Työ- ja elinkeinoministeriön julkaisuja • Yritykset • 2019:17

Kasvua digitaalisesta turvallisuudesta

Tiekartta 2019–2030

Työ- ja elinkeinoministeriö
Arbets- och näringsministeriet

Työ- ja elinkeinoministeriön julkaisuja 2019:17

Kasvua digitaalisesta turvallisuudesta
Tiekartta 2019–2030

Valmistelutyön loppuraportti

Antti Karjaluoto, DIMECC Oy
Ülo Parts, DIMECC Oy
Risto Lehtinen, DIMECC Oy
Tapio Frantti, Oulun yliopisto

Työ- ja elinkeinoministeriö, Helsinki 2019

Työ- ja elinkeinoministeriö

ISBN: 978-952-327-405-1

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2019

Kuvailulehti

Julkaisija	Työ- ja elinkeinoministeriö		8.3.2018
Tekijät	Antti Karjaluoto, Ülo Parts, Risto Lehtinen – DIMECC, Tapio Frantti – Oulun yliopisto		
Julkaisun nimi	Kasvua digitaalisesta turvallisuudesta Tiekartta 2019–2030		
Julkaisusarjan nimi ja numero	Työ- ja elinkeinoministeriön julkaisuja 2019:17		
Diaari/ hankenumero	TEM/1367/13.01.01/2018	**Teema**	Yritykset
ISBN PDF	978-952-327-405-1	**ISSN PDF**	1797-3562
URN-osoite	http://urn.fi/URN:ISBN:978-952-327-405-1		
Sivumäärä	78	**Kieli**	suomi
Asiasanat	Kyberturvallisuus, osaaminen, digitalisaatio		

Tiivistelmä

Digitaalisen turvallisuuden kasvun tiekartan tavoitteena on edistää digitaaliseen turvallisuuteen ja osaamiseen liittyvää yritysvetoista kehitystä, kasvua ja kansainvälistymistä yritysten, julkisen sektorin ja tutkimuslaitosten yhteistyönä. Raportissa esitetään digitaalisen turvallisuuden alan yhteinen tavoitetila ja tulevaisuuskuva vuodelle 2030, kuvataan alan osaaminen ja toimintaympäristö, määritetään teemakohtaiset visiot vuodelle 2030 ja keskeiset välitavoitteet vuosille 2021 ja 2025. Tiekartta voi toimia käytännön työkaluna suunniteltaessa uusia kyberturvallisuusosaamista vahvistavia politiikkatoimia ja niiden toteutusta sekä mahdollistettaessa toimijoiden kasvupolkuja esimerkiksi erilaisten ekosysteemien ja kiihdyttämöjen kautta.

Raportin on tilannut ja sitä on ohjannut työ- ja elinkeinoministeriö. Ohjausryhmätyöhön ovat lisäksi osallistuneet liikenne- ja viestintäministeriö, opetus- ja kulttuuriministeriö, Huoltovarmuuskeskus ja Business Finland.

Tiekartan valmistelutyön tarkoituksena on ollut tunnistaa tärkeimmät sidosryhmät ja muodostaa kansallinen viitekehys digitaalisen turvallisuuden tutkimus-, kehitys- ja innovaatiotoiminnan (TKI-toiminnan) investointien suuntaamiseksi. Lisäksi valmistelutyössä tunnistettiin toimenpiteitä, joilla voidaan vahvistaa Suomen asemaa kansainvälisesti tunnettuna digitaalisen turvallisuuden tutkimuksen, innovaatiotoiminnan, investointien ja uuden liiketoiminnan edelläkävijänä.

Valmistelutyön löydökset ja toimenpidesuositukset tarjoavat pohjan kyberturvallisuusosaamisen ja siihen tukeutuvan liiketoiminnan kasvua edistävän ohjelmatoiminnan käynnistämiselle ja jatkotoimenpiteiden suunnittelulle ja toteutukselle.

