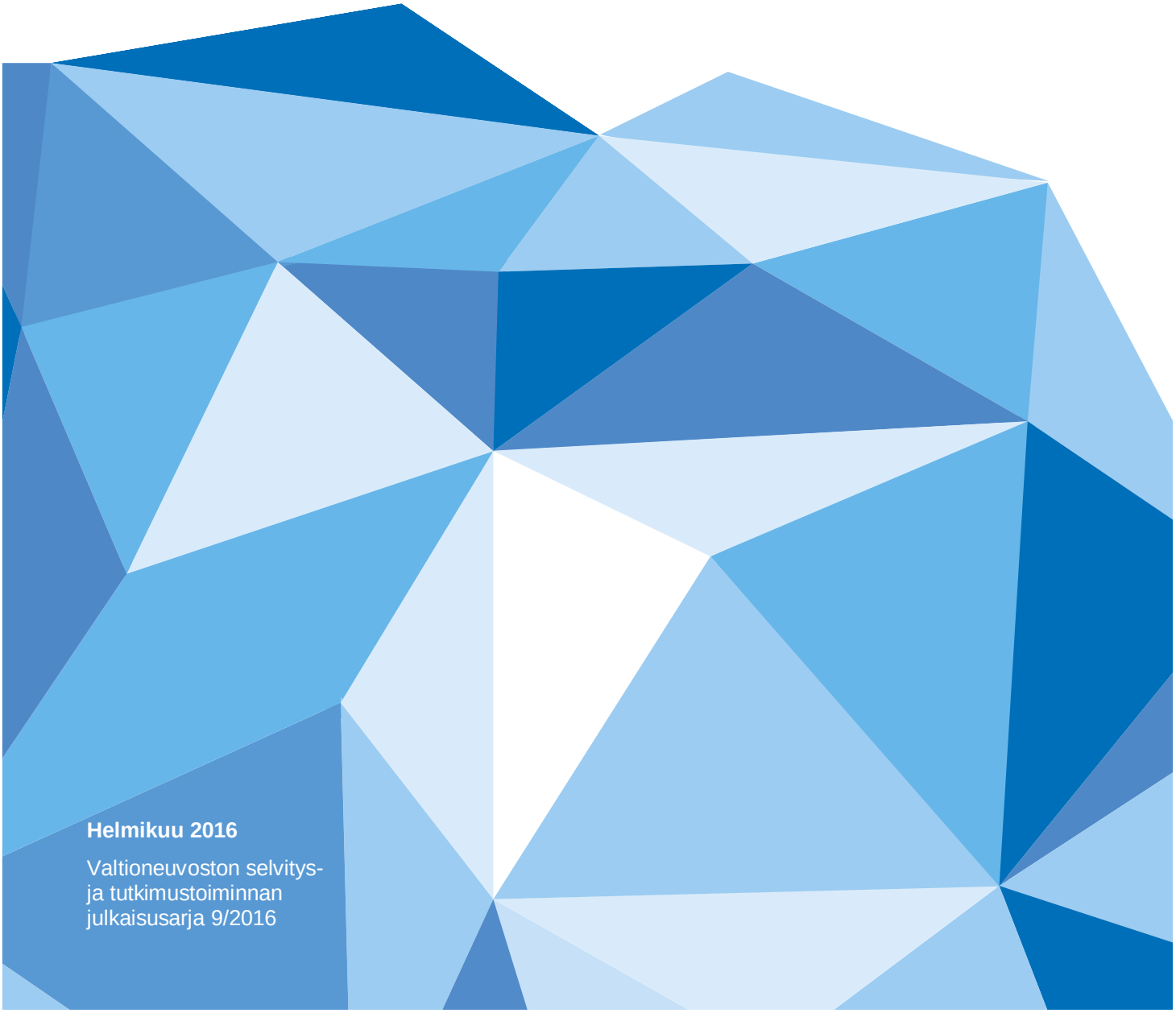
VALTIONEUVOSTON
SELVITYS- JA TUTKIMUSTOIMINTA

Antti Pelkonen, Toni Ahlqvist, Anna Leinonen, Mika Nieminen, Jarno Salonen, Reijo Savola, Pekka Savolainen, Arho Suominen, Hannes Toivanen, Jukka Kyheröinen & Juha Remes

Kyberosaaminen Suomessa –
Nykytila ja tiekartta tulevaisuuteen



Helmikuu 2016

Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2016

KUVAILULEHTI

Julkaisija ja julkaisuaika	Valtioneuvoston kanslia, 15.02.2016
Tekijät	Antti Pelkonen, Toni Ahlqvist, Anna Leinonen, Mika Nieminen, Jarno Salonen, Reijo Savola, Pekka Savolainen, Arho Suominen, Hannes Toivanen (Teknologian tutkimuskeskus VTT) & Juha Remes, Jukka Kyheröinen (Cyberlab)
Julkaisun nimi	Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen
Julkaisusarjan nimi ja numero	Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2015
Asiasanat	Kyberosaaminen, kyberturvallisuus, tietoturva, tietoturvallisuus, Suomi
Julkaisuaika	Helmikuu, 2016 **Sivuja** 90 **Kieli** Suomi

Tiivistelmä

Tässä tutkimuksessa tarkastellaan kyberosaamisen nykytilaa ja tulevaisuuden näkymiä Suomessa. Kyberosaamisella tarkoitetaan kyberturvallisuuteen liittyvää tutkimus-, kehitys- ja innovaatiotoimintaa. Raportissa analysoidaan suomalaisten yritysten, korkeakoulujen, ja tutkimuslaitosten kyberturvallisuuteen liittyvä tutkimustoimintaa, alan koulutusta, innovaatio- ja kehitystoimintaa sekä julkisen hallinnon roolia ja alan yhteistyön tilaa. Lisäksi siinä käsitellään Suomen vahvuuksia ja heikkouksia kyberturvallisuusosaamisessa sekä osaamisen puutteita ja kapeikkoja. Kansallisen tarkastelun ohella tutkimuksessa nostetaan esiin muutamia kansainvälisiä edelläkävijämaita (Hollanti, Viro, Israel), joita vastaan suomalaista kehitystä voidaan peilata.

Kyberosaamisen tulevaisuutta tarkastellaan kybertoimintaympäristön muutoksen ja tulevaisuuden kehitystarpeiden näkökulmista. Raportissa luodaan tulevaisuuskuva Suomen kybertoimintaympäristön kehityksestä 10 vuoden aikajänteellä sekä kolme tiekarttaa, jotka kuvaavat siirtymää nykytilasta kohti tavoitetilaa.

Tutkimus osoittaa, edellytykset kyberturvallisuusosaamisen ja -alan kehittämiselle ovat Suomessa hyvät. Suomessa on korkeatasoista kyberturvallisuuteen liittyvää tutkimus-, kehitys- ja innovaatiotoimintaa ja -osaamista. Vahvuuksia on sekä yrityskentällä että korkeakouluissa ja tutkimuslaitoksissa. Alan osaamispohja on kuitenkin varsin kapea ja kärkiosaaminen keskittyy varsin harvoille toimijoille. Osaaminen myös hajaantuu laajaan joukkoon organisaatioita ja toimijoiden välinen yhteistyö on vasta kehittymässä. Selkeitä osaamisen kapeikkoja ja puutteita on muutamalla osaamisalueella. Viime vuosina alan kansainvälinen kilpailu on myös kiristynyt ja Suomessa tarvitaan määrätietoisia toimenpiteitä kyberturvallisuusosaamisen edelleen kehittämiseksi. Alan yhteistyötä tulee tiivistää ja esimerkiksi julkisia hankintoja hyödyntää alan osaamisen vahvistamisessa. Raportissa esitetään toimenpidesuositusten kokonaisuus joka tähtää suomalaisen kyberturvallisuusosaamisen vahvistamiseen ja nostamiseen edelläkävijämaiden tasolle.

Tämä julkaisu on toteutettu osana valtioneuvoston vuoden 2014 selvitys- ja tutkimussuunnitelman toimeenpanoa (tietokayttoon.fi).

PRESENTATIONSBLAD

Utgivare & utgivningsdatum	Statsrådets kansli , 15.2.2016		
Författare	Antti Pelkonen, Toni Ahlqvist, Anna Leinonen, Mika Nieminen, Jarno Salonen, Reijo Savola, Pekka Savolainen, Arho Suominen, Hannes Toivanen (Teknologiska forskningscentralen VTT) & Juha Remes, Jukka Kyheröinen (Cyberlab)		
Publikationens namn	Cyberkompetens i Finland – Nuläge och färdplan för framtiden		
Publikationsseriens namn och nummer	Publikationsserie för statsrådets utrednings- och forskningsverksamhet 9/2015		
Nyckelord	Cyberkompetens, cybersäkerhet, datasäkerhet, informationssäkerhet		
Utgivningsdatum	Februari, 2016	**Sidantal** 90	**Språk** Finska

Sammandrag

Denna undersökning granskar nuläget inom och framtida utsikter för cyberkompetensen i Finland. Med cyberkompetens avses forsknings-, utvecklings- och innovationsverksamhet i anslutning till cybersäkerhet. Rapporten analyserar finländska företags, högskolors och forskningsinstituts forskningsverksamhet i anslutning till cybersäkerhet samt utbildning, innovations- och utvecklingsverksamhet inom området, den offentliga förvaltningens roll liksom situationen när det gäller samarbetet inom området. Dessutom behandlar rapporten Finlands styrkor och svagheter inom cybersäkerhetskompetens samt brister och flaskhalsar i kompetensen. Utöver en nationell granskning lyfter undersökningen fram några internationella föregångsländer (Holland, Estland, Israel), som den finländska utvecklingen kan jämföras med.

Framtiden för cyberkompetens granskas utifrån en förändrad cybermiljö och framtida utvecklingsbehov. Rapporten skapar en framtidsbild av utvecklingen i Finlands cybermiljö under en 10-årsperiod samt tre färdplaner som beskriver övergången från nuläget mot ett önskat mål.

Undersökningen visar att Finland har goda förutsättningar att utveckla cybersäkerhetskompetensen och cybersäkerhetssektorn. Finland har högklassig forsknings-, utvecklings- och innovationsverksamhet i anslutning till cybersäkerhet. Det finns styrkor såväl inom företagssektorn som inom högskolorna och forskningsinstituten. Kompetensbasen inom området är emellertid rätt smal och spetskompetensen är koncentrerad till rätt få aktörer. Kompetensen är också utspridd på en stor grupp organisationer, och samarbetet mellan aktörerna håller först på att utvecklas. Det finns tydliga flaskhalsar och brister i kompetensen inom några kompetensområden. Under de senaste åren har den internationella konkurrensen inom området också blivit hårdare och det krävs målmedvetna åtgärder i Finland för att vidareutveckla cybersäkerhetskompetensen. Samarbetet inom området bör bli intensivare och till exempel offentlig upphandling bör utnyttjas i arbetet med att stärka kompetensen inom området. Rapporten presenterar ett paket med åtgärdsrekommendationer som syftar till att stärka cybersäkerhetskompetensen och lyfta den till samma nivå som hos föregångsländerna.

Den här publikation är en del i genomförandet av statsrådets utrednings- och forskningsplan för 2014 (tietokayttoon.fi).

DESCRIPTION

Publisher and release date	Prime Minister's Office, 15.2.2016
Authors	Antti Pelkonen, Toni Ahlqvist, Anna Leinonen, Mika Nieminen, Jarno Salonen, Reijo Savola, Pekka Savolainen, Arho Suominen, Hannes Toivanen (VTT Technical Research Centre of Finland Ltd.) & Juha Remes, Jukka Kyheröinen (Cyberlab)
Title of publication	Cyber security competencies in Finland – Current state and roadmap for the future
Name of series and number of publication	Publications of the Govenrment´s analysis, assessment and research activities 9/2015
Keywords	Cyber security competence, cyber security, data protection, information security, Finland
Release date	February, 2016 **Pages** 90 **Language** Finnish

Abstract

This study examines the current status and future projections of cyber security competence in Finland. Cyber security competence refers to research, development and innovations relating to cyber security. The report analyses the cyber security research of Finnish businesses, universities and research institutions, cyber security education, innovation and development activities, as well as the role of public administration and collaboration within the sector. It also discusses the strengths and weaknesses of Finland's cyber security competencies, as well as knowledge gaps and shortages. In addition to a national analysis, the study highlights a few countries that are leading the international cyber security race (the Netherlands, Estonia, Israel), and against which Finnish development can be mirrored.

The future of Finland's cyber security competencies is approached from the perspectives of the changing cyber security environment and the sector's development needs. The report lays out a prospect for the development of Finland's cyber security environment over the next ten years, as well as three roadmaps for the route from the current situation towards the goal.

The study shows that there is a lot of potential for developing cyber security competencies and the cyber security sector in Finland. The country is already home to some high-quality cyber security research, development and innovation activities and know-how. Strengths can be found both in the business sector and in universities and research institutions. However, the scope of Finland's cyber security know-how is relatively narrow, and there are relatively few top experts. In addition, this know-how is scattered across a vast number of organisations, and partnerships within the sector are underdeveloped. There are obvious knowledge gaps and shortages in a few areas of competence. International competition in the sector has also increased in recent years, and Finland needs to take decisive action to boost its cyber security competencies. Partnerships within the sector need to be deepened, and public procurement contracts, for example, used to increase know-how. The report lists a number of recommendations of measures to strengthen Finland's cyber security competencies and bring the country up to par with international frontrunners.

This publication is part of the implementation of the Government Plan for Analysis, Assessment and Research for 2014 (tietokayttoon.fi).

SISÄLLYS

1. JOHDANTO

1.1 Tutkimuksen tausta ja tavoitteet

Kyberturvallisuus on jo nykypäivänä läpäisevästi läsnä ihmisten arjessa ja sen merkitys korostuu väistämättä lähitulevaisuudessa mm. digitalisaation voimistumisen ja esineiden internetin kehittymisen myötä. Yhteiskunnat ovat yhä riippuvaisempia digitaalisesta ympäristöstä, ja digitalisoituvassa maailmassa tietoliikenteen, palvelujen sekä tietoverkkojen ja -varantojen turvallisuus on yhteiskuntien toiminnan kannalta keskeisen tärkeää. Kyberturvallisuuden ajankohtaisuutta ovat lisäksi viime aikoina korostaneet useat muut seikat, kuten valtioiden yhä voimakkaampi mukaantulo kybermaailmaan, kiihtyvä kamppailu kyberpuolustuksen ja -hyökkäyksen välillä, valtioiden välinen kyberasevarustelu sekä kybermaailman kustannustehokkuus (Limnéll ym. 2014).

Kyberturvallisuuden merkitys näkyy vahvasti myös kyberuhkien ja -riskien kasvuna. Kyberturvallisuusriskeistä on tullut huomattavia niin yritysten liiketoiminnan, julkisen sektorin kuin kansalaisten ja kuluttajien näkökulmasta (esim. PriceWaterhouseCoopers 2014). Suomessa tuoreen tutkimuksen mukaan 84 prosenttia suuryrityksistä koki vuonna 2015 kyberturvallisuuteen liittyvät riskit merkittävinä ja 93 prosenttia yrityksistä arvioi joutuvansa varautumaan kyberriskeihin lähitulevaisuudessa aiempaa paremmin (Nordic Institute of Business & Society ym. 2016).[1] Huomionarvoista myös on, että vuonna 2014 kyberriskit merkittävinä kokeneiden yritysten osuus oli 57 prosenttia, eli kasvu on tässä suhteessa ollut merkittävää. Kysyntä alan ammattilaisille onkin voimakkaassa kasvussa: on arvioitu, että globaalisti seuraavan viiden vuoden aikana kyberturvallisuusosaajien vaje on 1.5 miljoonaa ammattilaista (Frost & Sullivan 2015).

Kyberturvallisuuden taloudellinen merkitys on myös huomattava. Maailmanlaajuisesti se on kasvava toimiala, ja on ennustettu että vuosina 2016-2020 globaali kyberturvallisuusmarkkina kasvaisi vuosittain keskimäärin 12 prosentilla[2] (Technavio 2016; ks. myös Frost & Sullivan 2014). Monet maat investoivatkin vahvasti alalle ja hakevat johtoasemaa. Myös Suomessa on tammikuussa 2013 julkaistussa kyberturvallisuusstrategiassa linjattu, että vuonna 2016 Suomi on kyberturvallisuuden kärkimaa ja ”maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa” (Valtioneuvosto 2013). Uusi strategiatyö, joka keskittyy digitaalisen liiketoiminnan tietoturvallisuuteen, on aloitettu ja siinä visioksi on asetettu, että ”maailman luotetuin digitaalinen liiketoiminta tulee Suomesta” (Liikenne- ja viestintäministeriö 2016).

Suomesta on kuitenkin puuttunut kokonaiskuva kyberturvallisuuteen liittyvän osaamisen tilasta ja tasosta. Onko Suomessa korkeatasoista kyberturvallisuuteen liittyvää tutkimus-, kehitys- ja innovaatiotoimintaa? Mitkä ovat Suomen vahvuudet ja heikkoudet kyberturvallisuuteen liittyvässä osaamisessa? Onko Suomessa puutteita tai kapeikkoja kyberturvallisuusosaamisessa? Entä miten Suomen kyberturvallisuuden toimintaympäristö on muuttumassa ja minkälaista osaamistarpeita muutoksesta seuraa? Tämä raportti pyrkii vastaamaan tähän tiedon tarpeeseen ja näihin kysymyksiin. Raportissa tarkastellaan kyberturvallisuuteen liittyvän osaamisen nykytilaa ja tulevaisuuden näkymiä Suomessa. Kyberosaaminen tulkitaan raportissa erityisesti kyberturvallisuuteen liittyvänä tutkimus-, kehitys- ja innovaatiotoimintana (TKI) ja raportti keskittyy näin ollen yritysten ja tutkimusorganisaatioiden TKI-toiminnan analysoin-

[1] Tutkimuksessa tehtyyn kyselyyn vastasi 109 suomalaista suuryritystä.

[2] Kertyvä vuotuinen kasvuprosentti, compound annual growth rate (CAGR)

tiin. Siten esimerkiksi kansalaisten kyberturvallisuusosaaminen rajautuu tämän raportin tarkastelun ulkopuolelle.

Raportti tarkastelee kyberosaamisen tilaa Suomessa, mutta siinä nostetaan esiin myös muutamia kansainvälisiä edelläkävijämaita, joita vastaan suomalaista kehitystä voidaan peilata. Kansainvälisinä esimerkkeinä kuvataan lyhyesti muutamaa alan johtavaa maata (Hollanti, Viro, Israel). Näissä maissa on panostettu huomattavasti kyberturvallisuuteen viime vuosina, ja ne ovat nousseet kansainvälisessä tarkastelussa kiinnostaviksi maiksi alalla.

Raportissa on kaksi pääjaksoa. Kyberturvallisuusosaamisen nykytilan analyysissä (luku 2) tarkastellaan kyberturvallisuuteen liittyvän tutkimustoiminnan, koulutuksen sekä alan yritysten ja niiden innovaatiotoiminnan tämän hetkistä tilannetta Suomessa. Lisäksi siinä käsitellään julkisen hallinnon roolia kyberosaamisen kehittämisessä sekä alan yhteistyön tilaa. Kyberosaamisen tulevaisuutta käsittelevässä luvussa 3 hahmotetaan kybertoimintaympäristön muutosta ja tulevaisuuden kehitystarpeita. Siinä luodaan tulevaisuuskuva Suomen kybertoimintaympäristön kehityksestä 10 vuoden aikajänteellä sekä kolme tiekarttaa jotka kuvaavat siirtymää nykytilasta kohti tavoitetilaa. Näiden kahden pääluvun jälkeen luvussa 4 luodaan katsaus kansainvälisiin esimerkkimaihin, luvussa 5 käsitellään yhteenvetävästi Suomen kyberosaamisen vahvuuksia ja kapeikkoja, ja luvussa 6 esitetään johtopäätökset ja toimenpidesuositukset.

Raportti perustuu Kyberosaaminen Suomessa: Nykytila ja tiekartta mahdollisuuksien tulevaisuuteen -hankkeeseen jonka toteutti Teknologian tutkimuskeskus VTT yhteistyössä Cyberlab Oy:n kanssa. Hanke käynnistyi joulukuussa 2014 ja se valmistui tammikuussa 2016. Tutkimus on osa valtioneuvoston selvitys- ja tutkimustoimintaa.

Suomen kyberosaamisen nykytilan ja tulevaisuudennäkymien ohella hankkeessa tehtiin selvitys jossa tarkasteltiin kansallisen tutkimustoiminnan kannalta tärkeän tietoteknisen infrastruktuurin sekä eräiden kansallisesti merkittävien digitaalisten tietovarantojen tilaa kyberturvallisuuden näkökulmasta ja niiden suojaamista kyberuhkien varalta. Tämän selvityksen tulokset ovat tämän raportin liitteenä 4.

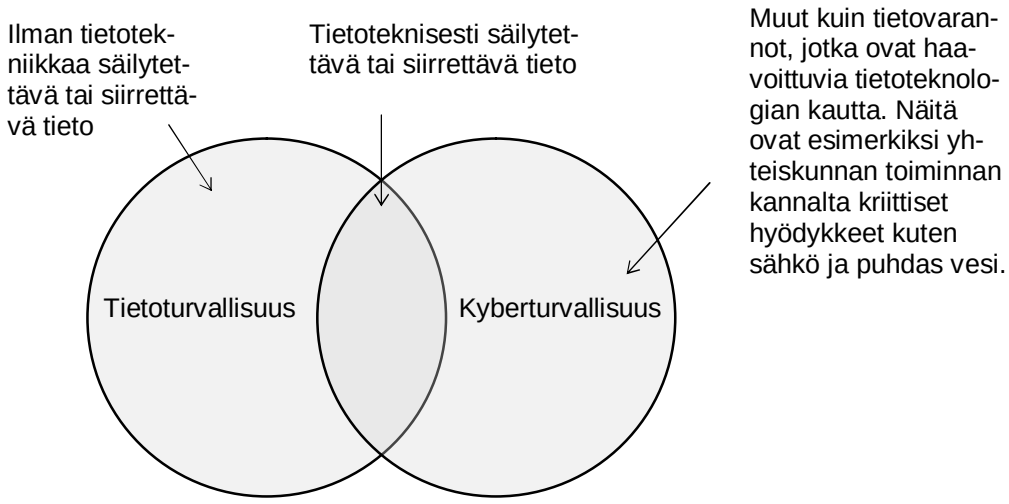
1.2 Mitä kyberturvallisuus ja tietoturva ovat?

Termeille kyberturvallisuus (cybersecurity) ja tietoturvallisuus (information security) on sekä suomen että englannin kielessä lukuisia määritelmiä. ”Kybertoimintaympäristö ja sen turvallisuus on Suomessa kokonaisvaltainen käsite, joka kattaa mm. tietoturvallisuuden, tietoverkkoturvallisuuden ja tietojärjestelmien turvallisuuden.” (Ulkoasiainvaliokunta 2013, Limnéll 2014). Kyberturvallisuudella tarkoitetaan yleisesti tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kybertoimintaympäristö on sähköisessä muodossa olevan informaation käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö, jolle on tunnusomaista elektroniikan ja sähkömagneettisen spektrin käyttö datan ja informaation varastointiin, muokkaamiseen ja siirtoon viestintäverkkojen avulla (Valtioneuvosto 2013).

Suomen kielessä englannin kielen termiä ”information security” vastaa termi ”tietoturvallisuus”. ”Cybersecurity”-termin vastineena käytetään termiä kyberturvallisuus: esimerkiksi (Suomen) kyberturvallisuusstrategia ja (Viestintäviraston) kyberturvallisuuskeskus. Kansainvälisessä tieteellisessä (englanninkielisessä) keskustelussa kyberturvallisuus määritellään

usein tietoturvatavoitteiden – tiedon saatavuus, eheys ja luottamuksellisuus – kautta (ITU 2008). Tämä vastaa yleisesti käytettyä (esim. ISO/IEC 2012, NIST 2013) tietoturvallisuuden määrittelyä.

Suomen kyberturvallisuusstrategia tekee eroa kyberturvallisuuden ja tietoturvallisuuden välille, tietoturvallisuuden tarkoittaessa em. tietoturvatavoitteiden saavuttamisen varmistamista ja kyberturvallisuuden kattaessa laajemmin koko kybertoimintaympäristön turvaamisen (Ulkoasiainvaliokunta 2013, Limnéll 2014). Kansallisessa keskustelussa termi kyberturvallisuus on 2010-luvulla tullut aiemmin käytetyn termin tietoturvallisuus rinnalle. Määritelmällisesti nämä kuitenkin ovat hieman eri asioita. Tarkasti ottaen kyberturvallisuus voidaan ajatella "pelkkää" tietoturvallisuutta laajempana käsitteenä, joka kattaa tietojen ja niitä käsittelevien laitteiden lisäksi myös niitä käsittelevät ja niihin luottavat ihmiset aina yhteiskunnan etuun ja kriittiseen infrastruktuuriin saakka (von Solms & van Niekerk 2013). Käsitteiden välisiä suhteita havainnollistaa alla oleva kaavio (kuva 1.1), missä tieto tarkoittaa tietovarantoja (engl. information assets).



Kuva 1.1. Tieto- ja kyberturvallisuuden suhde (von Solms & van Niekerk 2013. Muokattu.)

Tietoturvallisuuden lyhennemuotoa tietoturva käytetään edelleen vakiintuneesti yhdyssanoissa ja sanaliitoissa, jotka usein viittaavat tietoturvallisuuden saavuttamisen keinoihin: tietoturvatoimenpide, tietoturvaohje. Tietoturva ei ole sama kuin tietosuoja, jolla tarkoitetaan henkilön yksityisyyden (privacy) suojaamista oikeudettomalta tai henkilöä vahingoittavalta käytöltä.

Asiantuntijapiireissä käytetään termiä verkko- ja tietoturvallisuus tarkoittamaan kokonaisturvallisuuden digitaalista näkökulmaa. Erityisesti tämän julkaisun tavoitteena olevan verkko- ja tieto-/kyberturvallisuuden kehittämisen kannalta emme ole rajoittuneet tiettyihin kyberturvallisuuden määritelmiin, vaan esimerkiksi alan tutkimustoiminnan ja kouluttautumismahdollisuuksien osalta olemme kattaneet seuraavat osaamisalueet: laitteiston tietoturva (platform security technology), ohjelmiston tietoturva (software and application security), verkkoturvallisuus (telecommunication and network security), kryptografia (cryptography), virus- ja haittaohjelma-analyysi (malware analysis), fyysinen turvallisuus (physical and environmental security), jatkuvuus ja tietoturvariskien hallinta (risk management and business continuity), tietoturvan johtaminen (cybersecurity management), tietoturvan oikeudellinen sääntely ja tietosuoja (regulatory compliance), tietotekninen rikostutkimus (digital forensics), kyberturvallisuus turvallisuuspoliittisena kysymyksenä, kyberturvateknologia, ja elektroninen sodankäynti.

Kyberturvallisuutta voidaan myös lähestyä määrittelemällä sitä teknologisen ulottuvuuden kautta. Alla oleva käsitekartta (kuva 1.2.) havainnollistaa kyberturvallisuuden teknologioita. Kartta luotiin asiantuntijatyönä osana tämän tutkimuksen julkaisu- ja patenttianalyysiä (ks. tarkemmin liite 3).

Kuva 1.2. Kyberturvallisuuden teknologiat, käsitekartta.

Yllä oleva kartta jakaa kyberturvallisuuden teknologiat seuraaviin 12 osa-alueeseen:

1. Asymmetriset menetelmät: tiedon salauksen menetelmät jotka perustuvat eri avaimen käyttöön viestin salaamisessa ja purkamisessa.

2. Hyökkäysmenetelmät: tietoverkkoihin liittyvät hyökkäysmenetelmät sekä verkkokuunteluun liittyvät teemat.

3. Tietokoneverkot: tietoverkot, erityisesti mobiiliverkot sekä erityyppiset tietovarannot kuten pilvipalvelut.

4. Konfiguraation hallinta: tietoverkkoihin liittyvät hallintakysymykset, kuten tilannetieto ja turvallisuusprosessit.

5. Kriittinen infrastruktuuri: yhteiskunnan toiminnan kannalta kriittiseen infrastruktuuriin liittyvä toiminta.

6. Tulevaisuuden menetelmät: asiantuntijoiden näkemyksen mukaan tulevaisuuden salausteknologioita käsittelevä alue. Nämä teknologiat eivät ole käytössä, mutta osoittavat potentiaali kyberturvallisuuden teknologioina.

7. Identiteetin hallinta: digitaalisen identiteetin hallinta. Tämä luokka siis erotettuna konfiguraation hallinnasta joka keskittyy yrityksen järjestelmiin.

8. Tietojärjestelmät: tietojärjestelmät laajasti ymmärrettynä.

9. Riskien hallinta: uhka-arviot ja heikkouksien tunnistamisen tietojärjestelmässä.

10. Ohjelmistokehitys: ohjelmistotuotanto ja -kehitys

11. Symmetriset menetelmät: tiedon salauksen menetelmät jotka perustuvat saman avaimen käyttöön viestin salaamisessa ja purkamisessa.

12. Muut: luokka jossa on eksplisiittisesti käsitelty kyberturvallisuutta, mutta sen sisältö ei ole sisällytetty mihinkään muista mainituista luokista..

1.3 Aineistot ja menetelmät

Hankkeessa kerättiin hyvin monipuolinen ja laaja-alainen aineisto. Keskeisimmät aineistokokonaisuudet ovat avaintoimijoiden haastattelut, kyselyt kyberturvallisuusalan yrityksille ja tutkijoille, työpajat, erilaiset kyberturvallisuusalaa ja -tutkimusta kuvaavat tilastot ja tietokantatiedot sekä dokumenttimateriaali.

Hankkeen alkuvaiheessa haastateltiin alan avaintoimijoita yritysten, julkisen hallinnon ja tutkimusmaailman piiristä. Yhteensä haastateltiin 21 henkilöä. Haastattelujen tarkoituksena oli luoda yleiskuvaa kyberturvallisuusosaamisen ja -alan tilanteesta Suomessa. Haastattelujen teemat käsittelivät alan tutkimustoimintaa, yritysten tilannetta, julkisen sektorin roolia, yhteistyötä sekä osaamisen vahvuuksia ja mahdollisia puutteita. Haastattelut nauhoitettiin yhtä haastattelua lukuun ottamatta ja ne litteroitiin. Lista haastatelluista henkilöistä on liitteessä 1.

Tarkempaa kuvaa alan tilanteesta pyrittiin saamaan kahdella laajalla kyselyllä jotka suunnattiin yrityksille ja alan tutkijoille. Yrityskyselyn pääkohdejoukkona olivat kyberturvallisuuden tuotteita ja palveluja ydinliiketoimintanaan tuottavat yritykset Suomessa. Näiden yritysten lisäksi vastaajien joukossa on tietotekniikka- ja tietoliikennealan yrityksiä joiden liiketoiminnasta osa liittyy tieto- ja kyberturvallisuuteen. Yritysten identifioinnissa käytettiin pohjatietona Suomen tietoturvaklusteri FISC ry:n jäsenyrityksiä, jonka lisäksi yrityksiä identifioitiin tutkijaryhmän ja ulkopuolisten asiantuntijoiden avulla. Kysely lähetettiin 151 yritykselle, joista 61 yritystä vastasi. Vastausprosentti oli 40, jota voidaan pitää varsin korkeana yrityskyselyissä. Kyselyssä selvitettiin yritysten liiketoiminnan tilaa ja suuntautumista, innovaatiotoimintaa, yhteistyöverkostoja sekä näkemyksiä kyberturvallisuusalan tilanteesta ja osaamispohjasta Suomessa.

Kyberturvallisuusalan tutkimus- ja koulutustoimintaa selvitettiin kyselyllä joka suunnattiin alan tutkijoille yliopistoissa, tutkimuslaitoksissa ja ammattikorkeakouluissa. Vastaajajoukko muodostettiin siten, että alkuvaiheessa tutkijaryhmä koosti listan alan tutkijoista oman tietämyksensä pohjalta. Tätä alustavaa listaa täydennettiin käymällä yliopistojen, tutkimuslaitosten ja ammattikorkeakoulujen verkkosivuja läpi ja etsimällä sieltä tutkijaryhmiä ja alan tutkijoita.

Kyselystä tehtiin myös englanninkielinen versio, sillä ei-suomenkielisiä tutkijoita oli kohdejoukossa yli 20 henkilöä. Kysely lähetettiin 180 tutkijalle, joista 77 henkilöä vastasi. Vastausprosentti oli 43. Kyselyllä kartoitettiin alan tutkijoiden ja tutkimusryhmien tutkimuksen suuntautumista, koulutusta, resursointia ja organisoitumista, rahoitustilannetta, yhteistyötä sekä näkemyksiä kyberturvallisuusalan ja -tutkimuksen tilanteesta ja osaamispohjasta Suomessa.

Näiden kahden laajemman kyselyn lisäksi hankkeen loppuvaiheessa tehtiin lyhyt täydentävä kysely julkisen hallinnon kyberturvallisuusasiantuntijoille. Kysely käsitteli kyberturvallisuusosaamisen aukkoja ja puutteita Suomessa. Kysely lähetettiin 41 asiantuntijalle, joista 19 vastasi.

Hankkeen aikana järjestettiin kolme tulevaisuusorientoitunutta työpajaa, jotka toimivat pääaineistona kyberosaamisen tulevaisuutta tarkastelleessa osiossa. Työpajat järjestettiin toimijaryhmäkohtaisina tilaisuuksina siten, että yrityksille ja elinkeinoelämälle, tutkimustoimijoille sekä julkiselle hallinnolle ja viranomaisille järjestettiin kullekin ryhmälle oma työpaja. Työpajoissa rakennettiin Suomen kyberturvallisuusalan tulevaisuuskuva ja tiekartta ryhmätöinä. Luvussa 3 on kuvattu tulevaisuusosion toteutusta tarkemmin. Lista työpajoihin osallistuneista asiantuntijoista on liitteessä 2.

Erilaisia tilastoaineistoja hyödynnettiin monipuolisesti. Keskeisen tilastoaineiston muodostivat tiedejulkaisu- ja patenttiaineistot, joiden avulla selvittiin suomalaisten tutkijoiden ja yritysten julkaisu- ja patentointitoimintaa kyberturvallisuuden alueella. Tiedejulkaisuaineisto käsittää ISI Web of Science -tietokannan tiedejulkaisut, joissa on mainittuna suomalainen organisaatio kirjoittajan tutkimusorganisaationa. Patenttiaineisto koostuu Yhdysvaltain patenttiviranomaiselle rekisteröidyistä patenteista joissa on keksijän maakoodina Suomi. Sekä patentit että tutkimusjulkaisut on rajattu ajalle 1995-2013, jota voidaan pitää tutkimuksen tekohetkellä luotettavana aineistona. Käytetty aineisto koostuu yhteensä 16 393 patentista ja 169 438 tiedejulkaisusta. Tarkempi kuvaus patentti- ja julkaisuanalyysin aineistosta ja käytetystä menetelmästä on liitteenä 3.

Muita tilastoaineistoja olivat kyberturvallisuuteen liittyvän tutkimus- ja kehitystoiminnan rahoitustilastot, joita saatiin Tekesistä ja Suomen Akatemiasta. Alan yritystoimintaa kuvaavia tilastoja (esim. liikevaihto, työntekijämäärä, patentit jne.) saatiin Orbis-tietokannasta.[3] Alan innovaatioista on haettu tietoja VTT:n SFINNO™ suomalainen innovaatio -tietokannasta. Tietokanta sisältää noin 6 600 suomalaista kaupallistettua innovaatiota vuosilta 1945-2013 (SFINNO™-tietokannasta, ks. tarkemmin Van der Have et al. 2009).

Olemassa olevaa dokumenttiaineistoa on hyödynnetty soveltuvin osin siinä määrin kuin relevanttia materiaalia on ollut saatavilla. Keskeistä dokumenttiaineistoa ovat olleet mm. valtionhallinnon strategiat (esim. Suomen kyberturvallisuusstrategia, Suomen tietoturvallisuusstrategia jne.), aiemmat tutkimukset ja selvitykset (esim. Jyväskylän yliopiston selvitys alan tutkimus- ja koulutustarjonnasta, Lehto & Kähkönen 2015) ja osin esimerkiksi erilaiset kansainväliset vertailut (esim. Global Cyber Security Index jne.).

Kansainvälistä vertailutietoa kerättiin kolmesta maasta: Viro, Hollanti ja Israel. Viron osalta tiedonkeruu oli muita maita laajempaa sillä tutkijaryhmä teki vierailun Tallinnaan Naton kyberturvallisuusosaamiskeskukseen (NATO Cooperative Cyber Defence Centre of Excellence)

[3] Orbis-tietokanta sisältää yritysten taloudellisia tietoja globaalisti noin 180 miljoonasta yrityksestä. Ks. tarkemmin http://www.bvdinfo.com/en-gb/our-products/company-information/international-products/orbis?gclid=CNPUr6OPxcoCFSL4cgodA0MOrQ

marraskuussa 2015 ja haastatteli alan keskeisiä virolaisia toimijoita. Lista Virossa haastatteluista henkilöistä on liitteessä 1. Virossa tehdyissä haastatteluissa peilattiin myös haastateltujen henkilöiden näkemyksiä Suomen kyberturvallisuusosaamisesta. Hollannin ja Israelin osalta tiedot perustuvat dokumenttiaineistoon, Internet-läheisiin sekä Israelin osalta Suomen Israelin suurlähetystöstä saatuihin tietoihin.

Osana tutkimusta Cyberlab Oy teki erillisen liiketoiminta-analyysin joka kohdistui suomalaisten tietoturvayritysten osaamiseen ja kilpailukykyyn eSociety-palvelujen alueella. Tätä selvitystä varten tehtiin omaa tiedonkeruuta (mm. haastattelut, kysely). Liiketoiminta-analyysin raportti on saatavilla hankkeen verkkosivuilta (www.kyberosaaminen.fi) ja sen tuloksia on hyödynnetty osana tätä raporttia ja raportin johtopäätöksiä.

2. KYBEROSAAMISEN NYKYTILA

2.1 Tutkimustoiminta

Kyberturvallisuuteen liittyvä tutkimus on lähtökohtaisesti monitieteistä, mutta sen ytimessä ovat yleisen tietotekniikan, tietojenkäsittelytieteen ja tietoliikenteen tutkimus sekä matematiikka ja laskennallinen tiede (Lehto & Kähkönen 2015; Long & White 2010). Alan tutkimuksessa sekä perustutkimuksella että soveltavalla tutkimuksella on omat vahvat roolinsa. Perustutkimuksellinen ulottuvuus on erityisen vahvaa esimerkiksi kryptologiassa ja sen matemaattisissa perusteissa. Julkisten tutkimusorganisaatioiden ohella yrityksillä on keskeinen merkitys erityisesti soveltavassa tutkimustoiminnassa (ks. esim. Hentea ym. 2006). Tässä luvussa tarkastellaan tutkimustoimintaa erityisesti julkisissa tutkimusorganisaatioissa, kun taas yritysten tutkimus- ja kehitystoimintaa käsitellään luvussa 2.3.

Suomessa kyberturvallisuuteen liittyvää tutkimusta tehdään tällä hetkellä 16 yliopistossa, tutkimuslaitoksessa ja ammattikorkeakoulussa (Lehto & Kähkönen 2015). Lehdon ja Kähkösen (2015) mukaan kyberturvallisuuden eri tutkimusaiheita katetaan laajimmin Jyväskylän yliopistossa, VTT:llä ja Aalto-yliopistossa, joissa kussakin tutkimuksen piirissä on noin 25-30 tutkimusaluetta tai -aihetta.[4] Näiden jälkeen tulevat Tampereen teknillinen yliopisto, Oulun yliopisto, Helsingin yliopisto, Turun yliopisto sekä Maanpuolustuskorkeakoulu ja Puolustusvoimien teknillinen tutkimuskeskus, joissa katetaan noin 7-15 tutkimusaluetta. Julkaisutoiminnan perusteella alan suurimmat keskittymät yliopistoissa ja tutkimuslaitoksissa ovat Aalto-yliopistossa, VTT:llä, Tampereen teknillisessä yliopistossa, Oulun yliopistossa ja Helsingin yliopistossa, jotka ovat vastanneet yhteensä 45 prosentista alan julkaisuista.

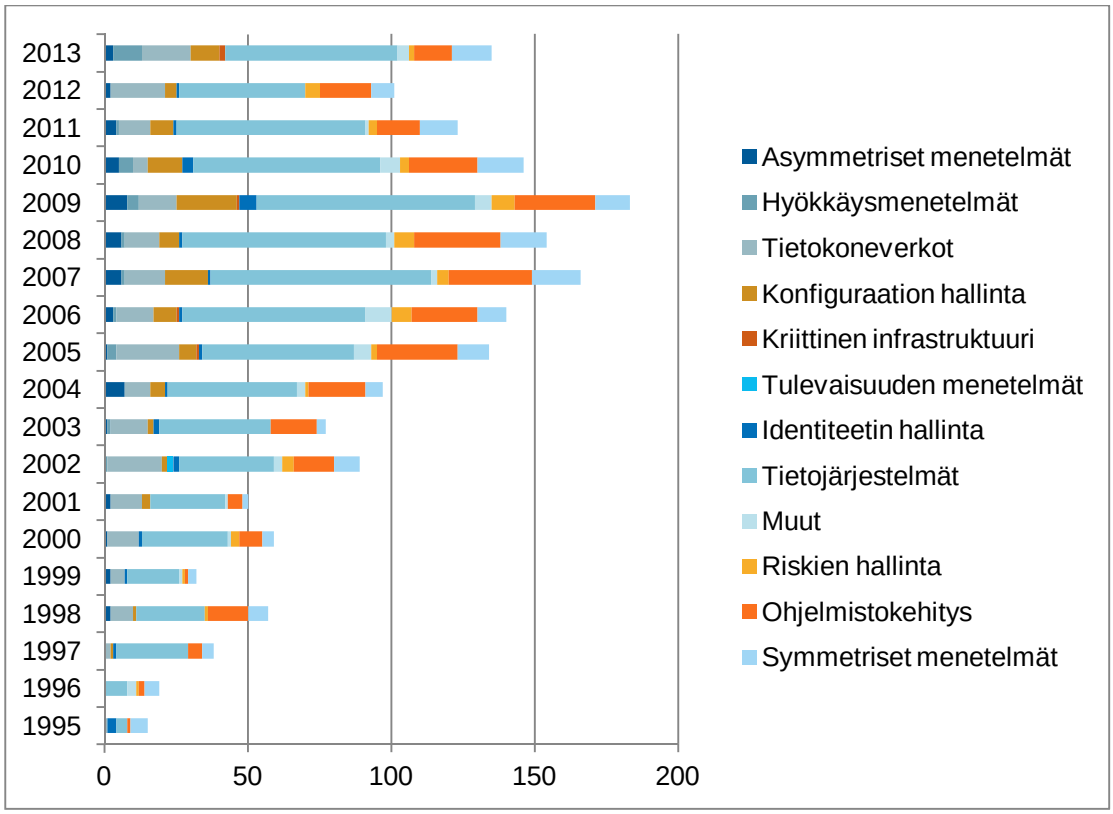
Käytännössä alan tutkimustoiminta jakaantuu varsin laajaan joukkoon organisaatioita ja tutkimus on eri organisaatioissa toimivien yksittäisten tutkimusryhmien varassa. Hajaantuneisuutta kuvastaa se, että eniten julkaisuja tuottanut organisaatio (Aalto-yliopisto) on vastannut vain hieman yli 10 prosentista julkaisuja ja käytännössä Aalto-yliopistossakin julkaisut jakaantuvat monelle laitokselle, yksikölle ja ryhmälle. Vastaavasti yhdeksän eniten julkaissutta organisaatiota ovat vastanneet 64 prosentista julkaisuja. Tutkijamäärältään isompia, eli yli 10 hengen yksiköitä, Suomessa on vähän. VTT:n kyberturvallisuuteen keskittyvä tutkimusryhmä on tutkijamäärällä mitattuna luultavimmin suurin yksittäinen yksikkö Suomessa ja siinä on hieman yli 30 tutkijaa.

