvelukehitysten tasovertailua voidaan havainnollistaa. Mikäli tarjontaa ei ollut olemassa edes lomakkeiden muodossa, tasoksi määriteltiin nolla.

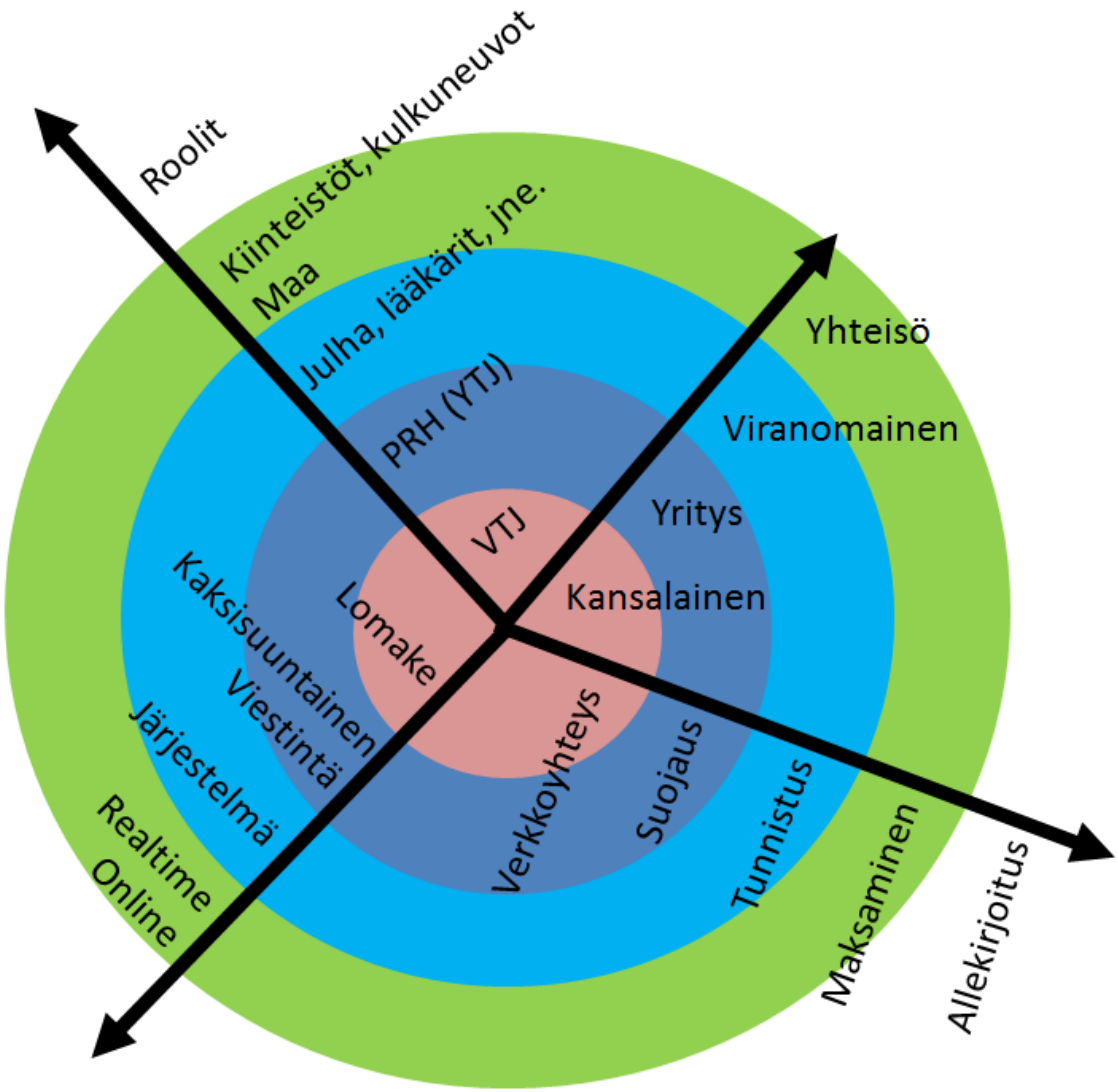
Ensimmäisen tason rakentaminen aloitettiin Suomessa 1990-luvun lopulla. Lomakepalvelut keskitettiin www.suomi.fi – portaaliin, joka helpotti erityyppisten viranomaisasioinnin toteuttamista.

Lomakepalvelut tulivat keskitetysti tarjolla 2000-luvun alkupuolella (2002). Samalla tuli www.julha.fi - rekisteri käyttöön helpottamaan oikeiden viranomaisten yhteystietojen ja aseman löytämistä.

Suomessa osa eSociety palveluista toimii nykyään tasolla iii. Näitä ovat verottajan palvelut, osa TEM:in palveluista, osa terveydenhuollon palveluista, tullin palveluita, auton rekisteröintiin liittyviä palveluita, yritysten perustaminen sekä joitakin kunnallisia palveluita.

Yhteiskunnallisesti eSociety palveluiden tarjonta voidaan kuvata eri ulottuvuuksia. Mitä kauemmaksi keskiöstä siirrytään, sitä pidemmällä ollaan eSociety palveluiden tuottamisessa.

Suomalaiset eSociety palvelut sijoittuvat pääosin lähelle ulkokehää.



Yhteiskunnalliset palvelut asetetaan arvoasteikolle 0 – 5, jossa arvolla 0 ei kehitys ole vielä edennyt ja arvolla 5 ollaan sähköisten yhteiskuntapalveluiden tarjonnassa parhaassa teknisessä kehitystilassa.

REKISTERIT (Suomessa ollaan tasolla 4 luomassa sähköisiä rekistereitä)

1	Rekisterit
5	Yritys- ja organisaatioroolit (mm. Katso keskeneräinen)
4	Maa, Kiinteistö, Kulkuneuvot (AKE)
3	Virkamies, lääkäri, poliisi (Julha)
2	Yritysrekisteri (PRH)
1	Kansalaisrekisteri (VTJ)

Rekistereiden tarjonnassa Viroa pidetään edelläkävijänä, mutta Virossa ollaan osin rekistereiden sähköistämisessä tasolla 3 ja osin tasolla 4.

JÄRJESTELMÄT (Suomessa ollaan tasolla 4 järjestelmäkehityksessä)

2	Järjestelmät
5	Monikanavinen Real Time järjestelmä
4	Järjestelmä johon tiedot syötetään
3	Järjestelmä johon tiedot syötetään
2	Lomake lähetys (kirjeenvaihto)
1	Lomake (web, email, posti)

Järjestelmien kehityksessä Virossa ollaan osin järjestelmien sähköistämisessä tasolla 4 ja osin tasolla 5 jossa xRoad tarjoaa järjestelmien välistä dynaamisuutta.

INFRASTRUKTUURI (Suomessa ollaan tasolla 4 infrastruktuurin kehityksessä)

3	Infrastruktuuri
5	Sähköinen allekirjoitus
4	Sähköinen maksaminen asioinnin yhteydessä
3	Käyttäjän tunnistus (luotettava ja vahva)
2	Verkkoyhteyden suojaaminen - turvallinen yhteys
1	Verkkoyhteys

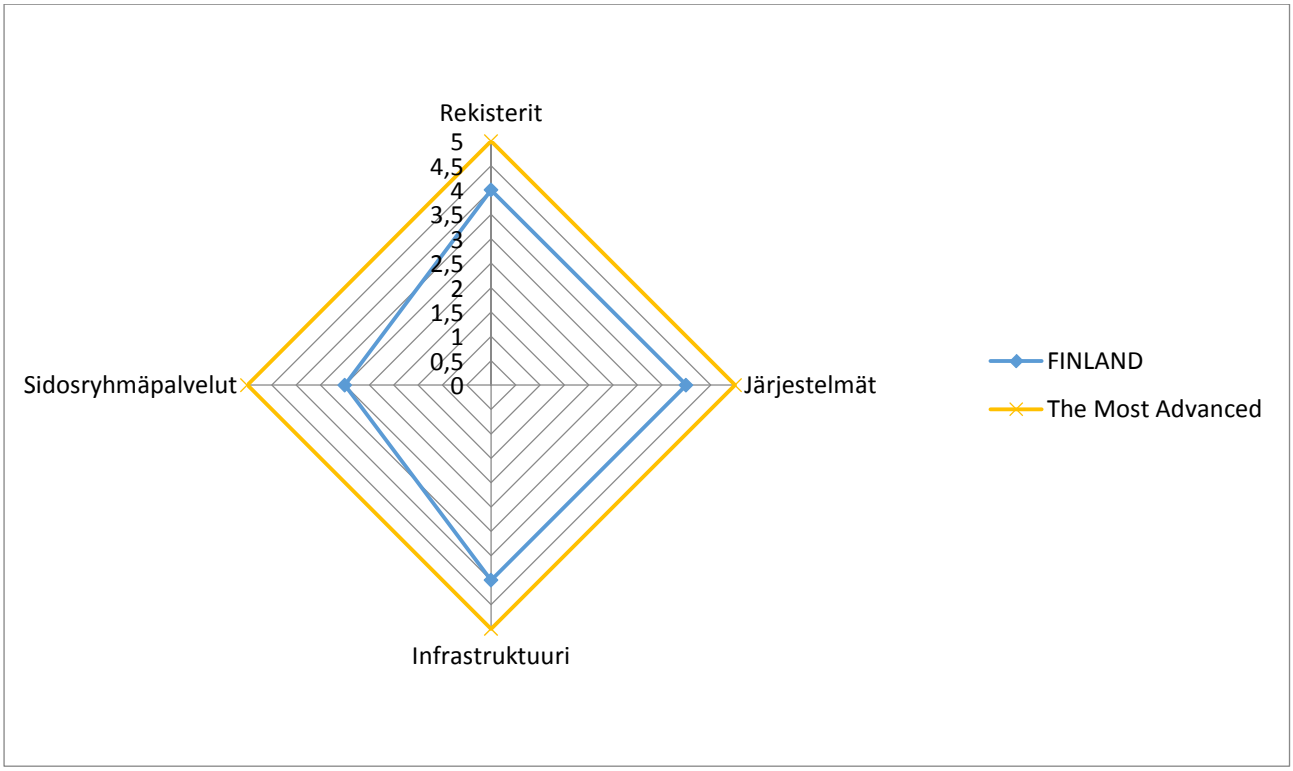
Infrastruktuurissa Virossa on saavutettu taso 5. Toisaalta käyttöaste sähköisessä maksamisessa on huomattavasti Pohjoismaita alemmalla käyttöasteella. Yhteiskunnallisesti ei riitä, että luodaan palvelurakenteet ja järjestelmät vaan yhteiskunnallinen hyöty turvallisuudesta ja digitaalisuudesta saavutetaan vasta kun palveluiden käyttöaste on korkealla lähes 80 prosentissa.

Virossa tunnistamisen kansallinen infrastruktuuri on laajassa käytössä ja samalla teknologialle toteutettu sähköinen allekirjoitus on toimivaa, mutta allekirjoitukselle ei ole juuri todellisia käyttökohteita.

SIDOSRYHMÄPALVELUT (Suomessa ollaan tasolla 3-4 sidosryhmäpalveluiden kehityksessä)

4	Sidosryhmäpalvelut
5	Globaalit organisaatiot
4	Yhteisöt ja muut organisaatiot
3	Viranomainen
2	Yritys
1	Kansalainen

Suomessa osin tarjotaan yhteisölle ja muille organisaatioille palveluita, mutta tarjonta ja käyttöaste ovat matalia. Virossa on tarjolla kansainvälinen e-kansalaisuus, joka mahdollistaa globaalin maan rajojen ylittävän palveluiden hyödyntämismahdollisuuden. Tämä on ainoa 5 tasolle yltävä malli, mutta toisaalta Viro on enemmän pilot-hanke tässä osassa kuin laajasti käytössä oleva kokonaisuus.



1.2 Tietolähteet

- Haastattelut: valitut tietoturvayritykset
- Ohjelmistoyrittäjien toteuttama ja 17.4.2015 julkaisema, ”Tutkimus kansallisesta tietoturvan liiketoimintavaikutuksista Suomessa”
- Yhteenveto keskusteluista kyberturvateknologian viennistä ja kilpailukyvystä (21.4.2015, Teknologiateollisuus ry:n tietotekniikka-alan johtoryhmä jäsenten kanssa)
- EU-Vietnam Business Network (EVBN) by the European Union (2014)
- NBCP, Country Report Philippines (2014)
- Kilpailukykyiset Sähköiset Verkkopalvelut, Ubisecure Solutions Inc. (2013)
- Jukka Kyheröinen omat palaverimuistiot 1.1.2012 – 31.5.2015
- Juha Remes, omat palaverimuistiot 1.1.2012 – 31.5.2015
- Suomen Valtiovarainministeriön, Finland’s performance in international ICT surveys – 13.5.2015, R018).
- ENINSAn tekemän haastattelututkimuksen perusteella (11-20 lokakuuta 2014), http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_fact_fi_fi.pdf)
- Kaakkois-Aasian liiketoimintaselvitysmatka ja siihen liittyvät haastattelut (9.3 – 13,32015)

- RIA, Viron sähköisen asioinnin kehittämistä vastaavien henkilöiden Riho Oks ja Marko Valing kanssa käydyt neuvottelut (14.-15.10.2014 sekä 2.2.2015, Virossa

1.3 Tekijät

Jukka Kyheröinen on prosessien, konsultoinnin sekä myynnin huippuosaaja. Jukka on toiminut erityyppisten sähköisten palveluiden sekä myyntistrategioiden kehittäjänä, valmentajana sekä myyntiorganisaatioiden vetäjänä hyödyntäen monikanavaisia liiketoimintakonsepteja työssään. Jukka on ollut mukana lukuisissa markkinointiselvityksissä sekä toiminut myös tiiviisti viimeiset kymmenen vuotta tietoturvan ja sähköisten palveluiden kehityksen parissa.

Juha Remes on toiminut 80 eri maassa. Juhalla on vankka kokemus teollisuudesta sekä sähköisten liiketoimintojen, maksamisen ja tietoturvallisuuden aloilta. Juha on toiminut laajasti eri yritysten hallituksissa sekä luomassa uusia innovaatioita eri liiketoimintaympäristöissä. Juha toimii tällä hetkellä myös Suomen tietoturvaklusterin toiminnan johtajana ja seuraa näköalapaikalla suomalaisen kyberturvallisuus alan sekä yrittämisen kehitystä.

2 Suomen yritysten palvelutarjoama

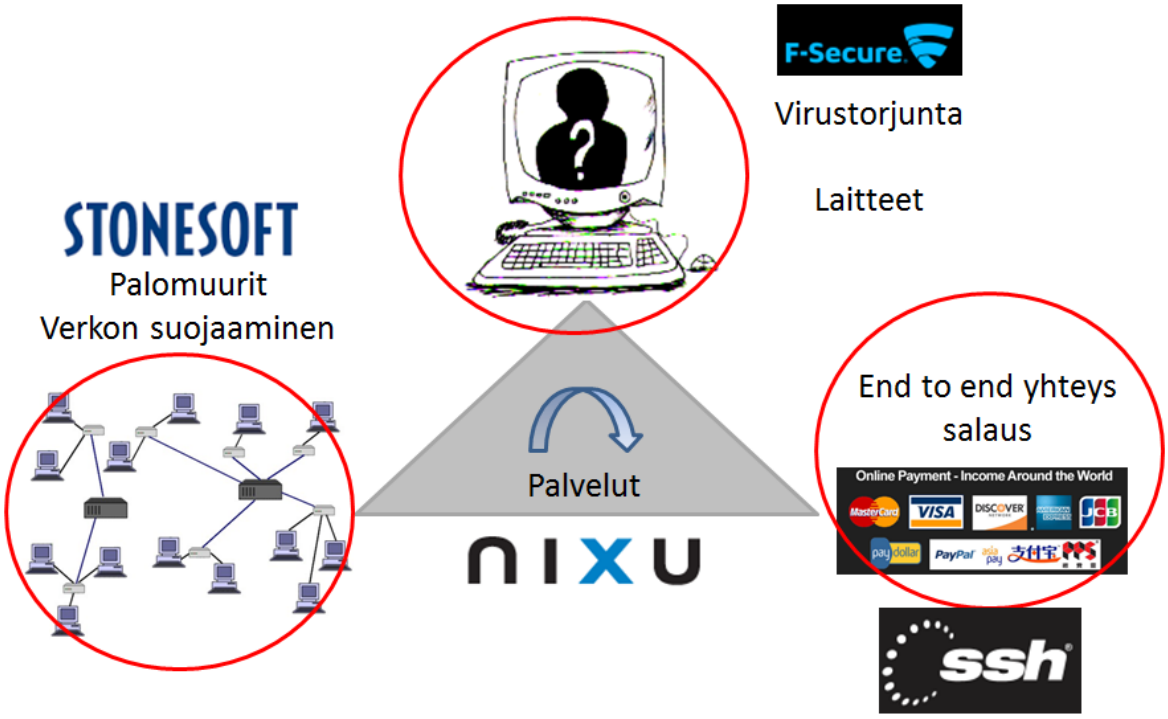
Suomessa on maan kokoon nähden suhteellisen paljon tietoturvayrityksiä osin juuri julkisen kentän kehittyneiden digipalveluiden vuoksi. Useammat tietoturvayritykset, joiden tuotteet sopivat eSociety-palveluihin ovat saaneet hyviä referenssitoteutuksia julkisen sektorin hankkeissa. Muita kybersektoria tukevia tekijöitä Suomessa ovat ainakin korkeatasoinen ohjelmistoalan koulutus, 2000-luvun alun Internethuuma, joka mahdollisti useamman yrityksen listautumisen aikaisessa vaiheessa sekä Nokian vaikutus. Nokiasta aloittaneita spin-off –yrityksiä on tullut melko vähän, mutta Nokia on ollut merkittävä asiakas osalle tietoturvayrityksistä.

1990-luvulla Nokia vastasi huomattavasta osasta kansallisista innovaatioista ja teknologien kehityksestä. Nokialla ei ollut kuitenkaan juuri merkitystä eSociety-palveluiden syntymiselle. Nokian taloudellisten vaikeuksien viime vuosina, osa Nokiassa kokemusta hankkineista osaajista on hakeutunut kyberturva-alalle ja he ovat osaltaan olleet mukana luomassa uusia innovaatioita ja kasvua joissakin kyberturva-alan yrityksissä.

Tässä kappaleessa käydään läpi tietoturvakentän syntyminen Suomessa sekä nykytilanne ja nyt toimivien yritysten palvelutarjoama.

2.1 Tietoturvatarjonnan syntyminen Suomessa

Suomessa on korkea tekninen koulutustaso ja teknologiaa on hyödynnetty varsin laajasti. Tietoturva tarjoaa paljon teknisiä haasteita, joiden ratkaisemiseksi ei ole ollut markkinoilla perinteisesti hyviä ratkaisuja. Aluksi haittaohjelmat levisivät levykkeiden välityksellä, mutta 1990-luvun alussa tietotekniikka alkoi verkkoon siirtymisen nopeasti. F-Securen edeltäjä Data Fellows oli yksi edelläkävijä haittaohjelmien torjunnassa Suomessa ja Euroopassa. Suomen tietoturva muodostui kolme yrityksen ympärille, Stonesoft, SSH Communications sekä F-Secure jotka kaikki edustivat tietoturvan eri osa-alueilta, palomuureja, tietoliikenteen suojaamista sekä virustorjuntaa.



Yhteiskunnallisten palveluiden kehittyminen muodosti markkinat tietoturvan ja myöhemmin kyberturvallisuuden tarpeisiin. Alkuvaiheessa tietoturva oli osana yleistä tietotekniikkaa mutta myöhemmin tämä tiedostettiin erilliseksi segmentiksi. Järjestelmien, teknologioiden, laitteiden ja palveluiden kehittyminen edellytti samalla palveluita, joiden ympärille syntyi tietoturvakonsultointi.

Pääosin tietoturvakonsultointi muodostui testauksesta sekä järjestelmä auditoinneista. Tietoturvakonsultoinnin edelläkävijänä oli Nixu Oy, joka aloitti palvelutarjonnan jo 1990-luvun alkupuolella. Tietoturvapalvelut kehittyivät pääosin maksupääteiden ympärille muodostuneista lukija/kortti turvallisuudesta sekä vastaavasti verkkopalveluiden suojaamisesta ja salaamisesta.

Palvelut perustuivat kysyntään, jossa kysyntä muodostui kansallisen eSocienty-palveluiden kehittymisen mukana rinnakkain. Maksaminen kortilla ja verkossa levisivät nopeasti maan kattaviksi, ja niin verkkopankin käytössä kuin korttimaksamisessa Suomi oli maailman johtava maa lähes vuosikymmenen ajan, ennen kuin muut Pohjoismaat sekä kehittyneet markkinat saivat Suomen kiinni.

Kansallisesti pankkien verkkopalvelut synnyttivät verkkopankkitunnistamisen välttämättömänä toimintona pankkitoiminnan rinnalle.

TUPAS (= Tunnistuspalvelustrandardi) levisi laajasti palveluihin sähköiseksi tunnistustavaksi. Vastaavaa kehitystä oli Norjassa ja Ruotsissa, joissa kummassakin oli olemassa pankkien luoma BankID palvelurakenne sisältäen paikallisen tunnistuspalvelun.

Tunnistaminen ja palveluiden kehitys on jakaantunut pääosin joko pankkien tai valtion toteuttamiksi ratkaisuiksi Pohjois-Euroopassa. Joissakin maissa mobiilitunnistaminen

on levinnyt näiden kahden vaihtoehdon rinnalle tiiviissä yhteistyössä joko pankkien tai valtion kanssa.

Suomessa 1990-luvun lopulla tuotiin markkinoille älykorttipohjaisia eSociety-palveluita. Näissä palveluissa haluttiin hyödyntää uusinta ja turvallisinta teknologiaa. Älykortit ja niihin liittyvät turvalliset sovellukset sisältäen tunnistamissovelluksen levisivät laajasti maailmalla ja tähän teknologiaan satsattiin Suomessa. Älykortti-ratkaisut, kortinlukijat, lukijaohjelmistot loivat laajasti tietoturvaosaamista ympärilleen. Vaikka Suomessa älykorttipohjainen tunnistaminen ei ole neljästä käynnistysyrityksestä huolimatta, ole ottanut menestystä alleen, on sen ympärille muodostunut paljon liiketoimintaa.