Kustantaja	Työ- ja elinkeinoministeriö
Julkaisun jakaja/myynti	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: julkaisutilaukset.valtioneuvosto.fi

Presentationsblad

Utgivare	Arbets- och näringsministeriet		8.3.2018
Författare	Antti Karjaluoto, Ülo Parts, Risto Lehtinen – DIMECC, Tapio Frantti – Uleåborgs universitet		
Publikationens titel	Tillväxt genom digital säkerhet Färdplan 2019–2030		
Publikationsseriens namn och nummer	Arbets- och näringsministeriets publikationer 2019:17		
Diarie-/ projektnummer	TEM/1367/13.01.01/2018	**Tema**	Företag
ISBN PDF	978-952-327-405-1	**ISSN PDF**	1797-3562
URN-adress	http://urn.fi/URN:ISBN:978-952-327-405-1		
Sidantal	78	**Språk**	finska
Nyckelord	cybersäkerhet, kunnande, digitalisering		

Referat

Målet med färdplanen för tillväxt genom digital säkerhet är att främja företagsdriven utveckling, tillväxt och internationalisering med anknytning till digital säkerhet och kompetens som ett samarbete mellan företag, offentlig sektor och forskningsinstitut. Rapporten innehåller en gemensam målbild och framtidsbild för 2030 för branschen digital säkerhet, en beskrivning av kunskaperna inom branschen samt dess verksamhetsmiljö, temaspecifika visioner för 2030 och centrala mellanliggande mål för 2021 och 2025. Färdplanen kan fungera som ett praktiskt verktyg för planering av nya politikåtgärder som stärker cybersäkerhetskunnandet och genomförandet av dem samt för möjliggörande av olika aktörers tillväxtstigar, t.ex. via olika ekosystem och acceleratorer.

Rapporten har beställts och utarbetandet av den letts av arbets- och näringsministeriet. I styrgruppsarbetet har dessutom deltagit representanter för kommunikationsministeriet, undervisnings- och kulturministeriet, Försörjningsberedskapscentralen och Business Finland.

Syftet med beredningen av färdplanen har varit att identifiera de viktigaste intressentgrupperna och bilda en nationell referensram för att rikta investeringar i forsknings-, utvecklings- och innovationsverksamhet som gäller digital säkerhet. I samband med beredningsarbetet identifierades dessutom åtgärder genom vilka man kan stärka Finlands ställning som en internationellt erkänd föregångare inom forskning, innovationsverksamhet, investeringar och ny affärsverksamhet på området digital säkerhet.

De upptäckter och åtgärdsrekommendationer som gjordes under beredningsarbetet ger en grund för att inleda programverksamhet som främjar kunnande inom cybersäkerhet samt tillväxt för affärsverksamhet som stöder sig på sådant kunnande. De ger också en grund för planering och genomförande av fortsatta åtgärder.

Förläggare	Arbets- och näringsministeriet
Distribution/ beställningar	Elektronisk version: julkaisut.valtioneuvosto.fi Beställningar: julkaisutilaukset.valtioneuvosto.fi

Description sheet

Published by	Ministry of Economic Affairs and Employment		8 March 2019
Authors	Antti Karjaluoto, Ülo Parts, Risto Lehtinen – DIMECC, Tapio Frantti – University of Oulu		
Title of publication	Growth from digital security Roadmap for 2019–2030		
Series and publication number	Publications of the Ministry of Economic Affairs and Employment 2019:17		
Register number	TEM/1367/13.01.01/2018	**Subject**	Enterprises
ISBN PDF	978-952-327-405-1	**ISSN (PDF)**	1797-3562
Website address (URN)	http://urn.fi/URN:ISBN:978-952-327-405-1		
Pages	78	**Language**	Finnish
Keywords	Cyber security, competence, digitalisation		

Abstract

The objective of the digital security roadmap is to promote the business-driven growth, development and internationalisation related to digital security and competence as a joint effort between the business sector, the public sector and research institutes. The report provides an outline for a shared target state and a vision of the future for the digital security sector for 2030, as well as a description of the skills and competences in the field and of the operating environment. It also contains theme-specific visions for 2030 and key milestones for 2021 and 2025. The roadmap may serve as a practical tool in the planning and implementation of new policy measures intended to enhance cyber security competence, and for enabling growth paths for various ecosystems and accelerators.