Yliopistoissa ja tutkimuslaitoksissa on korkeatasoista kyberturvallisuuteen liittyvää tutkimusta ja kapeita kärkiosaamisalueita. Tällaisia ovat esimerkiksi kryptologia, haavoittuvuustutkimus, tietoturvan hallinta ja mobiililaitteiden tietoturva. Kryptologiaan kytkeytyy myös ainoa Suomessa ollut alaan liittyvä akatemiaprofessuuri (Arto Salomaa 1995-1999). Toisaalta voidaan sanoa, että alan huippuosaaminen on varsin ohutta, ja monilla osa-alueilla kokeneita tutkijoita on vähän. Vaikka tilanne on looginen sikäli, että kyseessä on pieni maa ja varsin spesifi tutkimusala, se kuvaa myös tietynlaista haavoittuvuutta alan kehityksen kannalta. Tiettyjen erityisalojen huippuosaaminen on harvojen asiantuntijoiden käsissä. Suomen Akatemian huippuyksiköitä alalla ei ole ollut.

[4] Selvityksestä ei käy ilmi, miten tiedot tutkimuksen kattavuudesta eri yliopistoissa on kerätty, joten tietojen luotettavuutta on vaikea arvioida.

Alan tutkimuksen volyymi on kasvanut hyvin vahvasti 1995-luvun puolesta välistä lähtien. 1990-luvun lopulla Suomessa julkaistiin keskimäärin muutamia kymmeniä alan tieteellisiä julkaisuja vuosittain, kun taas 2010-luvulla on julkaistu keskimäärin noin 120-130 julkaisua vuosittain (kuva 2.1.). Huomionarvoista myös on, että vuosina 2010-2012 julkaisumäärä laski varsin merkittävästi (noin 40 prosentilla). Yksi pudotuksen taustatekijä on todennäköisesti Nokian murros, jossa yrityksen tietoturvatutkimusta vähennettiin rajusti. Nokialla verkostoineen onkin ollut huomattava merkitys alan tutkimuksessa, ja se on tuottanut viidenneksi eniten tieteellisiä julkaisuja alueella Suomessa. Nokian osuus alan kaikista julkaisuista on ollut kuusi prosenttia.

Vuonna 2013 kansallinen julkaisuvolyymi kääntyi taas nousuun, ja tässä hankkeessa tehdyn tutkimustoimijoille suunnatun kyselyn perusteella alan tutkimuksen volyymi tulee edelleen kasvamaan lähivuosina: lähes 90 prosenttia kyselyyn vastanneista tutkimusryhmän johtajista oli sitä mieltä, että kyberturvallisuuteen liittyvä tutkimus ryhmässä kasvaa ja lähes 70 prosenttia ryhmän johtajista arvioi, että ryhmä rekrytoi lisää tutkijoita alueelle lähivuosina.

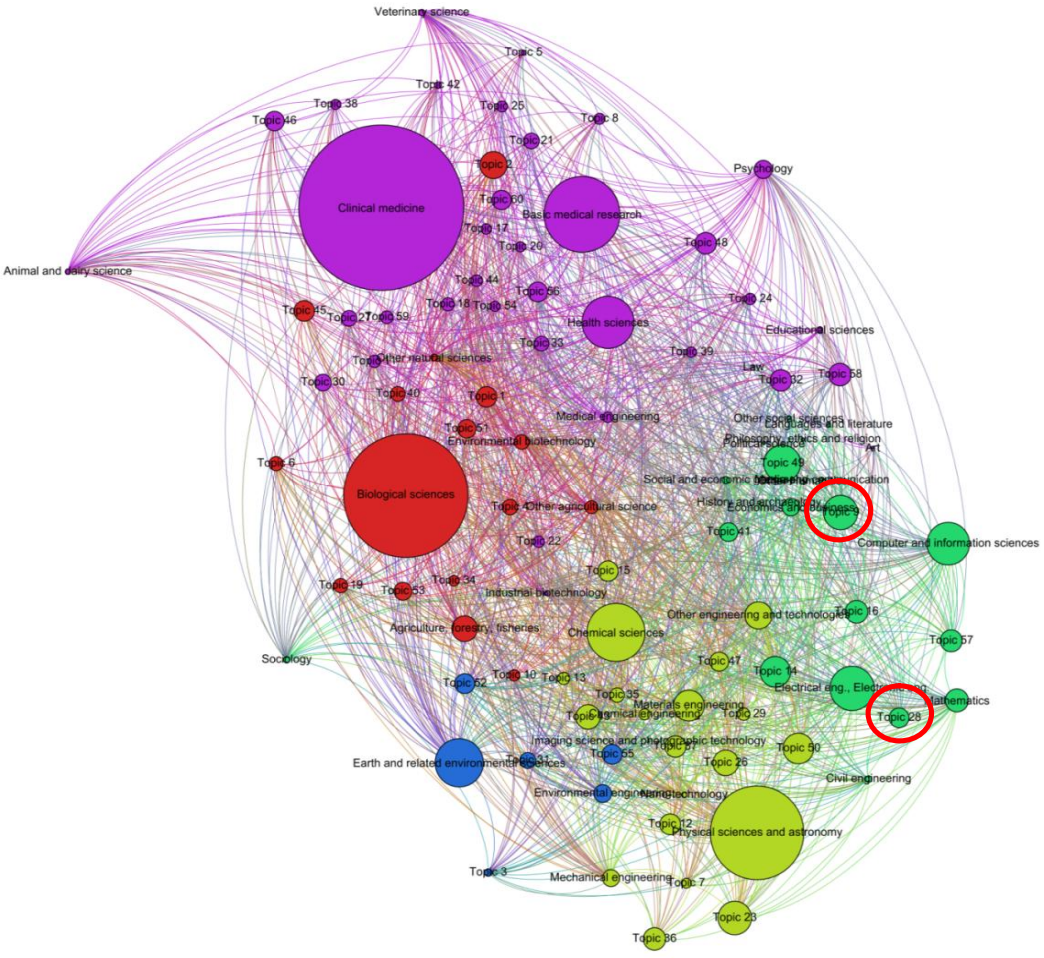


Kuva 2.1. Kyberturvallisuuteen liittyvä tieteelliset julkaisut Suomessa 1995-2013. Lähde: VTT.

Pitkän aikavälin kasvusta huolimatta kyberturvallisuusalan tutkimuskenttä on Suomessa edelleen pienehkö. Suomen tieteen kentässä tutkimusalue on volyymiltään varsin marginaalinen. Kuvassa 2.2. on VTT:llä luotu kartta Suomen tieteellisen tutkimuksen kentästä kokonaisuudessaan. Kartta kuvaa OECD:n määrittelemin luokin sekä koneoppimisella luoduin luokituksin Suomen tutkimuksen tutkimusvolyymiä eri aihepiireissä. Kuvassa oikealla vaaleanvihreällä värillä on informaatioteknologiaan, sähkötekniikkaa sekä yhteiskunta- ja kauppatieteisiin liittyvä tutkimus. Suhteessa kliinisen lääketieteen (violetti alue) ja biologian tutkimukseen (punainen alue) edellä mainitut tutkimusalat ovat volyymiltään pieniä. Kyberturvallisuuteen

liittyvä tutkimus on vaaleanvihreän verkoston osan sisällä, ja se keskittyy kahden punaisella ympyrällä merkityn alueen sisälle.

Kuvassa suurin osa kyberturvallisuuden tiedejulkaisuista luokitellaan koneoppimisella teemoihin 9 (50,1 %) ja 28 (13,4 %) (punaisella ympyrällä merkityt aiheet). Näistä teema 9, kuvassa ympyröitynä punaisella ylempänä, sijoittuu lähelle tietokone- ja informaatiotekniikan tutkimusta ja teema 28, kuvassa ympyröitynä punaisella alempana, sijoittuu lähelle matematiikan tutkimusta. Karttakuvan teemoja on tarkemmin analysoitu artikkelissa Suominen & Toivanen (2015), josta käy ilmi että molemmat mainitut teemat ovat kasvavia tutkimusalueita. Teema 9 on kasvanut ajalla 1995–2011 kahdeksana vuonna nopeammin kuin suomalainen tiedejulkaiseminen yleensä. Teema 28 on kasvanut vastaavasti samalla tarkastelujaksolla neljänä vuonna nopeammin kuin suomalainen tiedejulkaiseminen.



Kuva 2.2. Kyberturvallisuuteen liittyvä tutkimus Suomen tieteen kentässä. Lähde: VTT.

Voidaan sanoa, että kyberturvallisuustutkimus – kuten muutkin informaatiotieteisiin laajasti liitettävät tutkimusalueet – on osa Suomen tutkimuksessa käynnissä olevaa laajempaa muutosta jossa Suomen tiede on monimuotoistunut. Suomen tiede on perinteisesti nojannut kahteen tukijalkaan, lääketieteen ja luonnontieteen tutkimukseen. Näiden rinnalle on kehittymässä uusi, kansainvälisesti merkittävä tukijalka, joka koostuu laajasti informaatioteknologian ja yhteiskunta- ja kauppatieteiden tutkimuksesta. Näiden tieteenalojen yhdistelmä on ollut Suo-

men tieteen merkittävin kasvukomponentti kansainvälisillä tiedejulkaisuilla mitattuna. Tässä kehityksessä myös kyberturvallisuuden tutkimuksella on osansa.

Tutkimusalan volyymia kuvastaa myös se, että Suomessa on tällä hetkellä noin hieman toistakymmentä kyberturvallisuuden tutkimukseen keskittyvää professoria. Kuten edellä todettiin, suomalaiset tutkijat tuottavat noin 120 kyberturvallisuuteen liittyvää tieteellistä julkaisua vuosittain.

Kyberturvallisuuteen liittyvä tutkimus on Suomessa teknologisesti orientoitunutta ja tekniikkaan painottunutta. Alan tutkijat ovat valtaosin tieto- ja viestintätekniikan (ICT) tutkijoita. Tutkimustoimijoiden kyselyssä 66 prosentilla vastaajista pääasiallinen taustatieteenala oli joko tietotekniikka, tietoliikennetekniikka tai tietojärjestelmätiede. Näiden jälkeen merkittävin yksittäinen tutkimusala oli matematiikka, jota edusti noin 8 prosenttia vastaajista. Muita tieteenaloja (mm. politiikan tutkimus, sotatieteet, kognitiotiede jne.) edustavia tutkijoita oli muutamia kultakin alalta. Myös alan julkaisutoiminnassa näkyy vahvasti keskittyminen ICT-alueelle: valtaosa kyberturvallisuuteen liittyvistä julkaisuista kytkeytyy tietojärjestelmiin ja seuraavaksi merkittävimmät alueet ovat ohjelmistot ja tietoverkot (ks. kuva 2.1. edellä).[5]

Tutkimuksen painottuminen teknologisiin ulottuvuuksiin merkitsee myös sitä, ettei kyberturvallisuutta moni- ja poikkitieteellisestä näkökulmasta lähestyvä tutkimus ole Suomessa kovinkaan näkyvää. Esimerkiksi ihmis-, käyttäytymis-, talous- ja yhteiskuntatieteellisestä näkökulmasta kyberturvallisuutta tarkasteleva tutkimus on varsin vähäistä ja osin lähes olematonta. Kyberturvallisuus on kuitenkin laaja-alainen kokonaisuus ja ilmiökenttä, joka ei rajoitu teknologiseen komponenttiin vaan edellyttää monipuolista tarkastelua. Kansainvälisesti katsottuna monitieteinen kyberturvallisuustutkimus onkin yhä yleisempää (esim. Long & White 2010; Cresson-Wood 2004).

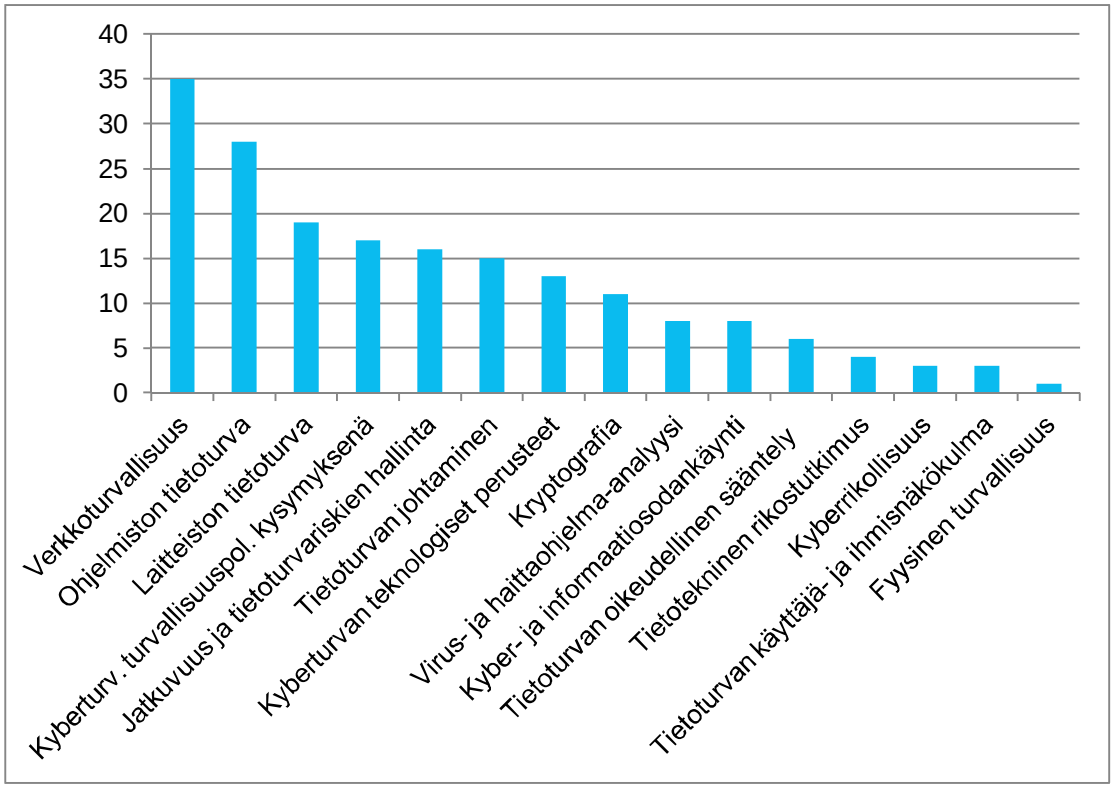
Kyberturvallisuusalan tutkijoille tehty kysely antaa hieman lisää kuvaa alan tutkimuksen suuntautumisesta Suomessa. Kyselyn mukaan verkkoturvallisuus sekä ohjelmiston ja laitteiston tietoturva ovat osa-alueita, joilla tehdään eniten tutkimusta (kuva 2.3.). Vastaavasti yhteiskunta- ja ihmistieteellisillä tutkimusalueilla, kuten tietoturvan käyttäjä- ja ihmisnäkökulma, kyberrikollisuus ja oikeudellinen sääntely, tutkimusta on huomattavan vähän. Mielenkiintoista myös on, että kyberturvallisuutta turvallisuuspoliittisena kysymyksenä tarkastelevaa tutkimusta on varsin monella tutkijalla. Toisaalta pääasiallisena tutkimuskohteena kukaan ei maininnut turvallisuuspoliittista tutkimusta. Tätä voidaan luultavasti tulkita niin, että monella tutkijalla laajempi turvallisuuspoliittinen ulottuvuus on jollain tapaa mukana tutkimuksessa mutta siihen keskittyviä tutkijoita ei juuri ole. Toinen mielenkiintoinen havainto koskee virus- ja haittaohjelma-analyysiä: sitä tekeviä tutkijoita on kyselyn perusteella varsin vähän, vaikka alueella osaaminen sinänsä on Suomessa hyvin vahvaa, erityisesti yrityspuolella.

Lehdon ja Kähkösen tutkimuksen (2015) mukaan laajimmin yliopistoissa ja tutkimuslaitoksissa katetut tutkimusalueet ovat kryptografia ja IoT-tietoturva.[6] Muita monissa organisaatioissa tutkittuja aiheita ovat esimerkiksi haavoittuvuusanalyysi, SCADA-turvallisuus, verkkoturvallisuus ja mobiililaitteiden turvallisuus (ks. liite 5). Sen sijaan esimerkiksi kyberturvallisuuden

[5] Kyberturvallisuuteen liittyvän tieteellisen julkaisutoiminnan kehitystä tarkasteleva kuva 2.1. pohjautuu asiantuntijatyönä koostettuun kyberturvallisuuden teknologioiden käsitekarttaan (ks. tarkemmin liite 3). Kuvassa huomionarvoista on käsitekartasta johtuva rajaus, joka sisällyttää tietojärjestelmät osaksi kyberturvallisuutta. Vaikka tarkastelussa on mukana vain ne tietojärjestelmätieteen teemat, jotka liittyvät kyberturvallisuuteen, tietojärjestelmät on tutkimuskenttänä volyymiltään suurin. Käytännössä analyysissä on pyritty rajaamaan kyberturvallisuus laajasti. Käsitekarttaan on sisällytetty aihepiirejä esimerkiksi tietokoneverkoista, ohjelmistokehityksestä ja tietojärjestelmistä silloin, kun voidaan laajasti tulkiten ymmärtää näiden liittyvän kyberturvallisuuden teknologioiden aihepiiriin. Tämä antaa monipuolisemman ja, väittäisimme, realistisemman kuvan Suomen kyberturvallisuustutkimuksen tilasta.

[6] Kryptografian osalta tutkimus suuntautuu pitkälti soveltavaan kryptografiaan, kun taas teoreettisen kryptologian tutkimus ja osaaminen on Suomessa vähäistä.

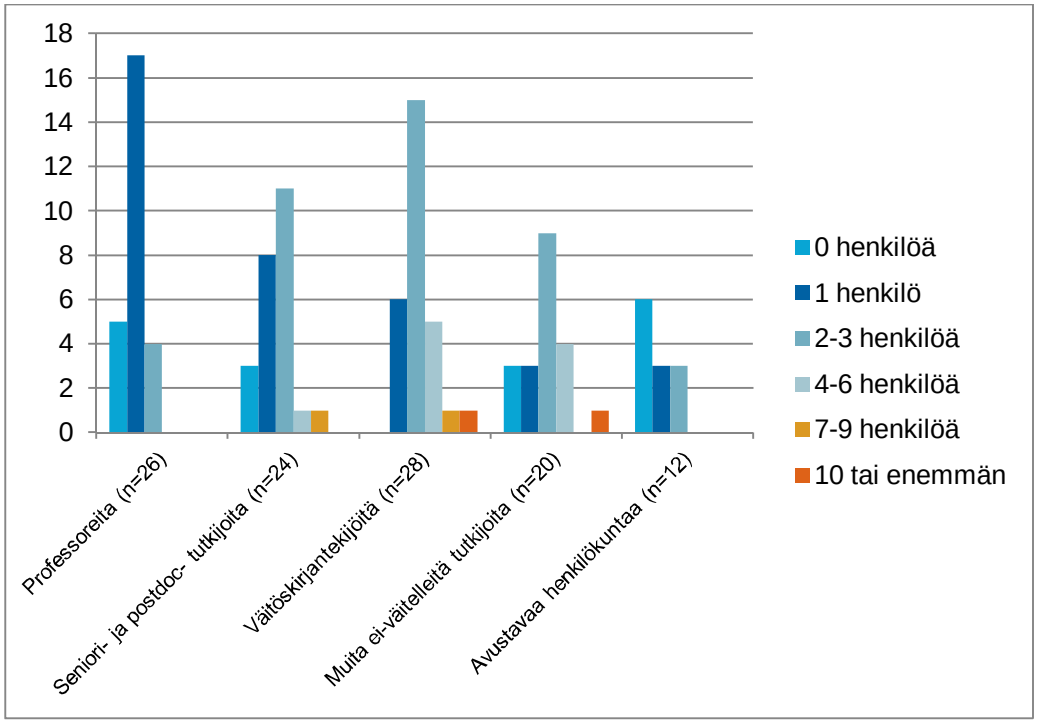
oikeudelliset näkökohdat ja investoinnit ovat aiheita, joita tutkitaan vain yhdessä organisaatiossa.



Kuva 2.3. Tutkimuksen suuntautuminen tutkimustoimijoiden kyselyn mukaan (mainintoja, n=76).

Kyselyn perusteella kyberturvallisuuteen liittyvää tutkimusta tekevät tutkimusryhmät ovat keskimäärin noin 6-7 hengen ryhmiä (kuva 2.4.).[7] Useimmiten ryhmät ovat yhden professorin vetämiä ryhmiä. Isompia, yli 10 hengen ryhmiä on kyselyn perusteella vähän. Merkillepantavaa myös on, että isot, 10-20 hengen tutkimusryhmät ovat pääasiallisesti sellaisia, joiden tutkimuksesta vain pienehkö osa liittyy kyberturvallisuuteen. Kyselyn perusteella kyberturvallisuuteen vahvasti fokusoituvat tutkimusryhmät ovat yleensä 4-7 hengen kokoisia.

[7] Tutkimusryhmien koon vaikutusta tieteelliseen tuottavuuteen on tutkittu varsin paljon. Vaikka tutkimustulokset vaihtelevat jonkin verran, monien tutkimusten mukaan 5-8 hengen tutkimusryhmät ovat usein tuottavampia ja tieteellisen luovuuden kannalta suotuisampia yksiköitä kuin suuremmat ryhmät (ks. esim. Heinze ym. 2009; Von Tunzelmann ym. 2003; Bloch & Sorensen 2014).

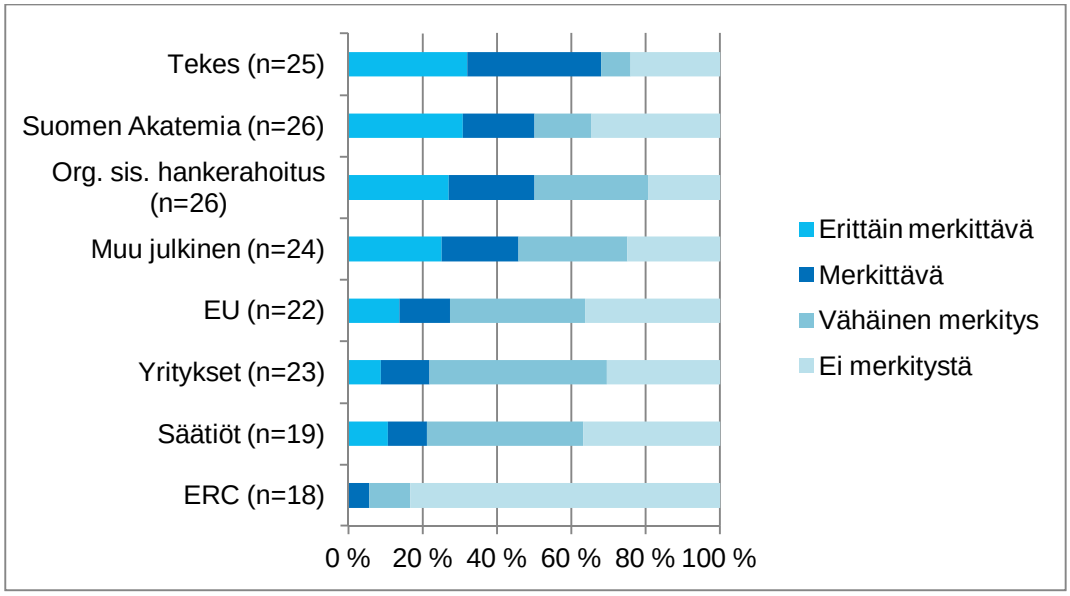


Kuva 2.4. Kyberturvallisuusalan tutkimusryhmien koostumus. Lähde: Kysely alan tutkijoille[8]

Ulkomaalaisia tutkijoita tutkimusryhmissä on keskimäärin kaksi. Toisaalta tutkimusryhmissä on paljon ryhmiä, joissa ei ole lainkaan ulkomaalaisia tutkijoita. Haastattelujen perusteella monet ryhmien vetäjät kokevat ulkomaalaisten tutkijoiden rekrytoimisen Suomeen vaikeaksi. Samalla kuitenkin nähdään, että kansainväliselle huipulle nouseminen edellyttää sekä kansainvälistä rekrytointia että lisääntyvää kansainvälisyyttä laajemminkin. Kansainvälisyyden osalta huomionarvoista on myös se, että kansainvälinen yhteisjulkaiseminen on kyberturvallisuustutkimuksessa hyvin vähäistä. Alan suomalaisista artikkeleista 15 prosenttia on kansainvälisesti yhteiskirjoitettuja, mikä on hyvin alhainen määrä verrattuna esimerkiksi luonnontieteisiin ja tekniikan alaan yleensä. Esimerkiksi vuosina 2006-2009 luonnontieteissä kansainvälisiä yhteisjulkaisuja oli kaikista julkaisuista 55 prosenttia ja tekniikassa 44 prosenttia (Muhonen ym. 2012). Haastattelujen ja kyselyn perusteella alan suomalaisen kyberturvallisuustutkimuksen kansainvälinen näkyvyys on kuitenkin tällä hetkellä parempi kuin joitakin vuosia sitten.

Alan tutkimusryhmille Tekes on selvästi merkittävin yksittäinen tutkimuksen ulkopuolinen rahoittaja (kuva 2.5). Muita tärkeitä rahoittajia ovat Suomen Akatemia ja muut julkiset tahot sekä tutkimusorganisaatioiden oma hankerahoitus. Huomattavaa on, että EU-rahoituksen merkitys on suhteellisen pieni. Suomen Akatemiasta saadut EU-tutkimusrahoitustiedot vahvistavat tätä kuvaa. Niiden mukaan esimerkiksi H2020-ohjelmassa suomalaiset ovat tähän mennessä olleet mukana muutamassa kyberturvallisuuteen liittyvässä tutkimushankkeessa. Myös yritysrahoituksen merkitys on tutkimusryhmille suhteellisen pieni.

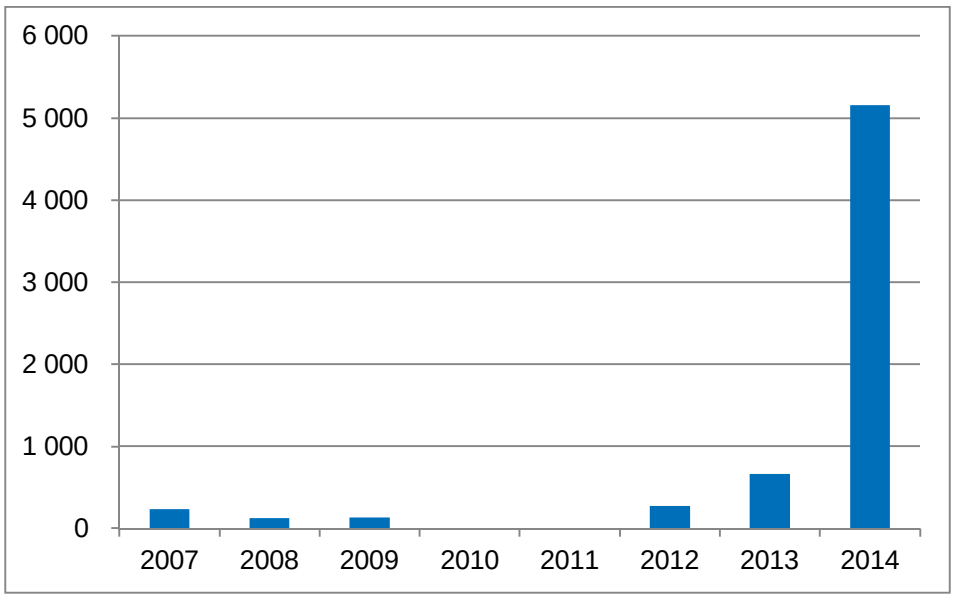
[8] Tämä kysymys suunnattiin vain tutkimusryhmien johtajille, ja tästä syystä vastaajamäärät ovat tämän kysymyksen osalta pienempiä kuin koko kyselyn vastaajamäärä. Tutkimusryhmän johtajia kyselyyn vastasi kaikkiaan 33.



Kuva 2.5. Tutkimusrahoituslähteiden merkitys tutkimusryhmien toiminnassa[9]

Tekesin merkitys alan t&k-toiminnan rahoituksessa on siis huomattava. Viimeaikaiset muutokset Tekesin rahoituksessa koskien erityisesti SHOK-toimintaa ja INKA-ohjelmaa aiheuttavatkin haastattelujen ja kyselyjen perusteella huolta alan toimijoiden keskuudessa. Erityisesti kyberturvallisuuden SHOK-ohjelma Cyber Trust on rakentanut yhteistyötä alan toimijoiden välille ja muutokset vaarantavat tämän kehityksen.

Suomen Akatemian rahoitus kyberturvallisuustutkimukseen on ollut niukkaa. Vuosilta 1995-2006 ei Akatemian hanketiedoista löytynyt lainkaan kyberturvallisuuteen liittyviä hankkeita. Ainoa isompi rahoitus on liittynyt Akatemian ja Tekesin yhteisen tietoturvatutkimuksen kokonaisuuteen vuonna 2014 (kuva 2.6.). Verrattuna Tekesin t&k-rahoitukseen alan yrityksille Akatemian rahoitus perustutkimukseen on ollut vähäistä (vrt. luku 2.3.1).



Kuva 2.6. Suomen Akatemian rahoitus tieto- ja kyberturvallisuustutkimukseen 1995-2014 (tuhatta euroa). Lähde: Suomen Akatemia.

[9] Tämä kysymys suunnattiin vain tutkimusryhmien johtajille, ja tästä syystä vastaajamäärät ovat tämän kysymyksen osalta pienempiä kuin koko kyselyn vastaajamäärä. Tutkimusryhmän johtajia kyselyyn vastasi kaikkiaan 33.

2.2 Koulutus yliopistoissa ja ammattikorkeakouluissa

Äskettäisen selvityksen (Lehto & Kähkönen 2015) mukaan kyberturvallisuusalaa on mahdollista opiskella seitsemässä yliopistossa ja seitsemässä ammattikorkeakoulussa. Koulutus muodostuu yhtäältä kyberturvallisuuteen keskittyvistä itsenäisistä koulutusohjelmista sekä toisaalta muuhun koulutukseen ja koulutusohjelmiin yhdistetystä kyberturvallisuuden opetuksesta. Koulutusohjelman tarjoavat kuitenkin vain Jyväskylän ja Turun yliopistot kun muualla on käytössä integroitu toimintamalli. Kyberturvallisuusalan opetusta antavia muita yliopistoja ovat Aalto-yliopisto, Helsingin yliopisto, Oulun yliopisto, Tampereen teknillinen yliopisto sekä Maanpuolustuskorkeakoulu. Ammattikorkeakouluista kyberalan koulutusta antavat Centria-ammattikorkeakoulu, Jyväskylän ammattikorkeakoulu, Kymenlaakson ammattikorkeakoulu, Laurea ammattikorkeakoulu, Oulun ammattikorkeakoulu, Poliisiammattikorkeakoulu sekä Turun ammattikorkeakoulu.

Koulutusohjelmamuotoinen koulutus on sekä Jyväskylässä että Turussa järjestetty kandidaatin tutkinnon jälkeen suoritettavana maisteriohjelmana. Vuonna 2014 aloitettu Jyväskylän ja 2011 aloitettu Turun maisteriohjelma ovat laajentaneet ja systematisoineet alan koulutusta. Sekä Jyväskylässä että Turussa maisteriohjelmaan valitaan vuosittain 20 opiskelijaa. Muualla kyberturvallisuuteen liittyviä opintoja voi suorittaa sivuaineena tai muihin opintoihin sisätyvinä kursseina. Aalto-yliopistossa on lisäksi pohjoismaiseen ja Tarton yliopiston kanssa tehtävään yhteistyöhön perustuva Master's Programme in Security and Mobile Computing, jossa tietoturvaopinnoilla on merkittävä rooli.[10] Alla olevissa taulukoissa on kuvattu karkeasti Lehdon ja Kähkösen (2015) selvitykseen perustuen yliopistojen ja ammattikorkeakoulujen koulutustarjontaa kyberturvallisuuden alueella. Kyberturvallisuuden oppilaitoskohtaista tarjontaa on tarkasteltu laajemmin kyseisessä selvityksessä.

Taulukko 2.1. Yhteenveto yliopistojen kyberturvallisuuskoulutuksesta (Lehto & Kähkönen 2015)

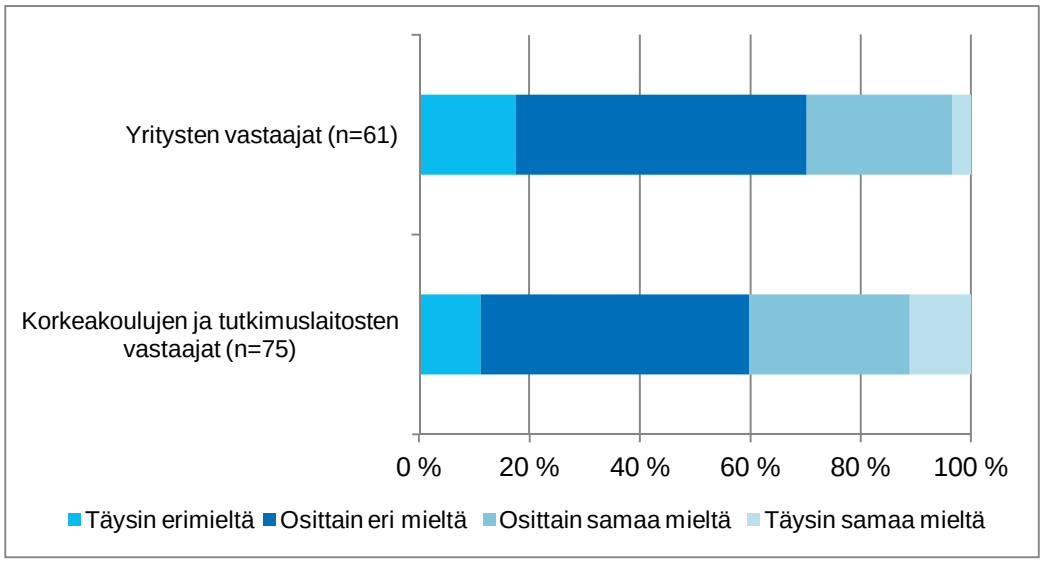
Aalto-yliopisto	Aalto-yliopistossa tietoturvallisuutta opiskellaan aina jonkin sovellusalueen rinnalla, ei pääaineena. Sivuaine-opintoja tietotekniikassa sekä tietojenkäsittelytieteessä, mahdollista yhdistää mihin tahansa tekniikan alaan, 'Master's Programme in Security and Mobile Computing', 10-15 opinnäytettä tietoturvallisuudesta vuosittain
Helsingin yliopisto	Tietojenkäsittelytieteen laitoksen erikoitumislinjalla "Hajautetut järjestelmät ja tietoliikenne" kyberturvallisuuden kursseja
Jyväskylän yliopisto	Informaatioturvallisuuden maisteriohjelma, vuosittain valitaan 20 opiskelijaa
Maanpuolustus-korkeakoulu	Kursseja integroitu eri laitosten kandidaatin, maisterin ja tohtori-opintoihin
Oulun yliopisto	Tietoturva osa tekniikan koulutuksen opintoja mm. tietoliikennetekniikassa ja tietojenkäsittelyssä
Tampereen teknillinen yliopisto	Tietoturvallisuuden sivuaine-opintokokonaisuus sekä erillisiä kursseja ohjelmisto- ja systeemitekniikan laitoksella
Turun yliopisto	Informaatioturvallisuuden ja kryptografian maisteriohjelma, vuosittain valitaan 20 opiskelijaa, lisäksi tietoturvajohtamisen opintoja Global Information Technology Management- maisteriohjelmassa

[10] Viimeisimpien tietojen mukaan tämä ohjelma on loppumassa.

Taulukko 2.2. Yhteenvetoa ammattikorkeakoulujen tarjoamasta kyberturvallisuuskoulutuksesta (Lähde: Lehto & Kähkönen 2015)

Centria ammattikorkeakoulu	Opintokokonaisuuksia ja erillisiä kursseja osana muita opintokokonaisuuksia tietoturvallisuudesta
Jyväskylän ammattikorkeakoulu	Erillisiä opintojaksoja ja ja jaksojen sisään integroituja kokonaisuuksia sekä osana Information Technology –maisteriohjelmaa
Kymenlaakson ammattikorkeakoulu	Kyberturvallisuuden opintoja osana tietotekniikan koulutusta
Laurea ammattikorkeakoulu	Kyberturvallisuuden opintoja osana turvallisuusalan koulutusohjelmaa
Oulun ammattikorkeakoulu	Tietotekniikan tutkinto-ohjelmassa tietoturvallisuuden suunnitteluosaaminen
Poliisiammattikorkeakoulu	Täydennyskoulutuksena tietotekniikkarikosten opintokokonaisuus
Turun ammattikorkeakoulu	Kaksi erityisesti tietoturvaan keskittyvää opintomoduulia (kumpikin 15 op) sekä tietoturvallisuuteen liittyviä kursseja

Tätä tutkimusta varten toteutettujen kyselyiden ja haastatteluiden perusteella alan koulutusta ei kuitenkaan ole riittävästi. Enemmistö sekä yritysten että tutkimus- ja koulutusorganisaatioiden edustajista oli tätä mieltä (kuva alla). Positiivisemmin koulutuksen nykytilaan suhtautuivat tutkimus- ja koulutusorganisaatioiden vastaajat.



Kuva 2.7. Kyselyvastaajien vastaukset väittämään ”Kyberturvallisuuteen liittyvää korkeatasoista koulutusta on Suomessa yliopistoissa ja ammattikorkeakouluissa riittävästi”. Lähde: Yritys- ja tutkimustoimijoiden kyselyt.

Yritykset tarkastelevat koulutuskysymystä luonnollisesti osaavan työvoiman saatavuuden näkökulmasta. Kuten koulutusta koskevat näkemykset antavat odottaa, kyselyyn vastanneista yrityksistä suurin osa katsoi myös, ettei osaavaa työvoimaa ole helposti saatavilla Suomessa. Rekrytointivaikeudet ovat kohdistuneet laajalle alueelle liittyen muun muassa applikaatio-osaamiseen, identiteetin- ja pääsynhallintaan, kryptografiaan, linux-palvelinjärjestelmiin, myyntiin, ohjelmistosuunnitteluun sekä palvelinosaamiseen. Negatiivisimmissa koulutusta koskevissa kommenteissa todettiin, että ”Suomessa ei ole mitään soveltuvaa koulutusta tarjolla, joka pätevöittäisi tehtäviin”, ”lähes kaikki on itse koulutettava” ja että ”osaaminen keskittyy hyvin perinteisiin tietoturvaratkaisuihin, kyberosaamista on heikosti”. Lisäksi osaavan työvoiman puutteen nähtiin joissakin kommenteissa vaikuttavan myös yrityksen kasvumahdollisuuksiin. Mikäli ala kasvaa, työvoimaa ja osaajia tarvitaan ulkomailta.

Kaiken kaikkiaan koettiin, että vaikka koulutusta on ryhdytty kehittämään, siinä ollaan vielä alussa. Osaajia ei kouluteta riittävästi ja varsinainen koulutus kyberturvallisuuskysymyksiin saattaa tapahtua tästä syystä yrityksissä. Tämä on ymmärrettävää myös sitä taustaa vasten että yrityskohtaisia kvalifikaatioita ei ole mahdollista opettaa korkeakouluissa ja yliopistoissa. Eräs haastateltava kuvasi tilannetta seuraavasti:

> ”Me otamme sellaisia hyviä tyyppejä, jotka osoittavat kiinnostusta, ja opetamme heidät itse. - - Otetaan tämänlaisella mentori-oppipoika -tyyppisellä.”

Tutkimus- ja koulutusorganisaatioiden edustajien näkemyksen mukaan opiskelijat ovat kuitenkin kiinnostuneita alasta. Peräti noin neljä viidesosaa korkeakoulujen ja tutkimuslaitosten vastaajista katsoi, että opiskelijat ovat kiinnostuneita kyberturvallisuuteen liittyvistä kysymyksistä. Tutkimus- ja koulutusorganisaatioiden edustajat moittivat kuitenkin resurssien riittämättömyyttä. Vaikka kiinnostusta ja tarvetta koulutukselle olisi, ilman lisäresursseja sitä ei ole mahdollista lisätä.