Suomen henkilökortti muodosti pohjan Viron henkilökortille sekä Norjan henkilökortille. Ruotsissa mentiin Suomen kanssa rinnakkain ja Ruotsissa älykorttipohjaiset ratkaisut tulivat kansalliseksi tunnistustavaksi pankkeihin, Suomessa ainoana pankkina Osuuspankki kokeili HST-tunnistusta verkkopankkiinsa, mutta noin 500-vuosikäyttäjän määrä ei riittänyt pitämään sitä kaupallisen ratkaisuna.

Palveluiden kehitys ja niiden monimuotoiset tunnistamismallit, turvaprosessit, turvaratkaisut, uudet tuotteet sekä auditointipalvelut lähtivät Suomessa vuosituhanteen vaihteessa leviämään yhteiskunnallisten palveluiden kehittyessä. Suomessa oli vahvoja älykorttien valmistajia Setec, Miotec, Aldata Solutions sekä Tag system jotka kaikki päätyivät myöhemmin yrityskauppojen myötä pois Suomalaisomistuksesta. Näiden ympärille rakennettiin lukuisia palveluita sekä palomuuriratkaisuja. InstaSec loi myös koko CA (Certificate Infrastruktuuri ratkaisun) kilpailemaan globaaleja toimijoita vastaan kuten Baltimore, Hewlett Packard sekä Siemens haastamaan, onnistuen myymään ratkaisuja useisiin pankkeihin eri puolelle maailmaa.

Suomeen muodostui identiteetinhallinta- ja tunnistamisratkaisujen ympärille kymmenen yritystä ja näiden ympärille luotiin palveluita, joita tarjosi parhaimmillaan lähes 20 yritystä. Suomessa yhteiskunnallinen palvelutarjonta kehittyi nopeasti mutta maasta puuttui selkeä koordinaatio. Pankkien, Operaattoreiden ja Valtiohallinnon välillä oli jatkuvasti kansallista kilpailuasetelmista, miten palvelut ja niihin liittyvät turvaratkaisut keskitetään. Pohjoismaissa oli hyvin saman tyyppistä kehitystä palveluissa, mutta Norja ja Ruotsi loivat pankkikeskeisen ekosysteemin, jossa kaikki pohjautui BankID koordinoituun älykortti ja PKI-sertifikaattiratkaisuihin. Ruotsissa markkinat rakennettiin parin ulkomaisen toimijan ja parin Ruotsalaisen toimijan kanssa suljetuksi kokonaisuudeksi. Näin Ruotsissa ei syntynyt laajamittaisemmin kilpailua turvaratkaisujen ympärille. Tämä keskitti kasallisesti alankehittymisen valittujen yritysten käsiin ja rajoitti vapaata kilpailua. Suomessa taas kaikkien toimijoiden ympärille muodostui tarjontaa ja maahan syntyi nopeasti lähes 50 yritystä, jotka tarjosivat tietoturva tuotteita ja palveluita sähköisen asioinnin ympärille. Laajemmin tämän tarjonnan ulkopuolella jäivät jo aiemmin markkina-aseman vakiinnuttaneet toimijat: F-Secure, joka nousi samalla koko Euroopan suurimmaksi tietoturvayritykseksi (keskittyen yksinomaan virustorjuntaan ja haittaohjelmiin), SSH Communication erikoistuen tietoliikenne salaamiseen ja Stonesoft palomuurien kehittämiseen.

2.2 Tarkasteltavat osaamisalueet

Kansallisesti palveluiden kehittäminen edistyy digitaalisuuden askelein eri vaiheissa. Yhteiskunnallisten palveluiden kehittäminen perustuu käyttäjien luotettavaan tunnistamiseen sekä tunnistettujen käyttäjien käyttöoikeuksiin ja valtuuksiin palveluissa.

Tunnistaminen ja Identiteetinhallinta ovat suomalaisten tieto- ja kyberturvaosaamisen vahvoja osa-alueita. Tunnistus ja käyttövaltuuksien hallita mahdollistavat asiointipalveluiden kehittämisen. Palveluissa on tarpeen suorittaa maksaminen sekä vahvistaa tai hyväksyä palvelutapahtumia, joita voidaan toteuttaa eritavoin. Teknologisesti hyväksyminen ja vahvistaminen perustuvat usein sähköiseen allekirjoitukseen.

Näiden ohella suomalaista osaamista on virustorjunnassa, erilaisissa tilannekuvajärjestelmissä, testaamisessa, palomuureissa sekä tieto- ja kyberturvapalveluissa.

Seuraavassa kappaleessa tietoturva-alan yritykset on jaoteltu seuraaviin luokkiin:

- Tietoturvan ja virustorjunnan tuotteet
- Käyttövaltuushallinta ja tunnistaminen
- Palomuurit ja muut innovatiiviset tietoturvapalvelut
- Auditointi ja turvallisuusprosessien kehittäminen
- Sähköinen hyväksyntä ja allekirjoitus
- Maksaminen
- Suomesta vielä puuttuva osaaminen

2.3 Yritysten palvelutarjonta ja kilpailukykyarviot

Suomessa on kyber- ja tietoturva-alaan erikoistuneita yrityksiä noin 80. Yritysten määrä vaihtelee, osa yrityksistä fuusioituu tai tulee ostetuiksi, uusia yrityksiä syntyy kasvavan kysynnän myötä kohtuullisesti. Suomessa on myös syntynyt muutamia alan yrityksiä yliopistojen spin-off ohjelmien kautta, tutkimusohjelmissa. Suurin alan yrityskeskittymä on mukana FISC ry toiminnassa, jonka kautta saadaan suomalainen osaaminen myös profiloitua tarkemmin eriosaamisalueisiin.

Seuraavassa on lueteltu eri kategorioita edustavia tietoturva-alan yrityksiä, niiden palvelu- ja tuotetarjontaa sekä arvioitu niiden kilpailukykyä kansainvälisesti.

2.3.1 Tietoturvan ja virustorjunnan tuotteet

SSH Communication

Yrityksen historia perustuu alun perin 1995 kehitettyyn Secure Shell-protokollaan, joka Open Source jakelulla on levinnyt laajasti maailmalla. Yrityksen kaupalliset tuotteet perustuvat yhteyksien salaamiseen sekä salaamiseen käytettävien avaimien hallintaan. SSH on yksi suomalaisen kyberosaamisen kulmakivistä. SSH:n ratkaisut ovat tiiviisti maksamisessa kortinlukijoiden yhteyksien salaamisessa sekä lukijalaitteiden avainten hallinnassa. SSH tuotteita käytetään myös verkkoyhteyksien salaamiseen yritys- ja

julkisten hallinnon verkoissa ja erityisesti terveyden huollossa jossa potilastietojen eheys ja turvallisuus on oltava aina kunnossa. SSH:n tuotteet ovat myös keskeisessä roolissa pilvipalveluiden yhteyksien salaamisessa. SSH toimii maailman laajuisesti eri markkinoilla ja yrityksen liikevaihdosta tulee vain pieni osa Suomesta.

F-secure

F-secure on Euroopan suurin virus- ja haittaohjelmiin keskittynyt yritys. Yrityksen tausta perustuu yli 25 vuoden taakse vuoteen 1988 jolloin Risto Siilasmaa ja Petri Allas perustivat Data Fellows nimisen yrityksen, joka nopeasti keskittyi antivirus toimintaa, tarjoten virusskanneriohjelmiston nopeasti yleistyville pöytätietokoneille.

F-Securen vahvin osaaminen keskittyy tänä päivänä päätelaitteiden virustorjuntaan. Päätuotteet ovat edelleenkin tietokoneiden virustorjunnassa, jonka rinnalle ovat tulleet mobiililaitteet. Merkittävänä alan yrityksenä F-Securen sisälle on kertynyt paljon tieto- ja kyberturvaosaamista. F-Securen osaajat ovat olleet usein kansallisesti tukemassa kyberkeskuksen sekä eri viranomaisten tarvitessa alan erityisosaamista. Lisäksi F-Secure on ollut luomassa kansallista tutkimus- ja koulutustoimintaa mm. Aalto Yliopiston kanssa. F-Secure on ollut merkittävässä asemassa maan laajan osaamisen kehittymisessä tarjoten lukuisia haasteellisia työpaikkoja alan tekijöille.

F-Secure on myös vahvasti kansainvälistynyt alan yritys ja on selkeästi Suomen näkyvin todiste tieto- ja kyberturva-alan huippuosaamisesta. F-Securen tuotekehitys ja tutkimustoiminta ovat keskittyneet kahteen pisteeseen Suomeen ja Malesiaan.

F-Securella on asiakkaita laajasti maailmalla ja F-Securen tuotemyynti on pääosin kanavoitunut telecom operaattoreiden kautta toteutettuun jakeluverkostoon.

Codenomicon

Yritys on perustettu Oulun yliopistossa ja VTT:llä tehtävän tutkimustyön tuloksena. Yrityksen pääliiketoiminta keskittyy tuotteiden ja järjestelmien haavoittuvuuksien etsimiseen. Yhteiskunnallisesti Codenomiconin ratkaisu on kansallisen HaVaRo järjestelmän ydin. Järjestelmä kerää jatkuvasti tietoa verkossa ja tarjoaa sekä yhteiskunnalle että yrityksille tietoa minkälaisiin uhkatilanteisiin tulisi varautua. Järjestelmä tarjoaa tietoa yhteiskunnalle haavoittuvuuksista mahdollistaen tärkeän osan yhteiskunnallisen tilannekuvan luomisesta. Codenomicon menestyy hyvin maailmalla ja sen tuotteita käytetään laajasti finanssi, telecom, teollisuuden ja julkishallinnon järjestelmissä. Codenomicon siirtyi tämä selvityshankkeen aikana (kesäkuussa 2015) ulkomaaliseen omistukseen, vahvasti kansainväliseen yritykseen Sypsyys, jonka kotipaikka on Yhdysvalloissa, Kaliforniassa; toiminta jatkuu Suomessa toistaiseksi entisellään.

2.3.2 Käyttövaltuushallinta ja tunnistaminen

Tämä sektori tarjoaa laajan tarjonnan kansallisesti. Kansallisesti tällä saralla on seuraavia yrityksiä: Globalsign (osti Ubisecure Solutions Oy:n), Propentus Oy, Digital Identity Solutions Europe (DISE), Effecte Oy (osti RMS Solutions Oy:n), Nixu Oy (osti Panorama Partners Oy:n), KPMG Finland (osti Trusteq Oy:n), Deloitte (osti Secproof Oy:n) sekä Spellpoint Oy. Lisäksi ratkaisuja on myös suurilla integraattoreilla kuten

Fujitsulla, Tiedolla ja CGI:llä. Tarjonta on laajaa sekä palveluiden, ratkaisujen että tuotteiden osalla. Alan toimijoiden ympärillä on ollut paljon yritysjärjestelyjä mikä osoittaa myös alan osaamisen herättäneen laajemmin mielenkiintoa. Tällä saralla toimivat yritykset ovat olleet pääosin kotimarkkinoilla. Tuotetarjonnassa Ubisecure Solutions on mukana laajimmin julkisen hallinnon eSociety järjestelmien käyttäjien tunnistamisessa sekä käyttäjäroolien hallinnassa. Ubisecuren ratkaisut ovat käytössä laajimmin valtion palveluissa joissa tunnistetaan palvelua hyödyntäviä tahoja. Ubisecuren tuotteet ovat mm. Katso-palvelun ja tunnistus.fi palveluiden taustalla. Kansallisesti Fujitsun Vetuma-palvelu on merkittävä kokonaisuus sekä kunta että valtiohallinnon palveluissa. Fujitsu kehittää tunnistus ja siihen liittyvät turvaratkaisut Suomessa. RM5:den tuotteet ovat myös useissa eri järjestelmissä joista laajimmin finanssialalla, erityisesti työeläkeyhtiöiden käytössä. Propentuksen toimitusten painopiste oin kuntapuolen järjestelmien käyttövaltuushallinnossa ja DISEllä on useita sairaanhoitopiirejä jotka käyttävät DISEn ratkaisuja. Panorama Partners, Nixu, Trusteq, Spellpoint ja Secproof ovat pääosin ratkaisujen toteuttajia jotka soveltavat sekä suomalaisia että kansainvälisesti pääosin Amerikkalaisia ratkaisuja (kuten IBM, Novell, Netegrity sekä RSA).

Insta Group Oy

Insta Group on ollut yksi alan pitkäaikaisista toimijoista. Instasec kehitti oman CA (Certficate Authority) tuotekokonaisuuden. Tuote oli hyvin kilpailukykyinen vaihtoehto sertifikaatien hallinnassa ja asiakkaita tuli finanssialalta sekä julkisesta sektorilta kotimaasta ja ulkomailta. Palvelu- ja tuotepaketit olivat varsin laajoja. Markkinatilanne muuttui nopeasti ja CA liiketoiminta kutistui olemattomaksi maailmalla. Tämän rinnalla Insta on kehittänyt turvalliset data-palvelukeskukset joita käyttää mm. Suomen Puolustusvoimat. Insta on ollut hyvin uudistuskykyinen ja pystynyt muokkaamaan omaa kyberturvallisuustarjontaa markkinaehtoisesti. Nyt painopoiste on johtamis- ja tilannekuvajärjestelmissä joilla turvaviranomaiset voivat rakentaa kokonaisvaltaisia tilannekuvavalvomoita. Insta on hyvä esimerkki tietoturva- ja kybermarkkinoiden nopeasti muutoksesta, jossa on oltava ketterä. Installa on myös ainoa suomalainen Viestintäviraston hyväksymä kryptosertifiointi Instan Securelink palomuurituotteelle. Ensimmäinen hyväksyntä on myönnetty tuotteelle vuonna 2012 SH3-tasoisena.

2.3.3 Palomuurit ja muut innovatiiviset tietoturvapalvelut

Intel Security (McFee, Stonesoft)

Stonesoft on ollut yksi suomalaisia tietoturva-alan pioneereja. Yritys on perustettu vuonna 1990. Stonesoft keskittyi palomuuri tuotteiden rakentamiseen. Stonesoft kansainvälistyi laajasti ja Stonesoftin asiakkaita on yli 6500 ympäri maailmaa.

Viimeisin innovaatio keskittyi evaasiotekniikoihin, joka mahdollisti suojautumista myös kehittyneille hyökkäyksille. Stonesoft ostettiin McAfeelle keväällä 2013 yli 300 miljoonan euron kauppasummalla, joka on erittäin vahva osoitus suomalaisesta kyberturvallisuus osaamisesta ja sen tunnustamisesta maailman laajuisesti. Myöhemmin McAfee muutti nimensä Intel Security brändiksi.

SecGo

Palomuuritekniikoiden kehittyessä Instagroup perusti SecGo Groupin. Insta luopui vuosituhannen vaihteessa SecGo:sta jolloin se myytiin pääomasijoittajille, sittemmin toimivalle johdolle. Secgo keskittyi uuden omistuksen myötä vahvemmin liikkuvuuden hallintaan. Ratkaisussa tietoturva oli merkittävässä roolissa. SecGo oli yksi alan edelläkävijöistä Suomessa, ja SecGon tuotteet levisivät varsin laajasti kotimarkkinoilla, mutta ei juuri kansainvälisillä markkinoilla. SecGo Software päätyi keväällä 2007 norjalaiseen Birdstepin omistukseen ja lopulta Elektrobitille takaisin Suomeen.

Jetico

Jeticon liiketoiminta on keskittynyt vahvaan kryptaukseen. Jetico tarjoa ratkaisuja joilla tiedot voidaan salata, hallita ja hävittää tietokoneessa ja päätelaitteessa. Tämä on erittäin keskeinen tieto- ja kyberturvan osaamisalue laitteiden ollessa ihmisten ja työntekijöiden mukana. Jeticon ratkaisut ovat pääosin käytössä maailmalla ja Jeticon päämarkkina-alue on Yhdysvalloissa. Tämä on osoitus siitä, että suomessa kehitetty alan krypto-osaaminen on myös haluttua kyberturvan suurmarkkinoilla.

Ymon

Kyberuhkien lisääntyessä, erityyppiset haavoittuvuustekniikat sekä tilannekuva valvomot ovat yleistyneet. Ymon on yksi suomalainen yritys, joka tarjoaa palvelukeskuksen avulla yrityksille tietoturvavalvontapalveluita. Ymon palvelukeskus sijaitsee Kajaanissa.

Capricode

Capricode edustaa mobiililaitelähtöistä tietoturvateknologiaa. Yhtiön hallintasovelluksilla yritys voi ylläpitää ja hallita kannettavien päätelaitteiden sisältöä sekä huolehtia ettei mobiililaitteisiin asenneta haitallisia tai turvallisuutta altistavia ohjelmistoja.

Envault Corporation

Tarjoaa mielenkiintoisen tavan huolehtia yrityksen tietoturvasta, kun pilviratkaisujen käyttö laajenee maailmalla räjähdysmäisesti. Tiedon taltiointi pilveen alkaa olla yrityksillä standardi tapa toimia. Envault mahdollistaa tiedon suojauksen pilkkomalla sen paloihin ja tallentamalla sen useisiin eri paikkoihin hajautetusti ja salattuna. Tämä poistaa pilvipalvelutarjoojalta mahdollisuuden päästä käsiksi yrityksen luottamuksellisiin tietoihin.

2.3.4 Auditointi ja turvallisuusprosessien kehittäminen

nSense

nSense on Pohjoismaissa toimivat tietoturva-alan palveluyritys. nSensellä on tarjontaa yritysten kyberturvajohtamisesta tietoturvatestaamiseen. Yritys on kansainvälinen Pohjoismaissa ja Balttiassa. Yrityksen omistus on tanskalaisten ja suomalaisten hallussa, ja yrityksellä on toimintaa Tanskassa, Suomessa, Norjassa, Puolassa ja

Ruotsissa. Palvelutarjonta on rakennettu eri maihin tukemaan kokonaisvaltaisesti asiakastoimituksia. Tuotekehitystä on Tanskassa ja Suomessa, yrityksen pääkonttori sijaitsee Tanskassa. Yrityksen kilpailukyky perustuu paikalliseen etabloitumiseen. nSensen osaamisessa yhdistyy laajemmin sekä suomalainen ja tanskalainen osaaminen. nSense on hyvä esimerkki, kuinka palvelua tuottavan tietoturvayrityksen kansainvälistäminen voidaan toteuttaa liittämällä useita eri maissa toimivia alan yrityksiä yhteen. nSense on nykyään osana F-Securea, joka osti koko nSensen osakekannan touko-kesäkuun vaihteessa tänä vuonna (2015).

Nixu

Nixu profiloituu Pohjoismaiden suurimpana kyberturvatalona. Yrityksellä on tarjottavana identiteetin– ja pääsynhallintaratkaisuja, joka on suurin kokonaisuus Nixussa. Nixu on merkittävä tietoturvatarkastusten toteuttaja, joista yhtenä merkittävänä osa-alueena PCI standardien ympärillä olevat ratkaisut. Lisäksi tarjontaa on turvallisesta ohjelmistokehityksestä, riskien ja jatkuvuuden hallinnasta sekä voimakkaasti kasvavana osa-alueena tilannekuva ja verkkoturvallisuus. Nixu listautui First North listalle pörssiin vuoden vaiheessa, ja tämä kuvastaa alan kehitystä. Nixun kansainvälistyminen on ollut varsin pientä ja alueellista tähän saakka. Nyt ostamalla Panorama Partners Oy:n sekä listautumisen tarjoamalla pääomistuksella, Nixulla on mahdollisuuden myös pyrkiä laajemmin kansainvälistymään. Nixulla on hyvin asiantuntijoita, mutta asiantuntijaliiketoiminnan vienti on haastavampaa kuin tuoteyrityksillä. Suomalainen kustannustaso on korkea, mutta toisaalta tietoturva-alan asiantuntijoiden hintataso on huomattavasti korkeammalla maailman laajuisesti pienen tarjonnan takia kuin lukuisilla muilla asiantuntija-aloilla. Tämä mahdollistaa myös Suomessa tuotettujen asiantuntijapalveluiden tarjoamisen kansainvälisesti.

KPMG Finland

KPMG on osana yhtä maailman suurinta tilin-, yritystarkastus ja yritysstrategia konsernia. KPMG on lisännyt strategiseen tarjontaa kansainvälisesti turvallisuus ja kyberturvallisuuspalvelut. Suomessa KPMG kyberturvallisuuspalvelut ovat kasvaneet nopeasti ja Trusteq Oy yritysosto vahvisti KPMG kilpailu asemaa Suomessa merkittävästi. KPMG on esimerkki kansainvälisen yrityksen tavasta etabloitua kansallisille markkinoilla ja samalla KPMG voi hyödyntää omasta verkostosta parasta osaamista sekä tarjota tarvittaessa suomalaisia alan osaajia kansanvälisen verkostonsa avulla maailmalle. KPMG toiminta keskittyy pääosin Suomeen. KPMG on varsin hyvä mittari suomalaisesta osaamisesta. KPMG toimii maassa aktiivisesti hankkimalla alan yrityksiä ja kehittämällä omaa tarjontaa Suomessa sekä tarjoten asiantuntemusta myös verkostoissaan maailmalle. Ala on vahvassa kasvussa ja KPMG panostus alaan kuvastaa kyberturvallisuuden merkitystä markkinoilla.

2.3.5 Sähköinen hyväksyntä ja allekirjoitus

Sähköinen allekirjoitus on yksi merkittävä sähköisen asioinnin kokonaisuus. Sähköisen allekirjoituksen teknologiat ovat pääosin PKI perustuvia ratkaisuja, joissa käytetään kolmea eri toteutustapaa. Toimikorttipohjainen kokonaisuus jossa allekirjoittamine toteutetaan toimikortilla sekä kortinlukijalla on tänä päivänä laajimmin levinnyt tapa toteuttaa sähköinen allekirjoitus. Tätä teknologiaa on kehitetty älykortti valmistajien Miotecin ja Setecin toimesta jo 1990-luvun lopulla. Mitotec ajautui myöhemmin konkurssiin ja Setecin osti Gemalto, joka on maailman suurin älykorttien valmistaja.

Ensimmäisiä suomalaisia sähköiseen allekirjoittamiseen erikoistuneita teknologia yrityksiä olivat Avaintec Oy sekä Fujitsu Finland Oy.