The report was commissioned by the Ministry of Economic Affairs and Employment, which also steered the preparation, together with the Ministry of Transport and Communications, Ministry of Education and Culture, National Emergency Supply Agency and Business Finland.

The objective when preparing the roadmap was to identify the key stakeholder groups and to build a national framework for targeting digital security research, development and innovation investments. The preparatory work also helped to identify measures that can help to strengthen Finland's position as an internationally renowned forerunner in research, innovation, investment and new business in the digital security sector.

Results of the preparatory work and recommendations for actions provide a foundation for the launch of programme activities promoting cyber security and related business, and for the planning and implementation of further action.

Publisher	Ministry of Economic Affairs and Employment
Distributed by/ publication sales	Electronic version: julkaisut.valtioneuvosto.fi Publication sales: julkaisutilaukset.valtioneuvosto.fi

Sisältö

ESIPUHE

Digitalisaation yhteiskunnalle tuomat edut ovat kiistattomat. Digitalisaatioon liittyy kuitenkin myös uhkia, kuten tietomurrot, identiteettivarkaudet ja informaatiovaikuttaminen. Näille altistuvat kaikki yritykset ja kansalaiset. Puhumme tietoturvasta ja digitaalisesta tai kyberturvallisuudesta, mutta meidän pitäisi puhua myös laajemmin digitaalisesta turvallisuudesta ja luottamuksesta.

Digitaalinen turvallisuus perustuu siihen, että meillä on riittävät tekniset ja tiedolliset valmiudet toimia turvallisesti digitaalisessa ympäristössä. Tähän kuuluu teknisten ratkaisujen ja teknologiaymmärryksen lisäksi ymmärrys ihmisten käyttäytymisestä. Luottamus puolestaan rakentuu eri toimijoiden välille ja se ansaitaan ennustettavalla, oikealla ja vastuullisella toiminnalla. Tällä hetkellä meillä kaikilla ei ole ymmärrystä siitä, millä kaikilla tavoin ihmisiin yritetään vaikuttaa. Eri maiden vaalikampanjoihin kohdistetut vaikuttamisyritykset sekä nuorten nettikiusaaminen ovat tästä varoittavia esimerkkejä. Mistä luottamus siis syntyy ja miten se voidaan synnyttää digitaalisessa toimintaympäristössä?

Tässä raportissa kuvatun valmistelutyön tarkoituksena oli selvittää koordinoidun ohjelmatoiminnan edellytyksiä ja tavoitteita digitaaliseen turvallisuuteen liittyvien kasvumahdollisuuksien hyödyntämiseksi. Raportissa käydään läpi ohjelmatoiminnan käynnistämisen edellytyksiä sekä esitellään viitekehys ja konkreettinen tiekartta ohjelmatoiminnan toteuttamiseen. Pitkän tähtäimen tavoitteena on luoda toimintaympäristö, joka mahdollistaa uusien liiketoimintamallien kehittämisen ja käyttöönoton Suomessa. Lisäksi tavoitteena on varmistaa kaikille kansalaisille yhtäläiset valmiudet ja mahdollisuudet ymmärtää muuttuvaa digitaalista maailmaa.

Digitaalisen turvallisuuden merkitys kasvaa edelleen, sillä se muodostaa perustan digitaaliselle yhteiskunnalle. Digitaalinen turvallisuus kytkeytyy oleellisesti

nouseviin teknologioihin ja tuleviin osaamisalueisiin, kuten esimerkiksi tekoäly, teollinen internet (IIoT, Industrial Internet of Things) ja Big Data. Kansallisella digitaalisen turvallisuuden osaamisella on tulevaisuudessa yhä suurempi merkitys kokonaisturvallisuuden ja yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta[i].