> ”Opiskelijoiden kiinnostus kasvaa vuosi vuodelta, osittain varmasti sen vuoksi, että olemme saaneet näytettyä heille, että aihe on olennainen yrityksille. Pikemminkin tarvitsisimme lisäpanostusta koulutukseen.” (Vastaus kyselyn avokysymykseen)

Eräs haastateltu kuvasi myös kuinka yritykset olivat lähestyneet yliopistoa koska ne tarvitsisivat lisää tietoturva-ammattilaisten koulutusta. Laajaa koulutuksen lisäämistä ei kuitenkaan ole kyetty toteuttamaan koska henkilöstöresurssit ovat riittämättömät. Tilanteeseen vaikuttavat hänen mukaansa yliopistojen kiristyneet resurssit.

Vaikka koulutuksessa nähtiin puutteita, monet katsoivat toisaalta, että hyvä koulutustaso on yksi Suomen vahvuus kyberturvallisuusalalla. Vahvuudeksi todettiin muun muassa korkea koulutus- ja osaamistaso tietotekniikassa. Toisaalta haasteena nähtiin vastavuoroisesti muun muassa alan osaajien vähäisyys ja ryhmien pienuus, mikä yhdessä riittämättömien resurssien kanssa johtaa pirstoutuneeseen toimintaan.

Kaiken kaikkiaan koulutuksessa on kahtalainen haaste. Yhtäältä kyberturvallisuuden koulutusta olisi perusteltua nivoa yhteen muuhun tietoliikennealan koulutukseen ja myös jo peruskouluasteelle yleisen tietoturvallisuustason ja tietoisuuden lisäämiseksi. Toisaalta tarvitaan spesialistikoulutusta, mikä puolestaan edellyttää hyviä pohjatietoja ja osaamista esimerkiksi matematiikasta.

> ”Siis missä on tietotekniikan opetusta, niin siellä pitäisi olla myös tietoteknisen turvallisuuden opetusta. Kyllä se on ihan elimellinen osa sitä, ainakin opetusta.”

> ”Se toinen haaste on, että sinun tarvitsisi olla matemaatikko ja sitten vielä vähän niin kuin hakkeri ja käyttisasiantuntija ja tietoliikenneinsinööri. Jos salaustekniikan toteuttamista ajattelee, niin diplomi-insinöörin matematiikan koulutus loppuu ihan auttamatta kesken, että pystyisi edes kuuntelemaan kryptografian kursseja.”

Kokonaisuudessaan aineiston pohjalta piirtyy kuva kehittymässä olevasta mutta toistaiseksi tarpeisiin nähden riittämättömästä koulutuksesta. Vaikka yrityksissä olisi kysyntää työvoimalle ja opiskelijoiden keskuudessa kiinnostusta alaan, haasteiksi näyttävät nousevan riittämättömät koulutusresurssit. Kuten edellä todettiin, edes yritysten suorat yhteydenotot yliopistoihin eivät ole johtaneet koulutuksen laajentamiseen koska henkilöstöresursseja ei ole. Yritykset joutuvat kouluttamaan alan osaajia tarpeisiinsa itse. Alan parantunut koulutustilanne saattaa ajan myötä lisätä myös saatavilla olevia koulutuksen henkilöstöresursseja yliopistoissa. Toisaalta yliopistot ovat kilpailutilanteessa yritysten kanssa osaajista. Lisäksi niukkenevat rahalliset resurssit yliopistojen rahoitusleikkausten myötä saattavat rajoittaa entisestään alan koulutuksen kehittämistä tulevina vuosina.

2.3 Yritysten liiketoiminta ja tutkimus-, kehitys- ja innovaatiotoiminta

Kyberturvallisuuteen liittyvä yrityskenttä on suhteellisesti katsottuna Suomessa melko suuri. Alalla toimivat yritykset voidaan jakaa kolmeen ryhmään. Ensimmäisen ryhmän muodostavat ydinliiketoimintanaan kyberturvallisuutta tekevät yritykset. Näitä yrityksiä on noin 70, ja niistä suuri osa on alan yritysten yhteistyöorganisaation Finnish Information Security Clusterin (FISC) jäseniä. Toisessa ryhmässä ovat tietotekniikka- ja tietoliikenneyritykset, joiden liiketoiminnasta osa liittyy tieto- ja kyberturvallisuuteen. Tällaisia ovat Suomessa esimerkiksi verkko- ja mobiiliyritykset (esim. Nokia, Ericsson), operaattorit ja eräät kansainväliset konsulttitoimistot. Kolmanneksi on olemassa tiettyjä toimialoja, joille tietoturvakysymykset ovat liiketoiminnan kannalta erittäin keskeisiä ja joilla on sen takia vahvaa tietoturvatoimintaa. Tällaisia ovat esimerkiksi pankit. Kahden ensimmäisen kategorian yrityksiä on Suomessa yhteensä arviolta noin 150-160. Kyberturvallisuuden tuotteita ja palveluja ydinliiketoimintanaan tuottavissa yrityksissä arvioidaan olevan noin 4500 työntekijää.[11]

Tietoturvaan ja kyberturvallisuuteen keskittyvä yrityskenttä alkoi muotoutua Suomessa 1990-luvun alkupuolella kolmen yrityksen ympärille: Data Fellows (perustettu 1988, nykyisin F-Secure), joka keskittyy haittaohjelmien ja virusten torjuntaan, Stonesoft (perustettu 1990, nykyisin osa Inteliä), jonka ydinliiketoimintaa ovat palomuurit ja SSH Communications (perustettu 1995), joka keskittyy tietoliikenteen suojaamiseen. Tietoturvakonsultoinnin puolella edelläkävijänä on ollut Nixu Oyj, joka on perustettu vuonna 1988.

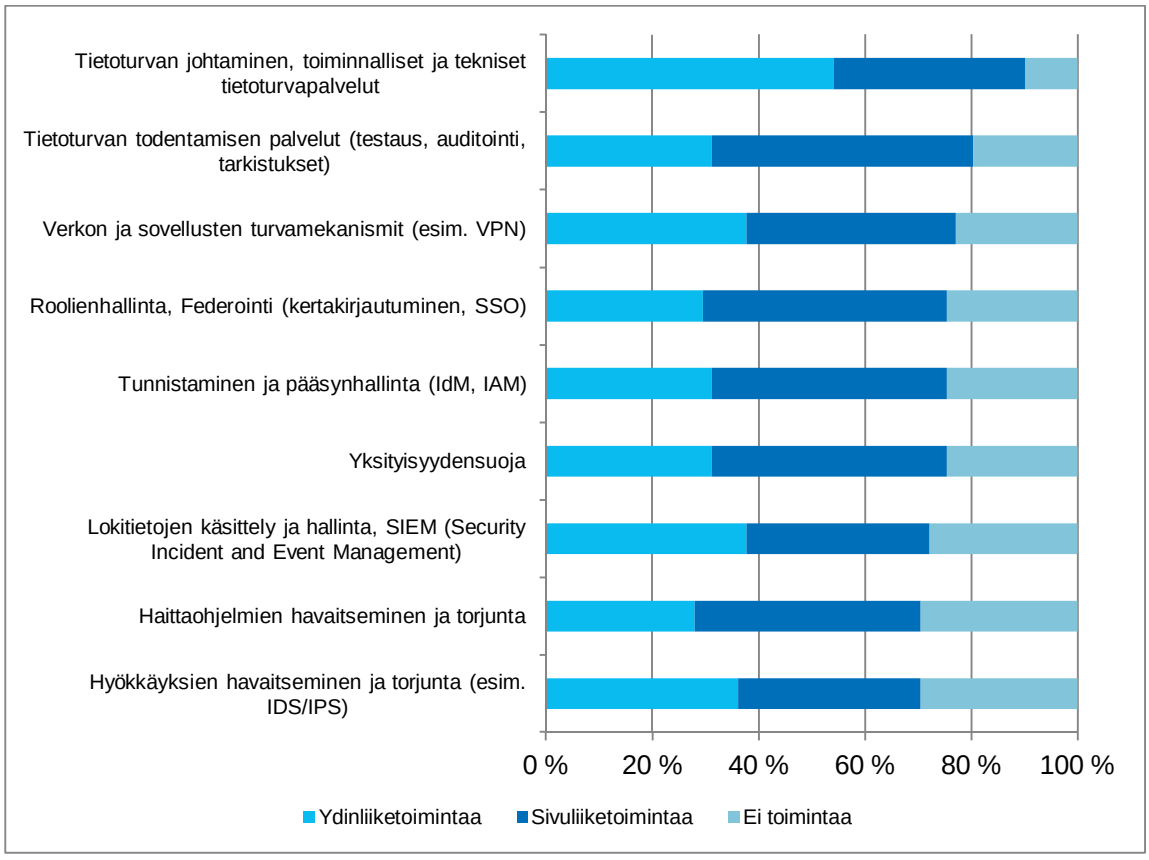
Tietoturvaan ja kyberturvallisuuteen liittyvän yritystoiminnan syntyyn on Suomessa liittynyt monia tekijöitä. Tällaisia ovat olleet mm. korkeatasoinen teknisten alojen ja erityisesti ohjelmistoalan koulutus, teknologian laaja-alainen hyödyntäminen, 2000-luvun alun Internethuuma, joka mahdollisti useamman yrityksen listautumisen aikaisessa vaiheessa, Nokian nousu mobiiliteknologian huipulle 1990-luvulla sekä julkisen sektorin hankkeet jotka ovat tuottaneet yrityksille referenssitoimituksia (Remes & Kyheröinen 2015). Nokialla oli 2010-luvun alkuun saakka merkittävä tietoturvaryhmä ja lisäksi se toimi merkittävänä asiakkaana osalle tietotur-

[11] Arvio perustuu Orbis-tietokannasta haettuihin alan yritysten taloudellisiin tietoihin. Arviota varten muodostettiin yritysjoukko johon identifioitujen arvioitiin olevan kyberturvallisuuden kyberturvallisuuden teknologioita ja palveluita ydinliiketoimintanaan tuottavia yrityksiä. Luvut sisältävät myös yritysten toiminnan Suomen ulkopuolella.

vayrityksistä. Sittemmin monet Nokian tietoturvaosaajat ovat hakeutuneet uusiin tehtäviin eri puolille yksityistä ja julkista sektoria ja siten osaaminen on levinnyt.

Kyber- ja tietoturvaan keskittyvistä yrityksistä varsin suuri osa on palvelu- ja konsultointiyrityksiä, kun taas omia tuotteita valmistavia yrityksiä on vähemmän. Merkittävää myös on, että suuri osa yrityksistä on pieniä. Yrityskyselyssä noin puolet vastanneista yrityksistä oli alle 10 hengen yrityksiä. Huomattavaa myös on, että ne yritykset joissa kyberliiketoiminnan osuus liikevaihdosta oli suuri (75-100 prosenttia), olivat keskimäärin henkilömäärältään pienempiä.

Yrityskyselyn perusteella alan suomalaisten yritysten liiketoiminta ja sitä kautta osaaminen kattaa varsin laajasti kyberturvallisuuden eri osa-alueita (kuva 2.8). Kyselyn perusteella liiketoiminta-alueita, joilla varsin suuri osa alan yrityksistä toimii, ovat tietoturvapalvelut, tietoturvan johtaminen ja tietoturvan todentamisen palvelut. Tämä kuvastaa alan yritystoiminnan tietynlaista orientoitumista palveluihin. Myös useilla muilla osa-alueilla on kyselyn perusteella runsaasti osaamista ja liiketoimintaa.



Kuva 2.8. Suomalaisten kyberturvallisuusyritysten liiketoiminnan suuntautuminen. Lähde: Yrityskysely (n=61)

Alan yrityskentässä voidaan myös tunnistaa vahvoja osaamisalueita. Tällaisia ovat esimerkiksi virustorjunta, tunnistaminen ja identiteetin hallinta, palomuurit, tilannekuvajärjestelmät sekä testaaminen ja tieto- ja kyberturvapalvelut (Remes & Kyheröinen 2015; ks. Taulukko 2.3). Monet näistä vahvoista osaamisalueista perustuvat johtavien yritysten toimintaan. Esimerkiksi virustorjuntaosaaminen on erityisesti F-Securen myötä Suomessa korkeatasoista. Edellä mainittujen alueiden lisäksi Suomessa on Nokian myötä korkeatasoista osaamista mobiililaitteiden tietoturvassa.

Taulukko 2.3. Kyberturvallisuusalan yrityksiä Suomessa eri osaamisalueilla.

Alue	**Esimerkkiyrityksiä**
Tietoturvan ja virustorjunnan tuotteet	SSH Communication, F-Secure, Codenomicon (Synopsys)
Käyttövaltuushallinta ja tunnistaminen	Globalsign (osti Ubisecure Solutions Oy:n), Propentus Oy, Digital Identity Solutions Europe (DISE), Effecte Oy (osti RMS Solutions Oy:n), Nixu Oyj (osti Panorama Partners Oy:n), KPMG Finland (osti Trusteq Oy:n), Deloitte (osti Secproof Oy:n), Spellpoint, Insta Group Oy. Lisäksi ratkaisuja myös suurilla integraattoreilla kuten Fujitsu, Tieto, CGI.
Palomuurit ja muut innovatiiviset tietoturvapalvelut	Intel Security (McAfee, Stonesoft), SecGo, Jetico, Ymon, Capricode, Envault Corporation
Auditointi ja turvallisuusprosessien kehittäminen	nSense (nykyisin osa F-Securea), Nixu, KPMG Finland, Granite Partners
Sähköinen hyväksyntä ja allekirjoitus	Gemalto (Setec), Avaintec Oy, Fujitsu Finland Oy, Valimo Wireless, Sonera (Smart Trust), Sopima Oy
Maksaminen	KPMG, Nixu, nSense, Solinor, Poplatek, Verifone, Sagem, Modirum Oy, Basware

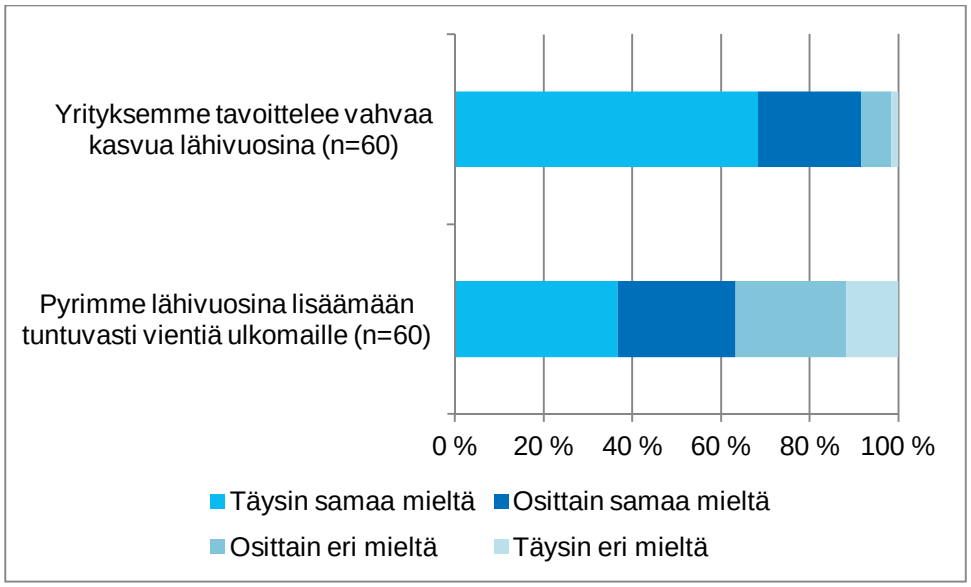
Suomalaisten kyberturvallisuusalan yritysten yhteenlaskettu liikevaihto vuonna 2014 oli arviolta 1091 miljoonaa euroa (taulukko 2.4). Liikevaihtoa yritykset tuottivat noin 240 000 euroa työntekijää kohti. Yritysten kasvu on ollut viime vuosina vahvaa: viimeisen kolme vuoden keskiarvoista laskettu keskiarvo kasvulle on 26 prosenttia. Kasvua voi verrata esimerkiksi informaatio ja viestintä -alaan, jonka vastaava kasvuprosentti oli 4,2 prosenttia.[12] Kyberturvallisuuden keskeiset yritykset ovat siis kasvattaneet liikevaihtoaan nopeammin kuin yritysten laajempi viiteryhmä.

[12] Kyberalan yritysten kasvua suhteutetaan tässä toimialan laajempaan kehitykseen vertaamalla liikevaihdon kasvua Tilastokeskuksen toimialojen liikevaihdon vuosimuutos -taulukkoon. Samalla tarkastelujaksolla liikevaihdon kasvu Informaatio ja viestintä -toimialan yrityksissä oli siis keskiarvona 4,2 prosenttia. Valittu palvelualan toimiala, Informaatio ja viestintä, on kyberturvallisuusalan yrityksille keskeisin viiteryhmä, mutta yritykset voivat kuulua myös muuhun toimialaan.

Taulukko 2.4.[13] Kyberturvallisuusalan liiketoiminnan tunnuslukuja (Lähde: Orbis).

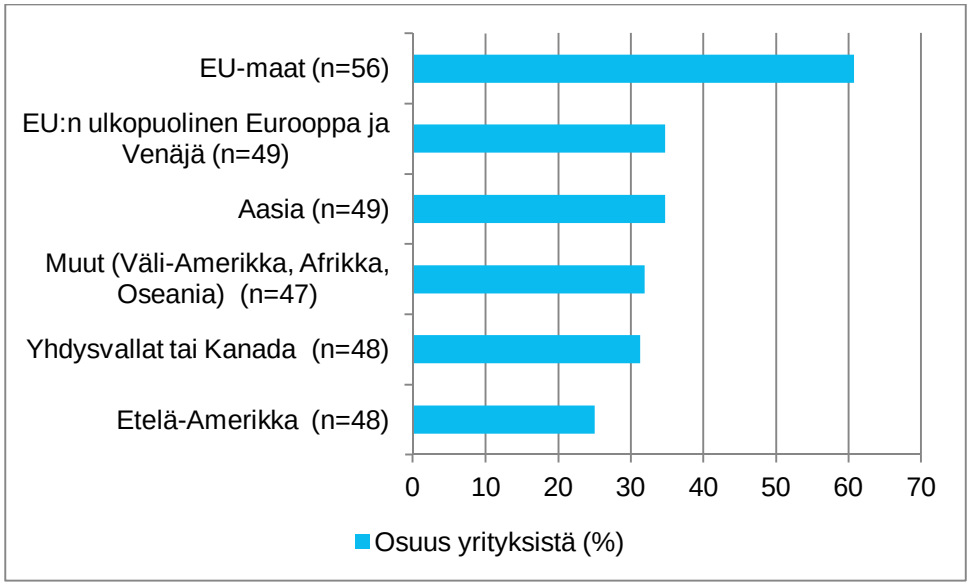
	Työntekijöitä	Liikevaihto t€	Liikevaihdon kasvu
Yhteensä	4518	1 091 795 t€	
Keskiarvo	74	14 365 t€	26 %
Mediaani	10	782 t€	9 %
Hajonta	160	38 644 t€	102 %
N	61	76	56

Myös yrityskyselyn perusteella alan yritykset ovat varsin vahvasti sekä kasvu- että vientiorientoituneita (kuva 2.9). Vastanneista yrityksistä 61 prosenttia vie tuotteita tai palveluita EU-maihin ja noin kolmasosa EU:n ulkopuolisiin Euroopan maihin ja Venäjälle tai Aasiaan (kuva 2.10). Kansainvälisillä ja myös kotimaisilla markkinoilla eräs tärkeä kilpailutekijä suomalaisille yrityksille on viime aikoina ollut luottamus ja neutraalisuus. Moni kansainvälinen yritys on menettänyt luottamuksen, mutta suomalaiset koetaan neutraaleina ja luotettavina toimijoina.



Kuva 2.9. Yritysten kasvu- ja vientihakuisuus. Lähde: Yrityskysely.

[13] Yritysten liikevaihtoa, työntekijämäärä ja kasvua tarkasteltiin siten, että muodostettiin yritysjoukko kyberturvallisuuden teknologioita tai palveluita ydin- tai pääliiketoimintanaan tuottavista yrityksistä. Rajauksesta johtuen tarkastelun ulkopuolelle jäävät siis mm. sellaiset yritykset, joilla kyberturvallisuuden tuotteet ja palvelut muodostavat vain osan liiketoiminnasta (esim. isot konsultointiyritykset, joilla kyberturvallisuus osa palvelutarjoamaa). Yrityksiä identifioitiin 78 kappaletta. Taulukossa esitetty liikevaihdon kasvu on laskettu jokaiselle aineiston yritykselle kolmen viimeisen vuoden keskiarvona. Otanta määrän erot perustuvat aineistossa oleviin puutteellisiin tietoihin. Tiedot perustuvat Orbis-tietokannan tietoihin. Lukuja tarkasteltaessa on otettava huomioon, että yritysjoukon rajaus ei ole yksiselitteistä johtuen kyberturvallisuusalan luonteesta ja näin ollen luvut ovat arvioita. Aiemmissa arvioissa on esitetty jossain määrin pienempiä lukuja. Esimerkiksi liikevaihdoksi on arvioitu noin 350 miljoonaa euroa ja täysipäiväisten työntekijöiden määräksi alan yrityksissä 1500 henkilöä, muissa yrityksissä ja julkisella sektorilla ja tutkimuksessa vajaat 1500 henkilöä ja lisäksi osana omaa työnkuvaa noin 2000 henkilöä (FISC ry:n arviot; Remes & Kyheröinen 2015). Erot johtuvat luultavimmin siitä miten yrityskenttä on rajattu ja miten ja mistä tietoja on kerätty. Tässä tutkimuksessa esitetyt luvut sisältävät suomalaisten yritysten toiminnan myös Suomen ulkopuolella.



Kuva 2.10. Yritysten viennin suuntautuminen maantieteellisille alueille. Lähde: Yrityskysely.[14]

Käytännössä kansainvälistyminen on kuitenkin alan yrityksille merkittävä haaste ja kasvun kannalta pääsy kansainvälisille markkinoille on avainasemassa. Vaikka Suomessa on myös nopeasti kansainvälistyneitä alan yrityksiä (esimerkiksi Codenomicon ja nSense)[15], kansainvälistyminen ja kasvu ovat yleisesti ottaen merkittävä pullonkaula alan yritystoiminnan kehittymiselle. Sekä yritysten pieni koko että kotimarkkinoiden pienuus hankaloittavat kansainvälistymistä. Osa yrityksistä myös toimii palvelu- ja konsultointiliiketoiminnassa jossa skaalautuminen kansainvälisille markkinoille on vaikeampaa kuin tuotepohjaisessa liiketoiminnassa. Kansainvälistymistä hankaloittaa myös pääomien puute (Remes & Kyheröinen 2015). Kasvupotentiaalia yritykset näkevät nimenomaan ulkomailla ja ala myös kasvaa kansainvälisesti vahvasti.

Yhtenä kasvun esteenä yritykset kokevat myös osaajien puutteen ja osaavan työvoiman saatavuuden: 60 prosenttia kyselyyn vastanneista yrityksistä sitä mieltä, ettei soveltuvaa työvoimaa ole Suomessa hyvin saatavissa. Rekrytointiongelmia yrityksillä on ollut liittyen mm. kryptologiaan, myyntiosaamiseen, tietoturvaan liittyvään syvälliseen ohjelmointiosaamiseen sekä identiteetin ja pääsynhallintaan.

Kasvun ja kansainvälistymisen haasteista osaltaan kertoo myös se, että vuoden 2012 jälkeen useita lupaavia alan yrityksiä on myyty ulkomaille: Stonesoft (ostajana Intel), Blancco (ostajana Regeneris), Secproof (ostajana Deloitte), Ubisecure Solutions (ostajana GlobalSign), Trusteq (ostajana KPMG) sekä Codenomicon (ostajana Synopsys). Näiden lisäksi alalla on tapahtunut konsolidoitumista, sillä Nixu listautui pörssiin ja osti Panorama Partnersin, F-Secure osti nSensen sekä Efecte osti RM5 Softwaren. Yritysostot sekä alan organisoituminen todistavat yhtäältä yritysten kilpailukyvystä. Toisaalta kärkiyritysten myynti ulkomaille saattaa olla haaste kansallisen kyberturvallisuuden osaamisen ja omavaraisuuden näkökulmasta, mikäli yritysostojen myötä osaamista siirtyy ulkomaille ja toimintaa lakkautetaan Suomessa. Toistaiseksi ei kuitenkaan ole näyttöä siitä, että näin olisi käynyt. Huomionarvoista alan kehityksessä on myös se, että sarjayrittäjyyttä ei merkittävässä määrin ole syntynyt, eli yritysten myynnistä saadun pääomat eivät ole kiertäneet takaisin alan kehitystä tukemaan.

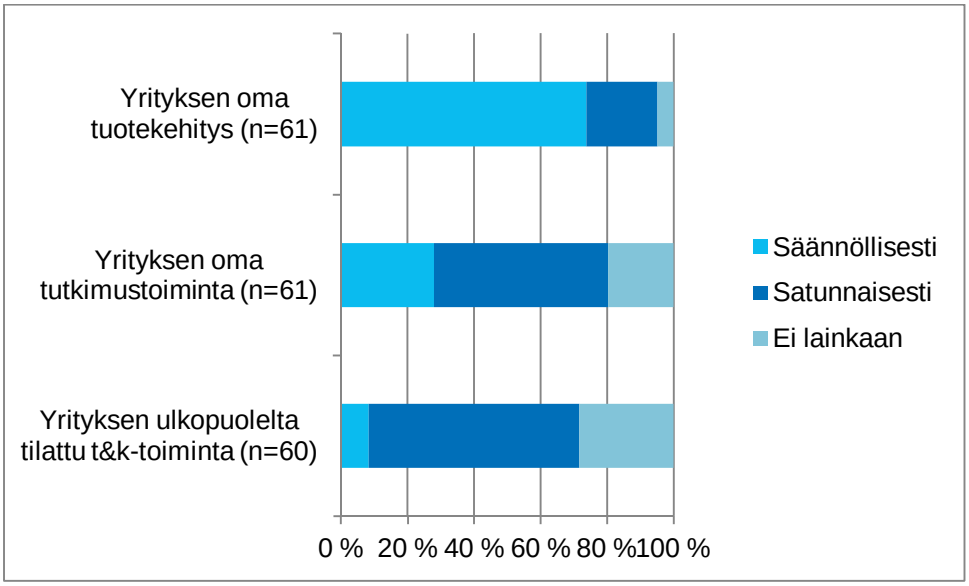
[14] Kyselyssä kysymys oli muotoiltu seuraavasti: ”Millä maantieteellisillä markkinoilla yrityksenne myy kyberturvallisuuteen liittyviä tuotteita ja/tai palveluja?”

[15] Codenomicon on vuodesta 2015 osa Synopsys-konsernia ja nSense osa F-Securea.

Toisaalta on huomattava, että kansainväliset yritykset ovat myös perustaneet tieto- tai kyberturvallisuuteen keskittyviä yksiköitä Suomeen. Yksi esimerkki on Huawein tutkimuskeskus, jossa vuonna 2014 työskenteli noin 50 henkilöä ja jonka yksi painopistealue on tietoturva (Kärkkäinen 2014). Myös esimerkiksi Ericssonilla on merkittävä tietoturvayksikkö Suomessa.

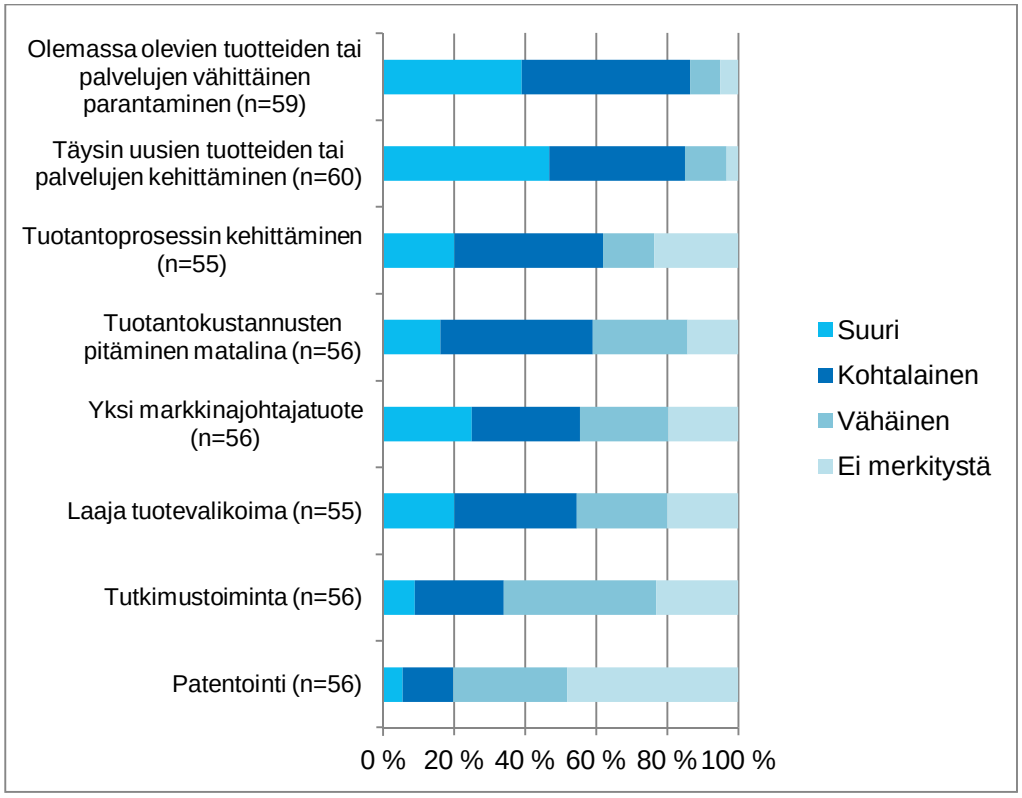
2.3.1 Tutkimus-, kehitys- ja innovaatiotoiminta

Yrityskyselyn perusteella alan yritykset tekevät varsin vahvasti tuotekehitystoimintaa: 80 prosenttia vastanneista yrityksistä tekee säännöllisesti omaa tuotekehitystä (kuva 2.11). Tutkimustoiminnan merkitys on sen sijaan huomattavasti vähäisempi. Säännöllisesti omaa tutkimustoimintaa tekeviä yrityksiä oli 28 prosenttia. Käytännössä suuri osa yrityksistä investoi t&k-toiminnassaan pitkälti käsillä oleviin ongelmiin, mutta tutkimukseen ja pitkäjänteisempään tulevaisuuden ymmärtämiseen panostetaan huomattavasti vähemmän. Alan nopean kehityksen vuoksi (merkittävä) osa kehityspanoksista menee myös olemassa olevien tuotteiden ylläpitoon ja päivittämiseen.



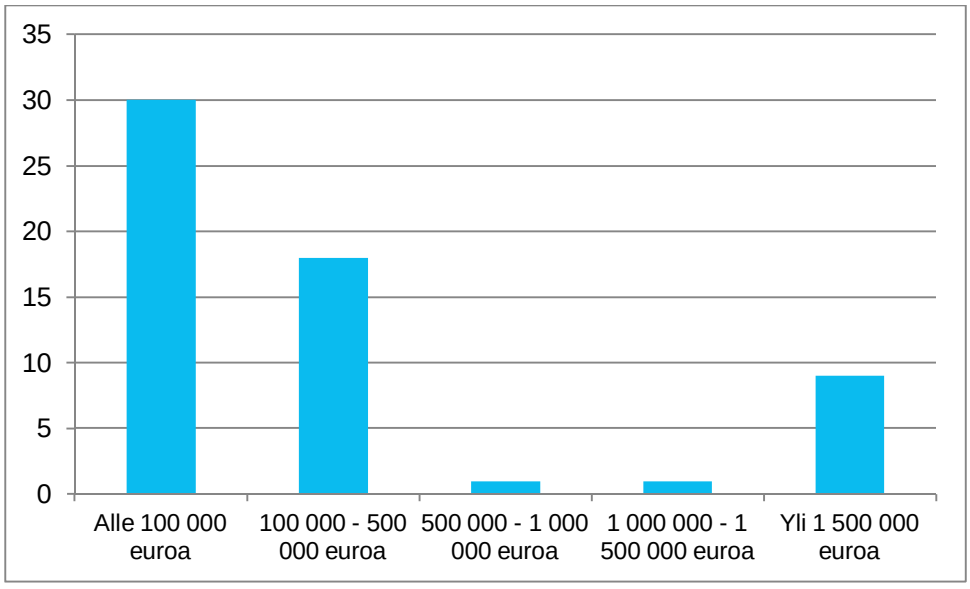
Kuva 2.11. Yritysten innovaatiotoimet. Lähde: Yrityskysely

Tuotekehityksen merkitys näkyy myös siinä, että olemassa olevien tuotteiden ja palvelujen vähittäinen kehittäminen ja täysin uusien tuotteiden ja palvelujen kehittäminen ovat alan yrityksille tärkeimpiä tekijöitä liiketoiminnan kehittämisen näkökulmasta (kuva 2.12). Vastaavasti tutkimustoiminnalla on suuri tai kohtalainen merkitys vain noin yhdelle viidesosalle yrityksistä.



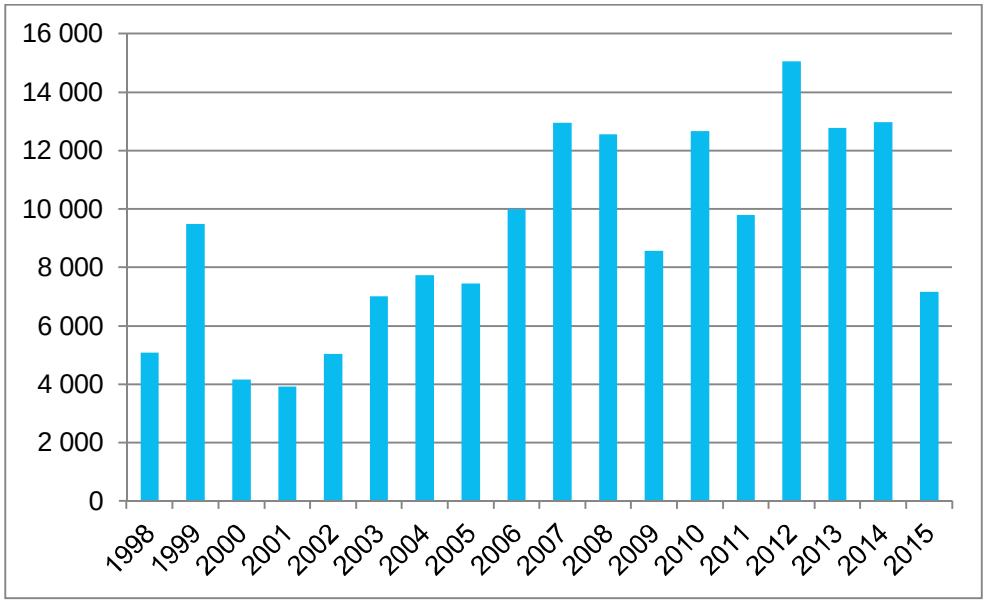
Kuva 2.12. Eri tekijöiden merkitys yritysten liiketoiminnassa. Lähde: Yrityskysely

Yrityskyselyn perusteella alan yritysten absoluuttiset t&k-panostukset eivät ole erityisen suuria (kuva 2.13.). Puolella yrityksistä vuosittainen t&k-budjetti on alle 100 000 euroa mikä vastaa noin yhden asiantuntijan palkkakustannuksia vuosittain. Huomionarvoista myös on, että yritykset, joilla on suuri t&k-budjetti (yli 1,5 miljoonaa euroa) ovat yhtä lukuun ottamatta sellaisia, joissa kyberliiketoiminnan osuus liikevaihdosta on pieni. T&k-panosten pienuuden taustalla on alan yritysten pieni koko sekä se, että monet yritykset tekevät palveluliiketoimintaa, jossa t&k-toiminnan rooli on pienempi.



Kuva 2.13. Alan yritysten vuosittainen T&K-budjetti yrityskyselyn mukaan. Lähde. Yrityskysely, (n=61).

Tekes on sijoittanut julkista tuotekehitysrahoitusta alan yrityksiin vuodesta 1998 lähtien yhteensä 164 miljoonaa euroa, ja rahoitusta on tänä aikana saanut 99 yritystä. Tekesin rahoitus on noussut selvästi vuodesta 2000 alkaen: vuonna 2000 rahoitus oli noin 4 miljoonaa euroa kun taas vuonna 2014 se oli yli 12 miljoonaa euroa (kuva 2.14.).[16]

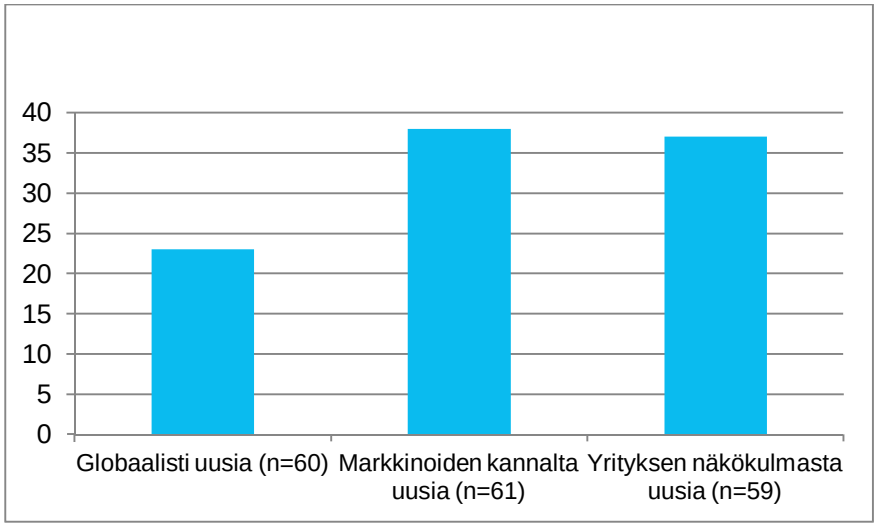


Kuva 2.14. Tekesin rahoitus kyberturvallisuusalan yrityksille 1998-2015 (tuhatta euroa). Lähde: Tekes.

2.3.2 Yritysten innovatiivisuus ja uudet tuotteet

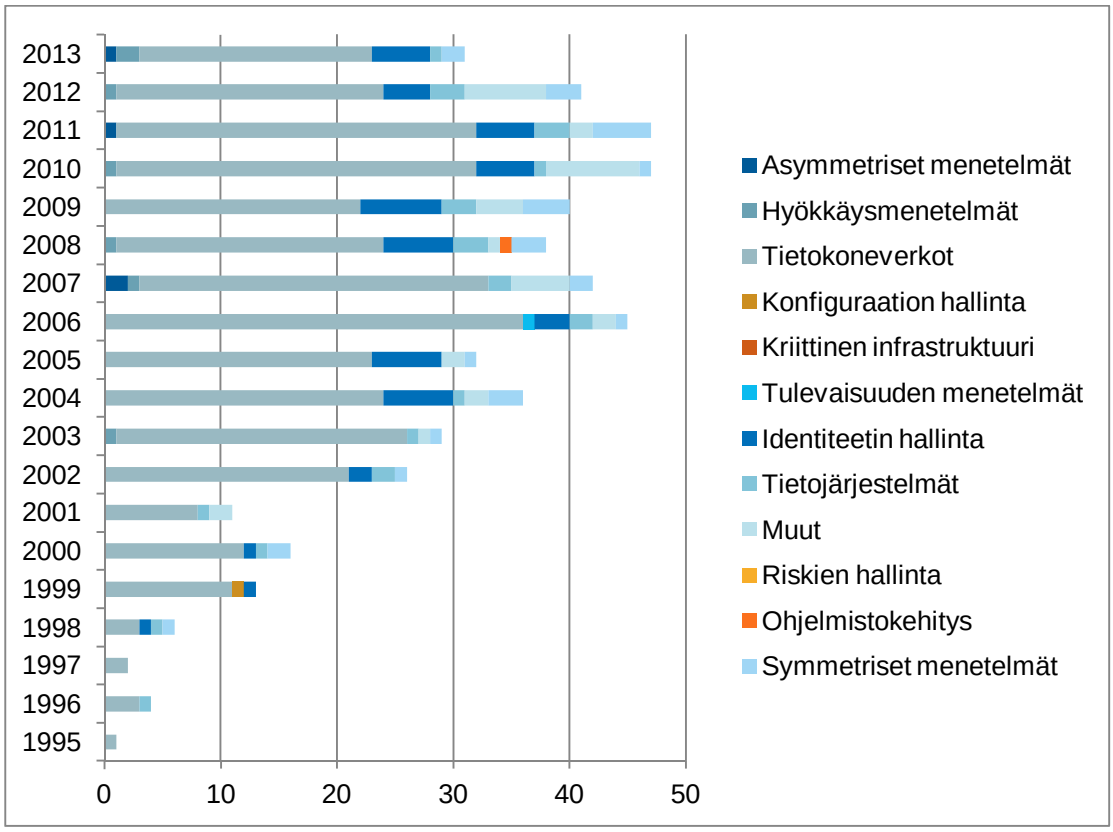
Tässä tutkimuksessa kerätyt aineistot luovat hieman ristiriitaista kuvaa alan yritysten innovaatiotoiminnasta ja uusista tuotteista. Yhtäältä yritykset näyttäytyvät varsin innovatiivisina: esimerkiksi yrityskyselyn mukaan 23 yritystä tuonut globaalisti uusia innovaatioita markkinoille viimeisen viiden vuoden aikana (kuva 2.15). Tätä voidaan pitää varsin merkittävänä, sillä globaalisti uuden innovaation määritelmä on, että vastaavaa tuotetta ei ole ollut saatavilla millään markkinoilla.

[16] Vuoden 2015 osalta kuvassa ei ole koko vuoden rahoitustietoja, joten vuosi 2015 ei ole verrannollinen muiden vuosien kanssa.



Kuva 2.15. Yritykset jotka ovat tuoneet globaalisti uusia, markkinoiden kannalta uusia tai yrityksen näkökulmasta uusi innovaatioita markkinoille viimeisen viiden vuoden aikana (kpl). Lähde: Yrityskysely.