Pohjoismaissa oli laajasti käytössä ”soft certificate” eli ohjelmistollisesti toteutettavat sähköiset allekirjoitusteknologiat. Näitä käytettiin Tanskassa, Norjassa ja Ruotsissa laajasti myös verkkopankeissa. Suomessa tätä teknologiaa on pidetty turvattomana.

Joustavampi tapa sähköiselle allekirjoitukselle on ollut mobile perusteinen MPKI ratkaisu. Suomessa Sonera SmartTrust oli tämän teknologia ensimmäinen toteuttaja maailmassa tullen markkinoille 1999. Soneran rinnalle tuli nopeasti Valimo Wireless (vuonna 2000), joka onnistui lopulta saamaan teknologian kaupalliseen käyttöön useille operaattoreille ja tähän teknologiaan perustuu edelleenkin pääosin Suomalainen MPKI tarjonta. Valimo Wireless päätyi 2008 Setecin tavoin Gemaltolle ja Sonera SmartTrust Gemalton suurimmalle kilpailijalle G & D:lle.

Sähköisen allekirjoitus ei ole saanut Suomessa suosiota vaikka teknologisesti Suomi on tämän alan yksi edelläkävijöistä.

Sähköisestä allekirjoituksesta on tehty palveluita jotka perustuvat pääosin dokumentin allekirjoittamiseen ja taltiointiin. Tähän sektoriin ensimmäiset toimijat olivat Sopima Oy sekä Onnistuu.fi.

2.3.6 Maksaminen

Maksamisen ympärillä on laajasti palvelutarjontaa. Korttimaksaminen on laajimmin levinnyt ja korttipäätteet tulevat ulkomailta. Suomessa tuotettiin Gemalton (osti Setecin) toimesta paljon erityyppisiä älykorttiratkaisuja kuten pankkikortteja sekä SIM-kortteja. Tämän lisäksi Miotec tuotti vastaavia älykortteja sekä TAQ Systems toteutti korttien profilointeja Suomessa. Tällä hetkellä korttituotantoa ei Suomessa ole muutoin kuin älypassien osalta. Kortti ratkaisujen ympärillä on laajasti PCI auditointi ja integrointi tarjontaa. Huomattavia toimijoita ovat KPMG, Nixu, sekä nSense. Osaamista löytyy myös suurista integraattoreista mutta pääosin palveluiden tarjonta keskittyy mainituille kolmelle toimijalle. Lisäksi alalla on pienempiä ohjelmistoalan yrityksiä esimerkkeinä Solinor ja Poplatek, jotka tarjoavat maksuratkaisuihin ja maksupäätteisiin ohjelmistokehitystä. Maksupäätteitä on ollut Suomessa myös tarjolla mutta kuten lukuisat muutkin ratkaisut, yritykset ovat päätyneet ulkomaisen omistukseen. Markkinoilla toimii 2000-luvun alkupuolella kolme maksupäätevalmistajaa, joilla oli yli 90% markkinaosuus ja niistä kaksi oli suomalaisia: Verifone (joka osti Pointin) sekä

Sagem (joka osti Manison Oy:n). Maksamisen ympärillä on ollut lukuisia innovatiivisia yrityksiä, joista Modirum Oy sovelsi 3D Secure-mallilla ensimmäisenä maailmassa verkkomaksamisessa. Pankit olivat edellä kävijöitä pienmaksamisessa tuomalla markkinoille Radiolinjan, Nordea ja Sampo Pankki yhteisen maksuratkaisun, Mobiilirahan ja Osuuspankkin tarjoaman Digirahan. Näiden lähimaksuratkaisujen tarve osoittautui Suomessa turhaksi, kun korttimaksujen käyttö oli jo ehtinyt levintä kaikkialle ja korttimaksuista perittävä maksuprovisio oli pudonnut 1-2% tasolle kauppahionnasta ja minimi maksuraja poistui korttimaksamisesta kokonaan. Kansallisesti matkakortti julkisessa liikenteessä sekä SMS-maksaminen (Plusdial Oyn) luova tapa tarjota SMS-lippua ovat esimerkkejä eSociety palveluiden kehityksestä maksamisen ympärillä Suomessa. Useimmat näistä ratkaisuista jäivät kansallisiksi tai niiden kansainvälistyminen levisi ainoastaan marginaalisesti ulkomaisille markkinoille (kuten Plusdial sai ratkaisunsa myös käyttöön Tukholmaan Helsingin pääkaupunkiseudun lisäksi). Maksutapojen määrä on Suomessa huomattava, jokaisella pankilla on oma verkkomaksamiseen soveltuva painike ja korttiyhtiöille omat ratkaisut. Näiden useiden maksutapojen liittämiseksi on syntynyt HUBeja, joista Fujitsun Vetuma-pavelu tarjoaa keskitetyn maksupalvelu julkisille toimijoille ja yksityisille kauppiaille on tarjolla lukuisia eri ratakisuja: Nets (osti Luottokunnan sekä Paytrailin (aiemmin Suomen Verkkomaksut Oy), Suomen Maksuturva Oy, Vilkas Oy sekä Suomen Maksukaista Oy. Nämä kaikki tarjoavat yhden luukun periaatteella maksamisen välityspalvelua.

Maksamisen ympärillä on kehitetty myös sähköistä laskuttamista, jossa Basware on kansainvälistynyt yhdeksi alan markkinajohtajiksi maailmalla. Sähköinen laskuttaminen ja Fininvoice-ratkaisu on levinnyt julkisen hallinnon perusmaksuratkaisuksi, joka on käytännössä ainoa tapa laskuttaa julkista sektoria. Sähköisen laskutuksen ympärillä on tapahtunut lukuisia innovaatioita ja yritysostoja. Norjalainen Visa on hankkinut laajasti yrityksiä sähköisen laskuttamisen ympärillä. Kansallisesti Basware rinnalla on Suomen posti, joka osti ensin Elma oy:n, joka oli ensimmäisiä sähköisiä laskutusoperaattoreita Suomessa ja myöhemmin OpusCapitan laajemman tarjonnan aikaansaamiseksi.

Koko maksamisen ympärille Suomessa on syntynyt huomattavasti kilpailukykyisiä yrityksiä ja innovaatioita, joissa kaikessa on ollut myös mukana turvallisuus. Tarjonta on keskittynyt nopeasti muuttuvan ja digitaalistuvan yhteiskunnan ympärille mutta muutamaa poikkeusta lukuun ottamatta yritykset eivät ole kyenneet kansainvälistymään itsenäisesti.

2.3.7 Suomesta vielä puuttuva osaaminen

Suomi on kyberuhkien osalta varsin rauhallinen maa. Suomeen kohdistuu huomattavasti vähemmän hyökkäyksiä kuin maailmassa keskimäärin. Suomalaiset yritykset eivät saa kotimarkkinoilla yhtä suuria kyberhaasteita ratkottaviksi kuin vastaavat yritykset esimerkiksi Etelä-Euroopassa. Suomessa ei myöskään panosteta samassa mittakaavassa sotilaallisiin resursseihin kuin alan kärkimaissa.

Kybervarustelu on kilpajuoksua rikollisuutta vastaan mutta jatkuvasti laajemmin myös maiden välistä kilpavarustelua. Suomessa on oltu edelläkävijöitä kansallisessa kyberstrategian luomisessa, mutta toteuttaminen on jäänyt toteutumatta, hyvin suunniteltu – muttei lainkaan toteutettu.

Kansallisesti maan kyberkoordinaatio on hyvin hajallaan. Tämä aiheuttaa lukusia haasteita maan toiminnassa. Julkisella sektorilla on tällä saralla paljon päällekkäisyyksiä ja toisaalta hyvin vähän resursseja. Private-Public-Partnership-kehitys on myös ollut hidasta, eikä se ole tuonut kansallisesti toivottua kilpailukykyä alan yrityksille.

Kansallisesti Suomessa yritykset ja yhteiskunta eivät panosta kyberturvallisuuteen riittävästi ja panostukset jäävät jälkeen kansainvälisistä keskiarvoista. Tämä tulee näkymään yhteiskunnallisesti heikompana suorituskykynä ja alan yritysten on toimittava globaalisti, jotta alan yritysten kilpailukyky säilyisi.

Suomi on pieni yhteiskunta jossa raja-aidat viranomaisten ja yksityisen sektorin välillä ovat matalia, mutta tästä huolimatta kyberosaamisen yhteistyössä ei näitä pienen maan hyötyjä ole pystytty tehokkaasti käyttämään. Lisäksi Suomessa on alan yrityksissä pulaa osaajista. Alalle valmistuu liian vähän osaajia yliopistoista, ja alan koulutus on hajallaan eri yliopistoissa.

Suomessa tieto- ja kyberturvan parissa työskentelee täysipäiväisesti noin 1 500 alan yrityksissä ja lähes saman verran muissa yrityksissä, julkisella sektorilla sekä oppilaitoksissa. Tämän lisäksi noin 2000 henkeä toimii tietoturva- ja kyberturvan alan tehtävissä osana omaa työkuvaa (perustuu FISC ry:n tekemiin arvioihin vuodelta 2014). Tietoturva-alan liikevaihto Suomessa oli noin 350 miljoonaa euroa vuonna 2014.

Suomessa ei ole merkittävästi APT hyökkäyksiä (= advanced persistent threat, edistynyt, pitkäkestoinen hyökkäys). Tämä rajoittaa alan yritysten sekä tutkimuslaitoksien mahdollisuuksia tutkia sekä selvittää näihin liittyviä tekniikoita, tapoja sekä ilmiöitä. APT sekä muuten selkeät Social Engineering-tyyppiset kyberrikokset ovat Suomessa harvinaisia, joten myös tähän kokonaisuuteen liittyvän osaamisen kehittämiseen tarvitaan enemmän kansainvälisiä asiakkaita.

3 Kilpailukyky kotimaisilla markkinoilla

Tässä osa-alueessa tarkastellaan suomalaisten yritysten kilpailukykyä Suomen markkinoilla. Tarkastelussa ovat kappaleessa 2.2 löydetyt osaamisalueet. Suomessa käynnissä olevat hankkeet käydään läpi ja tarkastellaan suomalaisten yritysten osuutta hankkeissa. Lisäksi arvioidaan yritysten mahdollisuuksia mahdollisissa tulevissa hankkeissa.

Tarkempaan tarkasteluun on valittu 16 alan yhtiötä ja intressiryhmää, joille on tehty kysely niiden itse näkemästä kilpailukyvystä Suomessa ja kansainvälisesti.

3.1 Kyberturva-alan kilpailukyvykkyydestä yleensä

Suomalainen kyberturva-alan tarjonta on varsin monipuolista. Alan innovaatiot ovat olleet varsin edistyksellisiä mutta vuoden 2013 kesäkuun Edward Snowden paljastusten jälkeen maailmalla on alettu panostamaan valtavasti kyberturvallisuuteen. Yhdysvalloissa alan investoinnit ovat olleet vuoden 2014 loppuun saakka noin 11 miljardin dollarin tasolla, mutta Barack Obama ehdotti alalle 14 miljardin dollarin lisäbudjettia vuodelle 2015. Tämä kuvastaa todellisuutta, ettei Yhdysvallat pysy kehityksen vauhdissa turvatakseen kansalliset intressit ellei kansallisesti lähes kaksinkertaisteta kyberturvaan liittyviä investointeja (http://www.reuters.com/article/2015/02/02/us-usa-budget-cybersecurity-idUSKBN0L61WQ20150202). Huomattavia panostuksia kyberalalle on toteutettu lukuisissa eri maissa, kuten Englannissa (600 hengen palkkaaminen kansalliseen kyberyksikköön), Intia (palkkaa yli 200 000 kybersotilasta), Kiinassa oli jo ennen Snowdenin paljastuksia yli 200 sotilaallista kyberyksikkö käsittäen jopa 100 000 kybersotilasta.

Suomi oli kansallisella kyberstrategiallaan edelläkävijä vielä vuonna 2012, mutta nyt Euroopassa on lukuisissa maissa tehty valtavia panostuksia alalle. Hollanti pyrkii yhdeksi johtavaksi maaksi painottuen myös siviilipuolen tarjontaan. Hollannissa on perustettu kymmenien miljoonien euron hanke, Haagin Security hub (https://www.thehaguesecuritydelta.com/), joka pyrkii saamaan alan yritysten keskittymän Hollantiin sekä toimimaan kansainvälisenä hub-keskittymänä kansainvälisten hankkeiden ja yritysten välillä.

Suomessa perustettiin vuonna 2012 Finnish Information Security Cluster (FISC), joka on alan yritysten yhteistyökoordinaattori. Tässä on kuitenkin periaatteena yritysten vapaaehtoinen panostaminen yhteistyöhön eikä organisaatio saa vastaavia resursseja käyttöönsä kuin muissa maissa. Tämän lisäksi Suomeen on rakennettu kansallinen kyberkeskus johon keskitetyt investoinnit ovat kansainvälisesti vertailtuna pieniä. Näiden rakenteiden rinnalla toimii Tekesin INKA ohjelma, jossa on erillinen Kyberohjelma, koordinoituna Jyväskylästä käsin. Hanke tarjoaa myös mahdollisuuksia alan kehittymiselle, mutta ohjelma ei ole kyennyt vielä laajentumaan maanlaajuiseksi.

Suomalainen kilpailukyky kybersektorilla tarjoaa jatkossa mahdollisuuksia suomalaisille yrityksille laajemmin mutta kyberturvaratkaisuiden integroiminen yleiseen ICT tarjontaan sekä teolliseen internetiin olisi tehtävä onnistuneesti. Nyt kyberalan pienet

toimijat eivät ole riittävän kilpailukykyisiä kansainvälistymään. Vuoden 2012 jälkeen useat lupaavat alan yritykset on myös myyty ulkomaille. Stonesoft (Intellille), Blancco (Regenerikselle), Secproof (Deloitelle), Ubisecure Solutions (Globalsignille), Trusteq (KPMG:lle) sekä Codenomicon (Synapsille). Lisäksi alalla on tapahtunut konsolidoitumista, Nixu listautui pörssiin ja osti Panorama Partnersin, F-Secure osti nSensen sekä Efecte osti RM5 Softwaren. Yritysostot sekä alan organisoituminen todistaa kansallisten yritysten olleen kilpailukykyisiä.

Alan suomalaisen kilpailukyvyn kannalta on tärkeää saada alalle pääomia, joiden avulla saadaan luotua suurempia ja kansainvälistymiseen kyvykkäämpiä yrityksiä. Suomessa olisi hyvä saada kyberturvallisuuden alalle keskittymistä. Maailmalla käytetään valtavia pääomia kyberturvateknologioiden kehittämiseen ja Suomi ei pysty vastaamaan tähän kilpailuun. Public-Private-yhteistyö on myös täynnä haasteita ja sen varaan liiallinen painostaminen alalla Suomessa voi johtaa lopulta yritysten keskittymisen vääriin hankkeisiin jotka eivät saa merkittävässä mittakaavassa yritysten menestystä aikaan. Toisaalta ilman PPP-yhteistyötä ja kansallisia huomattavia yhteiskunnallisia panostuksia, on kyberalalla kasvattaminen myös vaikeaa. Vastaaviin hankkeisiin panostetaan maailmalla paljon. Jotta yritysten menestymismahdollisuudet olisivat olemassa, yritysten kesken on perusteltua tehdä yhteistyötä erityisesti kansainvälistymisessä ja yhteistyön painopiste tulisi olla pyrkimyksissä mahdollisimman suoraviivaiseen kauppaan ja kv-liikevaihtoon.

Ohjelmistoyrittäjät ry toteutti laajan 12000 tarjoustilannetta sekä 112 yritystä käsittävän haastattelututkimuksen, jossa kartoitettiin tietoturvan merkitystä ohjelmistotuotteiden valinnassa. Lisäksi tutkimuksessa verrattiin kotimaisen ja ulkomaisen markkinoiden käyttäytymistä ohjelmistotuotteita valittaessa. Hämmentävää on, että tietoturva ja tietosuoja loistavat poissaolollaan vielä liian monessa suomalaisten yritysten ja julkishallinnon tarjouspyynnöissä ja myyntineuvotteluissa. Sitä ei aina vaadita, eikä siitä olla valmiita maksamaan. Kotimaisista suuryrityksistä peräti 79 % kysyi tarjoavalta ohjelmistoyritykseltä erikseen tietoturvan tai tietosuojan tasosta. Kotimaisen julkishallinnon vastaava luku oli 70 % ja kotimaiset pk-yritysten vain 60 %. Erikseen kysyttäessä tietoturvasta olivat valmiita maksamaan vain 45 % suuryrityksistä, 40 % julkishallinnon ostajista ja 33 % pk-yrityksistä.

Suomalaisostajat ovat suhteellisen valveutuneita ja olettavat tietoturvan olevan kunnossa ja kuuluvan tuotteen tai palvelun perushintaan, toisaalta suomalaiset asiakkaat eivät olleet valmiita maksamaan tietoturvasta lisää, mutta ulkomaiset ostajat olivat vastaavasti valmiita maksamaan tietoturvasta lisää. Kansainvälisillä markkinoilla ovat tietoturvamarkkinat kasvavat laajemmin kuin Suomessa, ja tämä on myös uhkana alan kasvulle mikäli kyberturvayritykset toimivat vain kotimaisilla markkinoilla.

Suomalaisen ala painottuu pieniin yrityksiin ja yritykset edustavat kilpailukykyisiä ratkaisuja, mutta yritysten mahdollisuudet kansainvälistyä ovat rajalliset ja tutkimuksen tulos tukee myös sitä näkemystä, että investointihalukkuus tietoturvaan on pieni ja sen oletetaan olevan kunnossa. Tämä rajoittaa alan yritysten kasvua kansallisen kysynnän ollessa suhteellisesti pienempää kuin ulkomailla. Tutkimuksen perusteella alan yritysten tulee kyetä paremmin perustelemaan investoinnit tietoturvaan sekä tietoturvapalveluihin kotimarkkinoilla sekä pyrkiä aktiivisemmin kansainvälisille

markkinoille alan kilpailukyvyn ylläpitämiseksi. Kansainvälisillä markkinoilla kasvu on selvästi merkittävämpää kuin Suomessa. Kyberturva-alan kasvun arvioidaan kansainvälisesti olevan yli 15% vuodessa kun Suomessa kasvu jää noin 5% tasolle (FISC ry:n tekemä markkina-analyysi elokuu, 2014).

ENISAn tekemän haastattelututkimuksen perusteella (11-20 lokakuuta 2014) suomalaisen valistuneisuus on verkossa ollut keskimäärin korkeammalla kuin muualla Euroopassa. Suomalaiset käyttävät laajemmin keinoja tietojen turvaamiseen, mutta toisaalta suomalaisen käyttäjän itseluottamus omaan turvallisuuteen verkossa on vastaavasti korkeammalla kuin keskimäärin EUssa (http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_fact_fi_fi.pdf).

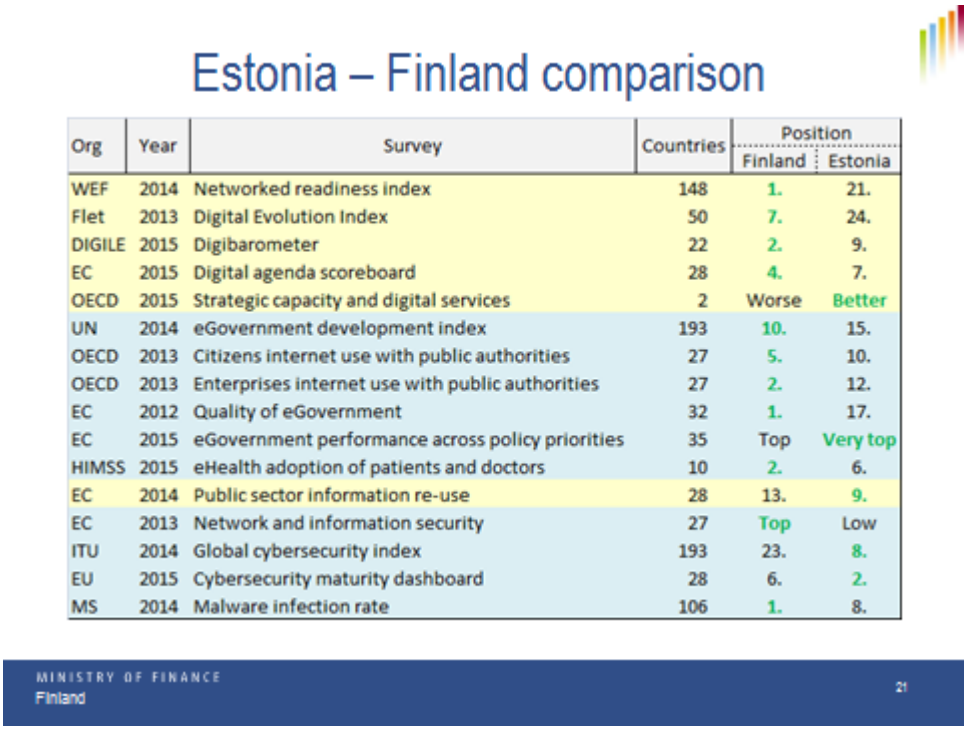
Tutkimus kuvastaa myös mielikuvaa jossa suomessa on totuttu tietoturvaan sekä turvalliseen verkkoasiointiin muuta Eurooppaa aiemmin, mutta toisaalta liiketoimintamahdollisuuksia vertaillen Suomessa on jatkossa yhä vaikeampi myydä tietoturvallisuuteen liittyviä ratkaisuja kuluttajille.

Suomi sijoittuu alana koskevissa kilpailukykyvertailussa hyvinkin vaihtelevasti eri tutkimuksissa kuitenkin varsin kilpailukykyisesti (lähde: Valtiovarainministeriön, Finland’s performance in international ICT surveys – 13.5.2015, R018). Tämä osoittaa hyvin sen, että Suomi on ollut vahvasti kehityksen kärkimaita, mutta toisaalta Suomen panostukset tulevaisuuteen ICT alalla osoittavat eritäin jyrkästi laskevia panostuksia globaaliin kilpailuun verrattuna.

Yhteenvetotaulukko VM: kokoamista tutkimustuloksista:

Org	Year	Survey	Countries	Best country	Finland's position in	
					Europe	World
WEF	2014	Networked readiness index	148	Finland	1.	1.
Flet	2013	Digital Evolution Index	50	Singapore	4.	7.
DIGILE	2015	Digibarometer	22	Denmark	2.	2.
EC	2015	Digital agenda scoreboard	28	Denmark	4.	N/A
UN	2014	eGovernment development index	193	South Korea	4.	10.
OECD	2013	Citizens internet use with public authorities	27	Iceland	5.	N/A
OECD	2013	Enterprises internet use with public authorities	27	Iceland	2.	N/A
EC	2012	Quality of eGovernment	32	Finland	1.	N/A
EC	2015	eGovernment performance across policy priorities	35	N/A	Top	N/A
HIMSS	2015	eHealth adoption of patients and doctors	10	Denmark	2.	N/A
EU	2014	Interoperability framework	25	N/A	Avg	N/A
OKFN	2014	Global open data index	114	UK	3.	3.
EC	2014	Public sector information re-use	28	UK	13.	N/A
EC	2013	Network and information security	27	N/A	Top	N/A
ITU	2014	Global cybersecurity index	193	USA	11.	23.
EU	2015	Cybersecurity maturity dashboard	28	Austria	6.	N/A
MS	2014	Malware infection rate	106	Finland	1.	1.

Vastaava vertailu Viron ja Suomen välillä:



Estonia – Finland comparison

Org	Year	Survey	Countries	Position	
				Finland	Estonia
WEF	2014	Networked readiness index	148	1.	21.
Flet	2013	Digital Evolution Index	50	7.	24.
DIGILE	2015	Digibarometer	22	2.	9.
EC	2015	Digital agenda scoreboard	28	4.	7.
OECD	2015	Strategic capacity and digital services	2	Worse	Better
UN	2014	eGovernment development index	193	10.	15.
OECD	2013	Citizens internet use with public authorities	27	5.	10.
OECD	2013	Enterprises internet use with public authorities	27	2.	12.
EC	2012	Quality of eGovernment	32	1.	17.
EC	2015	eGovernment performance across policy priorities	35	Top	Very top
HIMSS	2015	eHealth adoption of patients and doctors	10	2.	6.
EC	2014	Public sector information re-use	28	13.	9.
EC	2013	Network and information security	27	Top	Low
ITU	2014	Global cybersecurity index	193	23.	8.
EU	2015	Cybersecurity maturity dashboard	28	6.	2.
MS	2014	Malware infection rate	106	1.	8.

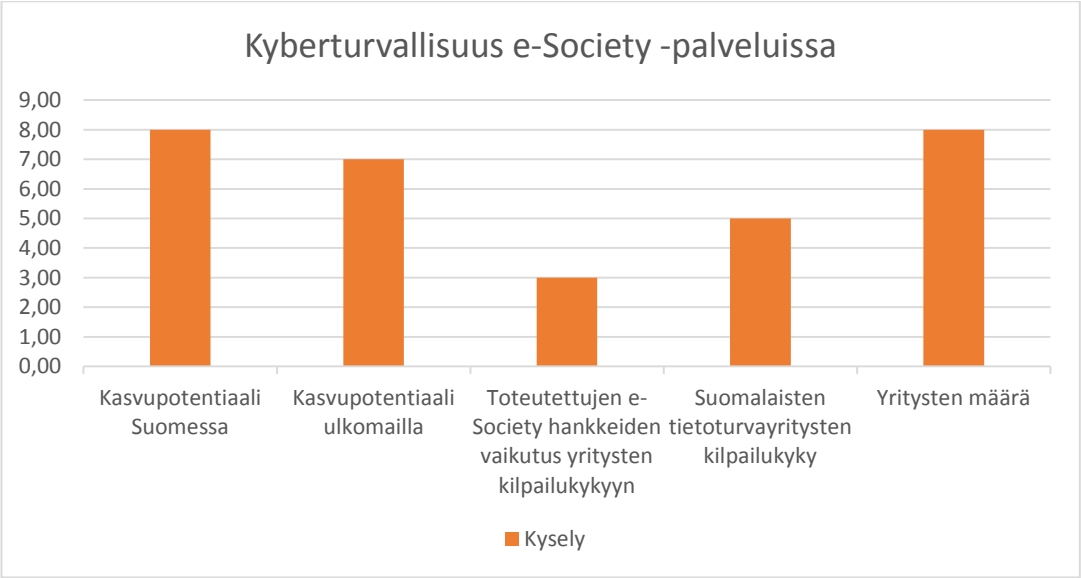
ENISAn tekemän haastattelututkimuksen perusteella (11-20 lokakuuta 2014) suomalainen valistuneisuus on verkossa ollut keskimäärin korkeammalla kuin muualla Euroopassa. Suomessa käytetään laajemmin keinoja turvautumiseen, mutta toisaalta itseluottamus omaan turvallisuuteen on vastaavasti korkeammalla kuin keskimäärin EUssa (http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_fact_fi_fi.pdf). Tutkimus kuvastaa myös kansallista mielikuvaa, jossa Suomessa on totuttu tietoturvaan omassa toiminnassa muuta Eurooppaa aiemmin. Toisaalta yritysten liiketoimintamahdollisuuksien kannalta Suomessa on tulevaisuudessa yhä vaikeampi myydä tietoturvallisuuteen liittyviä ratkaisuja kuluttajille. Tämä vaikeuttaa yritysten mahdollisuuksia Suomessa ja yritysten menestymisessä on pyrittävä nopeasti kansainvälistymään.

3.2 Kilpailukyvyn analyysi haastattelukyselyn perusteella

Tätä kilpailukykyanalyysiä varten toteutettiin haastattelututkimus suomalaisille kyberturva-alan yrityksille. Tutkimuksessa kysyttiin yritysten liikevaihtoa, henkilöstömäärää ja tarjoamaa e-Society –hankkeisiin liittyvässä tietoturvassa. Lisäksi kysyttiin yritysten arviota omasta kasvupotentiaalistaan Suomessa ja ulkomailla sekä yleensä Suomen kilpailukyvystä kansainvälisillä markkinoilla. Suomessa toteutettujen e-Society –hankkeiden vaikutukset yritysten liiketoimintaan selvitettiin myös.

Yhteenveto tutkimuksessa kysytyistä arvioista:

(Kyselyssä pyydettiin yrityksiä arvioimaan mm. omaa kilpailukykyään sekä Suomessa toteutettujen e-Society hankkeiden vaikutusta siihen. Taulukossa on laskettu vastanneista yrityksistä ne, jotka pitivät kyseistä asiaa merkittävänä omalta kannaltaan. Kyselyn tähän osuuteen vastasi 8 yritystä.)



Seuraaviin kappaleisiin on koottu keskeisiä tuloksia kyselyn vastausten perusteella.

3.2.1 Suomalaisten tietoturvayritysten kilpailukyky e-Society -hankkeissa

Kyselyssä pyydettiin arvioimaan kuinka kilpailukykyisiä suomalaiset yritykset ovat Suomessa toteutettavissa e-Society –hankkeissa ja mistä maista tulevat pahimmat kilpailijat.

Kilpailukyky arvioitiin keskimäärin hyväksi ja kilpailijoina nähtiin paljon suomalaisia yrityksiä. Vastaukset jakautuivat erittäin paljon ja erityisesti tulevaisuutta arvioitiin varovasti. Erityisesti ulkomaisen kilpailun nähtiin lisääntyvän, maista mainittiin USA, Japani ja joitakin Euroopan maita.

Kehitysehdotuksia yrityksiltä:

Suurin osa e-Society –hankkeista on julkisten organisaatioiden tilaamia. Siksi julkisilla kilpailutuksilla on tärkeä osa suomalaisen kilpailukyvyn kannalta. Suomalaiset tietoturvayritykset ovat keskimäärin pieniä, jolloin on oleellista, että julkisissa hankinnoissa mahdollistetaan myös pienten yritysten osallistuminen. Tietoturvan kannalta tämä tarkoittaisi esim. että mahdollistetaan osatarjousten tekeminen.

Julkisten hankintojen tiukat raamit nähtiin muutenkin ongelmallisina. Monilla hankintaorganisaatioilla ei ole juuri kokemusta tietoturvatuotteiden hankinnasta, jolloin ne pahimmassa tapauksessa jäävät pois tarjouspyynnöstä. Lisäksi hankintakriteerit eivät jousta, joten niiden määrittelyyn pitäisi käyttää riittävästi aikaa. Tuoteratkaisuja tulisi suosia, koska niiden avulla syntyy uutta vientikelpoista liiketoimintaa Suomeen.

Suomen tulisi aktiivisemmin osallistua alan julkisten standardien, määräysten ja EU-direktiivien kehitykseen erityisesti niiltä osin, kun Suomessa on tietoturva-alan kehitystä.

3.2.2 Toteutettujen e-Society –hankkeiden vaikutus yritysten kilpailukykyyn

Suomi on ollut edelläkävijänä digitalisoinnin ensimmäisessä aallossa ja kyselyllä pyrittiin selvittämään miten yritykset näkevät toteutettujen e-Society –hankkeiden vaikutukset suomalaisten yritysten kilpailukykyyn. Kyselyssä mainittiin

edelläkävijähankkeina Suomessa mm. pankkien verkkopalvelut ja maksuratkaisut sekä julkiset palvelut kuten verottajan palvelut.

Kyselyyn vastanneiden yritysten vastaukset jakautuivat selkeästi. Osa yrityksistä oli ollut mukana e-Society –hankkeissa ja pystynyt kehittämään tuotteitaan osana onnistuneita hankkeita. Innovatiiviset hankkeet Suomessa vetivät selkeästi mukaansa innovatiivisia yrityksiä ja synnyttivät vientikelpoisia tuotteita.

Toisaalta osa yrityksistä oli suoraan tähdännyt kansainvälisille markkinoille eikä nähnyt Suomen markkinoita erityisen kiinnostavina.

3.2.3 Yrityskohtainen kasvupotentiaali ulkomailla

Lähes kaikki yritykset näkivät ulkomailla merkittävää kasvupotentiaalia. Maailmalla on vielä paljon maita, jotka ovat e-Society –hankkeissa Suomea jäljessä ja joissa on selkeä tarve kyberturvallisuudelle.

Potentiaalia nähtiin mm. näillä alueilla:

- Turvallisuusviranomaisten palvelut
- e-Society –palveluiden suojaaminen
- Asianhallinta
- Työnkulkujen digitalisointi
- Sähköinen asiointi

Myytävät palvelut

- Varmennepalvelut
- Tunnistamisratkaisut
- Identiteetinhallinta, käyttövaltuuksien hallinta
- Älykorttijärjestelmät
- Tietoturvatestaus ja –analyysi
- Tilannekuvajärjestelmät
- Salausohjelmistot
- Tunnelointi

3.2.4 Yrityskohtainen kasvupotentiaali Suomessa

Suomessa kasvupotentiaali nähtiin luonnollisesti rajoitetumpana kuin ulkomailla. Kaikki yritykset kuitenkin näkivät vähintään pientä kasvupotentiaalia. Potentiaalia nähtiin samoilla alueilla kuin ulkomaiden tapauksessa. Lisäksi esim. sähköinen allekirjoitus ja identiteetinhallinta nähtiin Suomessa mahdollisena kasvun ajurina lähivuosina.

3.2.5 Viennin lisäämisen keinot

Viennin aloittaminen uudella tuotteella vaatii pääomia. Tuotteen kehittäminen on aina kallista ja vaatii yleensä enemmän tuotekehityspanoksia useammalla markkina-alueella. Lisäksi markkinointi, myynti ja muut toiminnot täytyy monistaa uusille markkina-alueille. Suomalaiset tietoturva-alan yritykset toimivat alkuvaiheessa usein hyvin pienellä pääomalla. Poikkeuksia syntyi lähinnä 2000-luvun alun pörssilistautumisissa, jolloin muutama alan yritys sai merkittävän pääoman listautumalla oikea-aikaisesti. Listautumismarkkinat ovat avautuneet uudestaan vuonna

2014, mutta kerättävät pääomat jäävät ainakin vielä huomattavasti pienemmiksi kuin aikaisemmin.

Muutamat kyselyyn vastanneet yritykset olivat jo onnistuneet viennin aloittamisessa. Tärkein tekijä olivat kilpailukykyiset tuotteet. Suomessa on syntynyt muutamia maailmanlaajuisesti uniikkeja keihäänkärkituotteita, jotka ovat saaneet riittävän rahoituksen alkuvaiheessa kansainvälistyäkseen. Näistä esimerkkejä ovat SSH:n, F-Securen ja Codenomiconin tuotteet. SSH ja F-Secure saivat riittävät pääomat listautumalla, Codenomicon on onnistunut kansainvälistymisessä pääomasijoittajien turvin. Puhtaita palveluyrityksiä, jotka olisivat aloittaneet viennin, ei kyselyssä löydetty.

Viennin kasvattaminen pienillä pääomilla vaatii hyviä kumppanuuksia, jotka mainittiinkin useissa vastauksissa viennin edistämisen pullonkauloiksi. Kaikki toimenpiteet kumppanuuksien ja suhteiden avaamiseksi nähtiin viennin kannalta tärkeinä. Tähän lukeutuvat erilaiset yhteistyökuviot kuten vientirenkaat. Lisäksi markkinoiden tuntemuksen kasvattaminen mm. markkinatutkimuksilla koettiin tärkeäksi.

3.2.6 Viennin esteet

Viennin esteiksi nähtiin juuri oikeiden kumppaneiden löytämisen haasteet. Parhaiten viennin nähtiin tosin usein onnistuvan oman organisaation voimin. Tässä haasteena oli erityisesti pienillä aloittavilla yrityksillä pääomien riittävyys, koska oma vienti vie enemmän resursseja kuin kumppanien kautta vienti. Muutkin esteet liittyivät usein omiin resursseihin kuten ajankäyttöön ja myyntivoimaan.

3.2.7 Yrityksiltä tulleita kehitysehdotuksia

Selkeänä ongelmana nähtiin osaavan työvoiman saatavuus. Yritysten mielestä alan koulutusta tarvittaisiin lisää ja erityisesti tulisi kouluttaa tuotekehitykseen kelpaavaa henkilökuntaa.

Julkisen hallinnon rooli kehittäjänä pitäisi pitää minimissä ja keskittyä soveltamaan olemassa olevia tuotteita ja tukemaan uusien tuotteiden kehitystä.

Kyberturva pitäisi ottaa kärkihankkeeksi kansainvälistymisen kehityshankkeissa.

Kansallisesti tulisi ratkaista Suomessa johtajuus ja alan kehittämisen koordinaatio.

Kyberturva-auditointien pitäisi olla osa jokaista toteutettavaa e-Society-hanketta.

Suomen pitäisi markkinoida itseään tietosuojan osalta kärkimaana ja tätä asemaa pitäisi edelleen lainsäädännöllä tukea, kun monet muut maat ovat olleet julkisuudessa tietosuojan rikkomuksista.

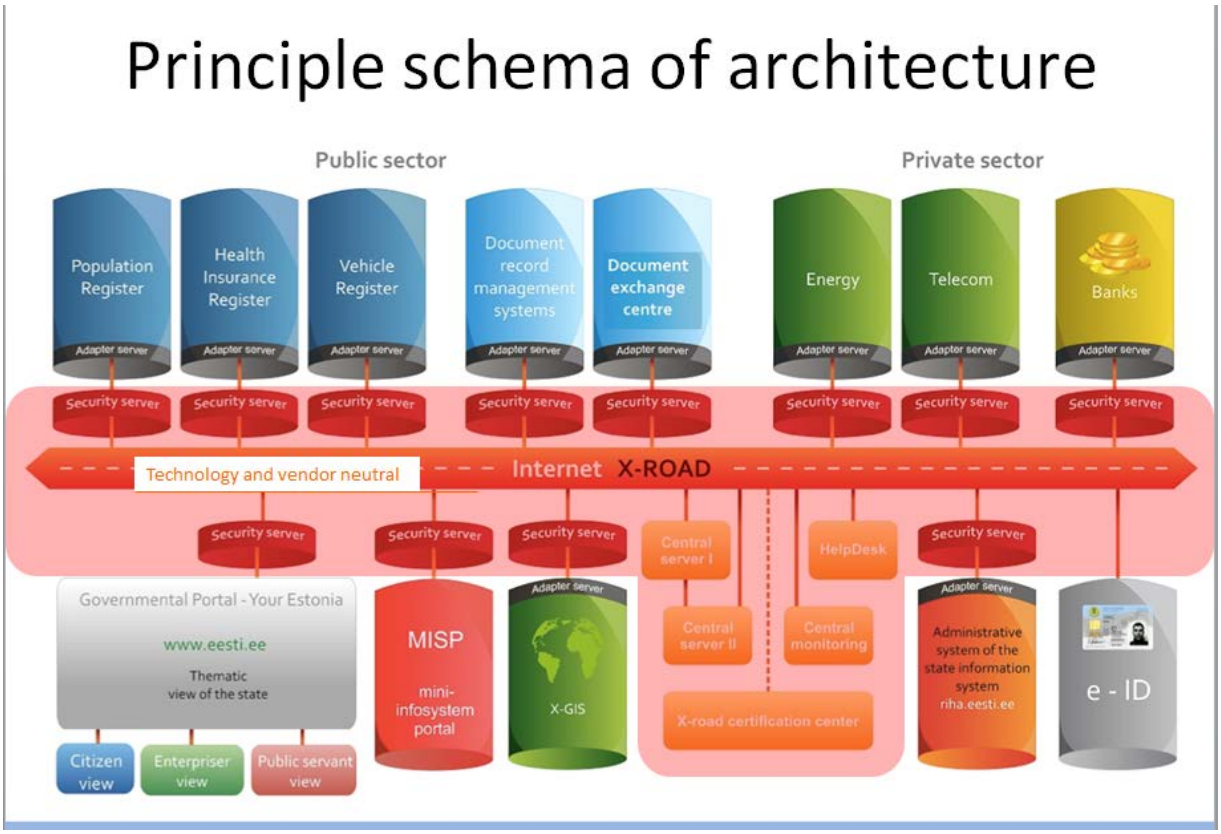
Riskipääomaa tulisi lisätä.

Ulkomaisilta toimijoilta pitäisi pystyä kilpailutuksissa vaatimaan samaa regulaatiota kuin kotimaisiltakin.

3.3 Suomen markkinoilla käynnissä olevat hankkeet ja yritysten kilpailukyky niissä

3.3.1 Kansallinen palveluväylä

Kansallisen palveluväylähankkeen juuren ovat Virosta. Viro on rakentanut XRoad-palveluväylää lähes kymmenen vuotta. Väylä pohjautuu vahvaan kansalliseen tunnistamiseen, väylään liitettyihin kansallisiin rekistereihin sekä sovellustarjontaan, jotka toimivat palveluväylän kautta tapahtuvilla suojatuilla xml-kyselyviesteillä.



Lähdekuva: Estonian Information System's Authority (2.12.2015 Riho Oks & Marko Valing)

Koko palveluväylä on kuitenkin perinyt lukuisia sovelluksia Suomesta, jotka ovat olleen Suomen Valtion toimesta tarjolla Open Source periaatteella tai rajoitetulla jakelulla.

XRoadissa yhdistetään pääosin avointa lähdekoodia hyödyntäen kansallinen palvelutarjonta. Tämän toteuttaminen on ollut mahdollista nopeasti ja pienin kehityskustannuksin, kun hanke on rakennettu ”tyhjälle pöydälle”. Suomen viranomaiset rakentavat Virossa käytössä olevan XRoad 5.0 päälle Suomen palveluväylähanketta jonka versio numeroksi on määritelty XRoad 6.0.

Hankkeessa saadaan koko palveluväylän arkkitehtuuri sekä sovelluskoodit avoimena lähdekoodina Suomen valtion käyttöön. Tälle ohjelmistopohjalle haetaan Suomesta jatkokehittäjiä. Varsinaisen palveluväylän kehittäminen on varsin suoraviivainen kokonaisuus, mutta sen integroiminen vanhoihin rekistereihin sekä sovelluksiin on muodostunut suurimmaksi haasteeksi. Tämän lisäksi kansallinen sähköinen tunnistaminen on yksi Suomen suurimpia ongelmia ratkottavaksi.

Suomalaisella alan teollisuudella olisi paljon osaamista tälle hankkeelle. Lisäksi Suomesta löytyy paljon jo tehtyjä toteutuksia, jotka soveltuisivat palveluväylään sellaisenaan. Ongelmana on kuitenkin valtiollinen toimintatapa joka ei mahdollista tehokasta ja yritysten kilpailukykyä parantavaa palveluyhteistyötä hankkeen ympärillä. Yhteistyössä suurimmat haasteet kohdistuvat ohjelmistojen omistusoikeuksiin sekä erittäin mataliin tuntityöhintoihin. XRoad voisi parhaimmillaan olla kansallinen polku näyttävästä referenssistä jota voitaisiin hyödyntää kansallisena ponnistuslautana kansainvälisille markkinoille alan yritysten toimesta mutta nykymallilla se tulee jäämään valtion kertatilaukseksi, yhdeksi kansallisesti räätälöidyksi sovelluskokonaisuudeksi.

3.3.2 Kansallinen tunnistusratkaisu

Suomessa on kansallinen tunnistaminen jäänyt alun perin pankkien toteutettavaksi. Pankit ovat kehittäneet ratkaisut omia tarpeita varten ja niitä on myöhemmin sovellettu laajemmin tunnistautumiseen julkisiin palveluihin sekä erilaisiin kaupallisiin palveluihin.

Tunnistamiseen on muodostunut kolme leiriä: pankit, operaattorien sekä julkinen sektori. Operaattorit ovat kehittäneet vuodesta 2001 mobiilitunnistamista ja julkisella sektorilla on ollut Viron mallin mukainen sähköinen asiointikortti (HST-kortti) tarjolla. Valtion malli on ollut kankea ja sitä on yritetty levittää lukuisilla eri tavoilla markkinoille kuitenkaan onnistumatta. Operaattorit ovat luoneet maahan soveltuvan tunnistamisinfrastruktuurin, mutteivat ole onnistuneet rakentamaan markkinoista liiketoimintaa pankkien rinnalle tai niiden kanssa yhteistyössä.