Suomalaisille yrityksille on myönnetty 2000-luvulla keskimäärin noin vajaat 40 US patenttia vuosittain (kuva 2.16). Patenttien määrä on noussut melko vahvasti vuodesta 1995 alkaen ja erityisesti 2000-luvun alussa. Merkillepantavaa on, että valtaosa patenteista liittyy tietoverkkoihin ja että Nokia on vastannut 67 prosentista alan suomalaisista patenteista. Toiseksi merkittävin patentoija on ollut Ericsson, joka on vastannut noin kuudesta prosentista patentteja.



Kuva 2.16. Suomalaisille yrityksille myönnetyt kyberturvallisuuteen liittyvät US patentit 1995-2013. Lähde: patentti- ja julkaisuanalyysi.

VTT:n Sfinno-tietokannassa on puolestaan 45 tietoturvaan liittyvää merkittävää innovaatiota vuosilta 1987-2013. Se vastaa noin 8 prosenttia ajanjakson kaikista ICT-alan innovaatioista. Keskimäärin kyberturvainnovaatioita on siis ollut vuosittain noin kaksi, mutta viimeisenä kahtena vuonna innovaatioita on ollut selvästi enemmän. Yrityksistä F-Secure on ollut merkittävin innovaattori (11 innovaatiota), sen jälkeen tulevat SSH (4 kpl), Sonera (4 kpl), Stonesoft (2 kpl), DNA (2 kpl).

Toisaalta Viestintävirasto tuotehyväksyntätilastot kertovat siitä, että kotimaisia salaustuotteita ei ole juuri lainkaan (Kyberturvallisuuskeskus 2015). Esimerkiksi vuonna 2014 Kyberturvallisuuskeskus hyväksyi kaksi salaustuotetta. Myös haastatteluissa esitettiin näkemyksiä, että täysin uusia tuotteita ei alalta Suomesta ole viimeisen viiden vuoden aikana juurikaan tullut.

Eräs haaste nimenomaan salaustuotteiden tuotekehitykselle Suomessa on eurooppalaisen AQUA-statuksen puute. Statuksen voi saada maa, jolla on vahva osaaminen ja resurssit salaustekniikoissa ja siten kyky arvioida muiden maiden salaustuotteita. Suomen kannalta statuksen puute merkitsee yhtäältä sitä, että Suomeen ei tule muiden maiden salaustuotteita arvioitavaksi, eikä Suomeen näin ollen saada arvokasta tietoa muiden tekemästä tuotekehityksestä. Toisaalta haitta on myös siinä, että statuksen saaneet maat saattavat jarruttaa sellaisten maiden tuotteiden hyväksyntää, joilla ei ole statusta.

2.4 Julkinen hallinto

Vaikka suuri osa kyberturvallisuusosaamisesta, ja etenkin valtaosa alan tutkimus- kehitys- ja innovaatiotoiminnasta, sijaitsee yritys- ja tutkimussektoreilla, myös julkisella hallinnolla ja viranomaisilla on keskeinen rooli kyberosaamisen kehittymisessä. Julkinen sektori mm. luo yleisiä puitteita ja toimintaedellytyksiä alan kehitykselle esimerkiksi lainsäädännön, resursoinnin ja strategiatyön kautta, rahoittaa ja tukee alan tutkimus- ja koulutustoimintaa yliopistoissa ja tutkimuslaitoksissa, toimii merkittävänä ostajana ja asiakkaana alan yrityksille, suuntaa alan kehitystä jne. Seuraavassa ei pyritä tyhjentävästi tarkastelemaan julkisen sektorin roolia kyberosaamisen kentässä, vaan keskitytään muutamaan olennaiseen seikkaan, jotka ovat nousseet esiin tutkimuksen kuluessa. Resursoinnin osalta tutkimus- ja kehitystoiminnan rahoitusta on käsitelty luvussa 2.1.

Ensinnäkin on syytä huomata, että julkisella sektorilla on Suomessa tärkeitä osaamiskeskittymiä kyberturvallisuusalueella. Tällaisia ovat esimerkiksi Viestintäviraston Kyberturvallisuuskeskus, Keskusrikospoliisin Kyberrikostorjuntakeskus ja Puolustusvoimat, mutta näiden lisäksi osaamista on luonnollisesti muissakin organisaatioissa. Osassa näistä organisaatioista tehdään myös omaa tuotekehitystoimintaa, kuten esimerkiksi Kyberrikostorjuntakeskuksessa. Kyberturvallisuuskeskus ja Kyberrikostorjuntakeskus ovat varsin uusia organisaatioita, sillä ne on perustettu vasta viime vuosina (2014 ja 2015). Organisaatioiden perustaminen kuvaakin hyvin kyberturvallisuuden merkityksen kasvua, johon näillä yksiköillä on pyritty vastaamaan.

Julkisen sektorin organisaatioissa on korkeatasoista osaamista ja haastatteluissa korostetaan erityisesti korkeatasoista CERT-toimintaa. Kansallisen kyberosaamisen näkökulmasta merkittävää kuitenkin on, että monien julkisen hallinnon kyberturvallisuustoimijoiden yhteistyö tutkimustoimijoiden (yliopistot, ammattikorkeakoulut, tutkimuslaitokset) kanssa on varsin vähäistä. Yhteistyön vahvistaminen olisi hyvin tärkeää kansallisen osaamisen hyödyntämisen ja kehittämisen näkökulmasta. Yhteistyötä on tarkasteltu lähemmin luvussa 2.5.

Suomeen luotiin 2010-luvun alussa kansallinen kyberturvallisuusstrategia joka julkaistiin tammikuussa 2013. Kansainvälisesti katsottuna Suomi oli tuolloin edelläkävijä kyberturvallisuusstrategian laatimisessa ja sittemmin monet maat ovat laatineet oman strategiansa (ks. esim. BSA 2015). Strategian tavoitteena oli, että vuonna 2016 Suomi on kyberturvallisuuden kärkimaa ja ”maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa”. Tätä tutkimusta varten tehdyissä haastatteluissa kyberturvallisuusstrategiaa kohtaan osoitetaan varsin paljon kritiikkiä. Kritiikkiä esitetään mm. liittyen strategian toimeenpanoon ja siihen kytkettyjen resurssien vähäisyyteen. Strategiaa pidetään osin eräänlaisena kompromissina ja siitä nähdään puuttuvan sellaisten tekijöiden identifiointi jotka todella veisivät Suomen edelläkävijäksi. Strategiaa arvostellaan myös siitä, että yritystoiminnan näkökulma siinä on vähäinen. Aineiston valossa strategia kaiken kaikkiaan näyttäytyy jossain määrin ristiriitaisena. Kyberosaamisen kehittämisen näkökulmasta erityisen merkittävää on, että strategia ei ole kyennyt luomaan vahvaa yhteistä visiota ja yhteistyön henkeä alan toimijoiden välille.

Kyberturvallisuuteen liittyvän osaamisen kehittymisen kannalta julkisen sektorin eräs merkittävä rooli liittyy julkisiin hankintoihin. Julkinen sektori ostaa merkittävässä määrin ICT-tuotteita ja -palveluita ja on siten merkittävä asiakas kyberturvallisuusalan yrityksille. Tutkimuksessa kerätyn aineiston perusteella syntyy kuva, että julkisia hankintoja ei tällä hetkellä toteuteta siten, että ne tukisivat alan kehitystä ja yritysten liike- ja innovaatiotoiminnan edistymistä. Esimerkiksi IT-palveluhankinnoissa on tapauksia, joissa on siirrytty suosimaan alhaista hintaa eikä ole korostettu alan erityisosaamista (ks. tarkemmin FISC 2015; Remes ja Kyheröinen 2015). Osa haastateltavista näkee myös, että keskitettyjen hankintajärjestelmien ja julkisen sektorin kustannuspaineen myötä hinnan merkitys hankinnoissa korostuu laadun sijasta. Hinnan merkityksen korostuminen ei ole omiaan edistämään turvallisuutta ja se saattaa myös vaikeuttaa kotimaisten ratkaisujen menestymistä tarjouskilpailuissa.

Hyvin toteutetuilla julkisilla hankinnoilla voitaisiin kuitenkin merkittävällä tavalla tukea alan kehitystä. Alan kehityksen kannalta olisi tärkeää, että julkisia hankintojen tehtäisiin siten, että alan osaaminen kumuloituisi Suomeen. Julkiset hankinnat ovat myös merkittäviä yritysten kansainvälistymisen kannalta, sillä julkisen sektorin referenssit ovat usein tärkeitä vientiponnisteluissa.

Alan hankinnoissa olisi syytä nykyistä enemmän pyrkiä myös innovatiivisiin julkisiin hankintoihin. Innovatiivisissa hankinnoissa hankitaan tilaajan tarpeeseen jotain sellaista jota ei vielä suoraan ole olemassa, vaan ratkaisun kehittäminen edellyttää toimittajilta kehitystyötä. Innovatiivisten hankintojen avulla voidaan tukea ja stimuloida yritysten tuotekehitystoimintaa ja julkinen hankkija voi saada käyttöönsä parempia ja tehokkaampia ratkaisuja.

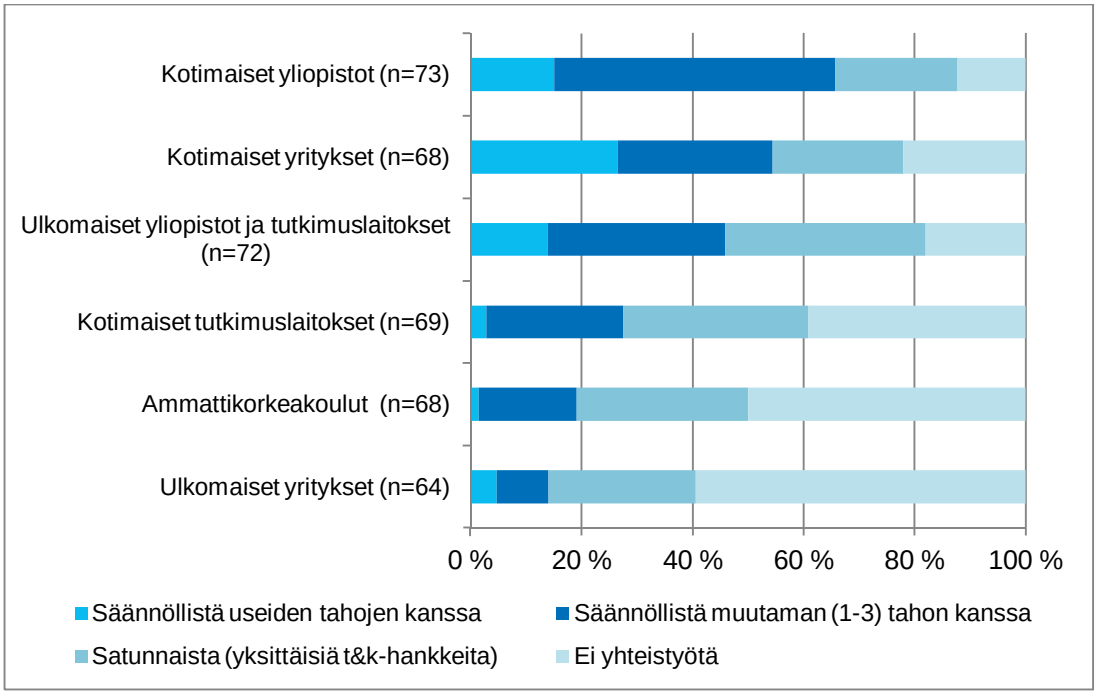
2.5 Yhteistyö ja vuorovaikutus

Kyberturvallisuusosaamisen edistämisen näkökulmasta alan toimijoiden yhteistyö on olennaisen tärkeää. Tutkimus- ja innovaatiotoiminnassa yhteistyön merkitys korostuu, ja erityisen tärkeää se on pienessä maassa, jossa toiminnan volyymilla ja resurssien määrällä ei voida kilpailla. Tutkimus- ja innovaatiotoiminnassa yhteistyö erityisesti yritysten, yliopistojen ja tutkimuslaitosten kesken on tärkeää. Tämän lisäksi on olennaista, että julkisella hallinnolla ja viranomaisilla on riittävän tiiviit yhteydet tutkimus- ja yritysmaailmaan, jotta kansalliset tarpeet kanavoituvat tutkimus- ja koulutusmaailmaan ja toisaalta tutkimusmaailman näkemykset ja ajankohtainen tieto välittyvät hallintoon.

Viime vuosina kyberturvallisuusalan yhteistyötä on pyritty vahvistamaan useiden uusien aloitteiden myötä. Näitä ovat olleet Finnish Information Security Cluster ry (FISC), Innovatiiviset kaupungit (INKA) -ohjelman kyberturvallisuusteema sekä DIGILE SHOKin alainen Cyber Trust -ohjelma. FISC on noin viidenkymmenen tieto- ja kyberturvatuotteita ja -palveluita tuottavan yrityksen vuonna 2012 perustettu yhteistyöorganisaatio. Sen tavoitteena on tukea mm. kasvattaa ja kansainvälistää alan liiketoimintamahdollisuuksia sekä edistää kyberturvaosaamisen laajamittaista hyödyntämistä yhteiskunnassa.[17] INKA-ohjelman kyberturvallisuusteema käynnistyi vuonna 2014 ja sen tavoitteena on kehittää kyberturvallisuusliiketoimintaa, luoda uusia alan yrityksiä ja saada ulkomaisia yrityksiä etabloitumaan Suomeen sekä muodostaa kansallinen kyberturvallisuuden innovaatiokeskittymä (Innovatiiviset kaupungit 2013). Olennaisena osana ohjelmaa on yritysten ja julkisten toimijoiden yhteistyö kyberliiketoiminnan kehittämisessä. Teemaa koordinoidaan Jyväskylästä. Vuonna 2015 aloitettiin DIGILE SHOKin alla kansallisen kyberturvallisuustutkimusohjelman Cyber Trust kehittäminen. Ohjelman muodostavat 19 yritystä ja 9 yliopistoa tai tutkimuslaitosta. Nämä aloitteet ovat osaltaan edistäneet alan yhteistyötä. On kuitenkin jossain määrin epäselvää, mikä niiden rooli on jatkossa, sillä pääministeri Juha Sipilän hallituksen hallitusohjelman mukaan INKA-ohjelma lopetetaan ja SHOKit ajetaan vaiheittain alas (Valtioneuvoston kanslia 2015).

Tässä tutkimuksessa tarkasteltiin erityisesti tutkimus- ja kehitystoimintaan liittyvää yhteistyötä kyberturvallisuusalalla. Aineiston perusteella alan tutkijat korkeakouluissa ja tutkimuslaitoksissa tekevät ensisijaisesti yhteistyötä kotimaisten yliopistojen ja yritysten kanssa (ks. kuva alla). Vähiten yhteistyötä tutkijat tekevät ammattikorkeakoulujen ja ulkomaisten yritysten kanssa. Kansainvälistä yhteistyötä tehdään puolestaan pääasiassa ulkomaisten yliopistojen ja tutkimuslaitosten kanssa. Kansainväliset kumppanit hajautuivat kuitenkin useisiin maihin. Näitä ovat esimerkiksi Yhdysvallat, Alankomaat, Itävalta, Australia ja Saksa.

[17] http://www.fisc.fi/



Kuva 2.17. Kyberturvallisuusalan tutkijoiden yhteistyö eri organisaatioiden kanssa viimeisen viiden vuoden aikana kyberturvallisuuteen liittyvässä tutkimuksessa (%). Lähde: Tutkimus- ja koulutusorganisaatioiden kysely.

Tutkijoiden yhteistyö on myös pääasiassa satunnaista tai sitä tehdään säännöllisesti muutaman (1-3) tahon kanssa. Suhteellisen vähäinen yhteistyö kotimaisten tutkimuslaitosten kanssa selittynee pääosin sillä, että tutkimuslaitoksissa ei tehdä laajasti kyberturvallisuuteen liittyvää tutkimusta VTT:tä lukuun ottamatta. Vähäinen yhteistyö ammattikorkeakoulujen kanssa puolestaan liittynee niiden painottumisella koulutukseen ja käytännölliseen kehittämiseen. Kansainvälisessä yhteistyössä on erilaisia vastaajakohtaisia profiileja. Osa tutkijoista tekee laajasti kansainvälistä yhteistyötä, toiset vähemmän.

Yhteistyötä tutkimusorganisaatioiden välillä hankaloittavat aineistojen mukaan mm. tutkimuksen poikkitieteellisyys, alan tutkimuksen vähäisyys sekä suuri opetusmäärä. Negatiivisimmissa kommenteissa todettiin kotimaisen tutkimuksen tason olevan huono. Lisäksi kommentoitiin muun muassa toimintakulttuuria, joka ei tue avointa tiedon jakamista, sekä yhteistyön vaikeutta jopa saman yliopiston sisällä.

Tutkijat kokevat haasteita myös yritysten kanssa tehtävässä yhteistyössä. Yritysyhteistyö saattaa olla hankalaa muun muassa siksi että yritykset varjelevat omaa osaamistaan ja epäilevät tietovuotoja kilpailijoille yliopistoyhteistyön kautta. Yhteistyötä saattavat vaikeuttaa myös resurssien vähäisyys sekä käytetyt rahoitusmallit. Yritysten näkökulmasta yliopistoyhteistyötä saattaa vaikeuttaa puolestaan tutkimusalan hajanainen rakenne, keskinäinen kilpailu ja tiedon puute.

> ”Olisi ihan hyvä tietää, että kun tehdään kyberturvallisuutta, eihän siitä kauhean selkeätä kuvaa ole, että kuka Suomessa, mikä oppilaitos on mihinkin erikoistunut. Tämä on hajanainen kenttä ja kaikki laitoksetkin kilpailevat keskenään. Ei ole sellaista yhtä puolueetonta tyyppiä, jolta sinä voisit kysyä, että kuka tämän oikeasti tietää. - - Epätoivoissaan kaikki laitokset vain yrittävät saada jonkun kulman edes itsellensä.”

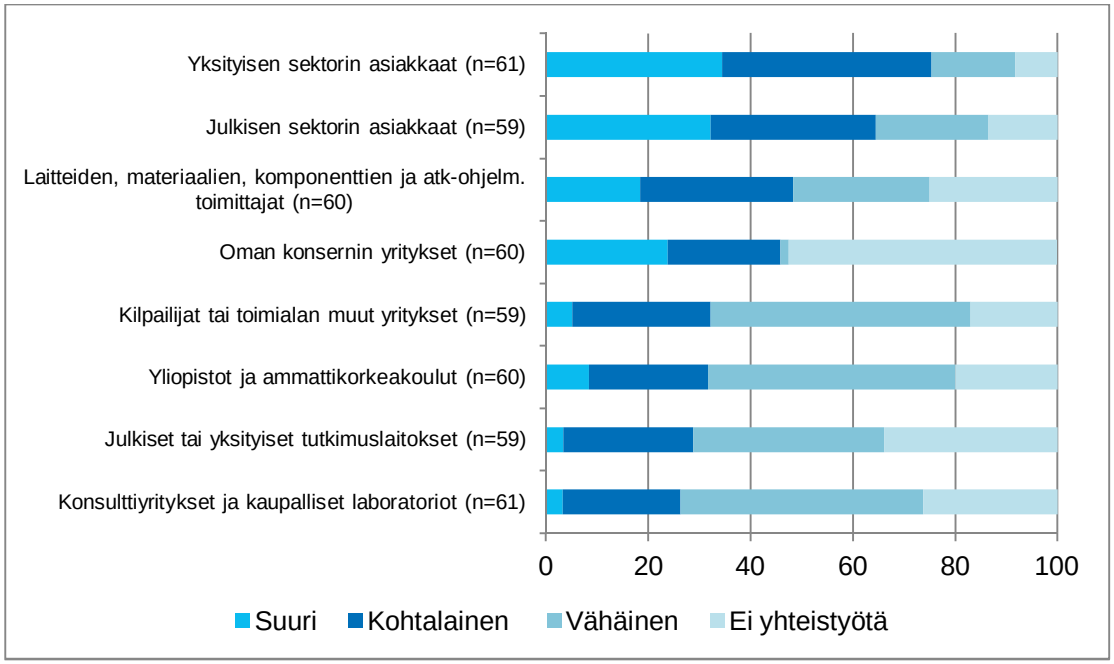
Tutkimusorganisaatioiden edustajat arvioivat myös sitä, kuinka hyvin yhteistyö toimii tutkijoiden ja viranomaisten välillä sekä korkeakoulujen, tutkimuslaitosten ja yritysten välillä. Vaikka yhteistyö näyttäisi olevan kummassakin tapauksessa useimmiten ainakin osin toimivaa, siinä on myös selkeästi parannettavaa kuten täysin samaa mieltä olevien vähäinen osuus sekä osittain sekä täysin eri mieltä olevien osuudet osoittavat (taulukko 2.5).

Taulukko 2.5. Yhteistyön toimivuus tutkimus- ja koulutusorganisaatioiden vastaajien näkökulmasta (%)

	Yhteistyö tutkimustoimijoiden ja viranomaisten välillä kyberturvallisuuteen liittyvissä kysymyksissä toimii hyvin (n=75) (%)	**Korkeakoulujen, tutkimuslaitosten ja yritysten yhteistyö kyberturvallisuuteen liittyvässä tutkimus- ja kehitystyössä on toimivaa Suomessa (n=74) (%)**
Täysin samaa mieltä	5,3	5,4
Osittain samaa mieltä	46,7	48,6
Osittain eri mieltä	21,3	28,4
Täysin eri mieltä	5,3	5,4
En osaa sanoa	21,3	12,2
Yhteensä (%)	100	100

Niiltä osin kun yhteistoiminta on toimivaa siihen saattaa vaikuttaa Suomessa suhteellisen pieni toimijoiden verkosto esimerkiksi viranomaistoiminnassa. Toisaalta haastateltujen mukaan yhteistyö edellyttäisi myös uudenlaisia avauksia ja kehittämistä sekä rakenne- että resurssimielessä. Huomionarvoista myös on, että eräiltä osin alan julkisen hallinnon ja viranomaistoimijoiden yhteydet tutkimusmaailmaan ovat vähäiset eikä hallinnossa tunneta alan tutkimustoimintaa ja sen tilaa.

Kyberturvallisuusalan yritysten innovaatiotoiminnan yhteistyössä painottuvat yliopistojen ja tutkimuslaitosten sijaan asiakkaat, alihankkijat ja muut toimialan yritykset (kuva alla). Yliopistoilla ja erityisesti tutkimuslaitoksilla on vähäisempi merkitys. Erityisen kiinnostavaa on, että julkisen sektorin asiakkaat ovat hyvin vahvoja kumppaneita yritysten innovaatiotoiminnassa yksityisen sektorin ohella.



Kuva 2.18. Eri yhteistyötahojen merkitys yritysten innovaatiotoiminnassa. Lähde: Yrityskysely.

Kyberturvallisuusalan yritysten innovaatiotoiminnan yhteistyö näyttäisi olevan samansuuntaista kuin yritysten innovaatioyhteistyö ylipäänsä Suomessa. Tilastokeskuksen tekemän innovaatiokyselyn mukaan suomalaisten yritysten merkittävimmät yhteistyötahot ovat oman konsernin yritykset ja asiakkaat (Tilastokeskus 2008)[18]. Kyberturvallisuusala poikkeaa tästä siinä, että oman konsernin yritysten merkitys on vähäisempi. Tätä eroa selittää kyberalan yritysten keskimäärin varsin pieni koko. Toinen ero on siinä, että yliopistojen, korkeakoulujen ja tutkimuslaitosten merkitys on kyberalalla hieman suurempi kuin yrityksissä yleensä. Lisäksi huomionarvoista on, kyberalan yritykset näyttävät tekevän useammin yhteistyötä kuin yritykset yleensä: niiden yritysten osuus, jotka eivät tee innovaatioyhteistyötä, on kaikissa kategorioissa selvästi pienempi kuin koko yrityskentällä. Tämän tutkimuksen yrityskyselyn ja Tilastokeskuksen innovaatiokyselyn tulosten vertailun osalta on kuitenkin syytä olla jossakin määrin varovainen, sillä kyberturvallisuusalan yrityskyselyn vastaajien määrä on kokonaisuudessaan varsin pieni.

Vaikka yliopistot eivät olekaan keskeisiä innovaatiotoiminnan kumppaneita yrityksille, niiden merkitys tunnistetaan erityisesti riskialttiimmassa tutkimustoiminnassa. Haastatteluiden mukaan uusia ideoita voidaan kokeilla ja riskialttiimpaa tutkimusta tehdä yliopistojen kanssa. Resurssien käyttöön liittyvät riskit pienenevät, mutta samalla on mahdollista että tutkimus tuottaa myös jotakin sellaista uutta, jota voidaan hyödyntää kaupallisissa sovelluksissa.

Varsin monesti yritysten välinen yhteistyö koettiin haastatteluissa ongelmallisena. Yritykset kokevat olevansa ensisijaisesti toistensa kilpailijoita jolloin edes esikaupallista yhteistyötä ei tehdä. Toimivia käytäntöjä on olemassa, mutta asenteisiin ja toimintamalleihin kaivattaisiin myös muutoksia. Yritysten nykyistä laajempi yhteistyö hyödyttäisi niitä muun muassa tietoturvariskeihin varautumisessa, jos esimerkiksi tietoa tapahtuneista tietomurroista jaettaisiin avoimesti yritysten kesken. Nyt käytäntö on rajallinen. Yhteistyön lisääminen hyödyttäisi

[18] Uudempaa tietoa ei ole ollut julkisesti saatavissa. Suomen virallinen tilasto (SVT): Innovaatiotoiminta [verkkojulkaisu].ISSN=1797-4380. 2008, Taulukko 26. Innovaatiotoimintaan liittyvä yhteistyö yhteistyökumppanin merkityksen mukaan 2006–2008, osuus innovaatiotoimintaa harjoittaneista yrityksistä . Helsinki: Tilastokeskus [viitattu: 26.1.2016]. Saantitapa: http://www.stat.fi/til/inn/2008/inn_2008_2010-06-10_tau_027_fi.html

myös yritysten kasvattamisessa sekä tuotteiden ja palveluiden viennissä. Tällainen yhteistyö on kuitenkin toistaiseksi ollut vähäistä tai satunnaista.

> ”Me olemme liian pieniä siihen [globaaleille markkinoille menoon] yksittäisinä yrityksinä. Jos me pystyisimme tekemään kattavampaa kokonaistarjontaa siihen, että me yhdistämme näitä osa-alueita. Meillä on osaajia, siis maailmanluokan osaamista virustorjunnassa, meillä on maailmanluokan osaamista verkkopuolen teknologioissa, päätelaitteissa. - - Mutta ne ovat siiloutuneita, ne ovat yksittäisissä yrityksissä. Ja ehkä niitä ei sinällään mielletä vientituotteiksi, mutta vähintä, mitä voisi tehdä, on se, että me saisimme tehtyä edes kansallisesti yhteistyötä.”

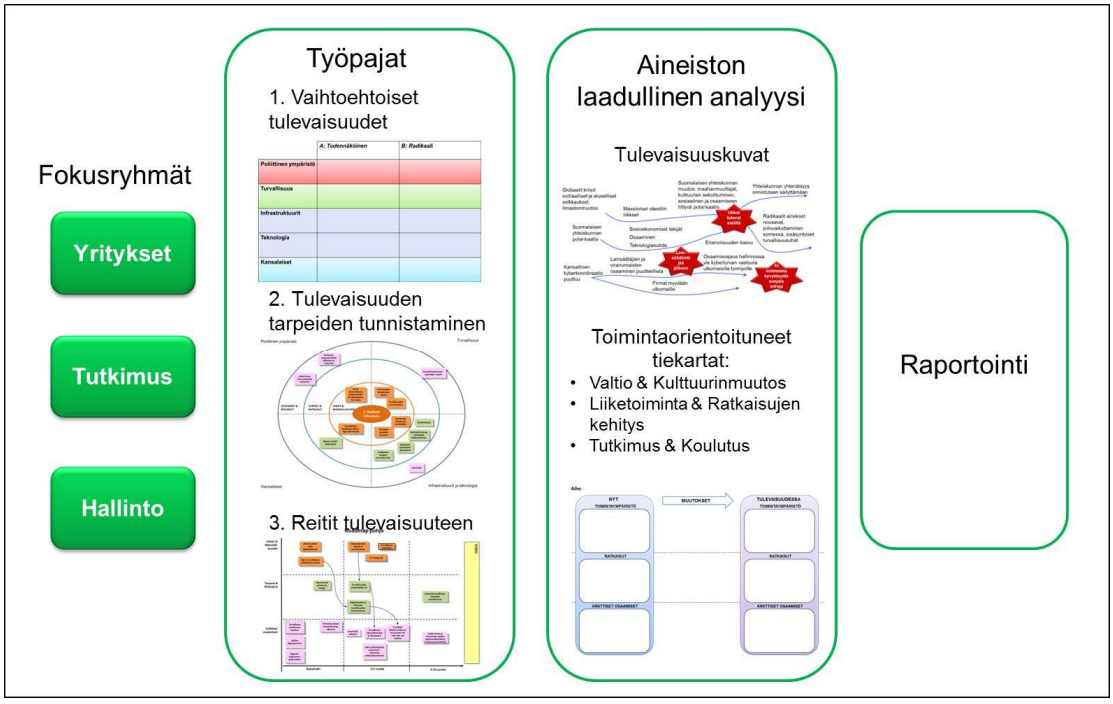
Kyberturvallisuusalalla ei voidakaan puhua toimivasta ekosysteemistä. Yhteistyötä ei ole riittävästi eri toimijoiden välillä. Tilanteen korjaamiseksi kaivataan julkisen toimijan aktivoivaa panosta sekä rahoitusta, joka mahdollistaisi toimivan ”ytimen” kehittämisen kyberturvallisuuden kentälle.

> ”Voi olla, että se jossakin piilossa on siellä, ja varmaan osittain joillakin toimialoilla saattaa olla ekosysteemi, joka käsittää sitten muutaman toimijan. - - Ekosysteemi vaatii sen, että joku joutuu aina potkimaan. Nämä eivät itsestään synny, vaikka sinulla olisi mahdollisuus. Toteutuakseen ekosysteemi mielestäni vaatii sen, että meillä on jonkunlainen perusta, rahoitusmalli, mistä me saamme rahoituksen. Se vaatii, että tämän sateenvarjon alla me mahdollistamme kaikkien toimijoitten keskinäisen kanssakäymisen jossakin muodossa. Sitä kautta se ekosysteemi syntyy pikkuhiljaa.”

Laajempaa kansallista koordinaatiota ja tukea kentän yhteistoiminnan vahvistamiseksi kaivattiinkin useissa haastateltavien kommenteissa. Sellaiseksi hahmoteltiin muun muassa jo olemassa olevien kansallisten kyberturvallisuusalueen toimijoiden yhdistämistä laajemmaksi kokonaisuudeksi tai uudenlaisen kyberturvallisuuden neuvottelukunnan perustamista.

3. KYBEROSAAMISEN TULEVAISUUS

Kyberosaaminen Suomessa -hankkeen tulevaisuuteen suuntaavassa osiossa toteutettiin tiekarttaprosessi. Sen tavoitteena oli kerätä kyberturvallisuusalan eri sidosryhmien näkemyksiä Suomen vahvuuksista, tulevaisuuden painopistealueista ja muutostarpeista, joiden avulla vahvistetaan kyberturvallisuusstrategian toteutumista sekä edistetään tietoyhteiskuntaa ja alan liiketoimintamahdollisuuksia. Tiekarttatyöskentely toteutettiin kolmessa erillisessä työpajassa (ks. kuva 3.1), jotka pidettiin lokakuussa 2015. Ensimmäiseen työpajaan osallistui liikeelämän ja yritysten edustajia, toiseen tutkimuksen ja kolmanteen valtionhallinnon edustajia. Työpajojen osallistujat on listattu liitteessä 2. Kaikki työpajat työskentelivät saman kolmivaiheisen rungon mukaisesti ja työskentely tapahtui kaikissa työpajoissa kahdessa pienryhmässä. Tulevaisuustyöskentely aloitettiin hahmottelemalla Suomen tulevaisuutta kymmenen vuoden aikajänteellä kyberturvallisuuden näkökulmasta. Tämän työvaiheen tarkoitus oli virittää osallistujat tulevaisuuden maailmaan. Toisessa vaiheessa tunnistettiin hahmotellun tulevaisuuskuvan synnyttämiä mahdollisuuksia, uhkia, muutostarpeita ja kriittisiä osaamistarpeita. Tämän ideointivaiheen jälkeen ryhmät muodostivat vielä tiekarttarunkoon oman tiivistyksensä olennaisimmista toimenpiteistä ja tehtävistä kohti toivottua tulevaisuuden tilannetta.



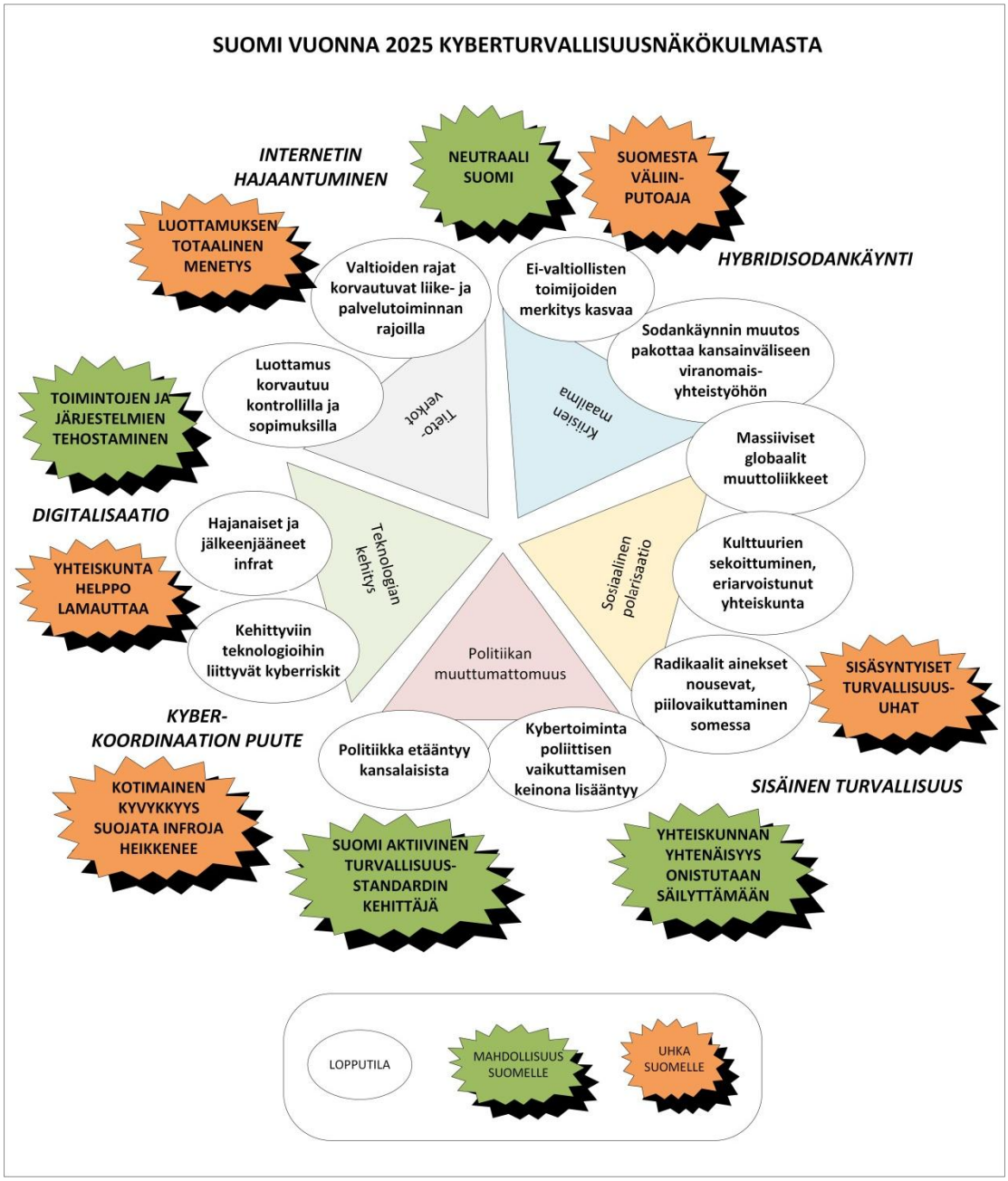
Kuva 3.1. Tulevaisuusaineisto tuotettiin kolmessa eri ryhmille suunnatussa työpajassa kolmivaiheisella työskentelyprosessilla. Aineistosta muodostettiin tulevaisuuskuva ja kolme tiekarttaa.

Työpajojen avulla saatiin kerättyä laaja laadullinen tulevaisuusaineisto. Aineiston analyysissä keskityttiin kahteen asiaan: tulevaisuuskuvan ja tiekarttojen muodostamiseen. Tulevaisuuskuvan muodostamista varten kaikkien työpajojen tulevaisuuskuvaa käsittelevä aineisto integroitiin yhteen ja siitä tunnistettiin yhteisiä teemoja ja niihin liittyviä kehityskulkujen kuvauksia. Näistä koostettiin yksi todennäköistä tulevaisuutta kuvaava esitys, jota käsitellään tarkemmin luvussa 3.1. Tämän tulevaisuuskuvan voidaan ajatella edustavan Suomen kyberturvallisuus-

alan toimijoiden tämänhetkistä näkemystä siitä, minkälaiseen tilanteeseen päädytään kymmenessä vuodessa, mikäli kehitys jatkuu sellaisena kuin se nyt on nähtävissä. Todennäköistä tulevaisuuskuvaa täydentävät eri pienryhmien tuottamat ”radikaalin tulevaisuuden” kuvaukset, joissa jonkin tulevaisuuden kehityssuuntaa ohjaavan muuttujan on ajateltu muuttuvan radikaalisti tämän päivän tilanteeseen verrattuna. Toinen osuus prosessin tuloksista muodostuu kolmesta tiekarttaesityksestä, jotka tarkastelevat Suomen kyberalaan liittyvää tulevaisuutta kolmesta eri näkökulmasta. Ensimmäinen on valtion ja kulttuurinmuutoksen näkökulma, toinen liiketoimintaan ja ratkaisujen kehitykseen liittyvä näkökulma ja kolmas liittyy koulutukseen ja tutkimukseen. Tiekartat esitellään tarkemmin luvussa 3.2. Tiekarttojen teemat ja niiden sisältö ovat nousseet eri ryhmien tuottamasta aineistosta kokonaisuutena, eivätkä ne sellaisenaan ole palautettavissa yksittäisen ryhmän tuottamiin tuloksiin. Tiekartat esittelevät siis sidosryhmien näkemyksiin perustuvaa ymmärrystä siitä, minkälaisia muutoksia olisi saatava aikaan, jotta toivottu tulevaisuuden tila voitaisiin saavuttaa. Tiekarttoja ei pidä tulkita yksiselitteisinä toimintasuunnitelmina tai toimenpidesuosituksina, vaan niissä esitettyjä asioita tulisi arvioida erikseen strategisen suunnittelun ja päätöksenteon yhteydessä. Tiekartat edustavat kuitenkin kyberturvallisuusalan piirissä toimivien henkilöiden näkemystä tulevaisuuden muutostarpeista ja toivotusta tulevaisuudesta.

3.1 Tulevaisuuskuvat

Työpajojen työskentely aloitettiin todennäköisenä pidetyn tulevaisuuskuvan hahmottelulla tulevaisuustaulukkosovelluksen avulla. Toisena vaiheena pohdittiin vaihtoehtoista tulevaisuutta, jossa jonkin tulevaa kehitystä määrittävän muuttujan ajateltiin muuttuvan radikaalisti nykytilanteeseen verrattuna. Sen jälkeen muodostettiin radikaali tulevaisuuskuva pohtimalla, miten kyseinen muutos vaikuttaa muihin tulevaisuutta määrittäviin muuttujiin ja sitä kautta tulevaisuuden tilaan. Aineiston analyysissä muodostettiin yksi todennäköistä tulevaisuutta kuvastava tulevaisuuskuva, johon integroitiin kaikkien työryhmien tuottama aineisto. Aineistosta tunnistettiin yhteisiä teemoja ja niihin liittyviä kehityskulkuja. Tiivistelmä kyseisestä tulevaisuuskuvasta on esitetty kuvassa 3.2.



Kuva 3.2. Todennäköinen tulevaisuus työpajojen perusteella.

Todennäköisessä tulevaisuuskuvassa Suomen kybertoimintaympäristön tulevaisuus hahmottuu viiden kentän avulla, jotka liittyvät Suomen ulkoisiin ja sisäisiin tekijöihin sekä teknologian kehitykseen. *(1) Kriisien maailma* kuvastaa globaaleja kehityskulkuja, jotka vaikuttavat suomalaiseen todellisuuteen. Globaalien kriisien ja alueellisten konfliktien ennakoidaan lisääntyvän ja suurvaltojen välisen vastakkainasettelun kiristyvän. Myös ei-valtiollisten toimijoiden merkityksen uskotaan kasvavan, mikä lisää jännitteitä maailmassa. Sodankäynnin tavat muuttuvat ja hybridisodankäynnin yleistyminen, yhdessä digitalisaation etenemisen kanssa, johtaa jatkuvan haavoittuvuuden ja turvattomuuden tilaan tulevaisuudessa. Yksi kriisien maailman seuraus on massiiviset muuttoliikkeet. Isojen siirtolaisvirtojen seurauksena kulttuurien sekoittuminen ja toisaalta eri väestöryhmien eriarvoistuminen lisääntyvät tulevaisuudessa. *(2) Sosiaalinen polarisaatio* kiihtyy myös muiden määrittävien tekijöiden, kuten työllisyyden, toimeentulon, koulutuksen ja osaamisen perusteella. Tämä johtaa eriarvoistuvaan yhteiskuntaan, joka tarjoaa pohjan radikaalien ainesten nousemiselle. Sosiaalinen media tarjoaa tällai-

sille aineksille mahdollisuuden organisoida toimintaansa ja vaikuttaa yhteiskuntaan. Samanaikaisesti Suomen poliittista järjestelmää leimaa (*3) politiikan muuttumattomuus*, eli edelleen jatkuva edustukselliseen demokratiaan ja konsensushakuisuuteen perustuva politiikanteon malli, sekä poliittisen kiinnostuksen marginalisoituminen kansalaisten keskuudessa. Nämä tekijät yhdessä johtavat siihen, että politiikka etääntyy kansalaisista. Kehityssuunta jättää entistä enemmän tilaa politiikan ulkopuoliselle vaikuttamiselle, kuten lobbaamiselle ja yhden asian liikkeiden toiminnalle. Myös kybervaikuttaminen lisääntyy poliittisen vaikuttamisen keinona. Tämä kehityskulku on yhteydessä erilaisten ääriliikkeiden lisääntymiselle yhteiskunnassa.