Suomessa tehdään noin 400 - 450 miljoonaa sähköistä vahvaa tunnistusta vuosittain. Näistä vain 50 -80 miljoonaa tapahtumaa ovat muita kuin verkkopankkikirjautumisia. Kaupallisesti tunnistaminen ei voi tapahtumana maksaa liikaa. Tunnistaminen ei ole ”liiketoimintasidonnainen toiminto” vaan se on pakollinen lisätoiminne, jotta asiointi sähköisesti olisi mahdollista.

Operaattorit pyrkivät vuosituhannen alussa tarjoamaan tunnistamista jopa 0.50€ - 1.00 euron tapahtumahinnoilla palvelutuottajille. Pankkien hintatarjonta vaihtelee noin 0.20 eurosta – 0.60 euroon tapahtumalta, mikäli palvelua käytetään pankin ulkopuolisissa sovelluksissa. Sovelluksissa, joissa tunnistustapahtumia tehdään päivittäin, voi hinta olla enimmilläänkin muutamissa senteissä per tapahtuma. Toisaalta palveluissa joissa vahvaa tunnistamista tarvitaan harvoin kerranpari vuodessa, voi tapahtuma hintakin olla huomattavasti suurempi.

Hinnoittelu tunnistamisessa on monimutkaista. Tunnistuksesta peritään tapahtuma tai kk-maksuja sekä palvelutarjoajalta että käyttäjältä. Suomessa verkkopankkien käyttäjät ovat tottuneet maksuttomaan tunnistamiseen, kuitenkaan ottamatta huomioon että heiltä peritään kk-maksua verkkopankin käytöstä ja tunnistaminen on hinnoiteltu kiinteään palvelumaksuun sisään.

Operaattoreilla on ollut viime vuodet tarjolla myös paketteja, joihin sisältyy rajaton tunnistaminen kiinteään kuukausihintaan käyttäjälle mutta palvelutarjoajille hinnoittelumallit ovat olleet vaihtelevia.

Nyt viimeinen muutos perustuu luottamusverkostomalliin, jossa rakennetaan luotettujen tunnistajapalvelutuottajien toimesta yhteensopivaa tunnistamisverkostoa, jossa pyritään määrittelemään siirtohintoja sekä tapahtumamaksuja toimijoiden välille.

Tunnistamisosaaminen on Suomessa maailman huippua. Maassa on kokeiltu ja käytetty laajasti eri tekniikoista ja niistä on innovoitu paljon uusia palveluita. Kansallisesti olemme kuitenkin olleet paikallaan pitkään. Teknologisesti pankkien TUPAS on ollut toimiva ja sen rinnalle ei ole pystytty luomaan taloudellisesti kestävälle pohjalle muodostuvaa tunnistusinfrastruktuuria. Yritykset ovat aina päättyneet kustannuksiin. Suomessa alalta löytyy osaamista laajasti, mutta sitä ei ole osattu hyödyntää kansallisessa tunnistamisessa riittävästi. Lisäksi taloudellisiin kysymyksiin ei ole löytynyt sopivia ratkaisuja. Kahden suuren pankin päätäntävallan siirtyminen Suomen ulkopuolelle on myös osaltaan rajoittanut investointi halukkuutta Suomessa. Suomi on pieni markkina-alue, jossa voidaan kokeilla asioita, mutta volyymien pienuus tarjoaa kuitenkin vain näyteikkunan, jolle on haettava kasvu kansainvälisiltä markkinoilta. Suomi on osana EU:ta ja EU:ssa pyritään ratkomaan tunnistamisen ja maksamisen suuntaviivoja keskitetysti. Onko tästä tulossa uusia haasteita ja ongelmia, jotain kautta tunnistamisratkaisut tulevat muuttumaan, tapahtuuko tämä EU:ssa kokonaisuutena. Vai johtaako tämä hajautumiseen niin, ettei yhteisiä ratkaisuja saada aikaan EU:ssa ja tämä on jälleen yksi EU:n ikuisuusprojekteja.

3.3.3 Katso

Suomessa verotus on yksi esimerkillinen edelläkävijä sähköisten palveluiden kehityksessä. Fyysistä asiointia ei tarvita kuin hyvin poikkeavissa tilanteissa. Yrityksien veropalvelut hoituvat myös laajalla tarjonnalla ja pienellä byrokratialla.

Yritysten palveluiden siirtäminen verkkoon on perustunut pääosin verottajan luomaan Katso-palveluun. Tässä yritykset voivat määritellä oman roolirekisterin viranomaisasiointiin. Palvelussa ”yritys” voi itse nimetä edustajansa sekä mahdolliset sidosryhmät jotka voivat edustaa yritystä sekä toimittaa yritysten puolesta tietoja viranomaisille. Palvelu on kehitetty pääosin verottajan omia palveluita varten, mutta järjestelmän tarjoamat laajat ominaisuudet on laajennettu yleisemmin eri viranomaispalveluihin. Katso mahdollistaa mm. tilitoimistojen oikeuden asioida yrityksen puolesta palvelussa. Katson tarjoamat edustusroolien ja tunnistamisen palvelut toimivat pohjana kattavillekin viranomaisasioinnin digitaalisille palveluille.

Katso on tarjonnut koko yritysmaailmalle huomattavia taloudellisia säästöjä kokonaisvaltaisella sähköisellä asioinnilla. Palvelun kehitys on toteutettu verottajan määritysten perusteella nykyisen CGI:n toimesta. Palvelun taustalta löytyy kuitenkin yksi alan edelläkävijä yritys, Ubisecure Solutions, joka on nykyisin japanilaisomistuksessa, ja toimii nimellä GlobalSignUbisecure. Katson palvelukehitys mahdollisti Ubisecurelle tuoteidean, joka lopulta tuotteistettiin ulkoisen käyttövaltuuksien ja roolihallinnan tuoteperheeksi. Nyt tuote on Suomessa laajasti käytössä, ja GlobalSign pyrkii kansainvälistämään tuotteen maailman laajuisiksi. Katso-palvelu ja sen ympärillä toiminut yrityskonsortio on esimerkillinen kokonaisuus, kuinka kansallinen PPP-yhteistyö on luonut julkiseen talouteen huomattavia säästöjä sekä lisäarvo koko kansantalouteen. Samalla palvelukehityksessä on jätetty riittävästi tilaa

yrityksille toteuttaa hankkeesta tuotteita laajemmin markkinoille. Tämä on myös malliesimerkki siitä kuinka julkisen hallinnon palveluiden kehitystyö tulisi toteuttaa kokonaisvaltaisesti kansantaloudellista etua silmälläpitäen, eikä vain yksittäistä työtuntikustannusta seuraten.

3.3.4 Sähköinen resepti

Sähköinen reseptihanke alkoi Suomessa loppuvuonna 2001 määrittelytyönä. Aluksi tavoiteltiin sekä digitaalista allekirjoitusta hyödyntävää että matkapuhelimella käyttöön soveltuvaa reseptijärjestelmää. Vuoden 2002 aikana toteutettiin Kelan ja STM:n (Sosiaali- ja Terveysministeriön) ohjaamana kaksi pilot-hanketta. Kohdealueina oli eri sairaanhoitopiirejä Lounais-Suomesta sekä Keski-Suomesta. Eri sairaanhoitopiirien väliseen sähköisen reseptin siirtoon valittiin pilot-vaiheeseen, Mediweb Oy, startup-yritys. Lopulta eri pilot-vaiheiden jälkeen kaupalliseksi toteuttajaksi valittiin Accenture. Hanke on ollut hyvin kivikkoinen ja vienyt lähes kymmenen vuotta. Yhtenä haasteen on ollut lääkärikunta joka ei ole ottanut sähköistä reseptiä myönteisesti vastaan. Samat lääkärit toimivat usein julkisella sekä yksityisellä sektorilla ja he kokivat sähköisen reseptin teknisesti vaikeaksi sekä osaksi vastustus kohdistui myös lääkärityön riippumattomuuteen jossa lääkärit eivät halunneet keskitettyä kontrollia omaan toimintaansa.

Keskitetyn reseptikannan rajapinnat sekä lukuiset turvakysymykset sähköisten reseptien siirrossa oli vaikeita kysymyksiä ratkottavina, jotka veivät paljon aikaa. Lopulta sähköisen resepti on otettu julkisella sektorilla maanlaajuisesti käyttöön vuoden 2015 alusta ja suositelluksi tavaksi myöntää reseptejä yksityisellä sektorilla. Kansallinen tavoite kaikkien reseptien sähköistämisestä tulee kuitenkin viemään vielä useita vuosia ja vaikka hanke alkoi vuosituhannen alussa hyvin lupaavasti, yhtenä maailman edelläkävijänä, nyt hanketta voidaan pitää yhtenä esimerkkinä tahmeasta kokonaisuudesta, jossa ei juuri ole syntynyt kansallisesti juuri erityisosaamista tai kilpailuetua kansainvälistymiseen.

Lisäksi suurien tilausten valuminen lopulta Amerikkalaisille alan jäteille ja myöhemmin keskitetyn potilastietojärjestelmän Abbott-hankkeen tilaaminen Epic:iltä, jättävät suuren loven suomalaisten Private-Public-yhteistyölle. Abbott-hanke on poikinut valituksia markkinaoikeuteen sekä herättänyt huomattavasti keskustelua koko ICT:n kansallisesta hankintapolitiikasta.

3.3.5 Verkkopankit

Suomessa verkkopankkien käytössä ollaan oltu maailman edelläkävijä. Koko pankkimaailman sähköisen asioinnin perustana oli 1990-luvun alun pankkikriisi. Kriisin tuloksena pankkisektorilta poistui toimijoita konkurssien kautta sekä hyvin merkittävien fuusioiden kautta.

Aggressiiviset muutokset johtivat lopulta kymmenien tuhansien työpaikkojen katoamiseen alalta ja erityisesti pankkikonttoreista. Konttoreita yhdisteltiin ja suljettiin nopealla aikataululla. Samalla pankkien tuli turvata pankkipalveluiden saatavuus, joka johti nopeaan pankkipalveluiden digitalisoitumiseen. 1990-luvun alkupuolella markkinoille tulivat modeemi-pohjaiset pankkiohjelmistot ja 1990-luvun loppupuolella internet-pankit yleistyvät nopeasti. 2000-luvun alkupuolella Suomalaisten internet-pankkien käyttäjämäärät olivat maailman korkeimpia ja palveluiden saatavuus hyvin kattavaa.

Turvallisuus liittyy aina rahaan. Kuluttajien käyttäytyminen ja huolet verkkopankkien turvallisuudesta olivat pieniä haasteita käytön yleistymisessä. Pankit rohkaisivat kuluttajia ottamalla verkkopankin väärinkäytöksistä riskien kannon pääosin itselleen. Tämä oli päinvastainen malli, kun maailmalla verkkopankin kautta tehdystä huijauksista pääsääntöisesti vastuun kantoi asiakas.

Verkkopankkien turvallisuus oli Suomessa vankalla pohjalla. Pankkiin käyttäjän tunnistaminen perustui vahvaan tunnistamiseen, jossa käytettiin muuttuvaa salasanalistaa yhdistämällä se vain asiakkaan itsensä tuntemaan omaan asiakastunnuksen, joka oli salassa pidettävä asiakaskohtainen tieto. Tämä esti pääosin väärinkäytöksiä ja sama tunnistamistekniikka yleistyi myös muihin verkkopalveluihin nopeasti. Verkkopankit tarjosivat turvallisen tavan sähköiselle asioinnille ja myös tavan toteuttaa turvallisemmin verkkokauppaostoksia.

Maailmalla verkkopankkien tunnistaminen perustui salasana/käyttäjätunnus-yhdistelmiin jotka osoittautuvat hyvinkin helpoiksi tavoiksi rikollisille toteuttaa verkkopankki huijauksia sekä rakentaa ”key logger” - haittaohjelmia asennettaviksi kuluttajien tietokoneisiin.

Tämä hidasti maailmalla verkkopankkien käytön leviämistä laajasti. Koko sähköisen maksamisen infrastruktuuri sekä siihen liitetty tunnistaminen johtivat nopeasti digitaalisten palveluiden laajaan leviämiseen Suomessa. Kansallisesti tämän ympärillä on käyty jatkuvasti kovaa keskustelua pankkien määräävästä asemasta markkinoilla, teknisten ratkaisujen käytettävyydestä ja edistyksellisyydestä sekä lukuisista muista haasteista joita tunnistamiseen on liitetty. Tosiasia on se, että tekniikka toimii, kuluttajat omaksuivat sen ja turvallisuus oli riittävää. Tämä loi pohjan Suomen nopealle digitalisoitumiselle sekä eSociety - palveluiden syntymiselle.

Suomi kehittyi koko 2000-luvun ensimmäisen vuosikymmenen vahvasti edelläkävijänä tällä saralla, mutta älypuhelimien käytön levitessä ja Nokian hiipuessa alkoi myös suomalaisten verkkopankkien kilpailukykyisyyden lama. Vuosituhannen alussa Suomesta vietin verkkopankkiteknologiaa useihin maihin Tiedon sekä Meridean toimesta kunnes älylaitteet pysäyttivät kehityksen. Verkkopankkeja voidaan pitää Suomen digitalisoitumisen perustana mutta samalla jarruna.

3.3.6 Mobiilipankit

Suomessa verkkopankkien levinneisyys ja Nokian puhelimien vahva markkinaosuus esti mobiilipankkien markkinoille rynnistyksen. Tunnistusratkaisu, muuttuvan salasanalistan mukana kantaminen ei soveltunut liikkuvaan ympäristöön ja vaihtoehtoisten tunnistusratkaisujen markkinoille tuleminen ei onnistunut pankkien vakiintuneiden ratkaisumallien takia. Mobiilipankkien käytölle ei ollut vastaavaa tarvetta kuin maailmalla jossa verkkopankkien käyttö oli huomattavasti pienempää kuin Suomessa ja verkkopankeissa ei ollut kussakin maassa laajasti levinneitä kansallisia tunnistusratkaisuja. Mobiillilaitteita kokeiltiin Suomessa paljon 2000-luvun alkupuolella. WAP-puhelin- sekä digi-TV-ympäristöön sovitettiin pankkitoimintoja, mutta WAP:in hitaus ja käyttöliittymien vaikeus ei innostanut kuluttajia.

Mobile-pankit tekevät vieläkin vasta ensiaskelia Suomessa ja nyt niitä otetaan laajemmin käyttöön. Tämä on ollut myös samalla yksi palvelukehityksen jarru. Mobile-palveluiden kehitys on ollut hidasta Suomessa, myös muissakin palveluissa. Ne eivät ole yleistyneet eSociety-palveluissa eivätkä verkkoasioinnissa laajemmin.

Suomessa on pudottu kehityksen kärkimaan asemasta keskikastiin. Suomessa on paljon osaamista mobiiliturvallisuudesta ja sitä osaamista voitaisiin hyödyntää laajemmin lukuisissa ratkaisuissa, mutta elämä Nokian jälkeisessä maailmassa on muodostunut rakenteellisesti vaikeaksi asiaksi. Ehkä yhtenä tekijänä on ollut Nokia kokoava voima. Nokian kautta tekniset innovaatiot päätyivät usein osaksi laajempia kokonaisuuksia, ja ratkaisut kansainvälistyivät Nokia kautta helposti yhden asiakassuhteen kautta. Nyt ratkaisuille olisi löydyttävä lukuisia asiakkaita, laajoja jakeluverkostoja sekä useita ratkaisuja yhteen kokoavia yrityksiä, joiden hakeminen on osoittautunut Suomalaisyrityksille suureksi haasteeksi ja kansallisten mobiilipalveluiden kehitys on hidastunut.

4 Kehitysehdotukset alan kilpailukyvyn parantamiseksi

Kansallisesti Suomessa toimitaan varsin epärationaalisesti. Kyberalalla olemme olleet kilpailukykyisiä edelläkävijöitä, mutta kansalliset toteuttamisten laiminlyönnit sekä lähes olemattomat taloudelliset panostukset alan kehittämiseen ovat syömässä kilpailuedun nopeasti.

4.1.1 Julkiset kilpailutukset ja puitesopimukset

Puitesopimukset

Kansallisesti Hansel kilpailuttaa neljän vuoden välein IT palveluhankinnat valtiohallintoon. Viimeksi toteutuneella kilpailutuskierroksella valituksi tulivat halvimmat tarjoajat, jotka eivät todellisuudessa ole valtiohallinnon kannalta parhaita ja oikeita toimittajavaihtoehtoja. Lyhytjänteinen tarkastelu sekä huonot valintakriteerit veivät tämän kilpailutuksen valintatuloksen valtakunnallisen kilpailukyvyn ja turvallisuuden kannalta huonoon lopputulokseen. Tietoturvapalveluiden edellisessä kilpailutuksessa neljä vuotta aiemmin valituksi tulivat kymmenen alaan erikoistunutta tunnettua yritystä, joissa työskentelee alan nimekkäimpiä osaajia. Tällä kertaa valituksi tuli kuusi yritystä, joista yksikään ei ole erikoistunut kyber- tai tietoturvallisuuteen. Valintakriteereissä arvostettiin yleistä tutkintotasoa, joka ei ollut sidoksissa mitenkään alan osaamiseen tai tietoturva-alan sertifikaatteja. Alalla työkokemus on yksi tärkeimmistä ominaisuuksista. Kyberosaaminen vaatii käytännönläheistä ja kokemusperäistä hands-on tekemistä ja se ei vaikuttanut valintakriteereissä lainkaan.

Kilpailutusmalli suosi verkostoja, joissa valintojen suorituspisteytykseen kannatti esittää tohtoritutkinnon suorittaneita henkilöitä riippumatta siitä, olivatko he todellisuudessa tietoturva-alan osaajia tai ylipäänsä saatavilla mahdollisiin toteuttaviin hankkeisiin resursseiksi muutoin kuin tarjouksessa. Kilpailutuksen lopputulos oli kansallisen kyberstrategian kannalta epäonnistunut ratkaisu. Yhteiskunta ei saanut käyttöönsä parhaita saatavilla olleita resursseja kilpailukykyiseen hintaan. Nyt saatiin kustannuksiltaan edullinen päivätyöhinta, muttei paras tai edes tyydyttävä laadullinen ja kokemuksellinen osaaminen projektikäyttöön.

Viron malli

Viro on hyvä esimerkki mallista, jossa maailmalta on kerätty avoimen lähdekoodin toteutuksia ja niiden varaan on rakennettu kansallinen palveluväylä. Lukuisat avoimen koodin toteutuksista ja malleista tulevat alun perin Suomesta. Tämä on ollut Viron valtiolle kertainvestointina edullinen toteutus. Virkamiehet vievät Viron sähköiset palvelut yhteen kokoavaan verkkopalveluun, XRoadiin ja nyt konseptia tarjotaan maailmalle avoimesti, vastikkeetta, ilman vientituloja. Suomessa hanketta on ihannoitu, ja siitä otetaan laajasti oppia. Viron yrityssektori ei ole kuitenkaan saanut koko kansakunnalle tehdystä toteutuksesta lainkaan uusia vientituotteita tai palveluja, vain vähän julkisuutta.

Samalla Virossa on huomattu, että yksityisen tuoteomistajuuden puuttuessa jatkokehittäminen on muuttunut työlääksi. XRoad 5.0 -version levitys onnistui helposti,

kun hidasteena ei ollut vanhoja olemassa olevia ”legacy” IT-järjestelmiä tai muita yhteiskuntarasitteita. Kaiken sai tehdä puhtaalta pöydältä. Ketterä kehitys on nyt juuttunut XRoad 6.0 -versioon, jossa lisävaatimuksena on sovitustyö kertaalleen rakennettuun avoimen lähdekoodin projektin järjestelmiin. Versiosovitukseen arvioitiin aluksi kuluvan vähän aikaa, joka venyi kahteen vuoteen ja lopullinen valmistuminen vain venyy. Nyt on huomattu, että aikataulun venymisen myötä kulubudjetti kasvaa yli ennakoidun ja jatkaa kasvamistaan.

Jos Viron XRoad-hanke olisi toteutettu projektina, jota yritykset jalostaisivat edelleen vientituotteeksi, olisi Viron kansantalous hyötynyt pitkällä aikavälillä huomattavasti nykyistä mallia enemmän.

IPR-oikeudet

Suomessa valtiohankinnoissa pyritään saamaan ICT alan yrityksiä luovuttamaan IPR:t toimituksistaan valtiolle. Tämä on yksi sopimusehto jota esimerkiksi Hansel noudattaa pääosin hankinnoissaan. Valtiolla on oikeus julkistaa toteutetut ratkaisut avoimeksi lähdekoodiksi jälleenjaettavaksi. Tästä on yhtenä esimerkkinä mm. xRoad syntyminen, jossa alkuperäisistä lähdekooditoteutuksista merkittäväosuus on peräisin Suomesta.

Tämän hankintapolitiikan lopputuloksena koko ICT sektori joutuu tuottamaan valtiolle projekteja sekä työtä, jota ei voi tuotteistaa kansainvälisille markkinoille liiketoiminnaksi. Lopputulos on erittäin epäedullinen kansantaloudellisesti ja erityisesti merkittävä este yrityksien kansainvälistymiselle. ICT alalla tuotteiden kansainvälistäminen on huomattavasti tuottavampaa kuin pelkän työn vienti.

4.1.2 Pääoma

Tekesin tuet

Suomessa ollaan luovia, innovatiivisia sekä teknisesti orientoituneita. Suomessa ei olla perinteisesti yrittäjiä, kasvuhalukkaita, kansainvälistyviä eikä myyjiä. Suurin alan kasvueste on suomalaisessa asenteessa. Yrittäjien tavoitteet ovat liian vaatimattomia ja yrittäjiltä puuttuu usein osaamista kansainvälistymiseen. Osa osaamisvajeesta olisi korjattavissa rekrytoimalla ja hankkimalla osaamista, mutta tässä on usein rajoitteena pääomien puute. Kansainvälistyminen on yksikertaisesti liian kallista ja riskialtista. Nokia ja muutamat vastaavat suuryritykset loivat Suomeen helpomman tavan kansainvälistyä hankkimalla näiltä yrityksiltä alihankintana ratkaisuja ja palveluita. Nokian kansainvälinen menestyminen tarjosi kanavan lukuisille yrityksille eri puolelle maailmaa lähes 15-vuoden ajan. Samalla panostukset kansainvälistymisen osaamiseen pienemmissä alihankintaan keskittyvissä yrityksissä jäivät tekemättä ja yhteistyövientiverkostot toteutumatta. Kansallisesti tämä joudutaan nyt opettelemaan uudelleen ja osaksi tulisi kerrata 1980-luvun lopun ja 1990-luvun alun menestysreseptejä, kun oltiin hyvin vastaavassa tilanteessa.