Kyberturvallisuuden näkökulmasta uhkakuvana pidettiin kyberkoordinaation puutetta valtionhallinnossa ja osaamisvajeita lainsäätäjien ja viranomaisten keskuudessa. Tämä voi johtaa siihen, että lainsäädäntö jää jälkeen tulevaisuuden vaateista esimerkiksi uusien *(4) teknologioiden kehitykseen* liittyen. Erilaiset IoT-ratkaisut, pilvipalvelut ja BigData-sovellukset yleistyvät yhteiskunnassa. Näiden teknologioiden ja sovellusten kehitykseen liittyy paljon epävarmuuksia, joiden kyberturvallisuusriskejä ei pystytä täysin ennakoimaan. Esimerkiksi IoT-teknologiat tulevat olemaan välttämättömiä tulevaisuuden tuotteissa niiden kilpailukyvyn varmistamiseksi, mutta niiden tietoturvallisuuden varmistaminen ei välttämättä toteudu teknologian kehityksen yhteydessä. Pilvipalvelut ja BigData-sovellukset voivat puolestaan muodostua ongelmallisiksi yksityisyyden suojan näkökulmasta. Keskeisin kyberturvallisuuteen vaikuttava teknologiankehitystrendi on kiihtyvä digitalisaatio eli yhä useampien palveluiden ja järjestelmien muuttuminen digitaalisiksi. Digitaaliset ratkaisut sulautuvat entistä enemmän ihmisten arkeen ja siten teknologiariippuvuus kasvaa.

Teknologisten järjestelmien uusiminen vaatii rahaa. Resurssiniukkuuden vuoksi uusimista on tehtävä inkrementaalisesti, pieni pala kerrallaan, mikä estää isojen kertaluontoisten parannusten tekemisen ja siten hidastaa kehitystä. Tämä voi johtaa siihen, että erilaiset teknologiset infrat muodostuvat hajanaisiksi ja jäävät jälkeen kehityksestä. Tällä seikalla on edelleen kyberturvallisuutta huonontava vaikutus. Erityisesti *(5) tietoverkot* ja niiden tila ovat keskeinen tekijä tulevaisuuden kybertoimintaympäristössä. Mahdollisena kehityssuuntana pidetään sitä, että Internet hajaantuu alueellisiin verkkoihin, joiden välille voi muodostua joko valtiovetoisia rajavyöhykkeitä siten, että toiset valtiot haluavat pitää verkon tiukemmin omassa valvonnassaan ja täysin vapaasta tietoverkosta ei voida puhua, tai rajalinjat voivat määrittyä kaupallisin perustein, jolloin valtioiden rajat korvautuisivat liike- ja palveluntarjoajien rajoilla. Joka tapauksessa todennäköisenä kehityssuuntana pidetään sitä, että verkkovalvonta kiristyy ja sisäiset ja ulkoiset uhkat toimivat perusteena tälle suuntaukselle. Suomalaisen yhteiskunnan näkökulmasta tämä tarkoittaa sitä, että entuudestaan luottamukseen perustunut yhteiskuntamalli korvautuu kontrollilla ja sopimuksilla.

Kuvassa 3.2 on tunnistettu keskeisimmät kyberturvallisuuteen vaikuttavat muutostrendit ja niiden luomat uhkat ja mahdollisuudet Suomelle. Tiivistelmä näistä on esitetty taulukossa 3.1.

Taulukko 3.1. Suomen kybertoimintaympäristön tulevaisuuteen vaikuttavat keskeiset trendit ja niiden synnyttämät uhkat ja mahdollisuudet Suomelle.

Keskeiset trendit	Kuvaus	Uhka Suomelle	Mahdollisuus Suomelle
Hybridisodankäynti ja suurvaltasuhteiden kiristyminen	Kiristynyt poliittinen tilanne ja sodankäynnin muutos edellyttävät kansainvälistä yhteistyötä ja liittolaisia.	Suomesta tulee väliinputoaja suurvaltojen välisessä kiristyneessä tilanteessa.	Suomi voi neutraalina toimijana löytää oman mahdollisuuksia tuovan toimintaposition kiristyneessä tilanteessa.
Sisäisen turvallisuuden muutos	Yhteiskunnan polarisoituminen aiheuttaa sosiaalisia jännitteitä ja sisäisen turvallisuuden heikkenemisen.	Kyberuhat voivat nousta entistä enemmän yhteiskunnan sisältä.	Pitkäjänteiset toimet yhteiskunnan yhtenäisyyden säilyttämiseksi voivat estää turvallisuustilanteen heikkenemisen.
Kyberkoordinaation puute	Kyberturvallisuuteen liittyvää johtovastuuta ei ole määritelty selkeästi ja yhteisen tahtotilan määrittely epäonnistuu. Alan toimintaa ei onnistuta kohdentamaan yhteiseen tavoitteeseen.	Pidemmän ajan kuluessa Suomen kyvykkyys suojata kriittisiä infroja heikkenee.	Mikäli koordinaatio toimii ja alan yhteisen suunta löytyy, Suomi voi toimia aktiivisesti myös kansainvälisesti, esim. turvallisuusstandardien kehityksessä.
Digitalisaatio	Digitalisaatio etenee ja entistä useammat tuotteet ja palvelut tulevat digitaalisiksi. Yhteiskunnan teknologiariippuvuus kasvaa.	Teknologiariippuvainen ja digitalisoitunut yhteiskunta on helppo lamauttaa.	Digitalisaation mahdollistaman toimintojen tehostamisen kautta saadaan taloudellisia hyötyjä.
Internetin hajaantuminen	Internet jakautuu erilaisilla ehdoilla toimiviin alueellisiin verkkoihin.	Luottamus verkossa tapahtuvaan toimintaan heikkenee ja menetetään kokonaan.	Suomi neutraalina toimijana ja teknologisesti edistyneenä alueena voi löytää mahdollisuuksia esim. tietovarastojen sijaintimaana.

Todennäköistä tulevaisuuskuvaa täydennettiin vaihtoehtoisen tulevaisuuskuvan pohdinnalla. Taulukossa 3.2 on esitetty kokoelma eri ryhmien muodostamista radikaaleista tulevaisuuskuvista. Radikaalit tulevaisuuskuvat sisältävät samoja elementtejä kuin kaikkien ryhmien tuloksista muodostettu todennäköisen tulevaisuuden kuvaus. Siten radikaaleja tulevaisuuskuvia voidaankin pitää eräänlaisina todennäköisen tulevaisuuden laajennuksina tai toteutumina tilanteessa, jossa tietty tulevaa kehitystä määrittelevä suuntaus on korostunut voimakkaasti. Radikaalien tulevaisuuskuvien avulla voi edistää tulevaisuuteen varautumista esimerkiksi arvioimalla erilaisten toimenpiteiden vaikutusta vaihtoehtoisissa tulevaisuuksissa.

Taulukko 3.2. Ryhmien tuottamat radikaalit tulevaisuudet.

Radikaalin tulevaisuuden määrittävä tekijä	Kuvaus	Vaikutus kyberturvallisuuden näkökulmasta	Tulevaisuus-kuvan muodostanut ryhmä
Verkon hajoaminen → uusi verkko	Internetin taloudellinen hyödynnettävyys häviää katastrofin tai terrorismin seurauksena. Impulssimainen häiriö koko maailman taloudelle.	Uusi verkko rakennetaan, mahdollisuus toteuttaa ilman nykyisiä heikkouksia.	Yritykset
Aivovuoto-Suomi	Kyberala ei pysty pitämään osaajista kiinni ja Suomesta tulee maa, joka kouluttaa osaajia muualle.	Osaamisen rapautuminen rapauttaa infrat ja kansallisen kyvyn tuottaa turvallisuusratkaisuja. Vähitellen myös kykyyn kouluttaa uusia osaajia heikkenee.	Tutkimus
Euroopan rooli veturina / kyydistä putoajana	Euroopan-laajuinen yhteistyö synnyttää Euroopan internetin sisämarkkinat ja lisää Euroopan kilpailukykyä (toivekuva). / Heikkenevän eurooppalaisen kompetenssin vuoksi valta siirtyy globaaleille yrityksille (uhkakuva).	Mahdollisuus: Eurooppa vahvistaa rooliaan tietoverkkojen kehityksen edelläkävijänä yhteistyöllä, standardoinnilla ja riittävillä resursseilla. Uhka: Haavoittuva, helposti lamautettava yhteiskunta menetetyn kybertoimintakyvyn vuoksi.	Tutkimus
Kidukset: Suomen oma lokero	Kansainvälisestä epävarmuudesta ja vastakkainasettelusta huolimatta Suomi löytää oman paikan, jossa se voi hyödyntää neutraliteettiaan ja vahvaa kyberosaamistaan.	Suomi tiennäyttäjänä salausteknologioissa, kyberturvallisuuden standardoinnissa. Suomalainen tietoturvallisten palveluiden ekosysteemi muodostunut, liiketoimintamahdollisuuksia konesaleista.	Hallinto
Kiihtyvä maahanmuutto	Globaalit muuttoliikkeet kiihtyvät, mikä lisää yhteiskunnallisia jännitteitä ja ääriliikkeiden yleistymistä.	Yhteiskunnan polarisoituminen (kulttuurien eriytyminen, koulutustason heikkeneminen). Kyberuhkat ovat sisäisiä.	Hallinto

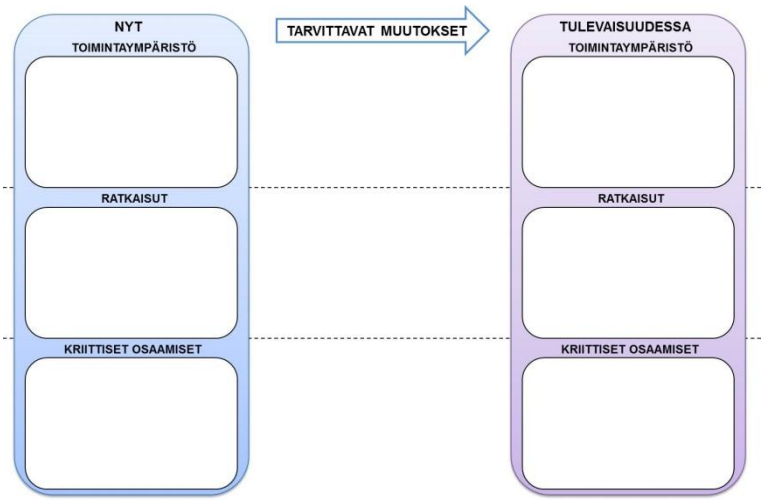
3.2 Tiekartat

Työpajojen tuottamasta aineistosta muodostettiin kolme tiekarttaa, joiden näkökulmat ovat:

- Valtio ja kulttuurin muutos,
- Liiketoiminta ja ratkaisujen kehitys,
- Tutkimus ja koulutus.

Kyseiset näkökulmat perustuvat yhtäältä työpajoissa esille tulleisiin teemoihin ja toisaalta heijastelevat myös innovaatiotoiminnan kolmijakoa valtion, yritysten ja tutkimuksen toimintakenttiin ja näiden leikkauspisteisiin. Tässä esitetyt tiekartat on syytä ymmärtää laajan sidosryhmäjoukon näkemykseksi siitä, mitkä asiat ovat keskeisiä Suomen kyberturvallisuusalan osaamisen kehittämisessä ja osaamiseen perustuvien mahdollisuuksien hyödyntämisessä.

Tiekarttarakenne (ks. kuva 3.3) esittelee ensin alan toimijoiden näkemyksen siitä, minkälainen on alan *nykytilanne* (vasen reuna). Tiekartan oikeassa reunassa on esitetty *tavoitetila* noin kymmenen vuoden päästä. Keskiosa käsittelee *tarvittavia muutoksia* ja toimenpiteitä, joita on tehtävä tavoitetilan saavuttamiseksi. Tiekarttoja ei kuitenkaan voida pitää suoraan toimintasuunnitelmina, koska niissä esitetyt asiat ovat luonteeltaan erilaisia eikä ehdotettujen toimien vaikutuksia ole mitenkään arvioitu. Tiekartta tarkastelee kyberosaamisen tulevaisuutta kolmella tasolla: *Toimintaympäristö, Ratkaisut, Kriittiset osaamiset*. Tasot voidaan tulkita niin, että keskimmäisellä, ratkaisut-tasolla, esitettyihin asioihin alan toimijoilla on parhaat mahdollisuudet vaikuttaa konkreettisilla toimenpiteillä. Toimintaympäristö-taso puolestaan käsittelee asioita, joissa muutokset ovat hitaita ja niihin vaikuttaminen voi olla ennemmin välillistä kuin suoraa tai toimenpiteiden toteuttaminen on riippuvaista myös muista kuin alan toimijoista. Alin taso, kriittiset osaamiset, on keskeinen tulevaisuuden rakentamisessa, mutta myös tällä tasolla saavutettavat muutokset ovat hitaita ja toimenpiteiden vaikutus voi olla välillistä.



Kuva 3.3. Tiekartan rakenne: Vasemmalla on kuvaus nykytilasta ja oikealla tavoitetilasta. Keskellä kuvataan tavoitetilaan pääsemiseksi tarvittavia muutoksia.

Tiekarttaesitykset on muodostettu työpajojen aineiston perusteella eli niiden sisältö pyrkii kattamaan mahdollisimman hyvin työpajoissa esille tulleet seikat. Tiekarttojen muodostamiseen ja aineiston esittämiseen valitussa tiekarttaformaatissa on kuitenkin väistämättä tarvittu tulkintaa. Aineiston käsittely ja tulkinta on tehty projektiryhmässä. Tiekarttojen tehtävä on esittää laaja-alainen katsaus alan toimijoiden näkemyksiin kyberturvallisuusalan toimintakentästä. Ne voivat toimia perustana tarkempien toimintasuunnitelmien esittämisessä. Seuraavat alaluvut esittelevät muodostetut kolme tiekarttaa.

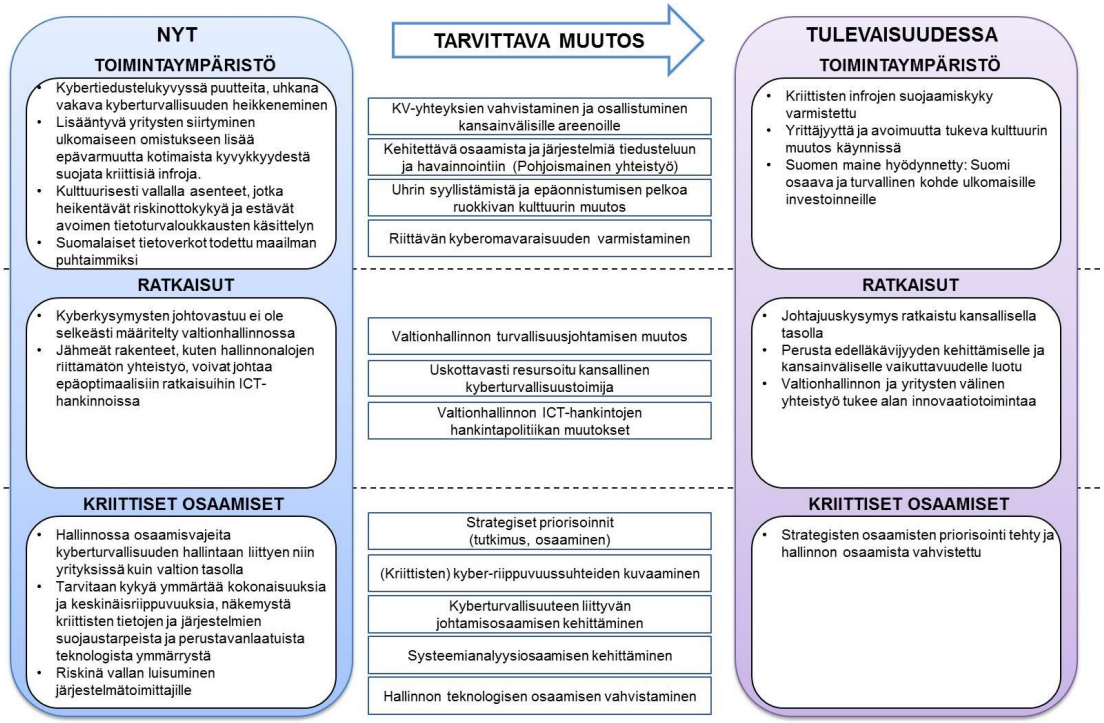
3.2.1 Valtion ja kulttuurinmuutoksen näkökulma

Nykytilanne: Suomen kybertiedustelukyvyssä koetaan olevan puutteita, jotka voivat johtaa vakavaan kyberturvallisuuden heikkenemiseen tulevaisuudessa. Toinen epävarmuutta lisäävä tekijä on jatkuva kotimaisten yritysten siirtyminen ulkomaiseen omistukseen. Tämän kehityssuunnan pelätään pidemmällä aikavälillä heikentävän kotimaista kyvykkyyttä suojata kriittisiä infrastruktuureja. Yleisessä ilmapiirissä alan kehittymistä haittaavat avoimuuden puute ja tietoturvaloukkausten uhriksi joutuneiden yritysten syyllistäminen. Nämä piirteet johtavat salailun kulttuuriin, jossa tietoturvaloukkauksista ei kerrota julkisuuteen ja siten tieto hyökkäyk-

sistä ja toisaalta niihin liittyvistä ratkaisumahdollisuuksista ei pääse leviämään. Myös suomalaisen kulttuurin turvallisuushakuisuus ja heikko valmius riskinottoon koetaan esteiksi, jotka vaikeuttavat alan mahdollisuuksien hyödyntämistä. Positiivisena tekijänä voidaan pitää sitä, että suomalaiset tietoverkot on todettu kansainvälisessä vertailussa maailman puhtaimmiksi. Tätä seikkaa voidaan hyödyntää ainakin imagon rakentamisessa, vaikka taustalla voi vaikuttaa se, että Suomea ei ole pidetty kiinnostavana hyökkäyskohteena.

Alan kehittymistä ja tulevaisuuteen varautumista voi heikentää se, että kyberkysymysten johtovastuuta ei ole määritelty selkeästi valtionhallinnossa. Jähmeät hallinnolliset rakenteet ja riittämätön yhteistyö eri hallinnonalojen välillä johtavat helposti osaoptimoituihin ratkaisuihin ICT-hankinnoissa. Eri organisaatioiden hallinnossa on tunnistettavissa osaamisvajeita kyberturvallisuuden hallintaan liittyen. Tämä tulee esille niin valtionhallinnossa kuin yritysten ja muiden organisaatioiden johdossa. Tilanteen parantamiseksi tarvittaisiin kykyä ymmärtää kokonaisuuksia ja asioiden keskinäisriippuvuuksia, näkemystä kriittisten tietojen ja järjestelmien suojaustarpeista sekä perustavanlaatuista teknologista ymmärrystä. Mikäli osaamista ei pystytä parantamaan, riskinä on vallan luisuminen järjestelmätoimittajille ja ulkomaisille yrityksille.

Tulevaisuudessa (tavoitetila): Keskeinen tulevaisuutta koskeva tavoite on varmistaa Suomen kyky suojata kriittiset infrastruktuurit. Yrittäjyyttä ja avoimuutta tukeva kulttuurin muutos tukee tätä kehitystä omalta osaltaan. Suomen maine osaavana maana ja turvallisena toimintaympäristönä on onnistuttu hyödyntämään ja ulkomaiset investoinnit Suomeen, esimerkiksi täällä sijaitseviin datavarastoihin, ovat korkealla tasolla. Kehityksen mahdollistajana on ollut johtajuuskysymyksen ratkaisu kansallisella tasolla ja sitä kautta luotu perusta alan edelläkävijyyden kehittämiselle ja kansainväliselle vaikuttavuudelle. Valtion ja yritysten välinen yhteistyö tukee alan innovaatiotoimintaa ja vahvistaa edelleen Suomen mainetta edelläkävijänä ja houkuttelevuutta sijoituskohteena. Kehitys on vaatinut osaamisten priorisointia strategisella tasolla ja panostamista valittuihin osaamisalueisiin. Myös aiemmin tunnistetut osaamisvajeet hallinnon eri tasoilla on saatu ratkaistua.



Kuva 3.4. Tiekartta: Valtio ja kulttuurinmuutos.

Tarvittavat muutokset: Pienenä maana globaalissa toimintaympäristössä Suomen on välttämätöntä vahvistaa kansainvälisiä yhteyksiään kyberturvallisuuden alalla. Euroopan tasolla kumppanuuksia kannattaa hakea etenkin Saksasta, joka on keskeinen toimija Euroopassa, ja kyberpuolustuksen kentällä myös Pohjoismaisesta yhteistyöstä. Kansainvälisten verkostojen vahvistamista ja sitä kautta syntyvää osaamisen vahvistamista on tarpeen tehdä niin hallinnossa, viranomaisyhteistyössä kuin tutkimuksessakin. Kyberturvallisuuteen liittyvän viranomaisyhteistyön epäonnistuminen voi synnyttää merkittäviä uhkia Suomelle. Kybertiedusteluun ja -havainnointiin liittyvää yhteistyötä voidaan rakentaa pohjoismaisessa kontekstissa. Yhteistyön muotoja voivat olla esimerkiksi yhteiset kyberharjoitukset, käytännön hyökkäys- ja puolustusosaamisen kehittäminen sekä erilaisten simulaatioiden toteuttaminen.

Kansallisella tasolla tarvitaan kulttuurin muutosta, jolla pyritään lopettamaan tietoturvaloukkausten uhrien syyllistäminen ja lieventämään kulttuurista epäonnistumisen pelkoa. Uhrien syyllistäminen estää kyberhyökkäyksistä tai tietoturvaloukkauksista kertomista. Avoimuuden kulttuurissa toimijat voivat oppia toisten mahdollisesti tekemistä virheistä tai järjestelmien heikkouksista. Avoimuuden kulttuurin tukemana voidaan järjestää myös mahdollisuuksia vertaistuelle, keskinäiselle sparraukselle ja luottamuksen ilmapiirin rakentumiselle. Samalla voidaan tunnistaa toimialan hyviä käytäntöjä ja levittää niitä. Toinen kansallisen tason kokonaisuus on varmistaa kriittisten infrastruktuurien ylläpidon kannalta riittävä kyberomavaraisuus. Tämän toteuttamiseksi täytyy ensin määritellä kriittiset infrastruktuurit ja niiden ylläpitoon liittyvät toimivalmiudet. Sen jälkeen on tehtävä linjaus tarvittavasta kyberomavaraisuuden tasosta sekä selvitettävä siihen vaikuttavat kriittiset tekijät. Viimeisenä vaiheena on tuettava määritellyn omavaraisuusasteen toetutumista kehittämällä keinoja kriittisten yritysten ja osaajien ankkuroimiseksi Suomeen.

Tämän tiekartan ratkaisukenttä käsittelee ensisijaisesti valtionhallinnon toimintaa hahmotellun tulevaisuuden saavuttamisessa. Turvallisuusjohtamisen muutoksessa on keskeistä selventää julkisen ja yksityisen sektorin yhteistyön malleja ja varmistaa yhteisten toimintatapojen muotoutuminen käytännössä. Johtamisen käytännöissä on keskeistä vahvistaa tulevaisuuden uhkiin varautuvaa toimintatapaa. Tässä yhteydessä voidaan hyödyntää tulevaisuudentutkimuksen ja ennakoinnin periaatteita ja pyrkiä kehittämään erityisesti tulevaisuudessa tarvittavia osaamisia. Osa tätä kokonaisuutta on kokonaisturvallisuusvastuiden selvittäminen ja vision realistisuus suhteessa käytettävissä oleviin voimavaroihin. Keskeinen osa johtamisen järjestämistä on uskottavasti resursoidun kyberturvallisuustoimijan muodostaminen. Kyseisen toimijan tehtävä olisi kyberturvallisuuden strategisen tason kokonaiskuvan ymmärtäminen, yhteisen toiminta-ajatuksen muodostaminen erilaisiin kyberpoikkeamatilanteisiin sekä ajantasaisen, eri lähteistä yhdistävän tilannekuvan luominen ja sen viestiminen muille toimijoille (kuten yrityksille ja virastoille). Kyberturvallisuuskeskuksella olisi hyvät valmiudet toimia tällaisena kärkiorganisaationa, mutta se tarvitsee riittävät resurssit tehtäväkentän laajentamiseen.

Muutoksia tarvitaan myös valtion ICT-hankintojen hankintapolitiikan toteuttamisessa. Valtionhallinto voi ja sen tulisi ottaa aktiivisempi rooli uusien innovatiivisten ratkaisujen kehittämisessä. Tässä toiminnassa voidaan hyödyntää julkisia hankintoja, vaikka hankintalaki koetaan nykyisin hankintoja rajoittavana tekijänä. Hankintoja tulisi suunnata enemmän uuden sukupolven, innovatiivisten tuotteiden kehittämiseen ja käyttöönottoon valmiiden ratkaisujen sijasta. Valtion ICT-hankinnoissa on tarpeen myös tarkentaa liikenne- ja viestintäministeriön sekä valtionvarainministeriön roolia ja kehittää näiden tahojen välistä yhteistyötä saumattomammaksi. Keskeinen haaste ICT-ratkaisuissa on vanhojen järjestelmien aiheuttama painolasti uusien kehittämisessä. Hankinnoissa tulisi pyrkiä siihen, että uusia ratkaisuja voidaan kehittää puhtaalta pöydältä ilman aiempien järjestelmien aiheuttamia rajoitteita.

Yllä kuvattuihin tarvittaviin muutoksiin liittyen tunnistettiin seuraavat *kriittiset osaamiset*:

- Koko kyberturvallisuusalan kehityksen ja siihen liittyvän osaamisen kehittämisen kannalta olisi ensiarvoisen tärkeää tehdä *strategisia priorisointeja* kansallisella tasolla. Tämä on perusedellytys sille, että tutkimusta ja osaamista voidaan suunnata pidemmällä aikavälillä haluttuun suuntaan.

- Kyberturvallisuuden johtamisessa ja hallinnassa tarvitaan näkemyksellistä systeemiajattelua ja kykyä ymmärtää kokonaisuuksia tilannekuvan muodostamiseksi. Näkemyksen muodostamiseksi on tärkeää kuvata kyberturvallisuuteen liittyvät *kriittiset riippuvuussuhteet* ja keskinäisvaikutukset.

- Työskentelyssä tunnistettiin osaamisvajeita erityisesti *kyberturvallisuuden johtamiseen* liittyen ja siksi tämän alueen *osaamista tulisi kehittää*.

- *Systeemianalyysiosaamisen kehittäminen* liittyy myös kahteen edellä mainittuun kohtaan, koska kyseistä osaamista tarvitaan kokonaisnäkemyksen ja tilannekuvan muodostamisessa sekä kyberturvallisuuden johtamisessa.

- Erityisesti innovatiivisten hankintojen edistämisen näkökulmasta tarvitaan *myös hallinnon teknologisen osaamisen vahvistamista*.

3.2.2 Liiketoiminnan ja ratkaisujen kehityksen näkökulma

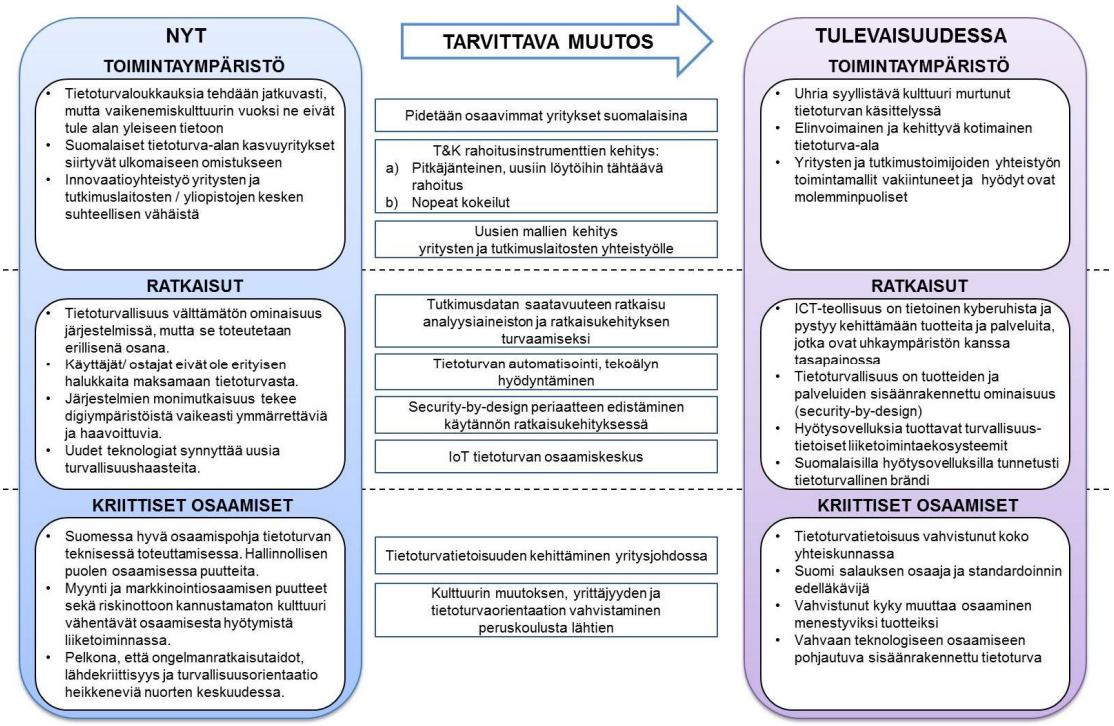
Nykytilanne: Kybertoimintaympäristön nykytilannetta leimaa se, että tietoturvaloukkauksia tehdään jatkuvasti, mutta suurin osa niistä ei tule yleiseen tietoon vallitsevan vaikenemiskulttuurin vuoksi. Suomeen on syntynyt maan kokoon nähden merkittävä joukko tietoturva-alan yrityksiä. Kansallisen pääoman vähäisyys ja riskinottohalukkuutta heikentävä kulttuuri ovat vaikuttaneet kuitenkin siihen, että alan kiinnostavimmat kasvuyritykset siirtyvät ulkomaiseen omistukseen. Innovaatioyhteistyö yritysten ja tutkimuslaitosten sekä yliopistojen välillä on suhteellisen vähäistä. Tähän vaikuttaa muun muassa toimivien rahoitusmallien puute ja yritysten keskittyminen omien olemassa olevien ratkaisujen kehittämiseen.

Järjestelmien kehityksessä tietoturvallisuus on tunnistettu välttämättömäksi ominaisuudeksi, mutta vallitseva käytäntö on toteuttaa tietoturvaratkaisut erillisinä järjestelmän osina. Tietoturvallisuuden välttämättömyys tulee esille myös sitä kautta, että ostajat tai järjestelmien käyttäjät eivät ole erityisen halukkaita maksamaan erikseen tietoturvasta. Järjestelmien vaiheittainen kehittäminen ja monimutkaisuus tekevät digiympäristöistä vaikeasti ymmärrettäviä ja haavoittuvia. Myös teknologian kehitys ja uudet teknologiat, kuten IoT-teknologia, luo täysin uusia turvallisuushaasteita, joita ei välttämättä osata ennakoida riittävästi.

Tietoturva-alalle syntynyt yritystoiminta on omalta osaltaan seurausta Suomen hyvästä teknisestä osaamispohjasta. Sen sijaan tietoturvallisuuteen liittyvässä hallinnollisessa osaamisessa, kuten johtamisessa ja hankintojen toteuttamisessa, on puutteita. Suomalaisten yritysten keskeisimmät haasteet liittyvät liiketoiminnan kasvuun ja kansainvälistymiseen. Näihin seikkoihin vaikuttavat kansallisella tasolla vallitsevat myynti- ja markkinointiosaamisen puutteet sekä riskinottoon kannustamaton kulttuuri. Laajemmassa yhteiskunnallisessa kontekstissa tietoturvallisuuteen voi tulevaisuudessa vaikuttaa se, että nuorten ikäluokkien ongelmaratkaisutaidot, lähdekriittisyys ja turvallisuusorientaatio heikkenevät merkittävästi.

Tulevaisuudessa (tavoitetila): Tulevaisuuden yhteiskunnassa tulee pyrkiä siihen, että tietoturvaloukkausten uhria syyllistävä kulttuuri saadaan murrettua. Tavoitteeksi on otettava elinvoimaisen ja kehittyvän kotimaisen tietoturva-alan muodostuminen. Osa tätä elinvoimaisuutta on yritysten ja tutkimustoimijoiden toimintamallit, joissa molemmat osapuolet hyötyvät yhteistyöstä. Tulevaisuuden ICT-teollisuus on tietoinen kyberuhista ja pystyy kehittämään tuotteita ja palveluita, jotka ovat uhkaympäristön kanssa tasapainossa. Tietoturvallisuus on tuotteiden ja palveluiden sisäänrakennettu ominaisuus, joka on saavutettu nk. security-by-design -ajattelun edistämisellä. Suomeen on kehittynyt hyötysovelluksia tuottavia turvallisuustietoisia liiketoimintaekosysteemejä ja suomalaisilla tuotteilla on tunnetusti tieturvallinen brändi maailmalla.

Osaamisen näkökulmasta tulevaisuuden tilaa tukee se, että tietoturvatietoisuus on vahvistunut koko yhteiskunnassa, myös sovellusten käyttäjien keskuudessa. Suomi on salauksen osaaja ja standardoinnin edelläkävijä. Liiketoiminnan elinvoimaisuutta lisää vahvistunut myyntiosaaminen ja kyky muuttaa teknologinen osaamien menestyviksi tuotteiksi. Teknologinen osaaminen on kuitenkin perusta, jonka pohjalle tuotteiden ja palveluiden sisäänrakennettu tietoturva on toteutettu.



Kuva 3.5. Tiekartta: Liiketoiminta ja ratkaisujen kehitys.

Tarvittavat muutokset: Edellisen tiekartan yhteydessä käsiteltiin riittävän kyberomavaraisuuden varmistamista ja siihen liittyvää kriittisten osaajien ja yritysten ankkuroimista Suomeen. Osaavimpien yritysten säilyttäminen suomalaisina ei ole yksinkertainen asia, sillä siihen ei voi suorilla ja yksiselitteisillä keinoilla vaikuttaa. Ennemmin kyse on yhteisen tahtotilan määrittelystä ja siihen sitoutumisesta niin valtion kuin yrittäjienkin taholta. Yksittäisen yrittäjän näkökulmasta oman elämäntyön rahastaminen ulkomaisen ostotarjouksen seurauksena voi olla houkuttelevampi vaihtoehto kuin kasvuhakuinen tulevaisuuteen suuntaaminen. Aiemmin käsitelty yrittäjyyttä ja riskinottokykyä vahvistava kulttuurin muutos vaikuttaa myös tässä, vaikka onkin hidas tie muutokseen. Yritysten kasvuvaiheen tukeminen esimerkiksi erilaisten rahoitusinstrumenttien avulla voi vahvistaa kotimaista omistajuutta ja sitä kautta palvella kyberturvallisuuden strategista kehittämistä.

Tutkimus- ja kehitysrahoituksessa tulisi tunnistaa kaksi erilaista linjaa. Yhtäältä tarvitaan rahoitusta pitkäjänteiseen, uusiin löytöihin tähtäävään tutkimukseen ja kehitykseen. Tällaisessa toiminnassa epävarmuudet ovat alussa suuria ja markkinoille tulevista ratkaisuista ei ole täyttä varmuutta. Toisaalta tarvitaan rahoitusta nopeisiin kokeiluihin, joissa ratkaisujen toimivuutta voidaan testata käytännössä. Pitkäjänteiseen kehitystyöhön liittyy myös yritysten ja tutkimuslaitosten yhteistyön lisääminen, mihin tarvitaan uusia malleja. Aiemmin käytössä ollut yhteisrahoitteinen malli (SHOK-tutkimus) edellytti avoimia ja julkisia tuloksia, mikä rajoitti yritysten halukkuutta tuoda liiketoimintalähtöisiä kysymyksiä tutkimuksen piiriin. Yritykset kokevat akateemisten kysymyksenasetteluiden ohjaaman tutkimuksen liian kaukaiseksi omiin tarpeisiinsa nähden. Uusia toimintamalleja tarvitaan siis akateemisen ja elinkeinoelämän rajamaastoon, joko tutkimustulosten kaupallistamiskynnyksen madaltamiseksi tai entistä tarvelähtöisemmän tutkimuksen tukemiseksi.

Kyberturvallisuuteen liittyvä ratkaisukehitys edellyttää häiriödatan saatavuutta, jotta häiriötilanteita pystytään analysoimaan ja niistä pystytään oppimaan. Datan tallentamiseen ja luovuttamiseen voi liittyä lainsäädännöllisiä esteitä, jotka on syytä tunnistaa ja poistaa. Erityisesti pienille yrityksille voi muodostua mahdottomaksi tehtäväksi tarjota analyysipalveluita, jos niillä ei ole tarvittavaa analyysidataa käytössään. Käytännön ratkaisukehityksessä on syytä edistää security-by-design -periaatetta, jossa kyberturvallisuus mielletään järjestelmän laatuun verrattavaksi ominaisuudeksi, joka toteutetaan jo järjestelmän suunnitteluvaiheesta alkaen. Tällaisten ratkaisujen kehittämisessä edellytetään eri osaamisalojen, kuten ohjelmistotekniikan, systeemisuunnittelun sekä riskienhallinnan ja kyberturvallisuuden, yhdistämistä.

Mahdollinen keino edistää tutkimuksen ja elinkeinoelämän yhteistyötä ja edelleen liiketoimintaekosysteemien muodostumista on perustaa osaamiskeskus. Sopiva aihealue osaamiskeskukselle voisi olla esimerkiksi IoT-teknologian tietoturva, joka tunnistettiin potentiaaliseksi kyberturvallisuusriskiksi. Yksi keskeinen tehtävä osaamiskeskukselle olisi kokeilujen edistäminen luomalla tarvittavaa infraa nopeiden kokeilujen tekoon. Myös tutkimuksen ja yritystoiminnan välisen raja-aidan madaltaminen ja esimerkiksi yrityshautomotyylinen toiminta voisi olla osa osaamiskeskuksen sisältöä.

Keskeiseksi osaamishaasteeksi tunnistettiin tietoturvatietoisuuden kehittäminen yritysjohdossa. Tällä viitataan esimerkiksi tietoisuuteen siitä, mitkä ovat yrityksen toiminnan kannalta keskeisimpiä tietoturvariskejä ja suojattavia tietoja, mitä asioita järjestelmien hankinnoissa on otettava huomioon ja miten tietoturvallisuutta johdetaan. Yritysjohdon tueksi voidaan myös kehittää erilaisia tarkastuslistoja tai tietoturvan osaamisprofiileja, jotka tukevat käytännön toimintaa esimerkiksi järjestelmien hankinnassa tai toiminnan organisoinnissa.

Jo aiemminkin esille tuotu asia on Suomessa tarvittava kulttuurinmuutos, joka tähtää epäonnistumisen pelon lieventämiseen, riskinottokyvyn parantamiseen, yrittäjyyden kannustamiseen sekä myynti- ja markkinointihenkisyyden edistämiseen. Näihin asioihin, kuten myös tietoturvaorientaation vahvistamiseen tulisi paneutua jo peruskoulusta lähtien. Tämä tarkoittaa ”digimaailman kansalaistaitojen”, kuten ongelmaratkaisutaitojen, lähdekriittisyyden ja tietoturvaorientaation, vahvistamista. Myös draaman ja esiintymistaitojen opetuksen kautta voitaisiin tukea kansalaisten itsetunnon kehitystä ja valmiutta myynti- ja markkinointityöhön tulevaisuudessa. Tie muutokseen on näiden asioiden huomioiminen jo opettajakoulutuksessa ja opetusohjelmissa.

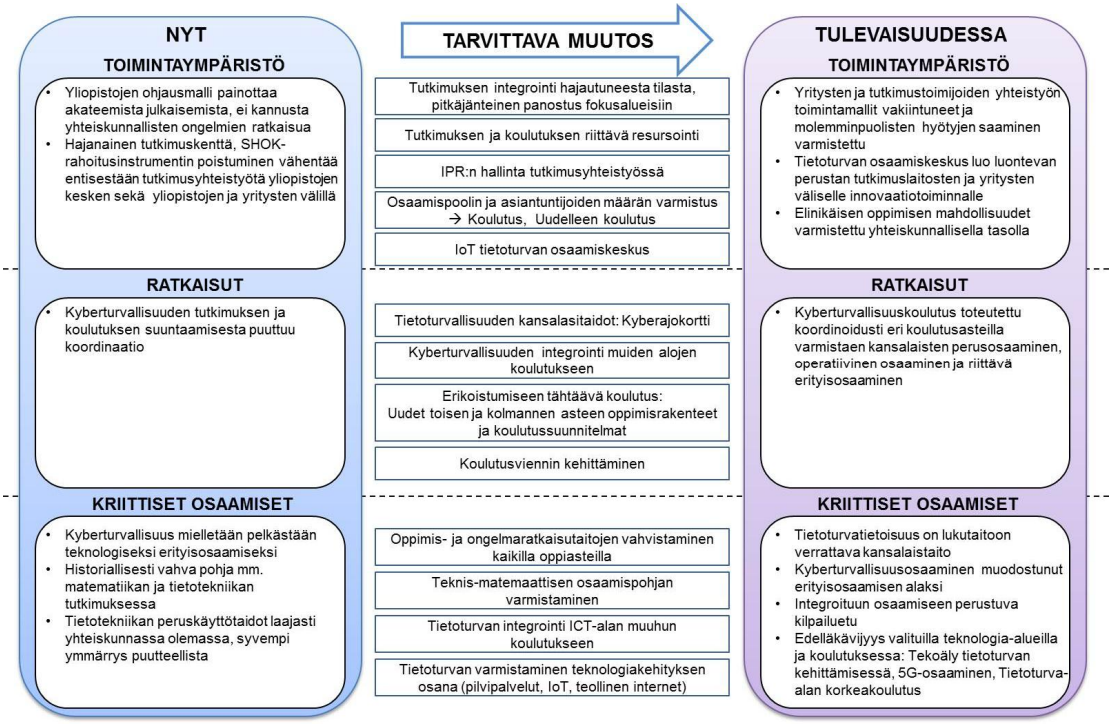
3.2.3 Tutkimuksen ja koulutuksen näkökulma

Nykytilanne: Nykytilanteessa yliopistojen ohjausmallissa painottuvat erilaiset suorituskykyindikaattorit, jotka painottavat esimerkiksi akateemista julkaisemista sen sijaan, että kannustai-

sivat ratkaisemaan yhteiskunnallisia ongelmia. Yliopistoilta edellytetään erikoistumista ja keskittymistä omiin vahvuusalueisiinsa. Kyberturvallisuuden alaa leimaa hajanainen tutkimuskenttä ja vähäinen yhteistyö eri tahojen välillä. SHOK-rahoitusinstrumentin poistuminen vähentää entisestään tutkimusyhteistyötä yliopistojen kesken sekä yliopistojen ja yritysten välillä. Kyberturvallisuuden tutkimuksen ja koulutuksen suuntaamista ei koordinoida kansallisella tasolla. Alaa leimaa se, että kyberturvallisuus mielletään ensisijaisesti ja lähes pelkästään teknologiseksi erityisosaamiseksi. Suomalainen kyberturvallisuuden osaaminen perustuu historiallisesti vahvalle pohjalle mm. matematiikan ja tietotekniikan tutkimuksessa. Yhteiskunnassa laajemmin on olemassa hyvät tietotekniikan peruskäyttötaidot, mutta syvempi ymmärrys tietoverkkojen ja teknologisten järjestelmien toiminnasta on puutteellista.

Tulevaisuudessa (tavoitetila): Yliopistojen rooli yhteiskunnallisten haasteiden ratkaisussa on vahvistunut ja uudet toimintamallit yritysten ja tutkimustoimijoiden yhteistyön vahvistamiseksi ovat vakiintuneet. Toiminnassa on pystytty varmistamaan molemminpuolisten hyötyjen saaminen, mikä luo hyvän motivaatiopohjan yhteistyölle. Käyntiin lähtenyt tietoturvan osaamiskeskus luo myös luontevan perustan tutkimuslaitosten ja yritysten väliselle innovaatiotoiminnalle. Nopeasti muuttuviin vaatimuksiin vastaamiseksi on tärkeää, että elinikäiselle oppimiselle on luotu toimivat mahdollisuudet yhteiskunnallisella tasolla. Kyberturvallisuuskoulutus on toteutettu koordinoidusti eri koulutusasteilla varmistaen kansalaisten perusosaaminen, operatiivinen osaaminen ja riittävä erityisosaaminen. Tietoturvatietoisuudesta on kehittynyt lukutaitoon verrattava kansalaistaito ja erikoistunut kyberturvallisuusosaaminen on muodostunut erityisosaamisen alaksi, johon on oma koulutustarjontansa. Ratkaiseva kilpailuetu saavutetaan kuitenkin integroidulla osaamisella, joka yhdistää kyberturvallisuuden teknologiseen ja operationaaliseen osaamiseen.

Saavutetun menestyksen taustalla ovat kirkkaat strategiset valinnat ja valittuun suuntaan kohdistetut toimet. Suomi on saavuttanut edelläkävijäaseman valituilla teknologia-alueilla ja koulutuksessa erityisesti tekoälyn hyödyntämisessä tietoturvan kehittämisessä, 5G-osaamisessa ja tietoturva-alan korkeakoulutuksen järjestämisessä. Näissä teemoissa Suomi on houkutteleva yhteistyökumppani niin koulutuksen, tutkimuksen kuin liiketoiminnankin näkökulmasta.



Kuva 3.6. Tiekartta: Tutkimus ja koulutus.

Tarvittavat muutokset: Tutkimuskentällä muutoksen perusta liittyy toiminnan koordinointiin ja hajanaisen kentän järjestäytymiseen. Tutkimus ja koulutus tarvitsevat myös riittävästi resursseja ja rahoituksessa on varmistettava toiminnan pitkäjänteisyys valituilla alueilla. Yksi ratkaistava kysymys on IPR:n hallinta tutkimustyössä. Tähän voidaan esim. kehitellä erilaisia malleja, joilla yritysyhteistyössä tehtävän tutkimuksen hinnoittelussa voidaan huomioida se, jääkö tutkimuksen IPR yliopistolle vai yritykselle. Kyberturvallisuusalan mahdollisuudet liittyvät suoraan osaajien määrään ja siten osaamispoolin ja asiantuntijoiden määrän varmistamiseksi on huolehdittava riittävästä koulutuksesta. Yhtä keskeistä on myös järjestää uudelleen koulutuksen mahdollistavat järjestelmät. Tutkimussektorilla tulee olla myös keskeinen rooli ehdotetussa IoT-tietoturvan osaamiskeskuksessa.

Kyberturvallisuuden koulutusta on tarpeen järjestää eri tasoilla ja erilaisilla painotuksilla alkaen tietoturvan kansalaistaidoista aina erikoistuneeseen korkeakoulutukseen asti. Kansalaistaitojen varmistamiseksi voidaan perustaa kyberajokortti, joka tarjoaisi perusymmärryksen henkilökohtaisesta kyberturvallisuudesta. Läpäisevyysperiaatteen mukaisesti kyberturvallisuustietoutta pitäisi integroida myös muiden alojen koulutukseen. Kyberturvallisuusalalla on tärkeää, että on saatavilla myös riittävän operatiivisen osaamisen omaavia ammattilaisia. Siksi esimerkiksi liikkeenjohdon, hallinnon tai IT-alan osaajat tarvitsevat myös kyberturvallisuusosaamista. Samanaikaisesti on tärkeää turvata erikoistumiseen tähtäävä koulutus. Tätä varten tarvitaan uusia toisen ja kolmannen asteen oppimisrakenteita ja koulutussuunnitelmia. Esimerkki tällaisesta on haastelähtöisen kandidaatintutkinnon muokkaaminen kyberturvallisuuteen. Erikoistumiskoulutuksen suunnittelussa ja toteutuksessa on tarpeen ottaa huomioon se, että ohjelmistoalalla huippuosaajat ovat tärkeitä ja siksi koulutus ei saa tasapäistää, vaan sen tulee tukea intohimoa ja luovuutta. Kyberturvallisuusalalla voidaan selvittää myös koulutusviennin mahdollisuuksia. Koulutusvientiä voidaan toteuttaa esimerkiksi kansainvälisillä maisteri- ja tohtorikoulutusohjelmilla, jotka tukevat myös kansainvälisen tutkimusyhteistyön syntymistä. Koulutusvienti voi tarjota mahdollisuuksia myös yksityiselle sektorille, jos alalle kehittyy yrityksiä.

Kriittisten osaamisten näkökulmasta voidaan erottaa seuraavat asiat:

- Teknologian nopean kehittymisen vuoksi koulutuksessa on painotettava enemmän periaatteiden ja kokonaisuuksien oppimista kuin yksittäisten teknologioiden tai ratkaisujen opiskelua. Oppimis- ja ongelmaratkaisutaitojen vahvistaminen kaikilla oppiasteilla on ensiarvoisen tärkeää.

- Teknis-matemaattisen osaamispohja on joka tapauksessa keskeisessä asemassa alan osaamisessa, joten siihen on kiinnitettävä huomiota. Ohjelmistotekniikka on peruslähtökohta, johon turvallisuusnäkökulma tulee integroida. Lisäksi tärkeitä aloja ovat matemaattinen kyptologia sekä protokolla- ja järjestelmäarkkitehtuurin suunnittelu.

- Erikoistumiskoulutuksen lisäksi tietoturva on tuotava läpäisyperiaatteen mukaisesti osaksi myös muuta ICT-alan koulutusta.

- Edelliseen kohtaan liittyen tietoturva on varmistettava teknologiakehityksen osana esimerkiksi pilvipalveluissa, IoT-ratkaisuissa ja teollisen internetin sovelluksissa sekä 5G-kehityksessä. Tästä näkökulmasta tärkeitä osaamisia ovat standardointi, tunnistamisratkaisuihin liittyvä osaaminen, krypto-osaaminen, kvantiturvalliset salausmene-

telmät, pilvi- ja Big data –osaamiset sekä 5G-osaaminen ja tekoälyn hyödyntäminen tietoturvan kehittämisessä.

3.3 Yhteenveto

Tässä projektissa toteutettu tiekarttaprosessi kokosi eri sidosryhmien näkemykset Suomen tulevaisuudesta kyberturvallisuuden näkökulmasta. Työskentelyssä hahmoteltiin todennäköisenä pidetty tulevaisuuskuva ja tunnistettiin sen avulla tulevaisuuden tarpeita, mahdollisuuksia ja uhkia. Todennäköisenä pidettyä tulevaisuuskuvaa leimaa ennemmin jonkinasteinen huoli tai synkkyys asioiden suunnasta kuin yltiöpäinen positiivisuus. Tulevaisuuteen on kuitenkin mahdollista vaikuttaa tämän päivän päätöksillä ja toiminnalla. Tätä ajatusta tukien kerätyn aineiston perusteella muodostettiin kolme tiekarttaa, jotka hahmottelevat toivottua tulevaisuutta ja tarvittavia muutoksia siihen pääsemiseksi. Tiekartoissa tulivat esille esimerkiksi tarve laajempaan kulttuurin muutokseen, joka liittyy yhtäältä avoimuuden ja luottamuksellisen ilmapiirin edistämiseen ja siihen, ettei tietoturvaloukkauksien kohteeksi joutuneita organisaatioita syyllistettäisi, ja toisaalta suomalaisten myynti- ja markkinointiosaamisen vahvistamiseen peruskoulusta alkaen. Esille nousevia teemoja olivat myös suomalaisen kyberturvallisomavaraisuuden varmistaminen ja tarve parempaan kyberturvallisuuskysymysten koordinaatioon ja selkeään vastuunjakoon valtionhallinnossa. Yleisesti ottaen kyberturvallisuuteen liittyviä osaamispuutteita arvioitiin olevan ennemmin johtamisen ja hallinnon piirissä kuin teknologisella puolella. Yksi käsitelty teema oli myös yritysten ja tutkimusorganisaatioiden välisen yhteistyön vahvistaminen esimerkiksi uusien rahoitusmallien avulla. Tietoturvan koulutuksessa tunnistettiin yhtäältä tarve erikoiskoulutuksen turvaamiseen riittävällä rahoituksella ja toisaalta tietoturvakysymysten integrointi paremmin muuhun teknologian kehitykseen ja siihen liittyvään koulutukseen. Myös yleisen tietoturvatietoisuuden vahvistaminen kansalaisten keskuudessa ja elinikäisen oppimisen mahdollistaminen tulivat esille tiekarttatyöskentelyssä.

Tiekarttatyöskentely perustui eri sidosryhmille – yrityksille, tutkijoille ja hallinnolle – järjestettyihin työpajoihin. Työpajoihin perustuvan menetelmän vahvuutena voidaan pitää mahdollisuutta törmäyttää erilaisia ajatuksia ja näkökantoja keskenään jonkin uuden luomiseksi. Toisaalta työskentelyyn osallistuvat tuovat siihen omat kokemukset, näkemykset ja tietonsa ja siten eri osallistujilla tulos saattaisi näyttää erilaiselta. Tässä hankkeessa työpajoihin osallistui yhteensä 32 henkeä. Käytettävissä olleiden näkemysten kirjoa voidaan siis pitää kohtuullisen laajana. Yksi työpajoihin perustuvan menetelmän haaste on saada osallistujat irrottautumaan nykypäivästä ja suuntaamaan ajatuksensa kauempana siintävään tulevaisuuteen. Tulevaisuusorientaatiota yritettiin tässä prosessissa tukea tarjoamalla osallistujille ennakkomateriaalina kuvauksia mahdollisesta tulevaisuuden teknologiaympäristöstä ja aloittamalla tiekarttatyöskentely pohtimalla ensin todennäköistä ja vaihtoehtoisia tulevaisuuksia. Kaikesta huolimatta ajankohtaiset tapahtumat suodattuivat aineistoon. Esimerkkinä tästä voidaan mainita maahanmuuttokysymyksen esiinnousu työpajoissa. Tähän vaikutti todennäköisesti työpajojen pitoajankohtaan, lokakuussa 2015, akuutti turvapaikanhakijoiden määrän äkillinen lisääntyminen. Toisaalta työpaja-aineiston analyysi oli vielä kesken marraskuun 13. päivän aikoihin, jolloin Pariisissa tehdyt terrori-iskut pysäyttivät maailman. Nämä tapahtumat toivat esille sen, että työpajojen tuottamassa aineistossa terrorismi ja siihen liittyvät kyberturvallisuuteen vaikuttavat ilmiöt olivat itse asiassa hyvin vähän esillä, lähinnä vain yleisinä mainintoina hybridisodankäynnistä ja erilaisten ääriliikkeiden lisääntymisestä yhteiskunnassa.

Tässä prosessissa valittiin tietoisesti lähestymistapa, jossa eri sidosryhmät osallistuivat omiin työpajoihin. Työpajojen järjestäminen erikseen eri sidosryhmille mahdollisti sen, että myös aineiston käsittelyssä oli mahdollista jäljittää mahdollisia eroja eri ryhmien näkemysten välillä. Yleinen tuntuma aineiston käsittelyn jälkeen on, että samankaltaiset teemat tulivat esille eri ryhmien työskentelyssä, mutta ryhmien välillä oli jonkinasteisia painotuseroja. Esimerkiksi koulutusteemaa käsiteltiin tavalla tai toisella kaikissa kolmessa sidosryhmässä. Yritysten edustajien ryhmässä esille tulleet näkökulmat liittyivät kuitenkin enemmän muuhun kuin varsinaiseen kyberturvallisuusratkaisujen erikoiskoulutukseen. Tässä ryhmässä korostettiin esimerkiksi tarvetta kouluttaa suomalaisista nuorista itsevarmoja esiintyjiä ja myyntihenkisiä, mutta kriittisiä ja ongelmanratkaisutaitoisia toimijoita. Toisaalta tuotiin esille tarve viedä kyberturvallisuusnäkökulmaa integroivasti muuhun teknologiakoulutukseen. Tutkimusalan ryhmässä, jossa oli paljon yliopistojen edustajia, korostuivat puolestaan koulutuksen riittävä resursointi ja sisällölliset kysymykset. Hallinnon ryhmässä näkökulma koulutukseen oli enemmän rakenteellinen ja työskentelyssä ideoitiin erilaisia koulutusohjelmia ja -järjestelmiä eri tasoille alkaen kansalaisten kyberajokortista aina erikoistuneisiin ongelmalähtöisiin koulutusohjelmiin asti.

Lopuksi korostamme vielä sitä, että tässä raportissa esitettyjä tiekarttoja ei voi sellaisenaan pitää valmiina toimintasuunnitelmina strategian suuntaamisessa. Tiekarttojen esittelemää sidosryhmänäkemyksiin perustuvaa käsitystä tarvittavista muutoksista voidaan kuitenkin hyödyntää päätöksenteon tukena. Osa tiekarttatyöskentelyssä esille tulleista asioista on mukana hankkeen johtopäätöksissä ja toimenpidesuosituksissa. Laajamittaisemmin tiekarttojen hyödyntäminen edellyttäisi yhteisen tahtotilan määrittäminen ja esitettyjen keinojen priorisointia ja tarkempaa vaikutusten arviointia.

4. KATSAUS KYBEROSAAMISEN KEHITTÄMISEEN ESIMERKKIMAISSA

Viime vuosina on julkaistu useita eri maiden kyberturvallisuuden tasoa ja valmiutta mittaavia vertailuja. Suomi menestyy näissä mittauksissa yleensä varsin hyvin. Esimerkiksi Global Cybersecurity Index -vertailussa, jossa mukana oli 195 maata, Suomi oli vuonna 2015 jaetulla 8. sijalla (ITU & ABI Research 2015). Suomen edellä oli kuitenkin 21 maata, koska monilla mailla on jaettu sijoitus. Indeksi mittaa maiden kehitystä kyberturvallisuudessa viidellä ulottuvuudella: lainsäädäntö, teknologia, organisaatiot, osaamisen kehittäminen ja yhteistyö. Vastaavasti vuonna 2012 Security & Defence Agendan (2012) tekemässä vertailussa Suomi oli kärjessä yhdessä Israelin ja Ruotsin kanssa. Suomi on usein ollut kärjessä myös tietoverkkojen puhtautta mittaavissa vertailuissa (ks. esim. Microsoft 2015). Jos vertailuja tarkastellaan laajemmin, havaitaan, että Suomi ei ole niiden maiden joukossa jotka menestyvät tasaisesti kaikissa vertailuissa. Useimmin kärjessä olevia maita ovat USA, Iso-Britannia sekä Saksa ja Hollanti (ks. tarkemmin Gehem ym. 2015).

Tämän tutkimuksen näkökulmasta vertailujen ongelma on, että ne eivät yleensä mittaa kyberosaamista, eli esimerkiksi innovaatiotoimintaa tai -kykyä tai tutkimus- ja kehitystoiminnan tilaa ja tasoa, vaan enemmänkin kyberturvallisuuden institutionaalisia puitteita. Osaamisen keskittyvälle barometrille tai vertailulle olisikin selvästi tilausta.

Seuraavassa luodaan lyhyet katsaukset kolmen vahvasti kyberturvallisuuteen panostaneen maan viimeaikaiseen kehitykseen.

4.1 Israel[19]

Israel on investoinut huomattavasti kyberturvallisuusalaan ja -osaamiseen viime vuosina. Panostusten taustalla on yhtäältä maan turvallisuuspoliittinen tilanne, joka on pitkään ollut hyvin epästabiili johtuen maan geopoliittisesta asemasta ja konflikteista. Maan pitkäntähtäimen vastaus geopoliittiseen asemaan on ollut puolustuspoliittinen strategia, jossa tieteellä ja teknologialla on suuri merkitys ja jossa korkeaan laatuun ja osaamiseen panostetaan vahvasti määrän sijasta. Tässä taustalla on se, että Israel on väkiluvultaan pieni maa, jossa asukkaita on noin 8 miljoonaa. Geopoliittisesta asemasta ja jatkuvasta konfliktitilanteesta johtuen Israeliin kohdistuu myös suuri määrä kyberhyökkäyksiä. Kyberinvestointien toisena taustatekijänä on maan tavoite nousta maailman johtavaksi ”kybertaloudeksi” ja globaalisti yhdeksi maailman merkittävimmäksi kyberratkaisujen tuottajaksi. Israel tunnetaan start-up -maana (”start-up nation”; ks. esim. Senor & Singer 2009), mutta nyt tavoitteena on yhä vahvemmin luoda kuvaa maasta johtavana kybermaana, ”cyber nation”. Tällä tavoitteella on vahva pääministeri Netanjahun tuki.

Israelissa kyberturvallisuuteen liittyvä keskustelu kohdistuukin pitkälti yhtäältä kyberhyökkäyksiin ja toisaalta kyberturvallisuuden tarjoamiin kaupallisiin mahdollisuuksiin. Yksityisyyden suojaa, takaportteja ja ihmisoikeuksia ja vastaavia poliittisia koskevia kysymyksiä käsitellään vähemmän.

[19] Tämä luku tukeutuu tekstissä mainittujen viitteiden ohella vahvasti Suomen Tel Avivin suurlähetystöstä saatuun materiaaliin.

Viime vuosina Israelin valtion kyberturvallisuusorganisaatiota on kehitetty voimakkaasti. Vuonna 2011 Israelin hallitus perusti uuden organisaation kyberkysymysten ympärille (Israel National Cyber Bureau, INCB) joka toimii pääministerin kanslian alaisuudessa. Se koordinoi Israelin kyberturvallisuuteen liittyviä toimintoja ja sen erityisenä tehtävänä on vahvistaa kyberalueen puolustusta ja kansallista osaamista sekä edistää Israelin asemaa kyberturvallisuudessa (Prime Minister's Office 2016). INCB on viimeisten tietojen mukaan kasvavamassa lähes 50 asiantuntijan organisaatioksi ja se on hyvin resursoitu. Sen alla toimii vuonna 2015 perustettu National Cyber Authority, joka keskittyy operationaalisiin tehtäviin, kuten esimerkiksi Israelin CERT-toimintoon ja kriittisen infrastruktuurin suojeluun. Merkittävä hallituksen päätös myös on, että vuodesta 2015 lähtien viranomaislaitosten on käytettävä 8 prosenttia IT-budjetista tietoturvaan.

Kyberturvallisuusosaamisen kehittäminen on Israelissa laaja-alaista ja tapahtuu monilla tasoilla. Kyberturvallisuuteen liittyviä kysymyksiä pyritään tuomaan esille jo koulussa. Kouluissa on ohjelmia lahjakkaille koodaajille. Myös armeijalla on osaamisen kehittämisessä tärkeä rooli. Maassa on pakollinen monivuotinen asepalvelus. Puolustusvoimien teknologiayksiköt rekrytoivat lahjakkaita asepalvelukseen tulijoita ja palveluksessa hankittujen taitojen pohjalta syntyy uusia yrityksiä. Puolustusvoimien ja yksityisen IT-sektorin välillä on vahva kytkentä kun puolustusvoimien palveluksesta siirtyy osaajia yksityiselle sektorille palveluksen päätyttyä (ks. tarkemmin Suciu 2015; Tabansky & Ben Israel 2015). Armeijan merkitys verkostoitumisessa on huomattava. Huomionarvoista myös on, että yliopistoissa kyberkysymyksiä pyritään huomioimaan paitsi tietotekniikan mutta myös esimerkiksi politiikantutkimuksen alueella.

Tutkimus- ja innovaatiotoimintaan panostetaan Israelissa perinteisesti paljon. Maan tutkimus- ja kehitysinvestoinnit ovat maailman korkeimmat, 4,2 prosenttia BKT:sta vuonna 2012 (OECD). Tämän päälle tulevat vielä puolustussektorin tutkimus- ja kehityspanostukset, jotka ovat Israelissa merkittävät. On arvioitu, että puolustussektorin T&K-panostukset huomioon ottaen BKT-osuus nousee noin 6 prosenttiin (Tabansky & Ben Israel 2015).

Israelissa uusi yrityksiä perustetaan eniten väkilukuun suhteutettuna maailmassa (Senor & Singer 2009) ja viime vuosina myös maan kyberalan start up -ekosysteemi on noussut merkittäväksi. Yhtenä taustatekijänä tässä on ollut vuoden 2010 National Cyber Initiative, jossa maan hallitus pyrki suuntaamaan maan high tech -ekosysteemiä entistä vahvemmin kyberturvallisuuden suuntaan (Tabansky & Ben Israel 2015). Tässä eräänä keskeisenä ulottuvuutena ovat olleet erilaiset koulutusohjelmat sekä kouluissa että yliopistoissa, sillä on huomattu, että kasvava kyberteollisuus tarvitsee lisää osaavaa työvoimaa.

Israelin start up -ekosysteemin menestyksen taustalla on monia tekijöitä ja menestyksen syyt ovat kiinnostaneet myös tutkijoita (ks. esim. Breznitz 2006). Taustatekijöitä ovat ainakin koulutettu väestö, hallituksen kannustimet, vahvat yliopistot ja tutkimuslaitokset, investoijat sekä kulttuuriin liittyvät tekijät. Tässä suhteessa huomattavaa on, että israelilaisessa kulttuurissa ei aristella epämukavuusalueelle joutumista ja siedetään muutosta, riskinottoa ja epäonnistumista. Myös tietynlainen röyhkeys ("chutzpah") on osa kulttuuria.

Merkittävää on myös israelilaisen innovaatiojärjestelmän kansainvälisyys: huomattava osa yritysten T&K-investoinneista on kansainvälisten yritysten tekemiä (Tabansky & Ben Israel). Tämä näkyy myös kyberturvallisuusalueella: esimerkiksi vuonna 2013 IBM, Cisco ja GE tekevät merkittäviä investointeja israelilaisiin kyberturvallisuusyrityksiin. Kahdellakymmenellä monikansallisella yrityksellä on kyberturvallisuuteen liittyviä t&k-toimintoja Israelissa. Amerikkalaisista yrityksistä esimerkiksi RSA, IBM, Microsoft, Akamai, Intel McAfee, Palantir, Intuit, AVG, F5 Networks, Palo Alto Networks ja PayPal ovat perustaneet tutkimusyksikön Israeliin

(Fisher & Meir 2015). Viime aikoina myös saksalainen tutkimuslaitos Frauhofer Institute sekä Lockheed Martin ovat ilmoittaneet aikeista perustaa tutkimuskeskuksia Israeliin.

Israelin kyberturvallisuusalan yritystoiminta on kasvanut 2010-luvulla voimakkaasti: muutamasta kymmenestä yrityksestä nyt jo kolmeensataan, joista yli puolet viimeisen kahden vuoden aikana. Vuonna 2013 kyberalan start-up -yrityksiä oli Israelissa yli 200 ja alan viennin arvo oli 3 miljardia US dollaria, joka vastaa noin viittä prosenttia globaalista kyberturvamarkkinasta (So 2014). Israel onkin maailman toiseksi suurin kyberalan tuotteiden ja palvelujen viejä Yhdysvaltojen jälkeen. Vuonna 2014 30 israelilaisyritystä keräsi yhteensä yli 200 miljoonan US dollarin edestä rahoitusta ja kahdeksan israelilaisyrityksen myynnin arvo oli 700 miljoonaa US dollaria.

Kyberturvallisuusalan osaamiskeskittymiä Israelissa on etenkin Tel Avivin yliopistossa ja Be'er-Shevassa Ben Gurion -yliopiston yhteydessä. Tel Avivin yliopistoon perustettiin vuonna 2014 monitieteinen kybertutkimuskeskus Blavatnik Interdisciplinary Cyber Research Centre (Tabansky & Ben Israel 2015). Ben Gurionin yliopiston yhteyteen on puolestaan keskittynyt sekä siviilihallinnon, armeijan, akateemisia että yksityisen sektorin toimijoita suurista monikansallisista yrityksistä pieniin start up -yrityksiin. Yliopistossa on mm. kyberturvallisuuden maisteriohjelma. Ben Gurionin yliopisto, Israel National Cyber Bureau ja Israelin puolustusvoimat ovat hiljattain perustaneet alueelle myös CyberSpark -tutkimuskeskuksen, jolle on INCB:n kautta ohjattu suoraa T&K-rahoitusta 8,5 miljoonaa US dollaria. Pääministeri Netanjahu tukee vahvasti Be'er-Shevan panostusta kyberturvallisuuteen ja haluaa kaupungista "kyberpääkaupungin" (Tabansky & Ben Israel 2015).

4.2. Viro [20]

Viro on noussut viime vuosina esiin kyberturvallisuuden edelläkävijämaana. Tähän on vaikuttanut 2000-luvulla käynnistynyt digitalisaatio, jonka johdosta Virossa otettiin käyttöön kansallinen palveluväylä (X-road) vuonna 2001, sähköinen henkilökortti vuonna 2002 ja kansallinen e-Palveluportaali vuonna 2003. Edellisten lisäksi Virossa on ollut käytössä sähköinen veroilmoitus (e-Vero) vuodesta 2000, Internet-äänestys vuodesta 2005 sekä e-Terveyspalvelu vuodesta 2008, jotka ovat osaltaan vaikuttaneet sähköisten palveluiden käytön kasvuun. Vuonna 2013 95 prosenttia veroilmoituksista täytettiin sähköisesti, yli 1,2 miljoonaa kansalaisista käytti e-ID -korttia aktiivisesti ja kansalliseen palveluväylään tehtiin yli 287 miljoonaa kyselyä. (e-Estonia.com)

Kyberturvallisuus nousi ajankohtaiseksi asiaksi Virossa kuitenkin vasta keväällä 2007, kun maahan kohdistui massiivinen hajautettu palvelunestohyökkäys lähes kuukauden ajan. Vaikka hyökkäys ei suoraan vaikuttanut Viron kriittisen infrastruktuurin toimintaan, se kuitenkin osoitti, että kyberympäristöstä oli syntymässä uusia ennalta-arvaamattomia riskejä sekä tuntemattomia vastustajia, joista ei ollut mainintaa vielä vuonna 2004 julkaistussa Viron kansallisen turvallisuuden selvityksessä (Republic of Estonia 2004; Czosseck et. al. 2011). Hyökkäyksen jälkeen hallitus päätti kyberturvallisuusstrategian luomisesta osana turvallisuuspolitiikkaa ja huomioi siinä mm. valtion suuren riippuvuuden informaatioteknologiasta (Jackson 2013; haastattelut)

Viron kyberturvallisuusstrategia julkaistiin puolustusministeriön toimesta vuonna 2008 ja se painottui voimakkaasti julkisen ja yksityisen sektorin yhteistyöhön mm. kriittisen infrastruktuurin suojelemisessa, mikä näkyi käytännössä esimerkiksi valtion kustantamana haavoittuvuus-

[20] Tämä luku pohjautuu asiantuntijahaastatteluihin, jotka suoritettiin Tallinnassa 11.-12.11.2015 sekä sähköisiin kirjallisuuslähteisiin.

ja tietoturvatestauspalveluina sekä auditointeina valituille kriittisen infrastruktuurin organisaatioille. Samana vuonna akkreditoitiin kansallinen CERT -toiminta (Computer Emergency Response Team) sekä perustettiin NATO-maiden yhteinen kyberturvallisuuskeskus (NATO Cooperative Cyber Defence Centre of Excellence) Tallinnaan. Kyberturvallisuuskeskuksessa työskentelee noin 50 tutkijaa eri NATO-jäsenmaista sekä yhteistyömaista, kuten Suomesta ja Itävallasta. Henkilöstön työajasta noin kolmannes kuluu tutkimukseen ja loput on harjoitusten sekä erilaisten koulutusten järjestämistä sekä valmistelua. Keskuksen suurin harjoitus on vuosittain järjestettävä Locked Shields, jossa lähes 500 asiantuntijaa eri NATO-jäsenmaista suorittaa kyberhyökkäyksiä tiimeissä sekä puolustautuu hyökkäyksiltä. Locked Shields -harjoituksen lisäksi keskus järjestää toistakymmentä erilaista kyberpuolustuksen koulutus- ja harjoitustilaisuutta vuosittain NATO-jäsenille, muille organisaatioille sekä esim. Tallinnan teknilliselle yliopistolle. (haastattelut)

Vuonna 2009 Virossa valmistui kyberturvallisuusstrategian toimintaohjelma sekä perustettiin kyberturvallisuusneuvosto, jonka tehtävänä oli raportoida kyberuhista hallituksen turvallisuuskomitealle. Samana vuonna perustettiin tärkeissä kriittisen infrastruktuurin tehtävissä toimivien kyberturvallisuusasiantuntijoiden tiimi, (EDL CU - Estonian Defence League's Cyber Unit tai toiselta nimeltään Cyber Defence League), jonka tehtävänä oli auttaa Viron kyberpuolustusta mahdollisissa kriisitilanteissa, vahvistaa julkisen ja yksityisen sektorin tietoturvaa ohjattujen harjoitusten ja testauksen kautta sekä vaihtaa kokemuksia ja jakaa tietoa verkoston sisällä. (Jackson 2013, Ministry of Economic Affairs and Communication 2014, haastattelut).

Vuonna 2011 Viroon perustettiin paikallinen "viestintävirasto" (RIA - Riigi Infosüsteemi Amet), jonka vastuulla on mm. kyberturvallisuuden osaamisen ja kilpailukyvyn ylläpitäminen sekä Viron kyberturvapolitiikan koordinointi. RIA:n tehtäviin kuuluu ylläpitää RIHA-toimintoa, joka hallinnoi mm. valtion tietojärjestelmien ja palveluiden tietoja sekä pääsyoikeuksia. Lisäksi RIA:n alaisuuteen on sijoitettu mm. CERT-EE, kansallinen palveluväylä (X-road), kriittisen infrastruktuurin suojaus (Critical Information Infrastructure Protection, CIIP) sekä valtion julkisen avaimen järjestelmän (PKI) keskeiset toiminnot. Keskeinen tietoturvastandardi julkiselle ja yksityiselle sektorille on RIA:n ylläpitämä ISKE, joka pohjautuu saksalaiseen standardiin (IT Baseline Protection Manual, IT-Grundschutz) ja joka tarjoaa hyvin yksityiskohtaisia tietoja tietoturvallisen verkon pystyttämisestä aina yksittäisen yrityksen tietokoneen tietoturva-asetuksiin. (Ministry of Economic Affairs and Communication 2014, RIA 2012, haastattelut)

Viron toinen kyberturvallisuusstrategia julkaistiin vuonna 2014. Erona aiempaan oli mm. se, että vastuuministeriönä strategian luonnissa toimi talous- ja viestintäministeriö (Ministry of Economic Affairs and Communication), kun aiempi strategia oli ollut puolustusministeriön kokoama. Vaihdoksen taustalla oli luultavimmin toive saada myös yksityinen sektori paremmin mukaan strategiaprosessiin. Taustatekijänä oli myös, että ensimmäinen strategia oli tehty palvelunestohyökkäysten aiheuttaman kriisitilanteen jälkeen, jolloin kansallisen puolustuskyvyn ylläpito oli varmasti tärkeimpänä asialistalla. Toisessa strategiassa nostettiin esiin termi "vital services" eli Viron kannalta elintärkeät palvelut, jotka tuli kartoittaa riippuvuuksineen sekä rakentaa varalle korvaavia palveluita ja mekanismeja kriisitilanteiden varalta. Myös ne tietojärjestelmät, jotka olivat tärkeitä yhteiskunnan toiminnalle, tuli varmistaa sekä julkisella että yksityisellä sektorilla. (Ministry of Economic Affairs and Communication 2014, haastattelut)

Viron ehkä merkittävin kyberturvallisuuden puolestapuhuja on ollut Presidentti Toomas Hendrik Ilves, joka on pyrkinyt edistämään mm. Viron ja Suomen yhteistyötä kyberturva-alalla ja ehdottanut myös pohjoismaiden sähköisten palveluiden yhteistä tiedonvaihtoa kansalaisille tarjottavien palveluiden kuten esim. e-Reseptin osalta. Maan rajat ylittävä yhteistyö onkin Virolle tärkeää, koska maan omat kyberturvallisuusmarkkinat ovat pienet. Virossa toimii arvi-

olta noin 50 kyberturvallisuuteen keskittynyttä yritystä, joista merkittävimmät toimivat haavoittuvuustestauksen tai tietoturva-auditointien parissa. Yrityksistä suurin, Cybernetica AS työllistää Virossa yli sata työntekijää, mikä on haastateltujen arvioiden mukaan yli viidennes maan kokoaikaisista tietoturva-asiantuntijoista. Osa-aikaisia tietoturva-asiantuntijoita maassa on noin tuhat. Viro tukee start up -toimintaa, mutta rahoitusmekanismit vaikuttavat riittämättömiltä eikä maassa ole haastateltavien mukaan lainkaan tutkimus- ja innovaatiotoimintaan keskittyvää kansallista rahoituselintä (vrt. Tekes Suomessa).

Tallinnan teknillisessä yliopistossa on kyberturvallisuuden maisteriohjelma, jossa on mukana yhteensä noin 200 opiskelijaa. Yliopisto toimii yhteistyössä Tarton yliopiston kanssa, jossa on tietoverkkorikosten tutkinnan (digitaalinen forensiikka) koulutusohjelma, jonka osana opiskelijat perehtyvät mm. kansainväliseen oikeuteen ja rikosoikeuteen. Tarton yliopistolla on myös kryptografian tutkimusosaamista, jossa on ilmeisesti kytkentä Aalto-yliopistoon.

Johtopäätöksinä voidaan todeta Viron kyberosaamisen tilan olevan kansallisella tasolla varsin hyvä. Viron kyberturvallisuusstrategia omalta osaltaan edistää julkisen ja yksityisen sektorin välistä aktiivista yhteistyötä PPP-toiminnan (Public-Private Partnership) kautta, jota RIA koordinoi. Kyberturvallisuutta pyritään myös tuomaan osaksi virolaisten arkea paitsi RIA:n toimintojen niin myös Presidentti Ilveksen lausuntojen sekä NATOn kyberturvallisuuskeskuksen toiminnan välityksellä. Haittapuolina Viron kyberturvallisuuden kehittymiselle ovat pienet markkinat ja toisaalta kansallisen tutkimusrahoituksen selkeä puute, joka voisi edistää varsinkin yliopistojen TKI -toimintaa.

4.3 Hollanti

Hollanti teki ensimmäisen kyberturvallisuusstrategiansa vuonna 2011. Järjestyksessä toinen strategia on tehty vuosille 2014–2016 (National Coordinator for Security and Counterterrorism 2014). Painopiste strategioiden välillä on siirtynyt kyberturvallisuustietoisuuden herättämisestä sekä rakenteiden ja toimintamallien muodostamisesta kohti kyvykkyyksien vahvistamista. Hollannin kyberturvallisuusstrategiadokumentti sisältää tavoitteiden määrittelyn lisäksi myös niihin sidotun kolmivuotisen toimenpideohjelman. Strategiassa esitetyt tavoitteet ovat:

1. Hollanti on resilientti kyberhyökkäyksien suhteen ja suojelee omia elintärkeitä intressejään digitaalisella alueella.

2. Hollanti taistelee kyberrikollisuutta vastaan.

3. Hollanti investoi turvallisiin ICT tuotteisiin ja palveluihin, jotka suojelevat yksityisyyttä.

4. Hollanti rakentaa vapautta, turvallisuutta ja rauhaa edistäviä koalitioita digitaalisella alueella.

5. Hollannilla on riittävä kyberturvallisuustieto ja -taidot ja se investoi ICT- innovaatioihin saavuttaakseen kyberturvallisuustavoitteet.

Hallinnollisesti kyberturvallisuus kuuluu Hollannissa turvallisuus- ja oikeusministeriön alaan (Ministerie Velligheid en Justitie). Ministeriön alaisuudessa toimii kansallinen kyberturvallisuuskeskus (Nationaal Cyber Security Centrum https://www.ncsc.nl/english), jonka tehtävät ovat kyberhyökkäyksiin ja -uhkiin varautuminen ja vastaaminen, tiedon tuottaminen ja jakaminen sekä toimiminen yhteistyön mahdollistajana julkisen ja yksityisen sektorin välillä esi-

merkiksi kriisinhallinnassa. Yksi kyberturvallisuuskeskuksen toimintamuoto on julkaista vuosittain arvio Hollannin kyberturvallisuustilanteesta. Raportti on ladattavissa kyberturvallisuuskeskuksen internet sivuilta (National Cyber Security Centre (2015).

Operatiivisen kyberturvallisuuskeskuksen lisäksi Hollannissa toimii myös Kyberturvallisuusneuvosto (Cyber Security Raad, http://cybersecurityraad.nl/), joka on neuvoa antava elin. Sen tehtävä on neuvoa hallitusta ja yksityisiä toimijoita, joko oma-aloitteisesti tai pyynnöstä. Lisäksi neuvosto seuraa kyberturvallisuusstrategian toteutumista ja antaa suosituksia sen päivittämisestä, osallistuu kansallisen kyberturvallisuuden tutkimusagendan määrittelyyn ja tukee viranomaisia mahdollisissa hyökkäys- tai kriisitilanteissa. Neuvostossa on pyritty tasapainoiseen näkemykseen varaamalla julkisen ja yksityisen sektorin edustajille yhtä monta paikkaa (molemmilla seitsemän edustajaa). Lisäksi neuvostossa on neljä edustajaa tutkimuksen piiristä.

Molemmat edellä kuvatut organisaatiot, neuvoa-antava kyberturvallisuusneuvosto ja operatiivinen viranomaistaho eli kyberturvallisuuskeskus, on perustettu ensimmäisen kyberturvallisuusstrategian seurauksena. Hollannin tapaus on hyvä esimerkki siitä, miten strategiatyö on vaikuttanut alan järjestäytymiseen ja on onnistunut kanavoimaan eri tahojen toimet yhteiseen suuntaan. Hollannin tavassa organisoida kyberturvallisuuskysymysten hallinta korostuu julkisen ja yksityisen sektorin yhteistyö. Myös innovaatiotoimintaan on kiinnitetty huomiota esimerkiksi määrittelemällä kansallinen tutkimusagenda kyberturvallisuuden alueelle. Myös tutkimusagenda on strateginen paperi, joka tarjoaa viitekehyksen julkisen ja yksityisen sektorin tutkimuksen yhteensovittamiselle ja keskinäiselle synkronoinnille aihealueella. Kuvassa 4.1. on listattu uusimman tutkimusagendan määrittelemät tutkimusteemat (National Cyber Security Centre 2013).

1. *Identiteetin, yksityisyyden ja luottamuksen hallinta*
2. *Haittaohjelmat ja tahalliset rakenteet*
3. *Hyökkäysten havaitseminen, estäminen ja monitorointi*
4. *Forensiikka ja tapahtumanhallinta*
5. *Data, menettelytavat ja pääsynhallinta*
6. *Kyberrikollisuus ja harmaa talous*
7. *Riskienhallinta, talous ja regulaatio*
8. *Turvallinen suunnittelu*
9. *Kyberhyökkäyskyvykkyydet*

Kuva 4.1. Hollannin kansallinen kyberturvallisuuden tutkimusagenda (NCSRA II) määrittelee yhdeksän tutkimusteemaa.