Yrityksille on ollut tarjolla tukea perinteisesti tuotekehitykseen ja Tekes on ollut yksi luotettava tuen myöntäjä ja kumppani tässä toiminnassa. Tämän lisäksi kansallisesti toimii muutamia kymmeniä Venture Capital-sijoitustoimijoita, joista muutama on kulloinkin aktiivinen sijoittamaan uusiin yrityksiin. Lisäksi rekisteröityjä enkelisijoittajia

on vähän yli 600, joista sijoituksia tekee 200 - 300 enkeliä vuosittain. Enkelisijoitusten keskiarvo on tyypillisesti 20 - 30 000 euroa, kun esimerkiksi USA:ssa vastaava summa on usein 100 000 USD tai enemmän. Vuonna 2014 enkelisijoitusten yhteisarvo oli noin 16 miljoonaa euroa Suomessa ja pääomasijoitusten arvo uusiin kasvuyrityksiin noin 70 miljoonaa euroa, kun kaikista investoinneista poistetaan yritysostoihin ja järjestelyihin käytetyt investoinnit. Näistä pääomainvestoinneista ei ole päätynyt kyberturvayrityksiin juuri lainkaan. Ala on kasvanut pääosin työvaltaisella mallilla projektien ja alihankintatoimitusten kautta. Näistä on tuotteistettu palveluita ja tuoteratkaisuja, mutta organisaatioon ei ole kertynyt kasvuun soveltuvia riskipääomia joita kansainvälistyminen edellyttäisi.

Kyberalalle Tekes on huippuvuosina sijoittanut tuotekehitysavustuksina yli 15 miljoonaa euroa vuodessa, mutta viime vuonna jatkuvasti jyrkästi laskeva trendi osoitti noin 12 miljoonaa euroa. Tämän realistisen tarkastelun tuloksena alan kasvunäkymät ovat huonot. Onko syynä ideoiden vähyys, koventuva kilpailu vai pääomien puute?

Kansainvälistymisen vaatima pääoma

Kyberalalla on nähtävissä samat ongelmat kuin muillakin kasvualoilla. Suomessa syntyy yritysideoita ja ne onnistuvat usein kansallisesti kasvamaan enimmillään muutaman miljoonan euron liikevaihtokokoon, mutteivat suuremmiksi. Kansainvälistymiseen ei ole tarjolla tarpeeksi riskipääomasijoituksia ja kansalliset kasvuinstrumentit kansainvälistymiseen puuttuvat lähes kokonaan. On huomattava, että kansainvälistyminen on B to B – markkinoilla kallista. Usein tässä vaiheessa yritys pyritään myymään tai yrityksen kasvu alkaa hidastua, ja yrityksen kilpailukyvyn kehittäminen muuttuu jatkuvasti haastavammaksi, kun alkuperäinen innovaatio alkaa vanheta.

Yhteiskunnallisesti juuri näiden yritysten kasvu seuraavalle portaalle mahdollistaisi suurempien suomalaisten kansallisten yritysmenestystarinoiden syntymisen ja riittävän suuren yrityskoon laajempaan kansainvälistymiseen.

Nyt kansainvälistämiseen ja huomattavan kasvupyrähdyksen toteuttamiseksi ei ole tarjolla yhteiskunnallisia rahoitusmekanismeja kuten lukuisissa muissa maissa. Maailmalla on useita menestysreseptejä kuten useissa maissa josta esimerkkeinä, Etelä-Korea ja Israel. Näissä maissa on olemassa kansallinen riskipääomarahastorakenne, jossa sijoitetaan kansallista pääomaa kasvuyritykseen. Kasvuyrityksen menestyttyä ja kasvettua, tuotoista osa palautetaan takaisin kansalliseen riskipääomarahastoon.

Suomessa on viennin edistämiseen oma organisaatio. Finpro todellisuudessa kykenee ainoastaan tukemaan yrityksiä kontaktien hankkimisessa. Finpro on vahvasti byrokratisoitunut rakenne, joka toimii laajasti maailmalla mutta tuottaa vähän. Finpron sijaan tarvittaisiin uudentyyppisiä vientiverkostoja, joissa tähdättäisiin hyvin suoraviivaisesti kauppojen toteuttamiseen sekä yritysten liikevaihdon mahdollistamiseen uusilla markkinoilla. Finpron sijaan tarvittaisiin hyvin operatiivisia kauppahuonemaisia malleja jossa kansallinen tuki kohdistuisi ”kauppahuoneiden” ja liiketoimintojen etabloimiseen eri maihin ja mantereille. Tässä tulisi luoda konsepteja jotka lisäävät kauppaa, edistää myyntiä, tukee toimituksia sekä edesauttaa toimitusten

ja asiakkuuksien jälkihoidossa. Lisäksi tarvittaisiin kansallisia rakenteita riskipääomien tarjoamiseen kasvuhalukkaille ja kasvupotentiaalia omaaville yrityksille kuten vaikka Etelä-Koreassa. Nämä kansainvälistämiseen tähtäävät mallit ja rakenteet olisi tehtävä tiiviisti julkisen sektorin, että yksityisen sektorin yhteistyöllä ja niitä tulisi mitata yritysmaailman mittareilla.

Kansallinen kyberstrategia

Suomessa suoraviivaisuus ja liiketoimintalähtöisyys vajoavat usein monimutkaisiin prosesseihin ja suunniteluun, jossa lopputuloksena syntyy hyvä jopa täydellinen suunnitelma. Ohjelmissa ja suunnitelmissa ei ole varattu rahaa toimeenpanoon. Hyvä esimerkki on kansallinen kyberstrategia, joka oli yksi maailman ensimmäisistä suunnitelmista ja laajasti hyväksi tunnustettu, mutta sen toimeenpanemiseksi ei ollut lainkaan pääomia. Jos kyberstrategia olisi viety toimeenpanoon ja siihen olisi sijoitettu 100 - 300 miljoonaa euroa, olisimme edelleen yksi edelläkävijä alalla, mutta kahden vuoden opettelu ja hyvä suunnitelma inspiroi muita maita tekemään suunnitelmansa ja panostamaan tekemiseen ajaen ohituskaistaa Suomen ohi.

Kehitysapuhankkeet

Kansainvälistymisen yhtenä mallina maailmalla on pidetty kehitysapua. Kehitysapuhankkeet olivat vielä 1980- ja 1990-luvulla hyvin infrastruktuurilähtöisiä. Hankkeissa toteuttajina olivat suomalaiset yritykset, jotka saivat hankkeiden kautta kansainvälistymisosaamista, ja kehitysapu palautui myös kansantaloutta hyödyntävällä tavalla takaisin yhteiskunnan rattaisiin. Nyt kehitysapu ei saa olla mitenkään sidoksissa liiketoimintaan. Tämä poikkeaa jälleen pääosasta maailman maista, joissa kehitysapua käytettään jatkuvasti välillisenä instrumenttina maan yritysten kansainvälistymiseen. Useissa tapauksissa kehitysapu tai kahdenvälinen apu tarjotaan kohdemaalle kahdella eri instrumentilla: avustuksena suunnitteluun sekä korkotuettuna halpakorkoisena lainana, jossa hankinnat toteutetaan pääosin myöntäjämaasta. Nämä mahdollistavat yritysten vahvan osallistumisen hankkeeseen ja myöhemmin etabloitumisen kohdemaahan luoden täysin kaupallisia kilpailukykyisiä hankkeita kohdemaissa. Samalla osaaminen kansainvälistymiseen lisääntyy yrityksissä sekä kansallisesti julkisella sektorilla. Kansainvälistymiseen ja kasvuun tulisi Suomessa keskittyä kokonaisvaltaisesti kansakuntana ja kybertoimialana voisi tarjota yhden uuden huomattavan mahdollisuuden Suomesta. Alalla on olemassa vahva osaamisklusteri joka voi toimia keihäänkärkenä viennille, kun sen kansainvälistämiseen tehtäisiin merkittävä yhteiskunnallinen panostus. Ala on uusi ja kilpailua sekä laadukasta tarjontaa on maailmalla vielä rajallisesti tarjolla. Samalla Suomen liittoutumattomuus ja luotettava maine rehellisenä vähiten korruptoituneena maana toimii ylimääräisinä brändeinä alalla, jossa luottamus on merkittävin menestyksen tae.

Kansainvälistymisen pullonkaulat

Kybersektori mahdollistaisi nopeasti ympärilleen lukuisia eri toimialoja läpileikkaavan osaamisen useiden muiden sektoreiden kasvupolkujen luomiseen linkittämällä ne kyberturvallisuuden kehittämiseen ja kokonaisvaltaisen digitaalisuuden kehittämiseen.

Kansainvälistymisen kannalta on erittäin tärkeää rakentaa asiakasreferenssejä. Kyberalalla useat merkittävät referenssit löytyvät julkiselta sektorilta. Suomessa on kyettävä jatkossa rakentamaan maan näyttävimmät ja parhaat alan referenssit uskottaviksi ja kansainvälistymiseen soveltuviksi kokonaisuuksiksi joissa myös julkisenvallan edustajat ”referenssiasiakkaana” tulevat vahvasti tukemaan yritysten viennin uskottavuutta. 1990-luvulla kunnat ja valtio hankkivat usein kotimaisilta yrityksiltä eikä hankinnoissa vältetty myöskään uusia yrityksiä ja niiden tarjoamia uusia innovatiivisia ”kokeiluasteellakin” olevia ratkaisuja. Nyt kansallinen kehitys on johtanut keskitettyihin hankintaorganisaatioihin Tiera ja Hansel. Nämä ovat byrokratisoituneita ja toiminta perustuu provisioon, joka kerätään hankintojen arvosta ilman hankkeisiin sisältyvää substanssiosaamista. Näiden toiminnassa suositaan keskittämistä, suuria yrityksiä ja lopulta hankinnat valuvat usein kansainvälisille ulkomaalaisille toimijoille. Suomalaisten yritysten asiakasreferenssien saamista rajoittaa vielä enemmän yrityksille asetetut korkeat liikevaihtorajat, laajat referenssivaatimukset sekä monimutkaiset puitesopimusjärjestelyt. Käytännössä uusien yritysten mahdollisuudet saada julkisten hankintojen kautta referenssiasiakkaita vaikeutuvat koko ajan. Tämä on huolestuttavaa kehitystä, kun sitä verrataan 1990-luvulle julkisen sektorin hankintapolitiikkaan, jossa joustavuus mahdollisti kokeilemisen, paikallisuuden, suomalaisuuden sekä mahdollisuuden olla se ensimmäinen asiakas, luoden uuden mahdollisuuden lukuisille yrityksille ja ensimmäisille onnistuneille toimituksille.

Kansallisesti kyberturva-alan kilpailukyky on liitoksissa koko maan tapaan luoda kasvua. Suomea tulisi johtaa päämäärätietoisesti kansainvälistymiseen sekä yritysten kilpailukyvyn parantamiseen. Suomalainen kyberala on vielä kilpailukykyinen alana maailmalla mutta tälläkin alalla on nähtävissä samoja haasteita kuin laajemmin muuten Suomessa. Mikäli näitä huomattavia rakenteellisia muutoksia ei toteuteta nopeasti ja määrätietoisesti, tulee myös kyberalan kilpailukyky heikkenemään ja tämä erittäin lupaava sektori menettää ”tuhannen taalan” mahdollisuuden.

Osaamisen kehittäminen

Lopuksi kyberalan yksi merkittävä haaste on myös osaamisvaje. Osaajia on maailmalla vähän ja niistä on kova kilpailu. Nyt Suomessa ei ole riittävästi alan koulutusta tarjolla. Maassa tulisi panostaa alan koulutukseen huomattavasti lisää, uusia professuureja sekä aloituspaikkoja eri koulutustasoille. Alalle olisi luotava myös uuden tyyppistä koulutusta joka olisi lähempänä työelämää ja hyvin paljon enemmän soveltavaa kuin monet muut IT painotteiset opinnot. Kyberosaaminen vaatii laajaa kokemuspohjaa. Alalle tarvitaan uutta soveltavaa koulutusta yliopistollisen lisäkoulutuspanostuksen lisäksi. Kansallisesti tarvitaan myös lisää erityisesti kryptografian osaamista, datan analysointiin liittyvää osaamista sekä soveltavaa matemaattista kykyä. Yritykset tarvitsevat myös osaajia heti, johon koulutukselliset panostukset eivät riitä, vaan alan osaajien saamiseksi on palkattava tekijöitä ulkomailta myös EU:n ulkopuolta. Tälle on luotava tarveperusteista joustavuutta. Nyt alan osaajia koulutetaan paljon Aasiassa josta osaajille tulisi luoda joustavammat mahdollisuudet hakeutua Suomeen alalle töihin.

5 Vahvuudet kansainvälisillä markkinoilla

Suomessa kyberturvallisuusstrategia julkaistiin 2013 vuoden alussa. Strategia oli kattava ja se oli yksi maailman selkeimmistä kuvauksista kyberkapasiteetin kehittämiseen liittyvistä tarpeista. Kybermaailman muutokset ovat kuitenkin nopeita ja panostukset kyberkyvykkyyksien kehittämiseen ovat olleet useissa maissa valtavia.

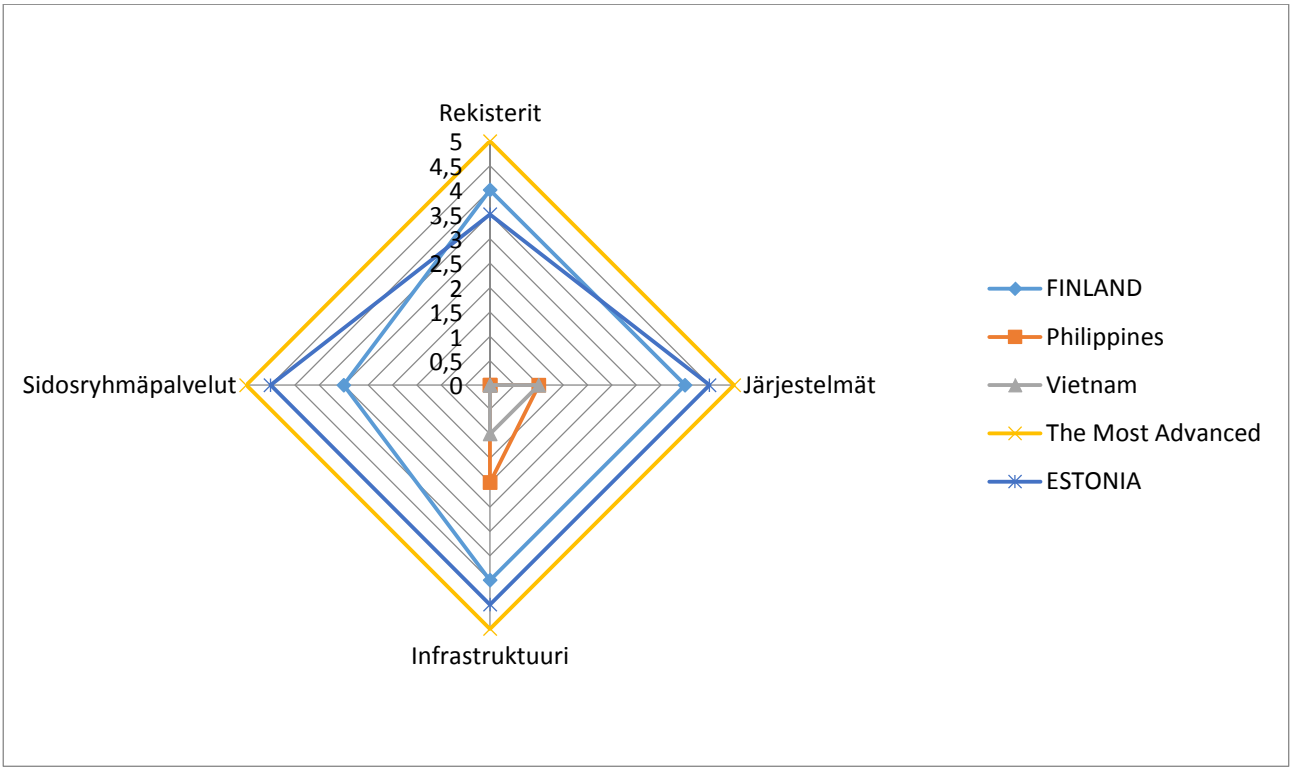
Koko kyber-domainia leimaa globaalisti kilpavarustelu joka muistuttaa toisen maailmansodan jälkeistä tilannetta ydinaseissa. Ydinase oli pelote maailman politiikassa, ja kenellä oli ydinasetekniikkaa hallussaan, saivat osallistua neuvottelupöytiin. Kyber-domainissa maat rakentavat kapasiteettia suojautumiseen ja hyökkäämiseen. Välineet vaihtelevat lainsäädännöstä psykologiseen toimintaan joka leviä trollien myötä mediassa, sosiaalisessa mediassa sekä tuettuna kyber-hyökkäyksin.

Tämä on johtanut maailmanlaajuiseen luottamuspulaan. Valtioiden välillä ei ole luottamusta. Tämä taas on johtanut painostukseen, jossa yrityksiä on vaadittu toteuttamaan tuotteisiinsa takaportteja sekä heikompaa tietoturvaa.

Suomi on maana onnistunut olemaan liittoutumattomana ja suomalaiset tunnetaan maailmalla luottamuksesta. Kyber-maailmassa Suomen luottamuspääoma on suurin mahdollisuus. Suomessa yritykset eivät rakenna takaportteja eikä Suomen valtio vaadi takaportteja suomalaisiin tuotteisiin.

Tämä viesti yhdistettynä laajaan ja laadukkaaseen kyberturvatarjontaan mahdollistaa suomalaisen alan teknologia levittämisen erityisesti kehittyville markkinoille. Jo nyt maailmalta on näyttöä siitä, että solidaarisen avun mukana tuotettuja ratkaisuja sekä tuotteita tietoturvaan ja kyberturvaan on väärinkäytetty.

Suomalainen tietoturvan tarjonta soveltuu hyvin kehittyville markkinoille. Se on luotettava vaihtoehto ja suomalaisella alan osaamisella ja teknologialla voidaan toteuttaa maalle eSocienty palveluiden kokonaisuus mikä on turvallinen ja toimiva maan digitalisoimiseksi. Suomalainen alan teollisuus ja julkiset referenssit yhdessä ovat lukuisissa kehittyvissä maissa suuri mahdollisuus johon tulee nyt panostaa. Alan kehitys on nopeaa ja luottamus on pääomaa. Tulevaisuudessa valtapoliittinen maailman jakautuminen saattaa muuttaa tilannetta, mutta tällä hetkellä maat haluavat rakentaa kilpailukykyisen ja riippumattoman digitaalisen yhteiskunnan fyysisen yhteiskunnan rinnalle.



Kaaviokuva perustuu kappaleessa 1.1.3 kuvattuun ja tässä selvityksessä luotuun arviointitapaan yhteiskunnallisten sähköisten palveluiden kehittymisasteesta.

Suomi on hyvin lähellä yhteiskunnallisesti maailman kärkeä. Viro ja osin muut Pohjoismaat saavuttavat Suomen tai ovat joillakin osa-alueilla Suomea edellä. Toisaalta muissa Pohjoismaissa sekä Virossa ei ole tietoturvan ja kyberturva-alan yrityksiä tuottamassa tarjontaa kansainvälisille markkinoille. Tämä tarjoaa vielä toistaiseksi suomalaisille yrityksille pienen kilpailuedun.

5.1 Vietnam

Vietnam on juuri juhlinut 40 vuotta sodan päättymisestä. Maan talous on rahoitettu nousuun merkittävässä määrin ulkomaisin sodan jälkeisin avustuksin. Kehitysavun ja ”softloan”-rahoituksen arvo on ollut 7-8 miljardia vuodessa. Vietnam jakautuu tänä päivänä vahvasti FDA (Foreign Developing Aid) hankkeisiin ja täysin kaupallisiin hankkeisiin. Muutos on ollut merkittävä, sillä vielä vuosikymmen aiemmin, maassa oli hyvin vähän yksityisiä pääomia käytettävissä. Nyt merkittävä osa liiketoiminnoista on puhtaasti kaupallista ja maassa on huomattavasti pääomia hankkia yrityksille sekä maalle tarpeellisia tuotteita ja ratkaisuja ulkomailta. Kehitysapu on ollut hyvin poliittista ja siihen liittyy tehottomuutta ja korruptiota. Nämä rakenteet ovat samalla vääristäneet hintatasoa sekä myös avointa kilpailua. Vietnamissa on 100 miljoonaa ihmistä, saman verran mobile liittymiä ja 30 miljoonaa internet liittymää. Maan bruttokansantuote on 171 Miljardia US dollaria ja vuotuinen kasvu noin 5.5%.

Suomalainen tieto- ja kyberturva ovat tarjonnaltaan ja sisällöltään kilpailukykyistä Vietnamin kaupallisille markkinoille. Maassa on kohtuullinen osaaminen tietotekniikasta

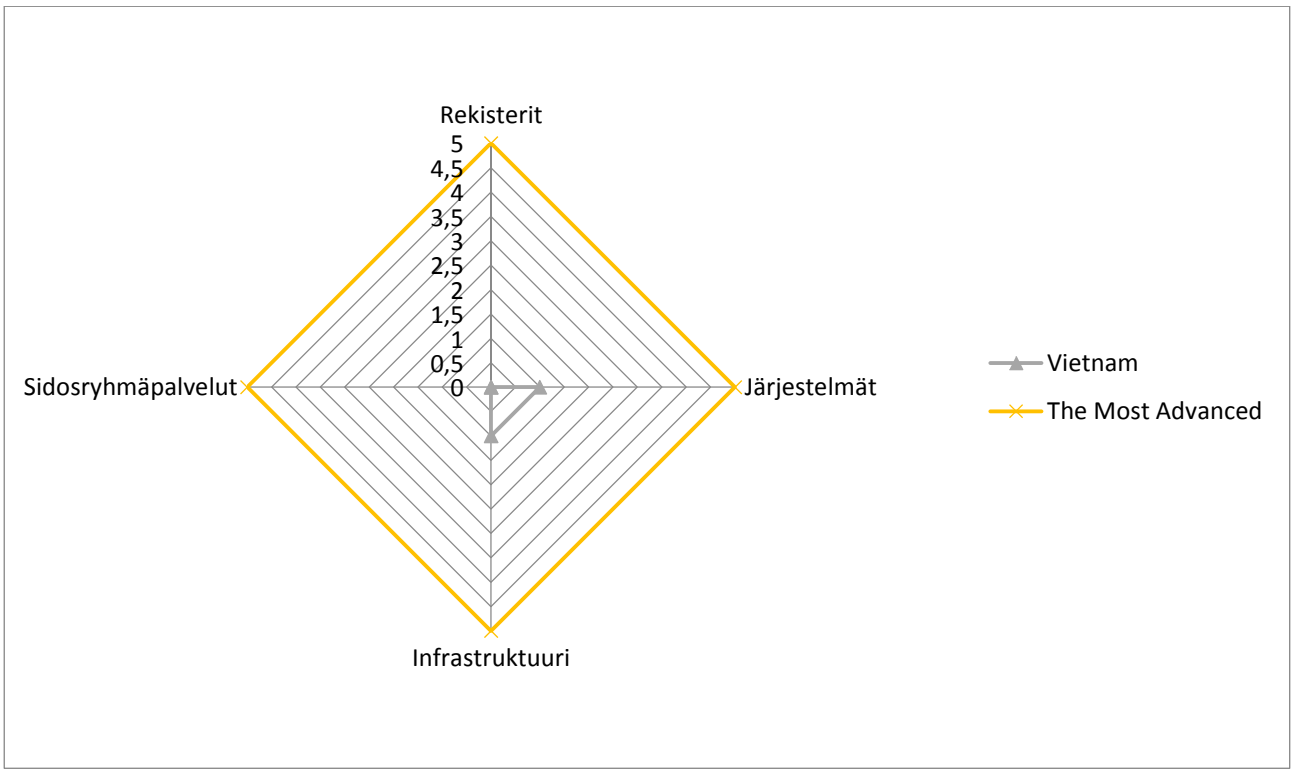
ja maassa on läsnä paljon globaaleja ICT alan yrityksiä. Alalle valmistuu yhdeksästätoista yliopistosta ja oppilaitoksesta noin 4 000 osaajaa nelivuotisella koulutuksella vuosittain. Tietoturvan merkitys on kasvanut ja siihen erikoistumista on ollut kahdessa yliopistossa, jota on laajennettu nyt neljään ja tulevaisuudessa kuuteen oppilaitokseen. Tietoturva on luokiteltu yhdeksi tärkeimmistä osa-alueista maan ICT kehityksessä. Tähän vaikuttaa alueella vallitseva poliittinen tilanne. Kiina ja Intia ovat kybersodassa suurvaltoja muihin alueella oleviin valtioihin nähden ja Tyynellämerellä on lukuisia aluekiistoja joista merkittävimmät johtuvat öljyesiintymien omistusoikeuksista kuten ”Spratly Island” jakamisesta. Lisäksi Kiinan ja Vietnamin välisellä maarajalla on ollut parin viime vuosikymmenen aikana rajaloukkauksia sekä ampumavälikohtauksia. Nämä konfliktit ovat siirtyneet verkkoon ja Vietnam on jatkuvasti ulkovalloista tulevien DDos hyökkäysten kohteena sekä systemaattisten haittaohjelmien ja muun internet häirinnän kohteena. Vietnamissa ei ole kyvykkyyksiä torjua näitä uhkia ja koko tilanteeseen odotetaan nopeasti uutta osaamista ja ratkaisuja.

Vietnam nopean talouskasvun siivittämänä tarjoaa paljon liiketoimintamahdollisuuksia myös erityisesti tietoturva- ja kyberturvaratkaisuille. Maan perusinfrastruktuurissa on paljon kehitettävää. Sähkön tuotanto on riittämätöntä ja sähköverkon luotettavuudessa on merkittäviä puutteita. Puhelin- ja tietoliikenneverkko toimii hyvin suurkaupungeissa, mutta siirryttäessä suurkaupunkien ulkopuolelle kattavuus heikkenee nopeasti. Yhteiskunnallisesti sähköisten palveluiden kehitys on joukko suunnitelmia ja muutamia alueellisia kokeiluja. Palvelutarjonta on pääosin verkkosivustoja, joista löytyy tietoja sekä joitakin lomakkeita.

Pankkipalvelut ovat tarjolla vain osalle kansalaisista. Vain pieni osa kansalaisista omistaa pankkitilejä Vietnamissa. Sähköinen maksaminen on kuitenkin käytössä varsin laajasti kaupoissa, ravintoloissa ja hotelleissa suurissa kaupungeissa. Elintasoerot maaseudun ja kaupunkien välillä ovat todella suuria.

Vietnamissa on perinteisen sosialismin jäljiltä paljon uudistussuunnitelmia. Tavoitteet on asetettu valtiollisella tasolla korkealle. Sähköisten palveluiden kehittäminen on valtiohallinnon kehityskohteista korkealla. Valtiohallinnossa yksi korkeimman prioriteetin kehityskohde on kansallisen Security Operation Centerin perustaminen sekä sen ympärille luotavien maan turvallisuutta lisäävien palveluiden ja järjestelmien kehittäminen. Massa tarvitaan myös laajempi kyberturvallisuuden kehittämisen roadmap.

Vietnamissa suunnitellaan lukuisien rekistereiden sähköistämistä. Tällä torjuttaisiin korruptiota sekä muita yhteiskunnallisia epäkohtia. Ensimmäisenä sähköistyssuunnitelmassa on kansalaisrekisteri, johon liitettäisi PKI-pohjainen tunnistaminen, maarekisterit sekä kiinteistöjen hallintarekisterit. Näiden hankkeiden kehittämisestä Suomessa on paljon kokemusta ja tämä tarjoaisi suomalaisille alan yrityksille paljon mahdollisuuksia. Hankkeissa voitaisiin soveltaa Suomessa opittuja hyviä käytäntöjä, joissa maamme julkinen sektori voisi olla referenssinä ja yritykset toteuttajina. Rekistereiden ja tunnistusjärjestelmän luominen vaatii huomattavasti tietoturvaosaamista, jota suomalaisista tietoturva-alan yrityksistä löytyy.



Vietnam on hyvin alkutaipaleella eSociety palveluiden tarjonnassa. Rekistereiden sähköistäminen on vasta suunnitteella (taso =0), Järjestelmäkehityksessä muutamat lomakepalvelut toimivat (taso =1), verkkoyhteydet ovat pääosin suojaamatta käytössä (taso = 1) sekä sidosryhmille rakennettavat palvelurakenteet puuttuvat kokonaan (taso =0). Tulokset perustuvat Vietnamin Ministry of Communicationin esittämiin arvioihin 9.3.2015 tapaamisen yhteydessä.

Muiden sähköisten palveluiden kehittäminen on riippuvainen kansallisista perusrekistereistä. Kansallisesti tavoitellaan jatkossa terveyden huollon kansallista ”KELA”-tyyppistä rakennetta jossa olisi sähköinen terveysvakuutusrekisteri.

Vietnam tarjoaa lukuisia mahdollisuuksia tietoturva-alan yrityksille, tarvetta olisi digitalisten palveluiden sekä tietoturvan yhteistarjonnasta. Lisäksi tarvetta on jatkuvalle kouluttamiselle ja osaamisen kehittämiselle. Pankkisektorilla tarvitaan kehittyneempiä ratkaisuja jotta myös sähköinen maksaminen olisi verkkopalveluissa mahdollista. Vietnam tarjoaa hyvä markkinan suomalaiselle tietoturva-alan viennille turvallisten e-Society palveluiden kohdalla.

Yhteiskunnallisesti Vietnam tarvitsee selkeän suunnitelman digitaalisuuden hyödyntämiseksi ja se ei ole mahdollista ilman erittäin kustannustehokkaita ja markkinoille soveltuvia tieto- ja kyberturvaratkaisuja. Tämä luo vahvan mahdollisuuden osallistua Vietnamin julkisten palveluiden sekä sitä tukevien yksityisten palveluiden kehittämiseen.

Maan rekistereiden sähköistäminen on alulla ja maahan on suunnitella kansalaisten tunnistamisjärjestelmä. Tämä avaisi lukuisia hyviä mahdollisuuksia huomioiden suomalaisten hyvän maineen ja pitkän läsnäolon markkinoilla kehitysapuyhteistyön kautta.

Lisäksi kansallisesti halutaan parantaa verkkoturvallisuutta, jossa erityisesti ollaan halukkaita luomaan turvallisuutta kriittisen infrastruktuurin sähköisten palveluiden luomiseksi. Näihin tarpeisiin löytyy Suomesta lukuisia mahdollisuuksia joissa kansalliset toteutukset voivat olla vahvoja ja uskottavia referenssejä.

5.2 Filippiinit

Filippiinit on Kaakkois-Aasian nopeimmin kasvava markkina-alue, jossa bruttokansatuotteen kasvu lähentelee 7% vuodessa (= 7.2% 2013). Maa on hyvin vastakkainen Vietnamille poliittisesti. Maa on kapitalistisin yhteiskunta Aasiassa. Maa perustuu pääosin yksityisten yritysten palvelutuotantoon. Maa on saanut vahvasti vaikutuksia USAsta. Maan sähkönjakelu, terveydenhuolto sekä tiestöjen rakentaminen ovat pääosin yhteiskunnan vastuulla, Filippiineillä näitäkin sektoreita hallitsee liike-elämä. Maan merkittävin yrityskenttä jakautuu kahdenkymmenen valtasuvun käsiin. Osa suvuista on espanjalaistaustaisia ja osa kiinalaistaustaisia. Kullakin varakkaalla suvulla on oma laaja liike-elämän klusteri ulottuen lukuisille toimialoille. Maan sisäinen kilpailu perustuu usein kahden kolmen suvun kilpailuun kullakin toimialalla. Esimerkkinä telesektori jolla toimii kaksi operaattoria Globe ja Smart. Näiden omistus jakautuu kahdelle kilpailevalle valtasuvulle. Maasta löytyy satoja pankkeja ja jokaisella valtasuvulla on omansa. Maan talous on lähes kaksi kertaa Vietnamin kokoinen 272 miljardia dollaria vuodessa. Maassa on varsin laaja keskiluokka, joka keskittyy erityisesti suurkaupunkeihin Metro-Manilaan sekä Cebun. Filippiinien suurin vientituote on ihmiset. Filippiiniläisiä työskentelee ympärimaailmaa 6-8 miljoonaa siirtotyöläistä jotka lähettävät säännöllisesti ulkomaista valuuttaa maahan. Tämä on aikaansaanut merkittävää aivovuotoa ulos maasta ja myöhemmin siirtotyöläisten palatessa huomattavaa kokomusta ja osaamista maahan takaisin.

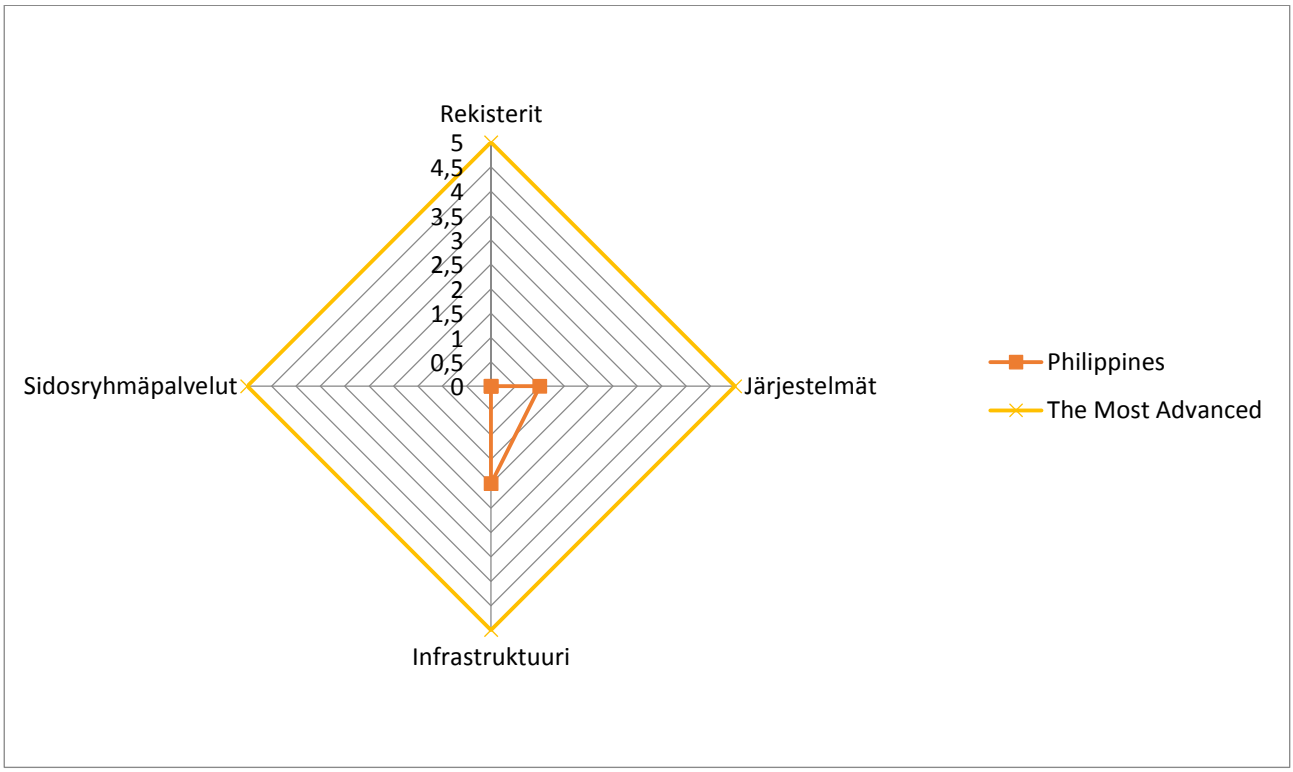
Suomalainen tieto- ja kyberturva ovat tarjonnaltaan ja sisällöltään hyvin kilpailukykyistä Filippiinien kaupallisille markkinoille. Filippiinit haluaa erottua vahvasti IT *(=Information Technology)* ja BMP *(=Business Process Management)* keskittymänä. Filippiinit kilpailee nyt hinta ja osaamistasollaan Intian kanssa ja maa houkuttelee jatkuvasti uusia suuryritysten palvelukeskuksia: puhelinpalvelu, asiakaspalvelutuki, kirjanpito sekä muilla palveluosaamisilla. Lisäksi IT alihankinta ja ohjelmistokehitysosaaminen ovat kasvussa. Maassa on läsnä laajasti globaaleja IT alan yrityksiä. Toimijat tulevat pääosin USAsta ja Japanista. Alemman ja ylemmän yliopistotason valmistuneita tulee markkinoille noin 500 000 vuodessa, josta noin 70 000 ovat ICT:n alaan osaksi tai täysin keskittyneitä. Tietoturvaan erikoistuvia valmistuu vuosittain tuhansia, tarkkaa määrää ei pysty arvioimaan, kun maassa koulutus toimii laajasti yksityiskoulussa. Näissä ohjelmat ja opiskelumallit vaihtelevat paljon.

Maan sähköisten eSociety palveluiden tarjonta on täysin olematonta. Rekisterit ovat hajallaan maakunnissa ”Provinceissa”. Sähkön saanti on heikkoa ja pääkaupunkiseudun ulkopuolella on usein sähkökatkoja. Lisäksi Filippiinit on sijainniltaan erittäin myrskyaltis ja maaperä on vulkaaninen. Maassa on paljon maanjärjestyksiä, tulivuorten purkauksia sekä vuosittain maahan iskee kymmeniä voimakkaita trooppisia myrskyjä aiheuttaen sähkön jakelulle ja tietoliikenteelle

huomattavia vaurioita. Maan tietoliikenneverkot ovat huonossa kunnossa. Jopa pääkaupunkiseudulla matkapuhelimet toimivat epäluotettavasti tukiasemakapasiteetin riittämättömyydestä johtuen. Jokaisella kansalaisella on matkapuhelin, mutta langallinen internet-liittymä melko harvinainen. Pankkisektori on laaja mutta pankkien palvelut ovat hyvin rajallisia vielä. Tavalliset Filippiiniläiset eivät käytä pankkeja vaan operoivat käteisellä.

Korteilla maksaminen on mahdollista kaupungeissa laajasti kauppakeskuksissa, ravintoloissa sekä hotelleissa. Yksityinen sektori on rakentanut vahvan ketjurakenteen kaikille palvelusektoreille. Kauppakeskuksia sekä ketjujen palveluita löytyy lähes kaikista suuremmista kaupungeista.

Muuten yhteiskunnallisten palveluiden kehittäminen on vasta suunnittelupöydällä. Yksi maan tärkeimmistä tavoitteista on luoda Vietnamin tavoin kansallinen identiteettirekisteri johon liittyisi kansallinen tunnistaminen. Tällä hetkellä kansalaisten syntymätodistukset hajautuvat kylien ja kaupunkien maistraatteihin ja niissä arkistoituihin mappeihin. Yksin oman passin hakeminen vaatii paljon papereita ja rajatonta jonottamista. Filippiineillä on valtavasti autoja, joiden rekistereiden sähköistäminen on toinen maan korkean prioriteetin eSociety hanke.



Filippiinit on hyvin alkutaipaleella eSociety palveluiden tarjonnassa kuten Vietnaminkin. Rekistereiden sähköistäminen on vasta suunnitteella (taso =0), Järjestelmäkehityksessä muutamat lomakepalvelut toimivat (taso =1), verkkoyhteydet ovat osin suojaamatta ja osin suojattuna käytössä (taso = 2) sekä sidosryhmille rakennettavat palvelurakenteet puuttuvat kokonaan (taso =0). Nämä arviot perustuvat Filippinien valtion Board of Investmentin esittämiin arvioihin 12.3.2015 tapaamisen yhteydessä.

Nämä maat ovat hyviä esimerkkejä joita vastaavissa kehitystilanteissa on suurin osa maailman maista tänä päivänä.

Filippiineillä on nyt huomattava kasvuboomi käynnissä. Maan perusinfrastruktuuri uudistuu nopeasti ja maa on saamassa kansainvälistä rahoitusta maailmanpankista näiden rakenteiden uudistamiseksi. Nyt maa on toteuttamassa digitalisoinnin masterplaniä jonka tekemiseen olisi hyvä suomalaisten osallistua ja näin varmistaa myös suomalaisten osallisuuden, kun suunnitelmaa aletaan toteuttaa. Filippiinit on luomassa kyberturvan ja digitaalisuuteen kansallista lainsäädäntöä sekä siihen liittyviä palveluita. Nyt kansallisessa budjetissa on varattu n. 36 miljoonaa dollaria sähköiseen kansalaisrekisteriin. Nyt kansalaisuus perustuu syntymätodistukseen, jota ylläpidetään eri kylien ja kaupunkien maistraateissa. Rekisterit ovat hyvin eritasoisia ja palveluiden laatu vaihtelee alueittain. Kotona syntyneet lapset saatetaan joskus jopa rekisteröidä vasta kun lapset ovat menossa kouluun. Kokonaisuuteen suunnitellaan myös tunnistusjärjestelmää hyvin vastaavilla tekniikoilla kuin VRK:ssa Suomessa.

Lukusien kehitystarpeiden kautta suomalaisilla yrityksillä on paljon tarjottavaa näihin hankkeisiin. Suomessa voitaisiin kansallisesti suunnitella Filippiineille erillinen valtion takaama lainaohjelma, jota voitaisiin hyödyntää alan kasvun aikaan saamiseksi sekä viennin helpottamiseksi.

Suomalaisilla yrityksillä on myös lukuisia mahdollisuuksia yksityisellä sektorilla Filippiineillä. Filippiinien yhteiskunta toimii hyvin laajasti yksityisten palveluiden varassa. Energia, Telecom, Finanssi, Terveydenhuolto sekä Vesi tuotetaan yksityisten yritysten avulla ja näillä yrityksillä on paljon tarpeita ja myös pääomaa tarjoten alan suomalaisille yrityksille paljon uusia liiketoimintamahdollisuuksia.

Suomalainen tarjonta olisi hyvä vaihtoehto nykyisten vahvasti amerikkalaisten yritysten vaihtoehdoksi.

5.3 Suomalaisen kilpailutekijät ja panostukset tarkastelluille markkinoille

Filippiinit on nopeimmin kasvava ja Vietnam maailman yksi nopeimmin kasvavista markkinoista maailmassa. Kummassakin maassa on suuria haasteita kyberturvallisuuden sekä yhteiskunnallisten eSociety-palveluiden rakentamisessa.

Kyberturvallisuuden mahtimaat: USA, Kiina, Israel sekä Venäjä ovat markkinoilla ja esimerkiksi kiinalaisten suuret investoinnit mutta samalla valtiolliset hyökkäystoimet kybermaailmassa herättävät luottamuspulaa molemmilla markkinoilla. USA sekä Israel on tunnettuja maita ja niistä tulevat yritykset löytyvät Gartnerin Magic Quadrantin listoilta, joten ratkaisut ovat levittäytyneet investointikykyisimpien yritysten käytössä. Markkinat ovat kuitenkin hyvin alkupisteessä ja mahdollisuuksia on paljon tarjolla. Aasiassa kaupankäynnin perustana ovat suhteet ja luottamus. Yrityskohtaisten tai valtiolle toimitettavien ratkaisujen myynnissä on oltava henkilökohtaisessa suhteessa etabloitumisessa markkinoille sekä palveluille tarjottava paikallinen tuki on merkityksellistä.

Suomalaisuuden vahvuuksia ovat luottamus, innovatiivisuus, insinöörimäisyys sekä Nokian alueella luoma maine. Suomalaiselle kyberturvatuotteille ja palveluille on

olemassa markkinapaikka näissä maissa. Yritystemme pienuus sekä tuntemattomuus ratkaisusta ovat suurimpia haasteita.