Yksi ilmentymä Hollannin julkisen ja yksityisen sektorin yhteistyöstä ja innovaatiotoimintaan keskittyvästä lähestymistavasta on The Hague Security Delta (HSD), joka kuvaa itseään Euroopan suurimmaksi turvallisuusklusteriksi (https://thehaguesecuritydelta.com/about-hsd). Kyseessä on kolmella paikkakunnalla (Haag, Twente ja Brabant) toimiva yritysten, julkisen sektorin ja tutkimusorganisaatioiden yhteenliittymä, joka tekee innovaatio- ja tutkimus- ja koulutustoimintaa määritellyillä aihealueilla. HSD:n teema-alueet ovat kyberturvallisuus, kansallinen ja urbaani turvallisuus, kriittisten infrastruktuurien suojelu ja forensiikka (rikostekninen tutkimus). Keskuspaikkana toimii HSD Campus Haagissa, joka tarjoaa toimijoille erilaisia fasiliteetteja, kuten linving lab -toimintaa, koulutustiloja, joustavia toimistotiloja ja kokoushuoneita. Kampus on ollut toiminnassa vuoden 2014 alusta ja siitä lähtien 31 organisaatiota on perustanut pysyvän toimipisteen alueelle. The Hague Security Delta aloitti toimintansa virallisesti kaksivuotisena projektina maaliskuussa 2012. Projektin taustaorganisaatioina tässä

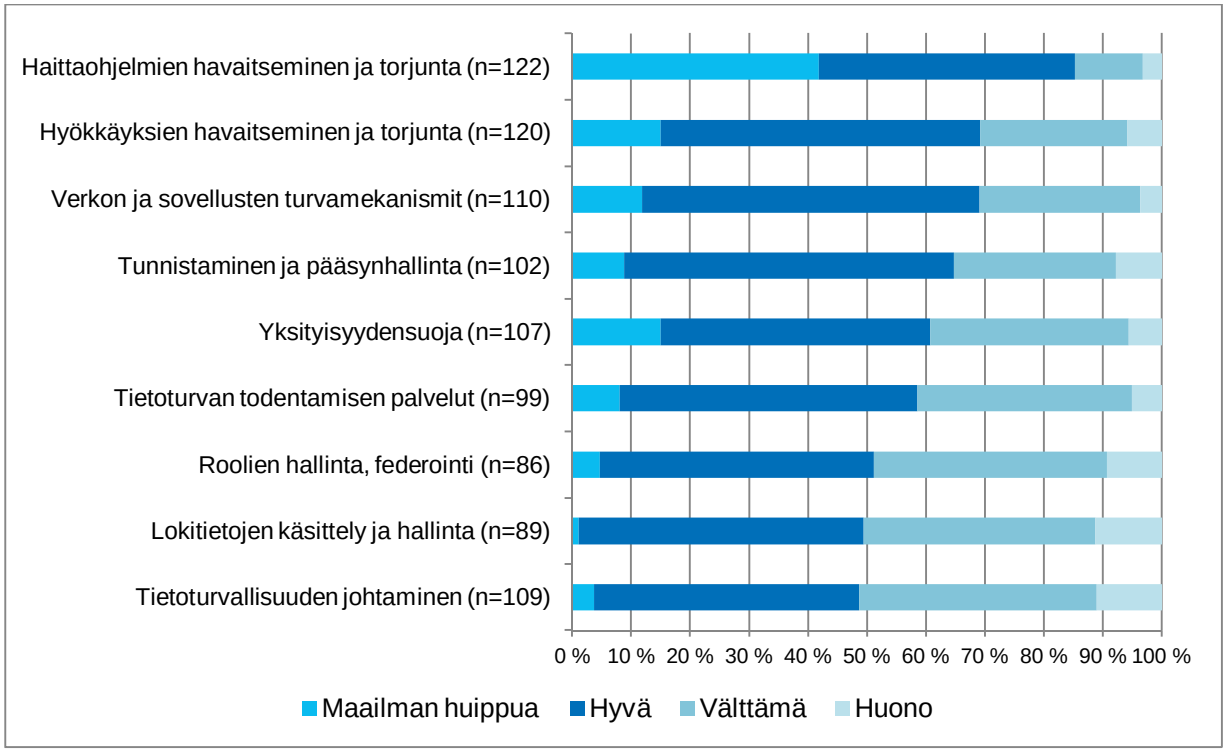
vaiheessa toimivat Haagin kaupunki ja Hollannin valtiovarainministeriö, myöhemmin toiminta muutettiin säätiömuotoiseksi. Toiminnan rahoituksesta vastaa noin kolmanneksen osuuksilla Haagin kaupunki, turvallisuus- ja oikeusministeriö sekä osallistujaorganisaatiot (HSD 2015).

5. SUOMEN KYBEROSAAMISEN VAHVUUDET, KAPEIKOT JA SWOT

Tässä luvussa laajennetaan kuvaa Suomen kyberosaamisen tilasta osaamisen vahvuuksien ja kapeikkojen sekä SWOT-analyysin kautta.

Kyberosaamista ja osaamisen vahvuuksia erityisesti yrityksissä ja tutkimusmaailmassa sekä osin myös julkisella sektorilla on käsitelty edellisissä luvuissa. Näistä tarkasteluista voidaan yhteen vetäen todeta, että alan suomalainen yrityskenttä on suhteellisesti katsottuna laaja ja yrityskentässä osaamista on varsin monipuolisesti eri osa-alueilla. Vahvuusalueita ovat mm. virustorjunta, palomuurit, identiteetin ja pääsynhallinta ja tilannekuvajärjestelmät ja tietoturvapalvelut. Kärkiosaaminen identifioituu erityisesti alan johtaviin yrityksiin. Korkeakouluissa ja tutkimuslaitoksissa alan tutkimus hajaantuu varsin suureen joukkoon organisaatioita. Kapeita kärkiosaamisalueita on mm. kryptologiassa, haavoittuvuustutkimuksessa, mobiililaitteiden tietoturvassa ja tietoturvan hallintaan liittyen.

Yksi yhteenvetävä näkökulma suomalaiseen kyberosaamiseen voidaan tuoda tässä tutkimuksessa tehtyjen kyselyiden perusteella. Alla olevassa kuvassa 4.1 on molempien kyselyiden vastaajien näkemykset siitä, minkälainen osaamisen taso Suomessa on tietyillä kyberturvallisuuden osa-alueilla. Tämän arvion mukaan korkeatasoista osaamista Suomessa on erityisesti haittaohjelmien havaitsemiseen ja torjuntaan liittyen. Yli 40 prosenttia vastaajista arvioi, että tällä alueella osaaminen Suomessa on maailman huippua ja yli 80 prosenttia vastaajista oli sitä mieltä, että osaaminen on vähintäänkin hyvää. Tässä arviossa taustalla on epäilemättä erityisesti F-Securen osaaminen tällä alueella. Heikointa osaamista kyselyiden perusteella olisi tietoturvallisuuden johtamisessa, mutta silläkin alueella noin puolet vastaajista on sitä mieltä että osaaminen on hyvällä tasolla. Merkittävää myös on, että hyvin pieni osa vastaajista oli sitä mieltä että osaaminen olisi huonoa millään osa-alueella.



Kuva 5.1. Yrityskyselyyn ja tutkimustoimijoiden kyselyyn vastanneiden näkemys suomalaisesta kyberturvallisuusosaamisesta eri osa-alueilla. En osaa sanoa -vastaukset poistettu.

Tässä tutkimuksessa kerättyjen aineistojen perusteella kyberosaamisen kapeikkoina tai vajeina nousee esiin muutamia osa-alueita. Selvästi merkittävin osaamiskapeikko liittyy kryptologiaan ja erityisesti teoreettiseen kryptologiaan. Itse asiassa kryptologia on hieman paradoksaalisesti tällä hetkellä sekä osaamisen vahvuusalue että osaamiskapeikko: alalla on erittäin korkeatasoista osaamista, mutta se on hyvin kapealla pohjalla. Merkittävää myös on, että kansallinen osaaminen ja suomalaiset osaajat ovat erityisen tärkeitä kryptologian kohdalla, koska vain suomalaisten salausratkaisujen avulla Suomessa voidaan varmistua, että tieto on aidosti suojattua. Kryptologian osalta tarvitaan nimenomaan suomalaisia osaajia. Olisikin tärkeää, että kun alalta eläköityy asiantuntijoita, tilalle rekrytoitaisiin kotimaisia osaajia. Vastaavasti olisi tärkeää, että alalla olisi suomalaisia jatko-opiskelijoita.

Toisena selvänä osaamisen vajeena esiin nousee kyberturvallisuuteen liittyvä myynti-, markkinointi- ja vientiosaaminen. Tässä on osin kyse ”perinteisestä” tilanteesta jossa suomalainen insinööriosaaminen ja tuotekehitysosaaminen ovat hyvällä tasolla, mutta kaupallistamis- ja markkinointitaidot ovat heikompia. Tämä tulee näkyviin myös kyberturvallisuuden alueella. Monen asiantuntijan mielestä suomalaiset ratkaisut ovat vähintään yhtä hyviä kuin maailmalla menestyvät tuotteet, ja ratkaiseva ero syntyy kyvystä ja taidosta myydä ja markkinoida tuotteita. Viime aikoina vienti- ja kaupallistamisosaamisen puute on osin saattanut olla taustatekijänä myös esimerkiksi tilanteissa joissa suomalaisia yrityksiä on siirtynyt ulkomaiseen omistukseen.

Kolmas osaamisvaje liittyy monitieteiseen kyberturvallisuusosaamiseen. Kuten edellä on todettu, tekninen kyberturvallisuuteen liittyvä osaaminen on Suomessa usein korkeatasoista. Laaja-alaisempi ja monitieteinen näkökulma kyberturvallisuuskysymyksiin on kuitenkin vielä selvästi heikommin kehittynyt. Esimerkiksi osaaminen liittyen kyberturvallisuuden ihmis- ja käyttäjänäkökulmaan, taloudelliseen näkökulmaan ja oikeudelliseen näkökulmaan on vähäi-

sempää Suomessa. Neljäs alue, jolla osaamista Suomessa on vähemmän, liittyy kybervaikuttamiseen ja kyberhyökkäämiseen. Tutkimuksessa kerättyjen aineistojen mukaan myös forensiikkaan sekä kyberjohtamiseen (esimerkiksi kyberturvallisuus strategisena johtamiskysymyksenä) liittyvä osaaminen on Suomessa vähäisempää.

Suomen kyberturvallisuusosaamisen tilaa voidaan vetää yhteen alla esitettävän SWOT-tarkastelun avulla. SWOT-analyysi kuvastaa tietyssä tilanteessa vallitsevien vahvuuksien, heikkouksien, mahdollisuuksien ja uhkien kokonaisuutta. Alla olevassa taulukossa on esitetty tämän tutkimuksen aineistojen perusteella syntynyt näkemys SWOT:n muodossa. Taulukko on luonteeltaan tässä raportissa esitettyjä tarkasteluja syntetisoiva. Osin taulukossa esitettyihin kohtiin palataan seuraavassa luvussa, jossa esitetään tämän tutkimuksen johtopäätökset ja toimenpide-ehdotukset.

Taulukko 5.1. Suomen kyberturvallisuusosaamisen SWOT.

VAHVUUDET	**HEIKKOUDET**
Historiallisesti vahva pohja mm. matematiikan ja tietotekniikan tutkimuksessa Laaja yrityskenttä (väkilukuun suhteutettuna), yritysten osaamispääoma ja liiketoiminta Yritysten liiketoiminnan vahva kasvu viime vuosina Korkeatasoista osaamista tutkimuksessa ja yrityksissä erityisesti tietyillä osa-alueilla, esimerkiksi virustorjunta, kryptologia, haavoittuvuustutkimus, konsultointi, mobiililaitteiden tietoturva. Varsin laaja-alainen teknologinen osaaminen, ei merkittäviä teknologisia osaamispuutteita Suomen hyvä maine kansainvälisesti ja neutraali asema	Tutkimuskenttä hajanainen, kriittisen massan ylittäviä yksiköitä vähän Tutkimuksen volyymi pieni, erityisesti tietyillä erikoisaloilla osaajia hyvin vähän, kärki kapea Yhteistyö alan toimijoiden välillä (tutkimus -yritykset -julkinen hallinto) vielä kehittymässä Esteet kyberuhka- ja tapahtumatiedon jakamisessa Alan laboratoriot/harjoitusympäristöt ovat suljettuja, eivätkä ne mahdollista laaja-alaista yhteistyötä. Monitieteinen kyberturvallisuustutkimus ja -osaaminen vähäisempää Markkinointi-, myynti- ja vientiosaaminen Alan koulutusta ei riittävästi Ei sarjayrittäjyyttä alalla
MAHDOLLISUUDET	**UHKAT**
Suomi on pieni ja ketterä maa, edellytykset yhteistyön vahvistamiseen hyvät Julkisten hankintojen hyödyntäminen alan kehityksen tukemisessa Tietojärjestelmätieteen tutkimuksen kriittinen massa tuo potentiaalia Yritysten vahvempi pääsy kansainvälisille markkinoille Suomen hyvän maineen parempi hyödyntäminen.	Yritysten laajamittainen siirtyminen ulkomaiseen omistukseen tavalla, joka siirtäisi myös osaamista pois Suomesta Osaamispohjan ohuus Kyberturvallisuuden epäselvä asema ja sijainti julkisessa hallinnossa. Vastuu hajaantuu eri ministeriöiden ja toimijoiden kesken.

6. JOHTOPÄÄTÖKSET JA KEHITTÄMISSUOSITUKSET

Kyberturvallisuus ja siihen liittyvä tutkimus-, kehitys- ja innovaatiotoiminta ja -osaaminen ovat tärkeitä sekä kansallisen huoltovarmuuden ja turvallisuuden näkökulmasta, yhteiskunnan toimivuuden kannalta että yritys- ja liiketoiminnan alueena. Digitalisoituvassa maailmassa kyberturvallisuuden merkitys tulee lähivuosina edelleen kasvamaan. Esimerkiksi teollisen Internetin ja esineiden Internetin myötä kyberturvallisuus korostuu entisestään. Suomelle kyberturvallisuus on mahdollisuus, sillä Suomella on potentiaalia kyberturvallisuuden ja kyberturvallisuusosaamisen alueella. Mahdollisuuksien hyödyntäminen edellyttää kuitenkin määrätietoisia toimenpiteitä.

Seuraavassa esitetään tutkimuksen johtopäätökset ja niihin liittyvät toimenpiteet Suomen kyberturvallisuusosaamisen edelleen kehittämiseksi ja vahvistamiseksi. Johtopäätökset ja ehdotukset toimenpiteiksi on jaettu neljään kokonaisuuteen: kyberosaamisen edellytykset ja osaamisen vahvistaminen, tutkimus ja koulutus, yritykset ja liiketoiminnan edistäminen sekä yhteistyö ja vuorovaikutus. Osa toimenpidesuosituksista kytkeytyy läheisesti toisiinsa ja näiltä osin suosituksia on syytä käsitellä kokonaisuutena.

Kyberosaamisen edellytykset ja osaamisen vahvistaminen

Edellytykset kyberturvallisuusalan ja -osaamisen kehittämiselle ovat Suomessa hyvät. Suomessa on korkeatasoista kyberturvallisuuteen liittyvää tutkimus-, kehitys- ja innovaatiotoimintaa ja -osaamista. Vahvuuksia on sekä yrityskentällä että korkeakouluissa ja tutkimuslaitoksissa. Korkeatasoista osaamista on esimerkiksi virustorjunnassa, tunnistamisessa ja identiteetin hallinnassa, palomuureissa, kryptologiassa, mobiililaitteiden tietoturvassa ja tieto- ja kyberturvapalveluissa. Suomi on myös ollut kansainvälisesti edelläkävijä esimerkiksi kansallisen kyberturvallisuusstrategian laatimisessa.

Kyberturvallisuusalalla kansainvälinen kilpailu on kiristynyt viime vuosina ja kansainvälisesti monet maat ovat panostaneet kyberturvallisuuteen merkittävästi. Esimerkkejä tällaisista maista ovat Viro, Hollanti, Iso-Britannia, Israel ja Saksa. Suomen kyberturvallisuusstrategiassa on asetettu tavoitteeksi, että Suomi on maailmanlaajuinen edelläkävijä kyberturvallisuudessa. Tämän tutkimuksen aikana kerättyjen aineistojen perusteella on selvää, että Suomessa alan kehitykseen pitää panostaa entistä vahvemmin, mikäli kyberturvallisuusstrategiassa asetettu tavoite halutaan saavuttaa. Tällä hetkellä Suomesta puuttuu vahva kansallinen tahtotila kyberturvallisuuden ja alan osaamisen kehittämisen suhteen. Suomen kansainvälinen kilpailuasema on heikentymässä.

> **Toimenpide 1:** Kansallinen tahtotila ja visio kyberturvallisuuteen ja -osaamiseen liittyen kirkastetaan. On päätettävä, halutaanko, että Suomi todella on globaali edelläkävijä kyberturvallisuudessa. Resurssit ja toimenpiteet tulee suhteuttaa asetettuun visioon ja tavoitteisiin. Tahtotilan tulee kulminoitua kyberturvallisuuden kärkiohjelmaan, joka kokoaa alan toimijoita yhteen. Vastuutahot: Valtioneuvosto, valtiovarainministeriö, sisäministeriö, puolustusministeriö, liikenne- ja viestintäministeriö, Turvallisuuskomitea.

Vaikka Suomessa on korkeatasoista osaamista kyberturvallisuudessa, kärkiosaaminen sekä tutkimuksessa että yrityksissä keskittyy varsin harvoille toimijoille. Osaamisen kärki on kapea, mitä kuvastaa esimerkiksi se, että Suomessa on vain noin hieman yli toistakymmentä tieto- tai kyberturvallisuuteen keskittyvää professoria. Eräillä tärkeillä osa-alueilla kärkiosaaminen on aivan yksittäisten henkilöiden varassa.

Viimeisen kolmen vuoden aikana merkittävä ilmiö Suomen kyberturvallisuusalan kentässä on ollut myös yritysten myynti ulkomaille. Alan kärkiyritysten siirtyminen ulkomaiseen omistukseen saattaa muodostaa riskin kansallisen kyberosaamisen ja ”kyberomavaraisuuden” näkökulmasta, erityisesti siinä tapauksessa että osaamista siirtyy pois Suomesta yritysostojen myötä. Tällä hetkellä Suomesta puuttuu kansallinen linjaus siitä, missä määrin Suomen halutaan olevan kyberomavarainen.

> **Toimenpide 2:** Kyberturvallisuuden huippuosaamista tulee pystyä pitämään Suomessa ja jatkuvuus ja osaaminen kriittisillä osaamisalueilla tulee varmistaa. Kansallisesti on linjattava, missä määrin ja miltä osin Suomen tulee olla omavarainen kyberturvallisuusosaamisen ja alan yritysten omistuksen suhteen. Mikäli kyberomavaraisuus katsotaan tärkeäksi, tulee harkita yritysten ja kriittisten osaamisten Suomeen ankkuroitumisen tukemista, esimerkiksi omistuksen kautta. Vastuutaho: Valtioneuvosto, valtiovarainministeriö, sisäministeriö, puolustusministeriö, liikenne- ja viestintäministeriö, työ- ja elinkeinoministeriö.

Kyberturvallisuusosaaminen pohjautuu pitkälti tietotekniikkaan, ohjelmointiosaamiseen ja matematiikkaan. Näillä alueilla osaaminen on Suomessa perinteisesti ollut varsin korkeatasoista, ja tutkimuksessa kerättyjen aineistojen perusteella Suomessa on laajemminkin korkeatasoista tieto- ja kyberturvallisuuteen liittyvää teknistä osaamista.

Vaikka Suomessa on korkeatasoista teknistä osaamista, myös osaamisen kapeikkoja ja puutteita on olemassa. Selviä osaamiskapeikkoja Suomessa on kolmella osa-alueella. Ensimmäinen liittyy kryptologiaan ja erityisesti teoreettiseen kryptologiaan, jonka osaaminen on Suomessa hyvin kapealla pohjalla. Toinen osaamiskapeikko on kyberturvallisuuteen kytkeytyvä myynti-, markkinointi- ja vientiosaaminen. Markkinointi- ja vientiosaamisen puute näkyy erityisesti siinä, että vaikka tekniset ratkaisut Suomessa ovat usein korkeatasoisia, alan vientitoiminta ei ole niin vahvaa kuin se voisi olla. Kolmas osaamisvaje koskee kyberturvallisuutta laaja-alaisena, monitieteisenä ja strategisena kysymyksenä tarkastelevaa näkökulmaa. Kyberturvallisuuden teknologinen ulottuvuus on luonnollisesti korostunut, mutta yhä syvemmin digitalisoituvassa maailmassa kyberturvallisuuskysymyksiin tarvitaan laaja-alaisempaa ja monipuolisempaa osaamista. Näiden kolmen alueen lisäksi on olemassa myös muita osaamisalueita, joilla osaaminen Suomessa on varsin vähäisempää. Tällaisia ovat esimerkiksi forensiikka ja kybervaikuttaminen.

> **Toimenpide 3:** Matematiikan ja ohjelmoinnin perusosaaminen on Suomessa pidettävä korkealla tasolla. Yliopistojen ja tutkimuslaitosten tulee vahvistaa panostuksia osa-alueille, joissa tällä hetkellä on osaamispuutteita, erityisesti kryptologiaan, ja varmistaa osaamisen jatkuvuus. Vastuutahot: opetus- ja kulttuuriministeriö, työ- ja elinkeinoministeriö, yliopistot, tutkimuslaitokset

Tutkimus ja koulutus

Kyberturvallisuuteen liittyvä tutkimustoiminta on kasvanut vahvasti Suomessa 1990-luvun lopulla ja 2000-luvun alussa, ja esimerkiksi alan julkaisumäärät ovat noin nelinkertaistuneet. Kyberturvallisuuteen liittyvää tutkimusta ja koulutusta onkin tällä hetkellä monissa organisaatioissa: tutkimusta tehdään 16 tutkimusorganisaatiossa ja koulutusta annetaan 14 organisaatiossa. Kasvusta huolimatta alan tutkimuksen kokonaisvolyymi on kuitenkin Suomessa edelleen pieni. Varsin pieni volyymi ja toiminnan jakaantuminen moniin organisaatioihin tarkoittaa, että alan tutkimus- ja koulutustoiminta on varsin hajaantunutta, ja kriittiseltä massaltaan suurempia osaamiskeskittymiä on vähän. Alan tutkimusryhmät ovat kooltaan suhteellisen pieniä.

Huomionarvoista on myös, että vaikka tutkimustoiminta on vahvistunut viimeisen 10 vuoden aikana, alan tutkimusta ja koulutusta ei ole kehitetty kovinkaan systemaattisesti ja alan institutionalisoituminen kesken. Strategista suunnitelmaa alan koulutuksen ja tutkimuksen kehittämisestä ei ole ollut.

Tässä tutkimuksessa kerättyjen aineistojen perusteella Suomessa tehtävä kyberturvallisuuteen liittyvä tutkimus ei ole vielä vahvasti kansainvälistynyt. Alan kansainvälinen yhteisjulkaiseminen on vähäistä, EU:n tutkimusrahoituksen merkitys tutkimusryhmille on suhteellisen pieni, ja on paljon tutkimusryhmiä, joissa ei ole lainkaan ulkomaalaisia tutkijoita. Alan tutkimus hyötyisi vahvemmasta kansainvälisestä kytkennästä.

EU:n kyberturvallisuuteen liittyvän tutkimusrahoituksen osalta Suomen olisi hyvä myös vaikuttaa aikaisemmassa vaiheessa rahoituksen suuntautumiseen. EU:n Horizon2020-ohjelma rahoittaa laajasti kyberturvallisuustutkimusta, mutta Suomen panos työohjelmien valmisteluun on tällä hetkellä liian vähäinen. Työohjelmavalmisteluun tulisi panostaa huomattavasti enemmän, jotta ohjelmiin saataisiin sisään suomalaisille relevantteja aihekokonaisuuksia.

Yliopistoissa, ammattikorkeakouluissa ja tutkimuslaitoksissa tehtävä kyberturvallisuuteen liittyvä tutkimus on Suomessa vahvasti teknologisesti orientoitunutta. Moni- ja poikkitieteellinen näkökulma on selvästi heikommin kehittynyt. Esimerkiksi talous-, käyttäytymis-, ja yhteiskunta- sekä hallinto- ja oikeustieteellistä kyberturvallisuustutkimusta ja -osaamista on Suomessa vähemmän. Kyberturvallisuus on kuitenkin hyvin laaja-alainen ja monisyinen kokonaisuus, jonka merkitys digitalisoituvassa yhteiskunnassa kasvaa ja jota tulee tarkastella laajasti eri tieteenalojen näkökulmasta.

> **Toimenpide 4:** Kyberturvallisuustutkimuksen kansainvälistä ulottuvuutta tulee vahvistaa. Monitieteistä kyberturvallisuustutkimusta ja -osaamista tulee edistää. Vastuutahot: Suomen Akatemia, Tekes, yliopistot, tutkimuslaitokset.

Yritykset ja liiketoiminnan edistäminen

Suomessa on suhteellisesti katsottuna melko laaja kyberturvallisuuteen liittyvä yrityskenttä, ja alalla on vahvoja ja innovatiivisia yrityksiä. Yritykset ovat suurelta osin kooltaan varsin pieniä ja suuri osa yrityksistä on palveluyrityksiä. Alan yritykset panostavat tuotekehitykseen, mutta pitkäjänteisempää tutkimustoimintaa panostaminen on vähäisempää. Yritysten absoluuttiset t&k-panostukset eivät kuitenkaan ole kovin suuria johtuen yritysten pienestä koosta.

Kyberturvallisuusalan kehityksen ja kasvun kannalta keskeinen pullonkaula on yritysten vähäinen kansainvälistyminen. Kansainvälistyminen on Suomen kyberturvallisuusalan kasvun suurimpia haasteita, mutta samalla välttämätöntä mikäli alan osaamisen ja osaajien määrän

halutaan kasvavan Suomessa. Yritysten kasvurahoitukseen ja kansainvälistymiseen tarvitaan lisää keinoja, jotta yritykset, tuotteet ja kasvu eivät valu ulkomaille ja liiketoimintaa pystytään generoimaan Suomeen. Julkisen sektorin referenssit ovat keskeisessä roolissa alan yritysten kansainvälistymisessä. Viime aikoina kansainvälistymistä ja vientiä on edistetty esimerkiksi Finnish Information Society Cluster FISC ry:n piirissä ja tätä työtä pitää jatkaa ja edelleen vahvistaa.

Toimenpide 5: Muodostetaan kansainvälistymistä tukeva kansallinen ohjelma tai kokonaisuus tiiviissä yhteistyössä alan eri toimijoiden kesken. Ohjelman keskeisiä elementtejä voivat olla esimerkiksi: julkisen sektorin referenssit, jotka tukevat kansainvälistymistä, kehitysapuhankkeet, kasvu- ja kansainvälistymisrahoitus, vientiverkostot ja myyntiosaamisen vahvistaminen. Vastuutahot: työ- ja elinkeinoministeriö, Tekes, Finpro, FISC, yritykset.

Toimenpide 6: Uuden kansainvälisen liiketoiminnan synnyttämiseksi ja alan toimijoiden yhteistyön vahvistamiseksi Tekes suuntaa liiketoimintakärjet ja ekosysteemit -rahoitusta kyberturvallisuusalueelle. Vastuutaho: Tekes

Kansainvälistymisen ja viennin suhteen Suomen etuna on kansainvälisesti hyvä maine tietoturvaosaamisessa. Suomen liittoutumattomuus, neutraali asema ja luotettavuus ovat vahvoja kilpailutekijöitä suomalaisille kyberturvallisuusalan toimijoille. Suomella on myös hyvä maine ICT- ja mobiiliteknologian osaamisessa. Näitä tekijöitä voitaisiin hyödyntää vielä nykyistä vahvemmin kansainvälisessä liiketoiminnassa, yhteistyössä ja markkinoinnissa. Suomessa voitaisiin ottaa mallia esimerkiksi Virosta siitä, miten kyberturvallisuudesta on luotu onnistuneesti maa-brändi.

Toimenpide 7: Suomen hyvää mainetta ja osaamista kyberturvallisuudessa tulee hyödyntää paremmin kansainvälisesti esimerkiksi maakuvaa rakentamalla ja vahvistamalla. Uskottava maakuvan rakentaminen edellyttää kuitenkin sitoutumista ja kansallisen tahtotilan vahvistamista toimenpide 1:ssä esitetyllä tavalla. Maakuvan vahvistamisen tulee perustua määriteltyihin vahvoihin sisältöihin ja osaamisiin. Kyberturvallisuuteen tarvitaan myös korkean profiilin johtohenkilö tai puolestapuhuja vahvistamaan viestiä Suomesta kyberturvallisuusmaana. Vastuutahot: Valtioneuvosto, työ- ja elinkeinoministeriö, FISC, yritykset

Kyberturvallisuusalan ja -osaamisen kehittämisessä julkiset hankinnat ovat tällä hetkellä lähes täysin hyödyntämätön voimavara. Julkinen sektori on merkittävä asiakas kyberturvallisuusyrityksille. Julkiset hankinnat eivät kuitenkaan nykymuodossaan tue alan yritystoiminnan kehitystä. Innovatiivisten hankintojen mahdollisuuksia ei ole hyödynnetty riittävästi. Viisas ja vaativa ostaminen voi parhaimmillaan muodostaa vahvan tuen ja referenssin alan yrityksille.

Toimenpide 8: Julkiset hankinnat tulee valjastaa kyberturvallisuusalan kehityksen tukemiseksi. Innovatiivisia hankintoja on hyödynnettävä sekä valtion että kuntien hankinnoissa, joissa on tietoturvaan liittyvä elementti. Innovatiivisten hankintojen toteuttaminen edellyttää uusien hankintamallien kehittämistä ja hankkijoiden koulutusta. Julkisia hankintoja ja yritysten kehitystyötä tulisi kytkeä paremmin toisiinsa myös siten, että esimerkiksi Tekesin ohjelmiin tulisi luoda malleja jotka tukisivat tulosten päätymistä julkisten toimijoiden käyttöön. Vastuutahot: työ- ja elinkeinoministeriö, Hansel, Valtori, kunnat, Tekes.

Toimenpide 9: Immateriaalioikeuksiin liittyvät käytännöt julkisissa ICT-palveluhankinnoissa tulee arvioida uudestaan. Hankinnoissa tulisi pyrkiä käy-

täntöihin, jotka tukevat yritysten liiketoimintaa ja kansainvälistymistä. Vastuutahot: työ- ja elinkeinoministeriö, Hansel, Valtori.

Yhteistyö ja vuorovaikutus

Eri toimijoiden välinen yhteistyö kyberturvallisuuteen liittyvissä kysymyksissä on lisääntynyt viime vuosina, mutta yhteistyötä on syytä tiivistää edelleen. Tämä on erityisen tärkeää, koska alan osaaminen on jakaantunut moniin organisaatioihin ja on hajallaan yrityksissä, korkeakouluissa ja tutkimuslaitoksissa. Yhteistyötä tarvitaan osaamisen edelleenkehittämiseksi ja alan edistämiseksi.

Kyberturvallisuusstrategia ei ole kyennyt luomaan yhteistä visiota ja yhteistyön henkeä, vaan on osin luonut säröjä kentän sisälle. Merkittävää myös on, että julkisen hallinnon ja tutkimusmaailman välillä tiedonvaihto, yhteistyö ja tietämys toisten tekemisistä ovat paikoin vähäisiä. Jotta osaaminen kehittyisi ja ala menestyisi hyvin jatkossa, tiedonvaihtoa tulee lisätä ja Suomeen tulee luoda vahva ”yhteen hiileen puhaltamisen” kulttuuri kyberturvallisuuteen liittyvässä kehitystyössä.

Suomesta puuttuu myös yhteistyön toimintamalli, jonka puitteissa eri toimijat voisivat käydä luottamuksellista ja syvällistä tiedonvaihtoa kyberturvallisuuteen liittyvistä kysymyksistä. Riskinä nykytilanteessa on, että kokonaiskuvaa kyberturvallisuuden, alan kehityksen ja osaamisen osalta ei muodostu kenellekään.

> **Toimenpide 10:** Suomeen tarvitaan toimintamalli tai yhteistyöelin (”kansallinen kyberturvallisuusneuvosto”), joka vahvistaa koordinaatiota ja tiedonvälistystä julkisen hallinnon avaintoimijoiden, tutkimusmaailman ja yritysten välillä. Yhteistyöelin voisi toimia Kyberturvallisuuskeskuksen tai Turvallisuuskomitean alaisuudessa. Vastuutahot: Valtioneuvosto, valtiovarainministeriö, Kyberturvallisuuskeskus, Turvallisuuskomitea

Kyberuhkiin ja -tapahtumiin liittyvän tiedon jakamisessa eri toimijoiden välillä on tällä hetkellä esteitä Suomessa. Kyse on sekä lainsäädännöstä että vallitsevasta toimintakulttuurista. Kyberuhka- ja tapahtumatietojen parempi saatavuus ja jakaminen edistäisivät yritysten tuotekehitystä ja mahdollistaisivat uudenlaisten tuotteiden kehittämisen. Myös alan tutkimuksen kannalta tietojen saannin esteet ovat merkittävä ongelma.

> **Toimenpide 11:** Selvitetään, miltä osin lainsäädäntö estää kyberuhka ja -tapahtumatietojen jakamista ja arvioidaan mahdolliset lainsäädännön muutostarpeet. Toimintakulttuuria on pyrittävä muuttamaan avoimemmaksi. Vastuutahot: liikenne- ja viestintäministeriö, valtiovarainministeriö, sisäministeriö, oikeusministeriö, Kyberturvallisuuskeskus, yritykset, tutkimustoimijat.

Suomessa on tällä hetkellä lukuisia kyberturvallisuuden harjoitus- ja laboratorioympäristöjä yliopistoissa, tutkimuslaitoksissa ja ammattikorkeakouluissa. Kansallisesti puuttuu koordinaatio siitä, missä ympäristöjä on ja mitä niillä voidaan tehdä. Ympäristöt eivät myöskään tue eri toimijoiden yhteistyötä, vaan ne ovat usein luonteeltaan suljettuja. Tämä rajoittaa alan kehityspotentiaalia.

> **Toimenpide 12:** Edistetään yhteistyötä ja koordinaatiota kyberturvallisuuden harjoitus- ja laboratorioympäristöjen käytössä. Yhteistyö ja yhteiskäyttö otetaan ehdoksi ympäristöjen julkiselle rahoitukselle. Järjestetään kansallinen ky-

berturvallisuusharjoitus, joka yhdistää useita harjoitusympäristöjä. Vastuutahot: valtiovarainministeriö, opetus- ja kulttuuriministeriö, Suomen Akatemia, yliopistot, ammattikorkeakoulut, tutkimuslaitokset.

LIITE 1. HAASTATELLUT HENKILÖT

Benson, Yrjö, erityisasiantuntija, valtiovarainministeriö

Candolin, Catharina, tietoverkkopuolustussektorin johtaja, Puolustusvoimat

Hautakangas, Marko, Vice President, Information Security, Insta DefSec Oy

Helenius, Marko, yliopistotutkija, Tampereen teknillinen yliopisto

Karlamaa, Kirsi, johtaja, Kyberturvallisuuskeskus, Viestintävirasto

Kataikko, Mika, johtaja, Jykes

Korkiakoski, Markku, ohjelmajohtaja, Elektrobit

Latikka, Juha, johtava tiedeasiantuntija, Suomen Akatemia

Lehto, Martti, dosentti, Jyväskylän yliopisto

Limnéll, Jarno, professori, Aalto-yliopisto & VP, Cyber Security and Business Development, Insta Group Oy

Mannila, Heikki, pääjohtaja, Suomen Akatemia

Nurmi, Tiina, ohjelmapäällikkö, Tekes

Nyberg, Kaisa, professori, Aalto-yliopisto

Piiroinen, Timo, rikosylikomisario, päällikkö, Kyberrikostorjuntakeskus, Keskusrikospoliisi

Röning, Juha, professori, Oulun yliopisto

Savola, Reijo, johtava tutkija, VTT

Savolainen, Martti, Senior Specialist, Elektrobit

Siltanen, Jarmo, koulutus- ja T&K-päällikkö, Jyväskylän ammattikorkeakoulu

Siponen, Mikko, professori, Jyväskylän yliopisto

Takanen, Ari, teknologiajohtaja, Codenomicon

Vepsäläinen, Pekka, projektipäällikkö, Jykes

Haastattelut Virossa 11.-12.11.2015

Aarelaid, Hillar, researcher, Technology Branch, NATO CCDCOE

Areng, Liina, Head of International Relations, NATO CCD COE, ambassador, Estonian Information System Authority (RIA)

Kaska, Kadri, researcher, NATO CCD COE

Ottis, Rain, Associate Professor at Tallinn University of Technology, NATO CCD COE Ambassador

Peterson, Raimo, Branch Chief, Technology Branch, NATO CCDCOE

Priisalu, Jaan, Senior Fellow, NATO CCD COE

Reintam, Aare, Cyber Defence Exercise Manager, NATO CCD COE

Vallaots, Allar, Deputy Chief, Estonian Defence Forces

Väisänen Teemu, researcher, Technology Branch, NATO CCDCOE

LIITE 2. TYÖPAJOIHIN OSALLISTUNEET ASIANTUNTIJAT

Aura, Tuomas, professori, Aalto yliopisto

Ferm, Tiina, lainsäädäntöneuvos, sisäministeriö

Haataja, Juha, opetusneuvos, opetus- ja kulttuuriministeriö

Hautakangas, Marko, Vice President, Information Security, Insta DefSec Oy

Honka, Hannu, Research Team Leader, VTT

Hummelholm, Aarne, erityisasiantuntija, valtiovarainministeriö

Huopio, Kauto, johtava tietoturva-asiantuntija, Viestintävirasto

Hyytiäinen, Mika, sotilasprofessori, Maanpuolustuskorkeakoulu

Janhunen, Kirsi, erityisasiantuntija, Valtiovarainministeriö

Jaakonaho, Jussi, Synopsys

Kataikko, Mika, johtaja, Jykes

Klemettinen, Mika, ohjelmapäällikkö, Tekes

Laine, Timo, poliisitarkastaja, Poliisihallitus

Limnéll, Jarno, professori, Aalto-yliopisto & VP, Cyber Security and Business Development, Insta Group Oy

Linna, Mka, johtava asiantuntija, Finanssialan keskusliitto

Lundberg, Jonas, Director, Head of Cyber Security Services Finland, F-Secure

Manninen, Olavi, tietoturvapäällikkö, Itä-Suomen yliopisto

Meskanen, Tommi, erikoistutkija Turun yliopisto

Mikkonen, Tommi, professori, Tampereen teknillinen yliopisto

Moilanen, Panu, lehtori, Jyväskylän yliopisto

Niemi, Valtteri, professori, Helsingin yliopisto

Nurmi, Tiina, Ohjelmapäällikkö, Tekes

Olin, Pentti, erikoistutkija, Turvallisuuskomitean sihteeristö

Paananen, Rauli, apulaisjohtaja, Viestintävirasto, Kyberturvallisuuskeskus

Pirhonen, Jari, Security Director, Samlink

Paavola, Jarkko, Turun ammattikorkeakoulu

Rousku, Kimmo, VAHTI-pääsihteeri, valtiovarainministeriö

Savola, Reijo, johtava tutkija, VTT

Tarkoma, Sasu, professori, Helsingin yliopisto

Vainio, Esko, erityisasiantuntija, valtiovarainministeriö, JulkICT-toiminto

Virtanen, Teemupekka, erityisasiantuntija, sosiaali- ja terveysministeriö

Vuorenvirta, Kati, erityisasiantuntija, puolustusministeriö

LIITE 3. PATENTTI- JA JULKAISUANALYYSIN AINEISTO- JA MENETELMÄKUVAUS

Tutkimuksen osana tehtiin kyberturvallisuuteen liittyvien suomalaisten tiedejulkaisujen ja patenttien analyysi. Julkaisujen osalta analyysin aineistona olivat ISI Web of Science -tietokannan tiedejulkaisut joissa on mainittuna suomalainen organisaatio kirjoittajan tutkimusorganisaationa. Patenttiaineisto koostui Yhdysvaltain patenttiviranomaiselle rekisteröidyistä patenteista joissa on keksijän maakoodina Suomi. Sekä patentit että tutkimusjulkaisut rajattiin ajalle 1995-2013, jota voidaan pitää tutkimuksen tekohetkellä luotettavana aineistona. Käytetty aineisto koostuu yhteensä 16 393 patentista ja 169 438 tiedejulkaisusta. Aineistorajauksen tarkempi kuvaus on saatavissa pyydettäessä kirjoittajilta.

Aineiston analyysi perustuu VTT:llä kehitettyyn analyysiprosessiin, joka yhdistää laadullisen ennakointiprosessin ja määrällisen aineistoanalyysin. Prosessi on kehitetty erityisesti vaikeasti määriteltävien aihepiirien, kuten esimerkiksi arktisuuden tai tässä tapauksessa kyberturvallisuuden, hahmottamiseen sekä muuntamiseen sellaiseen muotoon jossa aihepiiriin liittyvät julkaisut ja patentit ovat louhittavissa tietokannoista. Kyberturvallisuus on laaja kokonaisuus jota on vaikea hahmottaa yksittäisillä avainsanoilla tai tieteenala- ja patenttiluokituksilla, ja näin ollen kehitetty prosessi asettaa aineistohakujen lähtökohdaksi asiantuntijatyönä luodun käsitekartan. Käsitekartta operationalisoidaan hakupuuksi, joka tässä hankkeessa kirjoitettiin Python-ohjelmointikielellä koodiksi. Koodi käsittelee kaikki patentti- ja julkaisutietueet ja etsii näistä käsitekartassa määriteltyjä termejä. Kun ohjelmakoodi löytää tietueen, jossa esiintyy käsitekartan termi, tietue luokitellaan kuuluvaksi tiettyyn käsitekartan haaraan. Näin prosessoiden muodostuu käsitekarttaan perustuva määrällinen aineisto kyberturvallisuuteen liittyvien eri teemojen tiede- ja patenttituotannosta. Käytetty menetelmä on esitelty tarkemmin julkaisussa Leinonen ym. (2014).

Alla olevassa kuvassa on esitelty asiantuntijaprosessissa syntynyt käsitekartta. Kartan perusrunko laadittiin projektiryhmän sisäisen ryhmätyöskentelyn perusteella. Projektin alussa järjestetyssä työpajassa projektiryhmä määritteli yhteisesti sisällön termille ”kyberosaaminen”. Patentti- ja julkaisuanalyysin lähtökohdaksi valittiin ryhmätyön tuloksista teknologiaan liittyvät sisällöt, joista muodostettiin käsitekartan ensimmäinen versio. Käsitekarttaa laajennettiin ja tarkettiin tämän jälkeen VTT:n kyberturvallisuusasiantuntijoiden ja hankkeen ohjausryhmän näkemyksiä hyödyntäen. Alussa tehty teknologioihin keskittyvän rajaus ohjaa käsitekartan sisällön ja siten myös sen perusteella tehdyn analyysin lopputulokset teknologiseen näkökulmaan.