Suomessa on rakennettu hyviä kansallisia eSociety palveluita, joille on kysyntää myös Vietnamissa ja Filippiineillä. Ratkaisut on kuitenkin saatava koottua paremmin, sillä ostolistalle ne eivät tule mitenkään päätymään ilman kokonaisvaltaisempaa ja kootumpaa tarjontaa. Näille alueille pitää pystyä luomaan laajemmin suomalaisia ratkaisuja ja palveluita edustava verkosto, jossa on riittävä määrä paikallisia kumppaneita sekä malli jolla pienemmät alan yritykset voisivat olla läsnä markkinoilla. Markkinoilla olo ja paikallisuus ovat samoja haasteita jotka vaikeuttavat laajemmin suomalaisen PK-yrityksen kansainvälistymistä.

Filippiinit ja Vietnam ovat nyt etsimässä kasvun tueksi vaihtoehtoisia kilpailukykyisempiä ratkaisuja joita nykyisellään on markkinoilla tarjolla. Suomalainen tunnistaminen, roolien hallinta ja IAM-ratkaisut sopisivat laajasti molemmille markkinoille. Lisäksi tarvetta olisi SOCien perustamiselle, osaamisen lisäämiselle koulutuksen sekä paikallisten palveluiden kehittämiselle. HaVaRon malli Suomesta sopisi laajemminkin markkinoille, ei vain kansalliseen käyttöön, mutta myös yritystasolle suurimpiin pankkeihin, operaattoreille sekä jopa jatkossa infrastruktuuripalveluihin.

Suuri tarve on ”Master Planille” tai ”Roadmapille” jolla joko yritys tai valtiohallinto voisi edetä kyberturvallisesti ja taloudellisesti digitaalisuuteen. Tilanne muistuttaa 1990-luvun kasvuboomia, kun perusinfrastruktuurin kehittäminen ja huomattavat investoinnin alkoivat massiivisesti Kaakkois-Aasiassa.

Suomessa tulisi valtion olla myötävaikuttamassa nyt alan kansainvälistämistä. Painopisteeksi tulisi valita tapa, jolla Suomesta saataisiin kehittyville markkinoille lukuisissa maissa käytettävä referenssitapa, jossa Suomen valtio tukee kphdemaan kansallisten ”Road Mapien” tekemistä ”Free Consulting” idealla ja tarjoaa ”Road Mapien” toteuttamiseen korkotuettuja lainoja joihin liittyy vahvasti sidos hankkia teknologiaa ja palveluita Suomesta.

Kybermarkkinat ovat nopeassa kasvussa ja ylivoimaisesti suurimmat useiden kymmenien prosenttien kasvulukemat saavutetaan mm. Granderin mukaan seuraavan viiden vuoden aikana erityisesti Aasiassa. Suomalaisen alan viennin kannalta on kiire toimia ja saada jalansija näillä markkinoilla kasvattaen tunnettavuutta, läsnäoloa sekä aloittamalla myös valtiohallinnon tehotoimet viennin lisäämiseksi ja yritysten onnistumisen tueksi.

6 Johtopäätökset ja toimenpidesuositukset

Suomessa on kansainvälisesti kilpailukykyistä osaamista sekä kyberturvan tuotteissa että palveluissa. Ala työllistää jo merkittävän määrän suomalaisia ja kasvaa markkinoiden yleisestä kutistumisesta huolimatta. Suomen neutraali asema on lisäksi etu, joka auttaa suomalaisen kyberturvan markkinoinnissa maailmalla nykyisten vakoiluskandaalien keskellä. Alakotiaset erityiskehitysideat ovat esitetty kappaleessa 4.

Lisäksi Suomi on hyvissä asemissa e-Society –palveluiden kehittämisessä ja käytössä. Suomen vakiintunut yhteiskuntajärjestelmä, pitkät etäisyydet ja kehittynyt mobiiliteknologia antavat erittäin hyvät edellytykset ja toisaalta pakottavat myös jatkossa panostamaan e-Society –hankkeisiin.

Suomalaisilla yrityksillä ja julkisilla organisaatioilla on hyvää osaamista nämä alueet yhdistävistä hankkeista. Osaamisalue tarjoaa erinomaisen mahdollisuuden synnyttää uutta kansainvälisesti kilpailukykyistä osaamista ja työpaikkoja mm. toimivan Private-Public-Partnership eli yksityisten ja julkisten toimijoiden yhteistyöllä.

Suomalaisilla tietoturva-alan yrityksillä on esimerkiksi seuraavia tuotteita ja osaamista, joita voitaisiin hyödyntää e-Society-hankkeissa:

- Turvallinen kirjautuminen
- Identiteetinhallinta
- Turvalliset tietovarastot
- Virustorjunta
- Tilannekuvajärjestelmät
- Tietoturvatestaus ja konsultointi

Hankkeita, joissa näitä voitaisiin hyödyntää ovat mm.

1. Sähköinen äänestäminen sekä kansalaisten osallistuminen päätöksentekoon
2. Terveydenhuollon hankkeet
    a. Potilastiedot
    b. Arkistot
    c. Asiointipalvelut
    d. Online-terveydenhuolto
    e. Ennaltaehkäisevä terveysneuvonta/terveysportaalit
3. Viranomaispalvelut
    a. Poliisi
    b. Tulli
    c. Verottaja
    d. Kansallinen kyberturvallisuus
    e. ym.
4. Rekisterit ja avoimen datan hankkeet
    a. Väestörekisteri
    b. Kiinteistörekisteri
    c. ym.

Lisäksi mm. seuraavia keinoja tarvittaisiin e-Society –alueen tietoturvayritysten liiketoiminnan edistämiseksi:

6.1 Määrätietoiset julkiset kehityshankkeet

Suomalaista alan yritystoimintaa tukevat parhaiten Suomessa toteutettavat e-Society hankkeet. Parasta olisi, jos hankkeet olisivat kunnianhimoisia ja kokeilevia. Myös epäonnistumisia pitää sietää, jotta voidaan oppia ja luoda uusia, kilpailukykyisiä tuotteita. Samalla hankkeiden lopputuloksissa olisi myös tarkasteltava jatkuvuutta, jotta ratkaisuilla olisi myös mahdollisuuksia kansainvälistymiseen. Tätä näkökulmaa ei voi enää nykyisessä taloudellisessa tilanteessa sivuttaa.

Julkisten hankintojen tulisi painottua tuoteratkaisujen käyttöön, jotta suomessa syntyisi monistettavaa osaamista. Samalla kaikki tutkimustyö tulisi olla asiakaslähtöistä jossa tavoiteltava lopputulos olisi aina tulossa ”asiakkaan hyödyksi” ja mihin julkisen sektorin asiakkuus toisi arvokkaan referenssin kansainvälistymisen tukemiseen

Julkisen sektorin ei tulisi kerätä tai tuottaa itselleen IPR-oikeuksia, vaan ainoastaan riittävät käyttöoikeudet käyttämiinsä tuotteisiin ja asiakaskohtaisiin ohjelmistoihin.

6.2 Lainsäädäntö

Uber ja Airbnb ovat esimerkkejä palveluista, jotka mullistavat kokonaisia liiketoiminnan aloja. Kun taksien tilausjärjestelmä tehdään maailmanlaajuiseksi käyttäen valtavia kehityspanoksia, sitä vastaan ei kannata kilpailla yksittäisen kaupungin tai edes maan tasolla. Sen sijaan kannattaa lähteä kehitykseen mukaan ja etsiä mahdollisuuksia toteuttaa lisäpalveluja tai innovoida seuraavan sukupolven ratkaisuja. Itse kulkevien autojen hallintajärjestelmä voi sisältää myös suomalaista insinööriosaamista.

Näiden ja muiden vastaavien palvelujen leviämistä pitäisi pyrkiä edistämään myös lainsäädännön avulla, jotta Suomi pysyy kehityksen eturintamassa. Lainsäädännössä tulisi vähentää säännöstelyä painottaen uudistumisen mahdollisuuksia. Viro on hyvä esimerkki, jossa lainsäädäntö tukee vahvasti uudistumista, innovointia, kasvua ja yrittäjyyttä. Tämä on ainoa keino varmistaa, että Suomessa syntyisi jatkuvasti uusia innovatiivisia palveluita seuraavan digitaalisuuden aallon kärkeen jossa kyberturvallisuus on erittäin tärkeä mahdollistaja palveluiden syntymiselle.

6.3 Koulutus

Tietoturva-alalle tarvitaan jatkuvasti uusia osaajia. Alalla työllistyvät parhaiten erityisosaajat, jotka pystyvät sopeutumaan jatkuvasti muuttuvaan ympäristöön ja teknologiaan. Koulutus pitäisi siksi pyrkiä järjestämään yhdessä yritysten kanssa ja sen pitäisi sisältää tietoturvayrityksissä tarvittavaa osaamista kuten soveltavaa kyberosaamista sekä matemaattisia taitoja kuten kryptografiaa. Koulutuksen on oltava dynaamisesti uudistuvaa, kyberala kehittyy päivittäin, joten koulutus ei voi perustua pitkäaikaissuunnitelmiin vaan ohjelmat ja painotukset on kyettävä muuttamaan joustavasti jopa vuosittain.

6.4 Rahoitus aloittaville yrityksille

Aloittavilla yrityksillä on jatkuvasti ongelmana rahoituksen puute. Mm. Tekes tekee Suomessa erittäin tärkeää työtä aloittavien yritysten rahoittamisessa. Lisää panostuksia kuitenkin tarvitaan, jotta lupaaville alueille saataisiin syntymään onnistumisia ja sitä kautta kansainväliset startup-rahoittajat kiinnostuisivat Suomesta.

Aloittavien yritysten koulutus ja neuvonta rahoituksen hakemisessa on myös erittäin tärkeää. Lisäksi kansallisiin tutkimusohjelmiin tulisi luoda jatkossa ”tilaaja – toimittaja” malli jossa tutkimusohjelman tulokset päätyvät konkreettisesti tilaajalle käyttöön ja tutkimusohjelmaan osallistuvat tahot saavat kokemusta verkottuvasta yhteistyöstä. Samalla saadaan nopeammin markkinoille soveltuvia ratkaisuja, joilla on jo olemassa ”asiakasreferenssi” mikä on perus edellytys kansainvälistymiselle.

6.5 Rahoitus pidemmälle ehtineille yrityksille

Alkuvaiheen jälkeen yrityksille tulee vastaan valintatilanne, jossa ne voidaan joko myydä tai jatkaa toimintaa itsenäisenä. Myynti on usein ainoa ratkaisu, joka varmistaa riittävät pääomat yrityksen kehittämiseen seuraavaan vaiheeseen. Tämä johtaa usein ratkaisujen valumisen ulkomaisiin käsiin ja useissa tapauksissa myös työpaikat siirtyvät maan rajojen ulkopuolelle. Kasvurahoitukseen ja kansainvälistymiseen ei ole Suomessa pääomaa juuri tarjolla. Tämä on kriittinen vaihe 5-10 vuotta toimineelle yritykselle, jolla on rahoitusta vaativaa tuotekehitystä tai huomattavampaa pääomitusta vaativaa kansainvälistymistä. Suomessa tulisi luoda kokonaan uusia rakenteita yritysten pääomittamiseen ja löytää aktiivisia ja tehokkaista tapoja siirtää suomalaisten pääomia myös pienempiin yrityksiin.

6.6 Verotus

Tulevaisuudessa Suomessa tulisi rakentaa pääomasijoittamisessa kotimaisiin start-up:eihin kunnia-asia kuten urheilusankaruus. Uusiin yrityksiin sijoittavat saisivat verotuksellisesti erityisetua vaikkapa Exitin yhteydessä. Sama malli tulisi toteutua kaikkia voittoja kotiutettaessa, jolloin osakkeiden tai omaisuuden myyntivoitosta ei verotettaisi siltä osin kun niitä sijoitettaisiin kasvuyrityksiin. Tapoja näille toimille voisi olla lukuisia, esimerkiksi rahastot tai eläkesäästömallit, joita on toteutettu Suomessa.

6.7 Työvoimakustannukset

Tämä lisäksi tarvitsemme joustavampia tapoja työllistää yrityksissä. Työvoiman sivukustannukset sekä palkkarakenteet ovat liian kankeita. Ne eivät sovellu tulevaisuuden kansainvälistyvään kilpailuun. Työntekijä – työnantaja jaottelu on vanhanaikaista ja jokaisen tulisi muuttua ”yrittäjähenkiseksi ihmiseksi” miettien miten minun panokseni voisi olla jatkossa merkityksellisempi työnantajalleni ja samalla saavutettaisiin lopputulos jossa oma ja muiden työpaikka olisi varmemmalla pohjalla. Nyt työpaikkaa pidetään jokaisen oikeutena Suomessa. Vastaavasti maailmalla tehdään valintoja siitä, mistä maasta työtä kannattaa hankkia vaikuttaen tulevaisuudessa kokonaisiin toimialoihin työpaikkojen sijaintimaina. Meidän on kyettävä luomaan malli, jossa tavoitellaan kokonaisvaltaista menestystä yhdessä.

Yrityksissä on panostettava ilmapiiriin jossa työntekijät ovat osana kokonaisuutta tavoitellen yhdessä yrityksen ”työnantajansa” kanssa menestystä. Meidän on kyettävä luomaan kansallinen ilmapiiri rakentavaksi, yhteistyöhenkisemmäksi, jossa leivotaan suurempaa kakkua, josta on yhä enemmän jaettavaa kuin jakamalla kakku ennekuin se on edes leivottu. Palkkarakenteiden tulisi kyetä joustamaan heikkoina aikoina alas ja vastaavasti hyvinä aikoina onnistumisesta palkittaisiin. Nyt yrityksen ajautuessa taloudellisiin vaikeuksiin, ratkaisuna on vain irtisanominen. Periaatteenamme on se, että kun irtisanotaan 1 niin 9 saa jäädä ja pitää kiinni saavuttamistaan edusta, kun malli voisi olla se, että jokaisen palkkoja lasketaan 10% ja kaikki voisivat tsempata yhdessä pahimman yli. Ei tulisi työttömyyttä ja kokonaisvaltaisemmin olisimme kilpailukykyisempiä, tuottaisimme yhtä paljon pienemmällä kustannuksella. Vastaavasti menestymisestä tarjottaisiin korkeampia palkkoja yrityksen tuloskyvyn mukaisesti.

6.8 Kansainvälistymisen tukeminen

Kyberturva-alan yritykset ovat keskimäärin pieniä, mutta kasvuhakuisia. Niiden tuotteilla on usein pienet markkinat Suomessa, jolloin kansainvälistyminen on välttämättömyys. Kansainvälistyminen on kallista, jolloin tarvittaisiin resursseja alan yritysten auttamiseen kansainvälistymisen alkuun. Tarvetta on kaikesta yllä mainitusta kuten pääomasta ja osaavasta työvoimasta. Kansainvälistyminen tuo vielä lisänä sen, että osaamisen ja pääoman tarve ja käyttötarkoitukset lisääntyvät.

Yritysten perustukimuodot kuten Tekesin tuotekehitystuet eivät mahdollista yrityksen rahoittamista kansainvälistymisen mahdollistamiseksi. Kansainvälistymisrahoitukseen tulisi luoda kokonaan uusia malleja jotka toimisivat hyvin lähellä operatiivista kansainvälistymistä. De minimis ehtojen asettaminen EU:ssa on johtanut hyvin suuriin haasteisiin yritystoiminnassa. Ne koskevat EU:n alueelle kohdistuvaa kilpailua ja viranomaiset käyttävät siihen liittyviä rajoitteita varmuuden vuoksi vaikka hankkeet kohdistuisivat 100% EU:n ulkopuolelle. Vastaavasti meidän kilpailijamaat toimivat juuri päinvastoin ja yrittävät tulkita kaiken siten, ettei tukitoimille olisi rajoitteita.

Koko kansallinen kansainvälistymiseen tähtäävä toiminta tulisi rakentaa tehokkaammaksi ja operatiivisemmaksi. Esimerkiksi Finpron kanssa toimiminen on yritysten näkökulmasta hyvin vaikeaa, kun rajanvedot ja palveluiden sisältö on epäselvää. Koko Team Finlandin toiminta tulisi muodostua operatiivisemmaksi jossa luodaan konkreettisesti verkostoja kaupan ja vientitulojen aikaansaamiseksi. Team Finlandin kautta voitaisiin kehittää tiiviimpiä verkostoja, joiden kautta pyrittäisiin suoraviivaisesti kansainvälistymiseen ja kaupan kasvattamiseen. Kohdemaihin tulisi saada jatkossa yhä ”myyntihenkisempiä” henkilöitä joiden tehtävänä olisi rakentaa asiakasverkostoja erityyppisille suomalaisille yrityksille ja panostamalla erityisesti uusien innovatiivisten yritysten tuotteiden ja ratkaisujen markkinoille saamiseen.

Samalla valtion luomien rahoitusinstrumenttien tulisi erityisesti jatkossa mahdollistaa viennin edistämiseen sekä kansainvälisten asiakasreferenssien hankkiminen.

7 Menestyksekkäitä eSociety-palveluita Suomessa

Maailmalla Viro pidetään digitalisoitumisen edistysmaana. Maan presidentti on vahvasti myymässä digalisuuden maabrändiä. Viroa listautuu maailman 4. mielenkiintoisemmaksi sijoituskohteeksi stratup-maailmassa. Viro tekee paljon uusia asioita, kuten ohjelmistokehittämisen opiskelun tuominen ala-asteelle, kaikille oppilaille, ekansalaisuus avoimesti kaikille maailmassa sekä XRoad. Ekansalisuus, on kuitenkin hyvä myyntivaltti joka todellisuudessa ei tarjoa mitään, mutta herättää huomiota, ihastusta sekä kiinnostusta.

Viro on malli esimerkki siitä, kuinka Suomessa olisi pitänyt toimia jo 2000-luvun alusta alkaen. Viro käyttää esimerkkeinään malleja joita on pääosin kopioitu Suomesta ja ne on vain yhdistelty keskitettyyn yhden pisteen asiointiportaaliin.

Valitettavasti Suomessa puuttuu myynti osaamista, uskallusta markkinoinnista, rohkeutta kansainvälistymään sekä tukea toisiamme verkostona näiden päämäärien aikaansaamiseksi.

Seuraavassa kuvataan eSociety-palveluita jotka osittavat Suomen kansallisia vahvuuksia. Näiden kehityksen perusta pohjautuu vahvasti tietoturvaosaamiseen sekä suomalaiseen palvelukehityksen osaamiseen (näitä palveluita on analysoitu myös tässä hankkeessa):

Verottajan asiointipalvelut: http://www.vero.fi/fi-FI/Asioi_verkossa

Suomessa kaikki verotukseen liittyvät asiat voidaan hoitaa verkossa.

Tullin palvelut: http://www.tulli.fi/fi/yrityksille/sahkoinenasiointi/internet/index.jsp

Tullaus onnistuu lähes kaikessa verkon kautta ja jopa ulkomailta hankittavat tuotteet verkkokaupoista voidaan tullata verkossa taaten tavaroiden helpon kotiin toimituksen.

KELA:n laaja palvelutarjonta: http://www.kela.fi/

Monipuolinen asiointi verkossa mahdollistaa lähes kaikki elinkaaripalvelut kansalaisille sekä myös yrityksille.

Kansallinen tunnistaminen:
https://www.suomi.fi/suomifi/tyohuone/yhteiset_palvelut/verkkotunnistaminen_ja_maksaminen_vetuma/

https://www.fkl.fi/teemasivut/sahkoinen_asiointi/tupas/Sivut/default.aspx

Suomessa on jo 1990-luvun loppupuolelta lähtien ollut käytössä vahva sähköinen tunnistus lukusiin palveluihin.

Kattavat finanssipalvelut: https://www.pohjola.fi/

Vakuuttaminen ja pankkiasiointi hoituvat lähes kaikilta osin verkossa ja palvelutarjonta on laajaa kaikilta maassa toimivilta pankeilta ja vakuutusyhtiöiltä.

Reseptipalvelut: http://www.kanta.fi/

Lääkereseptit ja kansalaisen terveystiedot ovat keskitetysti sähköisessä palvelussa. Reseptien uusiminen sekä useat terveydenhoitopalveluihin liittyvät hallintoasiat ovat sähköisesti kansalaisten ulottuvilla.

Kunnat tarjoavat kattavasti sähköistä asiointi:
https://asiointi.hel.fi/wps/portal/asiointi/

Lähes kaikki kuntalaispalvelut alkavat olla sähköistettyjä suurimmissa kaupungeissa ja kunnissa. Koulut, lastenhoito, terveydenhuolto, rakentaminen sekä muut kuntalaispalvelut ovat keskitetysti saatavilla.

Yrityksen perustaminen: https://www.prh.fi/fi/index.html

Yrityksen perustaminen onnistuu verkossa ilman yhtään lähetettyä lomaketta. Samoin onnistuu tuotemerkkien rekisteröinti sekä patenttiehakeminen.

Asuntojen pohjakuvat löytyvät sähköisesti: https://asiointi.hel.fi/arska/

Maarekisterit: http://www.maanmittauslaitos.fi/aineistot-ja-palvelut

Maarekisterit ja kiinteistöihin liittyvät kartat ja palvelut on koko maata kattavasti saavilla.

Kyberturvallisuuspalvelut: https://www.viestintavirasto.fi/kyberturvallisuus.html

Lisäksi kansallisen kyberturvakeskuksen palvelut tarjoavat laajasti tukea ja turvallisuutta verkkoasiointiin kansallisesti.

Kansallinen huoltovarmuuskeskus: http://www.huoltovarmuuskeskus.fi/

Tarjoaa kriittisen infrastruktuurin ylläpitämiseen ja kehittämiseen kokonaisvaltaista palvelua.

eSociety - palvelutarjonta on Suomessa kattavaa ja monipuolista. Tämä olisi liitettävä yhdeksi kansallisen kilpailukyvyn peruspilariksi. Ei Suomessa tarvita välttämättä XRoad:ia ja 200 miljoona investointia sen levittämiseksi vaan Suomessa on jo realisoituna sähköisen asioinnin yhteiskunnallisia hyötyjä kattavasti. Olisi huomattavasti edullisempaa ja tuottavampaa käyttää näitä jo kehitettyjä palveluita kansallisina referensseinä maailmalla uusia ideoita myytäessä, yrityksiä kansainvälistettäessä sekä sijoituksia houkuteltaessa Suomeen. Ei meidän kannata kehua Viron erinomaisuutta vaan tunnistaa oma erinomaisuutemme ja hyödyntää sitä täysimääräisesti kaikessa.