Kuva. Asiantuntija-arvioiden perusteella luotu käsitekartta, jonka keskiössä on termi ”Kyberturvallisuuden teknologiat”.

Asiantuntijatyönä tehdystä käsitekartasta muodostui ohjelmalliseen analyysiin 12 haaraa, joille annettiin nimet:

13. Asymmetriset menetelmät. Tiedon salauksen menetelmät jotka perustuvat eri avaimen käyttöön viestin salaamisessa ja purkamisessa.

14. Hyökkäysmenetelmät. Hyökkäysmenetelmät kattavat laajasti tietoverkkoihin liittyvät hyökkäysmenetelmät sekä verkkokuunteluun liittyvät teemat.

15. Tietokoneverkot. Käsitekartta kattaa tältä osin tietoverkot, erityisesti mobiiliverkot sekä erityyppiset tietovarannot kuten pilvipalvelut.

16. Konfiguraation hallinta. Konfiguraation hallinta kattaa laajasti tietoverkkoihin liittyvät hallintakysymykset, kuten tilannetieto ja turvallisuusprosessit.

17. Kriittinen infrastruktuuri. Käsitekarttaan rajattiin aihe yhteiskunnan toiminnalle kriittistä infrastruktuuria käsitteleville dokumenteille. Tämä aihepiiri oli vaikeimmin operationalisoitavissa ja jäi kooltaan pieneksi.

18. Tulevaisuuden menetelmät. Käsitekarttaa on rajattuna asiantuntijoiden mielestä tulevaisuuden salausteknologioita käsittelevä alue. Nämä teknologiat eivät ole käytössä, mutta osoittavat potentiaali kyberturvallisuuden teknologioina.

19. Identiteetin hallinta. Käsitekarttaan rajattiin erikseen suppea alue joka käsittää digitaalisen identiteetin hallinnan. Tämä luokka siis erotettuna konfiguraation hallinnasta joka keskittyy yrityksen järjestelmiin.

20. Tietojärjestelmät. Luokka kattaa tietojärjestelmät laajasti ymmärrettynä. Tiedejulkaistu sisältävät esimerkiksi tietojärjestelmätieteen soveltuvin osin.

21. Riskien hallinta: Käsitekartan tämä osa kattaa uhka-arviot ja heikkouksien tunnistamisen tietojärjestelmässä.

22. Ohjelmistokehitys: Käsitekartan tämä osa pyrki rajaamaan ohjelmistotuotannon laatuun liittyvän tutkimuksen. Haku on toteutettu laajempana ja ottaa huomioon ohjelmistotuotannon tutkimuksen ja patentoinnin laajasti.

23. Symmetriset menetelmät. Tiedon salauksen menetelmät jotka perustuvat saman avaimen käyttöön viestin salaamisessa ja purkamisessa.

24. Muut: Luokka jossa on eksplisiittisesti käsitelty kyberturvallisuutta, mutta sen sisältö ei ole sisällytetty mihinkään muista mainituista luokista.

Edellä listatut luokat pyrkivät kuvaamaan mahdollisimman tarkasti jokaisen haaran sisältöä. Ohjelma mahdollistaa lisäksi sen, että yksittäinen tietue voidaan luokitella useampaan kuin yhteen luokkaan. Käsitekartan perusteella luotu ohjelmakoodi palautti 2322 tietuetta, joista 1815 oli tiedejulkaisuja ja 507 patentteja. Aineistossa oli kokonaisuudessaan 2199 uniikkia tunnistetta, joten aineisto sisältää 123 duplikaattitietuetta.

Tehty määrällinen analyysi on osa laadullisen ja määrällisen analyysin kokonaisuutta. Määrällisen aineiston keskeinen tavoite on tukea laadullista ennakointityötä. Tässä työssä esiteltävät määrälliseen aineistoon perustuvat taulukot kuvaavat käsitekartan eri haaroihin kohdistettuja tietueita, hahmottaen lukumääriä ja organisaatioita eri teemoissa. Kuten muutkin laajoja tietoaineistoja käsittelevät prosessit myös tämä osittain automatisoitu prosessi tuottaa virheellisiä ja puuttuvia havaintoja. Näitä on pyritty poistamaan analysoimalla tulosaineistossa mahdollisesti esiintyviä systemaattisia virheitä. Virheitä on korjattu kunnes kymmenessä tulosjoukosta satunnaisesti valitussa tietueessa ei ole havaittavissa selkeää systemaattista virhettä ja yhdeksän kymmenestä on selkeästi aineistoon kuuluvia. Aineistoon oletettavasti jääneet merkittävimmät virhetekijät liittyvät bio- ja lääketieteen terminologiaan, jossa termien käyttö aiheutti aineistoon virheitä.

LIITE 4. TUTKIMUKSEN TIETOTEKNINEN INFRASTRUKTUURI JA DIGITAALISET TIETOVARANNOT KYBERTURVALLISUUDEN NÄKÖKULMASTA

Kyberosaaminen Suomessa -hankkeen osana tehtiin selvitys kansallisen tutkimus-, kehitys- ja innovaatio-osaamisen kannalta kriittisestä tietoteknisestä infrastruktuurista ja kansallisesti merkittävistä kulttuurin ja tutkimuksen digitaalisten tietovarantojen säilyttämiseen liittyvistä järjestelmistä. Selvityksen tavoitteena oli tunnistaa infrastruktuuriin liittyviä tieto- ja kyberturvallisuuden kehitystarpeita sekä tarkastella tietovarantojen tilaa kyberturvallisuuden näkökulmasta. Selvitys jakaantuu kahteen osaan, joiden keskeiset tutkimuskysymykset olivat: [21]

1. Mikä on kansallisen TKI-osaamisen kannalta kriittisen tietoteknisen infrastruktuurin tila tieto- ja kyberturvallisuuden näkökulmasta?

2. Miten kansallisesti eräät kansallisesti merkittävät digitaaliset tietovarannot on suojattu kyberuhkien varalta?

Selvityksen tutkimusmenetelminä käytettiin aineistokatsausta, kirjallisuusselvitystä sekä tutkimusinfrastruktuurin ja tietovarantojen näkökulmasta keskeisiin organisaatioihin suunnattuja asiantuntijahaastatteluita. Näiden avulla täydennettiin Kyberosaaminen Suomessa -hankkeen muissa työosioissa tehtyjen haastatteluiden sekä kyselyiden pohjalta saatuja tietoja. Alkuperäisenä tavoitteena oli haastatella asiantuntijoita yhteensä kymmenestä organisaatiosta, mutta haastatteluita tehtiin lopulta kuudessa organisaatiossa. Kohdeorganisaatiot sekä niissä haastateltujen henkilöiden lukumäärä on esitetty alla:

- Kansallinen audiovisuaalinen instituutti (KAVI), 2 henkilöä
- Sodankylän geofysiikan observatorio (SGO, Oulun yliopiston erillislaitos), 4 henkilöä
- Oulun yliopisto – Tietotekniikkakeskus, 3 henkilöä
- Luonnonvarakeskus (LUKE), 2 henkilöä
- Ilmatieteen laitos, 1 henkilö
- CSC – Tieteen tietotekniikan keskus Oy, 1 henkilö

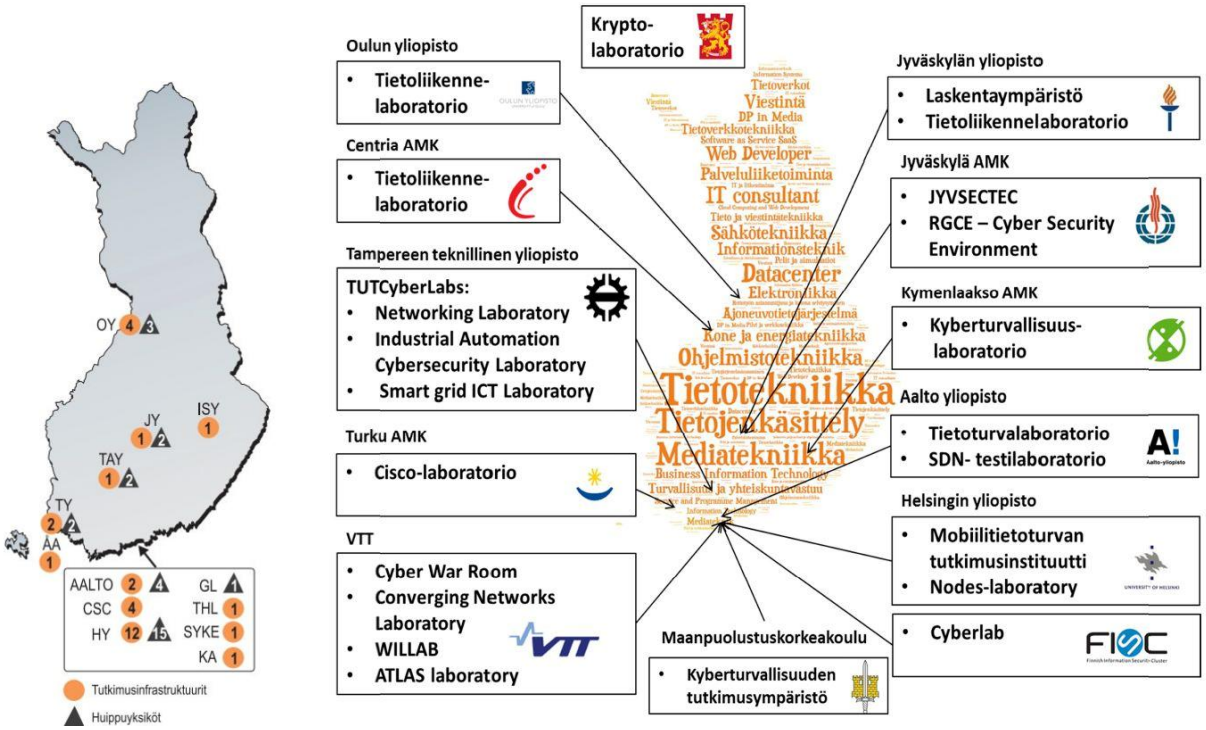
Haastattelukysymykset kartoittivat mm. kohdeorganisaation kyberturvallisuuden nykytilaa ja kypsyysastetta (itsearviointina), tietoturvakäytäntöjen implementointia sekä hallintaa, mahdollisesti havaittuja tietoturvauhkia/-tapauksia sekä haasteita liittyen esim. osaamiseen, yhteistyöhön sekä resursseihin. Haastatellut henkilöt on listattu tämän liitteen lopussa.

[21] Näiden kahden tutkimuskysymyksen lisäksi Kyberosaaminen Suomessa -hankeen ohjausryhmän kokouksissa keskusteltiin keväällä 2015 mahdollisuudesta jatkaa Jyväskylän yliopiston kyberturvallisuusselvitystyön (Lehto & Kähkönen 2015) tuloksena syntynyttä karttaa suomalaisten yliopistojen ja tutkimuslaitosten kyberlaboratorioista siten, että siihen sisällytettäisiin myös yritysten vastaavat ympäristöt. Tämä tehtävä todettiin kuitenkin mahdottomaksi, koska yritykset eivät julkaise tietoja omista kyberlaboratorioistaan ja toisaalta kyberlaboratorion määritelmä vaihtelee hyvin paljon yrityskentän sisällä.

Kansallisen TKI-osaamisen kannalta kriittisen tietoteknisen infrastruktuurin tila kyberturvallisuuden näkökulmasta

Suomen tutkimusinfrastruktuurien strategia ja tiekartta 2014-2020 -selvitys määrittelee tutkimusinfrastruktuurit seuraavasti: tutkimusinfrastruktuurit ovat tutkimusvälineiden, laitteistojen, aineistojen ja palveluiden varanto, joka mahdollistaa innovaatiotoiminnan eri vaiheissa tapahtuvan tutkimus- ja kehitystyön, tukee organisoitunutta tutkimustyötä, tutkijankoulutusta ja opetusta sekä ylläpitää ja kehittää tutkimus- ja innovaatiokapasiteettia. (Suomen Akatemia 2014)

Suomen tutkimusinfrastruktuurien ekosysteemiin on valittu 31 kansallista tutkimusinfrastruktuuria, joista 18 on kansainvälisiä ESFRI-kumppanuuksia (European Strategy Forum on Research Infrastructures). Lisäksi kahdella hankkeella on mahdollisuudet kehittyä merkittäviksi kansallisiksi tutkimusinfrastruktuureiksi. Kyberosaaminen Suomessa -hankkeen kartoitustyön näkökulmasta tietotekniikka ei ole merkittävässä roolissa kaikissa tutkimusinfrastruktuureissa, mutta tutkimustiedon tallennuksen ja säilytyksen näkökulmasta voidaan olettaa sen olevan kriittinen osa niitä. Alla olevassa kuvassa on esitetty kansalliset tutkimusinfrastruktuurit sekä Akatemian huippuyksiköt kartalla, jonka viereen on sijoitettu INKA-ohjelmassa tunnistettuja kyberturvallisuuden kehitys- ja laboratorioympäristöjä suomalaisissa korkeakouluissa ja tutkimuslaitoksissa.



Kuva. Suomen tutkimusinfrastruktuurit kartalla (Suomen Akatemia 2014) sekä Kyberturvallisuuden kehitys- ja laboratorioympäristöjä (Lehto & Kähkönen 2015)

Kuvasta voidaan havaita, että kahta tutkimusinfrastruktuuria lukuun ottamatta (Itä-Suomen yliopisto sekä Sodankylän geofysiikan observatorio, joka on kuvassa sijoitettu Oulun yliopistoon) kyberturvallisuuden tutkimus- ja kehitystoimintaa on samoilla alueilla tai jopa samoissa organisaatioissa kansallisten tutkimusinfrastruktuurien kanssa. Edellytykset yhteistyölle TKI-

osaamisen kannalta kriittisen tietoteknisen infrastruktuurin kehittämiseksi riittävälle tasolle voidaan todeta olevan olemassa. Tätä väitettä tukee myös Elixir Finlandin vuonna 2013 julkaisema raportti biopankkien yhteisestä BBMRI.fi -infrastruktuurista, jonka mukaan ”Suomessa tietotekninen infrastruktuuri on suhteessa moneen muuhun eurooppalaiseen maahan kehittyneessä vaiheessa.” (Elixir 2013).

Myös suoritetut asiantuntijahaastattelut sekä niiden perusteella suoritettu arviointi organisaation tilasta tukivat sitä olettamusta, että (kriittisen) tietoteknisen infrastruktuurin tila on hyvä. Arvioinnissa sovellettiin CMM-mallia (Capability Maturity Model), josta oli poistettu viides (jatkuva parantaminen) taso. Haastatteluiden perusteella organisaatiot sijoittuivat pääsääntöisesti kypsyystasolle 3, jossa tietoturvaprosessit ja tavoitteet on määritelty ja organisaatio noudattaa laadittua kehittämissuunnitelmaa (Valtiovarainministeriö 2006).

Haastatteluiden pohjalta nousi esiin seuraavia yleisiä haasteita ja kehityskohteita liittyen tutkimuksen kriittiseen tietotekniseen infrastruktuuriin kyberturvallisuuden näkökulmasta:

1. Tietohallinnon keskittäminen erilliseen organisaatioon tai jopa oman organisaation ulkopuolelle (esim. Valtori) vaikeuttaa kommunikointia sen ja TKI-toiminnon välillä sekä heikentää mahdollisuuksia tukea tutkimusympäristöjä näiden kyberturvallisuuteen ja tietojärjestelmiin liittyvissä resurssi- ja muissa tarpeissa. Esimerkiksi tietojärjestelmien ja -työkalujen homogenisointi aiheuttaa enemmän räätälöinnin tarvetta tutkimusympäristöissä, mikä edellyttää niiltä omaa IT-osaamista. Tämä haaste kasvaa tulevaisuudessa, kun tutkimusympäristöt ovat entistä enemmän riippuvaisia erilaisista tietojärjestelmistä. Yksi keino parantaa TKI-toiminnon resursseja on lisätä aktiivista vuoropuhelua sen ja tietohallinnon välillä liittyen toiminnon osaamistarpeisiin kyberturvallisuuden suhteen sekä tarvittavaa tiedonvaihtoa esim. koulutuksen tai erilaisten tietoiskujen muodossa.

2. Valtionhallinto ja suomalaisten yliopistojen yhteinen FUCIO-verkosto voisivat ottaa vastuulleen tietoturvakoulutusten keskitetyn hankkimisen ja tarjoamisen oman verkostonsa sisällä. Tällä hetkellä tarjolla on lähinnä verkkokoulutusta ja korkeakoulut järjestävät pääsääntöisesti itse omat koulutuksensa. Keskittämisellä olisi mahdollisuus yhtenäistää koulutuksia sekä saada kustannussäästöjä.

3. Myös muita tietoturvaan ja TKI-infrastruktuurien toimintavarmuuteen liittyviä palveluja voisi keskittää valtionhallinnon ja FUCIO-verkoston taakse; esim. tietoturvatestaus, lokitietojen analysointi tai laajempi tietoturvatiedon ja tapahtumien hallinta (SIEM). Myös erilaisten yhteishankkeiden järjestäminen em. tahojen toimesta mahdollistaisi organisaatioiden tietoturvan kohottamisen ja siihen liittyvän osaamisen kasvattamista kustannustehokkaalla tavalla.

4. Tutkijoiden liikkuvuus nähdään kasvavaksi ongelmaksi tulevaisuudessa erityisesti omien laitteiden käytön yleistyessä vierailevien tutkijoiden kohdalla. Kansainvälisen tutkimusyhteistyön myötä myös mittalaitteita vaihdetaan eri tutkimusyksiköiden välillä, mikä aiheuttaa ongelmia niiden tietoturvallisen sijoittelun osalta. Toistaiseksi vieraat laitteet on sijoitettu vieras- tai muuten erilliseen verkkoympäristöön, koska niiden tietoturvaa ei voida luotettavasti testata resurssi- ja osaamispuutteen vuoksi.

Kansallisesti merkittävien digitaalisten tietovarantojen suojaaminen kyberuhkien varalta

Selvityksen toisessa osassa tarkasteltiin kansallisesti merkittäviin tietovarantoihin kohdistuvia kyberuhkia sekä tietovarantojen suojaamista. Kansallisesti merkittävällä digitaalisella tietovarannolla tarkoitetaan tässä tapauksessa kulttuurin ja tutkimuksen digitaalisia tietovarantoja, joita ylläpitävät jo aiemmin mainittujen tutkimusinfrastruktuurien lisäksi mm.:

- Arkistolaitos
- CSC - Tieteellinen laskenta Oy
- Ilmatieteen laitos
- Kansallinen audiovisuaalinen instituutti (KAVI)
- Kansalliskirjasto
- Luonnonvarakeskus (LUKE)
- Suomen ympäristökeskus (SYKE)

Edellä mainituista organisaatioista CSC tarjoaa tiedonhallintaa ja tietojen pitkäaikaissäilytystä palveluna muille organisaatiolle.

Pitkäaikaissäilytykseen liittyvää määrittelytyötä on tehty opetus- ja kulttuuriministeriön Kansallinen digitaalinen kirjasto (KDK) -hankkeessa, jonka kolmas vaihe on käynnissä 2014-2016. Hankkeen pitkäaikaissäilytyspalvelun (KDK-PAS) sekä pitkäaikaissäilytysratkaisun (PAS) lisäksi hankkeessa on kehitetty yhteisiä standardeja digitaalisten aineistojen ja palveluiden tiedonsiirtoon ja säilytykseen. KDK-hankkeen rinnalla opetus- ja kulttuuriministeriöllä on käynnissä myös Avoin tiede ja tutkimus -hanke (2014-2017), joka edistää tieteen vaikuttavuutta yhteiskunnassa erilaisin avoimen tieteen mahdollistamin keinoin. Yhtenä osana hanketta kehitetään tutkimusten tulosten pitkäaikaissaatavuutta. Tämä edellyttää sisällön ymmärrettävyyden varmistamista sekä sen vaatimien sisältömenetelmien soveltamista, mikä mahdollistaa aineistojen avaamisen ja hyödyntämisen myös tulevaisuudessa. Aineistojen mukana pitkäaikaissäilytykseen tallennettavat metatiedot parantavat tiedon hyödyntämistä sekä käytettävyyttä kuvaamalla esim. tutkimusaineiston tarkoitusta, syntyä ja tekijöitä sekä mahdollistamalla aineiston löydettävyys, saavutettavuus ja uudelleenkäyttö. (Opetus- ja kulttuuriministeriö 2015)

Kyberturvallisuuden näkökulmasta pitkäaikaissäilytys edellyttää siihen tarkoitetuilta järjestelmiltä riittävää tietoturvaa tunkeutumisen estämiseksi. Pitkäaikaissäilytykseen tallennettavan datan salaus puolestaan takaa tiedon säilymisen vain siihen oikeutettujen henkilöiden saatavilla, mikä on myös luottamuksellisuuden edellytyksenä. Mikäli tiedolle halutaan taata pitkäaikaissaatavuus, edellyttää se varmuuskopiointia ja toisaalta tarkistussummien laskemista tiedon myöhempää validointia sekä digitaalista allekirjoitusta varten. Digitaalisella allekirjoituksella voidaan varmistaa tiedon eheys paitsi käyttöä varten niin myös siinä tapauksessa, että tietoa pitää konvertoida tulevaisuuden järjestelmiä tai ohjelmia varten.

Aineistokatsauksen sekä haastatteluiden perusteella ei merkittäviä tietoturva-/kyberuhkia ole havaittu tietovarantoja omistavissa organisaatioissa, mutta kyberuhkien määrän kasvu on

tiedostettu ja suunnitelmia niihin varautumiseksi on joko tehty tai niitä tehdään lähitulevaisuudessa. Haastatteluissa korostui CSC:n merkittävä rooli keskeisenä palveluntarjoajana kriittisten tietovarantojen pitkäaikaissäilytyksen sekä tiedon hallintapalveluiden osalta. Koska nämä kuuluvat CSC:n ydintoimintaan, yrityksen tietojärjestelmiin kohdistuvan hyökkäyksen riski on vähäinen verrattuna sen asiakkaiden tietojärjestelmien vastaaviin riskeihin.

Kyberuhat voivat kohdistua paitsi tietovarantoihin niin myös itse organisaatioon tai kolmanteen osapuoleen ja uhan aikajänne voi olla myös pitkä. Alla on listattu haastatteluissa esitettyjä kehitysehdotuksia ja tietovarantoihin liittyviä kyber- ja muita uhkia, jotka voivat kohdistua myös organisaatioon tai kolmanteen osapuoleen:

- **Metatietojen puute tai niiden vähäisyys heikentää tutkimustiedon hyödyntämistä.** Pitkäaikaissäilytykseen siirrettävän metatiedon vähäinen määrä ja niiden heikko laatu vaikeuttaa tutkimuksen ja tutkimustulosten validointia sekä sen hyödyntämistä. Pitkäaikaissaatavuuden edellyttämä tiedon ymmärtäminen helpottaa konvertointia, mikä saavutetaan kattavien metatietojen kautta. Tutkimusorganisaatioiden ja tutkimusta rahoittavien tahojen tulisi edistää tutkimustulosten hyödyntämistä edellyttämällä tutkijoilta tiedonhallintasuunnitelman tekoa sekä varmistamalla sen noudattaminen myös tutkimuksen valmistumisen jälkeen.

- **Suomen ulkomaan verkkoyhteyksiin kohdistuvat uhat.** Kriittiset tietovarannot eivät koostu pelkästään kotimaassa olevista tutkimuslaitteista ja järjestelmistä vaan reaaliaikaista tietoa tulee yhä enenevässä määrin myös ulkomailla sijaitsevista tutkimus- ja mittalaitteista. Suomen ulkomaan verkkoyhteyksiin kohdistuvat uhat saattavat lamaannuttaa reaaliaikaisen tiedon saamisen, mikä voi aiheuttaa uhkia ja jopa vaaratilanteita reaaliaikaista tietoa hyödyntävissä organisaatioissa. Tätä riskiä voidaan pienentää lisäämällä runkoverkon yhteyksiä ulkomaille.

- **Tutkimus- ja mittalaitteisiin sekä niiden tiedonsiirtoon kohdistuvat uhat.** Tämä korostuu erityisesti mittalaitteissa, jotka on sijoitettu toiseen maahan tai syrjäseudulle, jolloin etäyhteys on yleisin ratkaisu laitteen hallintaan sekä tutkimustulosten keräämiseen. Kolmas osapuoli voi päästä käsiksi laitteeseen, poistaa tai muokata dataa tai lisätä sinne haittaohjelman, joka aktivoituu vasta myöhemmin. Tätä riskiä voidaan pienentää parantamalla laitteiden tietoturvaa sekä noudattamalla yhteisiä tietoturvakäytäntöjä tutkimuslaitteiden ja -verkkojen osalta. Myös mittausdatan automaattinen skannaus haittaohjelmien varalta pienentää riskiä, mutta sekään ei poista tuntemattomien haittaohjelmien aiheuttamaa uhkaa.

- **Yhteistyöorganisaatio toimii astinlautana hyökkäykselle**. Automaattinen tiedonsiirto sekä tietojärjestelmien yhteiset rajapinnat organisaatioiden välillä voivat mahdollistaa kyberuhan. Siinä organisaatioon kohdistetaan hyökkäys yhteistyökumppanin kautta, jonka tietoturva on alemmalla tasolla kuin varsinaisen kohteen. Mikäli yhteistyöorganisaation järjestelmään saadaan lisättyä haittaohjelma, se voi päästä kohdeorganisaatioon normaalin tiedonsiirron yhteydessä. Myös pelkkä kohdeorganisaatioon siirrettävän tiedon muuttaminen voi aiheuttaa uhkatilanteen, mikäli kohteen toiminta edellyttää luotettavaa tietoa. Tätä riskiä voidaan pienentää esim. parantamalla yhteistyöorganisaation tietoturvatasoa tai käyttämällä jotain luotettavaa tarkistusmenetelmää datan validointiin.

Viitteet

Elixir (2013). Elixir FI Node – Finnish Life Science Infrastructure for Biological Information. BBMRI: yhteinen biopankkien IT-infrastruktuuri. http://www.elixir-finland.org/wp-content/uploads/2013/04/WWW.ELIXIR_BBMRI_artikkeli.pdf

Opetus- ja kulttuuriministeriö (2015). Avoin tiede ja tutkimus -hankkeen kotisivut. http://avointiede.fi/

Suomen Akatemia (2014). Suomen tutkimusinfrastruktuurien strategia ja tiekartta 2014-2020.Helsinki. 28.2.2014 http://www.aka.fi/globalassets/awanhat/documents/tiekartta/tutkimusinfrastruktuurien_strategia_ja_tiekartta_2014_20.pdf

Valtiovarainministeriö (2006). VAHTI 6/2006, Tietoturvatavoitteiden asettaminen ja mittaaminen. Valtiovarainministeriö, Hallinnon kehittämisosasto 20.07.2006 http://vm.fi/dms-portlet/document/371414

Tutkimuksen tietotekninen infrastruktuuri ja digitaaliset tietovarannot kyberturvallisuuden näkökulmasta -selvityksessä haastatellut henkilöt:

Ali-Hokka, Arto, tietoturvapäällikkö, Luonnonvarakeskus

Forsström, Pirjo-Leena, kehitysjohtaja, CSC - Tieteen tietotekniikan keskus Oy

Keränen, Matti, Sääpalvelujen tuotantojärjestelmät –yksikön päällikkö, Ilmatieteen laitos

Kuutti, Mikko, apulaisjohtaja, Kansallinen audiovisuaalinen instituutti

Lindberg, Kai, tietohallinnon kehittämispäällikkö, Oulun yliopisto

Murto, Kimmo, pääsuunnittelija, Luonnonvarakeskus

Määttä, Kaarlo, tietoturvapäällikkö, Oulun yliopisto

Oinas, Jaana, sovellussuunnittelija, Sodankylän geofysiikan observatorio

Rantala, Timo, käyttöinsinööri, Sodankylän geofysiikan observatorio

Suorsa, Veikko, tietotekniikkapäällikkö, Oulun yliopisto

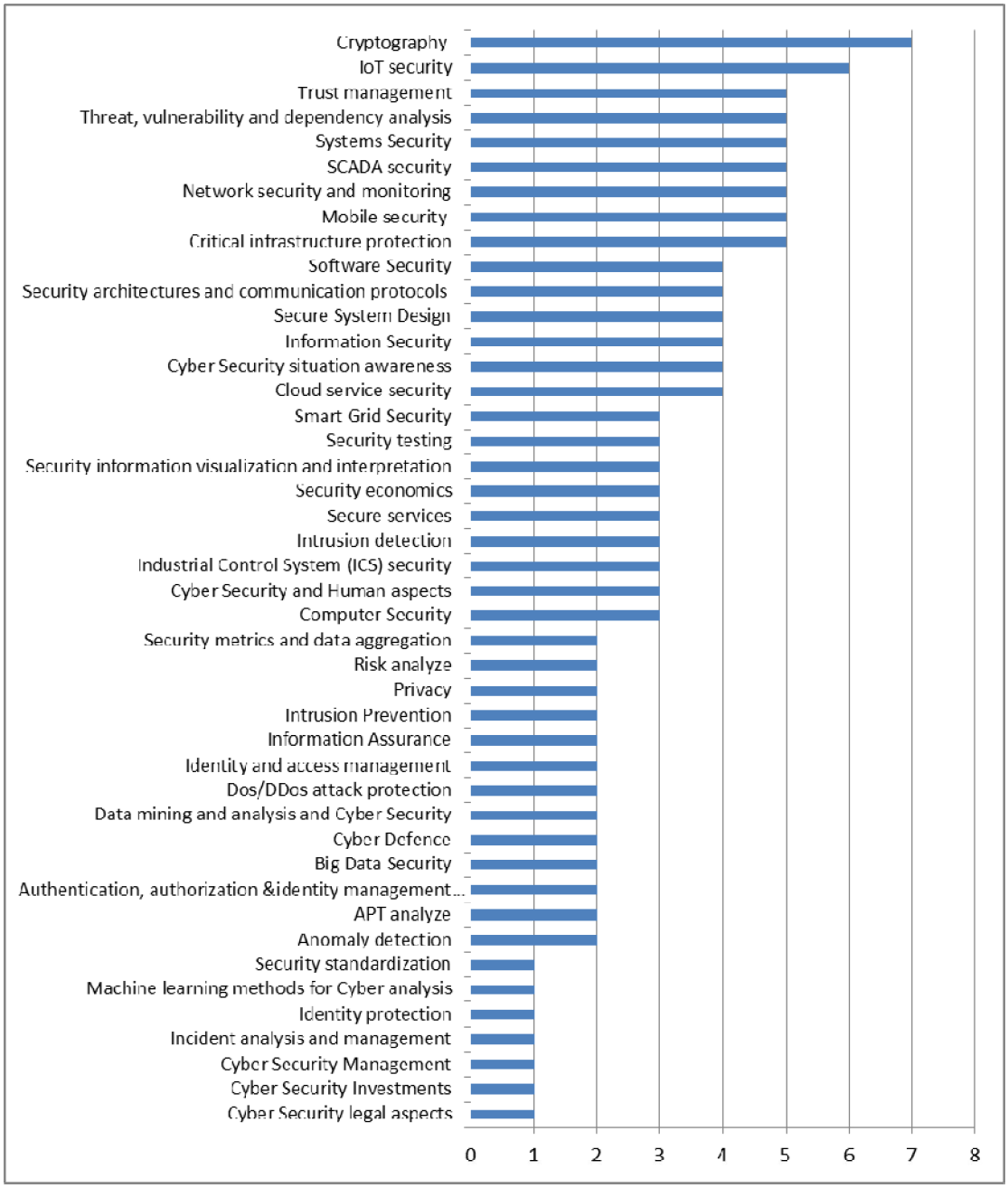
Turunen, Esa, johtaja, Sodankylän geofysiikan observatorio

Tähtinen, Pekka, erikoissuunnittelija, Kansallinen audiovisuaalinen instituutti

Ulich, Thomas, havaintopäällikkö, Sodankylän geofysiikan observatorio

LIITE 5. KYBERTURVALLISUUDEN TUTKIMUSALO- JA YLIOPISTOSSA JA TUTKIMUSLAITOKSISSA

Alla olevassa kuvassa on esitetty Lehdon ja Kähkösen (2015) tutkimuksen perusteella eri tutkimusaiheiden kattavuutta Suomen yliopistoissa ja tutkimuslaitoksissa. Lukumäärä kuvaa sitä kuinka monessa organisaatiossa aihetta tutkitaan. Lehdon ja Kähkösen tutkimuksessa ei kuvata sitä miten tiedot on kerätty, joten tietojen luotettavuutta on vaikea arvioida.



LÄHTEET

Bloch, Carten & Sorensen, Mads P. (2015). The size of research funding: Trends and implications. Science and Public Policy, 42: 1, 30-43.

Breznitz, Dan (2006). Innovation and the State. Political Choice and Strategies for Growth in Israel, Taiwan and Ireland. Yale University Press, New Haven.

BSA (2015). EU Cybersecurity Dashboard. A Path to Secure European Cyberspace. http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf

Cresson-Wood, C. (2004). Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. Computer Fraud & Security, 2004: Issue 1, 16–17.

Czosseck, C., Ottis, R., & Talihärm, A. (2011). Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. International Journal of Cyber Warfare and Terrorism (IJCWT) 1:1, 24-34. doi:10.4018/ijcwt.2011010103

e-Estonia.com (2016). e-Estonia Showroom Website, MTÜ IKT Demokeskus. https://e-estonia.com/

Estonian Ministry of Defence (2004). National Security Concept of the Republic of Estonia. (Unofficial version)
http://www.defesa.gov.br/projetosweb/livrobranco/arquivos/pdf/Estonia%202004.pdf

Estonian Ministry of Economic Affairs and Communication (2014). Cyber Security Strategy 2014-2017. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Estonia_Cyber_security_Strategy.pdf

FISC (2015). Kommentti julkisten hankintojen rooliin Suomen kyberkilpailukyvyn kehittämisessä: strategia ei toteudu käytännössä. Tietoturvaklusteri FISC ry 3.6.2015. www.fisc.fi

Fisher, Adam & Meir, Netanel (2015). Mapping Israel's Cybersecurity Start-ups.
http://techcrunch.com/2015/08/10/mapping-israels-cyber-security-startups/

Frost & Sullivan (2015). The 2015 (ISC)2 Global Information Security Workforce Study. A Frost & Sullivan White Paper.
https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-%28ISC%29%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

Frost & Sullivan (2014). Global Cyber Security Market Assessment. www.frost.com

Gehem, Maarten, Usanov, Artur, Frinking, Erik & Rademaker, Michel (2015). Assessing cyber security. A meta-analysis of threats, trends, and responses to cyber attacks. The Hague Centre for Strategic Studies, the Hague.

Heinze, T., Shapira, P., Rogers, J. D. and Senker, J. M. (2009). Organizational and institutional influences on creativity in scientific research., Research Policy, 38: 610–23.

Hentea, M., Dhillon, H., & Dhillon, M. (2006). Towards changes in information security education. Journal of Information Technology Education, 5, 221–233.

HSD (2015). The Value of Cooperation Innovation in Dutch Security in Perspective, The Hague Security Delta, 2015. http://www.hcss.nl/reports/the-value-of-cooperation-innovation-in-dutch-security-in-perspective/162/

Innovatiiviset kaupungit (2013). INKA - Innovatiiviset kaupungit 2014–2020. Kyberturvallisuusteeman toimintasuunnitelma. 30.8.2013.

ISO/IEC (2012). Information technology — Security techniques — Guidelines for cybersecurity, ISO/IEC JTC 1/SC 27. 27032:2012. 07/2012.

ITU, International Telecommunication Union (2008). Overview of cybersecurity. Recommendation ITU-T X.1205. http://www.itu.int/itu-t/recommendations/rec.aspx?id=9136.

ITU & ABI Research (2015). Global Cybersecurity Index & Cyberwellness Profiles. Report. April 2015.

Jackson, C.M. (2013). Estonian Cyber Policy After the 2007 Attacks: Drivers of Change and Factors for Success. In: New Voices in Public Policy, Vol. 7 No. 1 (2013). George Mason University - School of Policy, Government, and International Affairs. ISSN: 1947-2633

Kärkkäinen, Henrik (2014). Huawein tutkimuskeskus on erityislaatuinen. IT-viikko 9.7.2014.

Kyberturvallisuuskeskus (2015). Kyberturvallisuuskeskuksen vuosikatsaus. Vuosi 2014. https://www.viestintavirasto.fi/attachments/tietoturva/Kyberturvallisuuskeskuksen_vuosikatsaus_2014.pdf

Lehto, Martti & Kähkönen Aili (2015). Kyberturvallisuuden kansallinen osaaminen. Informaatioteknologian tiedekunnan julkaisuja No. 20/2015, Jyväskylän yliopisto. www.jyu.fi/it/tutkimus/202015_Kyber_kansallinen_osaaminen_VERKKO.pdf

Liikenne- ja viestintäministeriö (2016). Maailman luotetuinta digitaalista liiketoimintaa. Työryhmän ehdotus Suomen tietoturvallisuusstrategiaksi. Liikenne- ja viestintäministeriön julkaisuja 4/2016.

Limnell, Jarno (2014). Kyber rantautui Suomeen. Aalto-yliopiston julkaisusarja. https://aaltodoc.aalto.fi/bitstream/handle/123456789/14606/isbn9789526060224.pdf?sequence=1

Limnéll, Jarno, Majewski, Klaus & Salminen, Mirva (2014). Kyberturvallisuus. Docendo, Jyväskylä.

Long, Ju & White, Garry (2010). On the global knowledge components in an information security curriculum – a multidisciplinary perspective. Education and Information Technologies 15:4, 317-331.

Microsoft (2015). Microsoft Security Intelligence Report. www.microsoft.com/security/sir/default.aspx

Muhonen, Reetta, Leino, Yrjö & Puuska, Hanna-Mari (2012). Suomen kansainvälinen yhteisjulkaiseminen. Opetus- ja kulttuuriministeriön julkaisuja 2012:4. http://www.minedu.fi/export/sites/default/OPM/Julkaisut/2012/liitteet/okm04.pdf?lang=fi

National Coordinator for Security and Counterterrorism (2014). National Cyber Security Strategy 2, From awareness to capability. https://www.ncsc.nl/english/current-topics/national-cyber-security-strategy.html

National Cyber Security Centre (2015). Cyber Security Assessment Netherlands CSAN2015. https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands/cyber-security-assessment-netherlands-2015%5B2%5D.html

National Cyber Security Centre (2013). National Cyber Security Research Agenda II, NCSRA II, 2013. https://www.ncsc.nl/

NIST, National Institute of Standards and Technology (2013). NISTIR 7298: Glossary of Key Information Security Terms. Richard Kissel (ed.). U.S. Department of Commerce. May 2013 (Revision 2). http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Nordic Institute of Business & Society, OP-ryhmä & Miltton (2016). Toivon ja riskin aika. Suoraa asiaa suuryrityksiltä. OP:n suuryritystutkimus 2016. https://www.op.fi/media/liitteet?cid=-74948&srcpl=3&srcpl=3

PriceWaterhouseCoopers (2014). Managing cyber risks in an interconnected world. Key findings from The Global State of Information Security® Survey 2015. www.pwc.com

Prime Minister's Office (2016). Background for the establishment of the National Cyber Bureau
http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/Background.aspx

Remes, Juha & Kyheröinen, Jukka (2015). Kyberosaaminen Suomessa – Liiketoiminta-analyysi. Suomalaisten tietoturvayritysten osaaminen ja kilpailukyky eSociety-palvelujen alueella. Cyberlab Oy. Raportti osana Kyberosaaminen Suomessa -hanketta.
www.kyberosaaminen.fi

RIA - Riigi Infosüsteemi Amet (2012). Three-level IT baseline security system ISKE.
https://www.ria.ee/en/iske-en.html

Security & Defence Agenda (2012).
http://www.mcafee.com/in/about/news/2012/q1/20120130-02.aspx

Senor, Dan & Singer, Saul (2009). Start-up nation: The story of Israel's economic miracle. by Dan Senor and Council of Foreign Relations, Hachette Book Group, New York, NY.

So, Dyana (2014). Cyber Security Nation: Why Israel Leads the World in Protecting the Web. http://nocamels.com/2014/12/cyber-security-nation-israel/

Suciu, Peter (2015). Why Israel dominaters in cyber security. Fortune 1.9.2015

Suominen, Arho & Toivanen, Hannes (2015). Map of science with topic modeling: comparison of unsupervised learning and human-assigned subject classification. Journal of the Association for Information Science and Technology.

Tabansky, Lior & Ben Israel, Isaac (2015). Cybersecurity in Israel. SpringerBriefs in Cybersecurity. Springer.

Technavio (2016). Global Cyber Security Security Market 2016-2020. http://www.technavio.com/report/global-it-security-cyber-market-overview

Tilastokeskus (2008). Innovaatiotoiminta. Suomen virallinen tilasto (SVT) www.stat.fi

Ulkoasiainvaliokunta (2013). Ulkoasiainvaliokunnan mietintö 1/2013 vp s. 23.

Valtioneuvosto (2013). Suomen kyberturvallisuusstrategia. Valtioneuvoston periaatepäätös 24.1.2013. http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit

Valtioneuvoston kanslia (2015). Ratkaisujen Suomi. Pääministeri Juha Sipilän hallituksen strateginen ohjelma. 29.5.2015. http://valtioneuvosto.fi/sipilan-hallitus/hallitusohjelma

Van der Have, Robert, Saarinen, Jani, Pesonen, Pekka, Rilla, Nina (2009). Innovation as Objective: The Sfinno Approach. Teoksessa: Changes in Innovation - Towards an improved understanding of economic renewal. Toim. Saarinen, J. & Rilla, N. Palgrave Macmillan, Basingstoke.

Von Solms, R. & van Niekerk, J (2013). From information security to cyber security. Computers & Security 38: 97-102. doi:http://dx.doi.org/10.1016/j.cose.2013.04.004

von Tunzelmann, N., Ranga, M., Martin, B., Geuna, A. (2003). The Effects of Size on Research Performance: A SPRU Review. University of Sussex, Brighton.

VALTIONEUVOSTON
SELVITYS- JA TUTKIMUSTOIMINTA

tietokayttoon.fi

ISSN 2342-6799 (pdf)
ISBN 978-952-287-215-9 (pdf)