Kansallisen tietoturvastrategian mukaan Suomen visiona on: **Maailman luotetuin digitaalinen liiketoiminta tulee Suomesta**[ii]. Valmistelutyön perusteella sitä ehdotetaan päivitettäväksi muotoon: **Maailman luotettavin digitaalinen liiketoiminta ja kattavin digitaalisen turvallisuuden osaaminen tulevat Suomesta**. Suomea pidetään jo nyt luotettavana ja neutraalina maana ja toimintaympäristönä, mikä muodostaa hyvän lähtökohdan alan liiketoiminnalle ja kasvulle. Suomalaisten hyvä koulutustaso luo tukevan pohjan Suomen nousulle digitaalisen turvallisuuden ja luottamuksen ykkösmaaksi.

Digitaalisen turvallisuuden kasvumahdollisuuksien tiekartan valmistelutyö on nyt tehty, mutta tämä on vasta alku, ei päätepiste. Valmistelutyön löydökset ja toimenpidesuositukset tarjoavat hyvän pohjan ohjelmatoiminnan käynnistämiselle ja jatkotoimenpiteiden suunnittelulle ja toteutukselle.

Antti Karjaluoto, valmistelutyön vastaava johtaja
DIMECC Oy

Ülo Parts, vastaavan johtajan varahenkilö
DIMECC Oy

Risto Lehtinen, valmistelutyön prosessivastaava ja pääfasilitaattori
DIMECC Oy

Tapio Frantti, kyberturvallisuuden erityisasiantuntija
Oulun yliopisto

Tiivistelmä

Lähtökohta

Tässä raportissa kuvataan syksyllä 2018 laaditun digitaalisen turvallisuuden kasvun tiekartan valmistelutyön keskeiset tulokset.

Digitaalisen turvallisuuden kasvun tiekartan tavoitteena on **edistää digitaaliseen turvallisuuteen ja osaamiseen liittyvää yritysvetoista kehitystä, kasvua ja kansainvälistymistä** yritysten, julkisen sektorin ja tutkimuslaitosten yhteistyönä. Valmistelutyössä on laadittu digitaalisen turvallisuuden alan yhteinen tavoitetila ja tulevaisuuskuva vuodelle 2030, kuvattu alan osaaminen ja toimintaympäristö, määritelty teemakohtaiset visiot vuodelle 2030 ja keskeiset välitavoitteet vuosille 2021 ja 2025 sekä tehty ehdotus ohjelman edistymisen aktiivisesta seurannasta. Tiekartta voi toimia käytännön työkaluna suunniteltaessa uusia politiikkatoimia ja niiden toteutusta sekä mahdollistettaessa toimijoiden itse muodostamia kasvupolkuja esimerkiksi erilaisten ekosysteemien ja kiihdyttämöjen kautta.

Tiekartan valmistelutyön on tilannut ja sitä on ohjannut työ- ja elinkeinoministeriö. Ohjausryhmätyöhön ovat lisäksi osallistuneet liikenne- ja viestintäministeriö, opetus- ja kulttuuriministeriö, Huoltovarmuuskeskus ja Business Finland. Valmistelun aikana ohjaus- ja työryhmäkokousten lisäksi järjestettiin viisi teematyöpajaa sekä toteutettiin toimijoiden haastatteluja. Työn tekemiseen osallistui lähes 150 eri alojen asiantuntijaa (liite 6).

Tavoitteet

Valmistelutyön tarkoituksena oli tunnistaa tärkeimmät sidosryhmät ja muodostaa kansallinen viitekehys digitaalisen turvallisuuden tutkimus-, kehitys- ja innovaatiotoiminnan (TKI-toiminnan) investointien suuntaamiseksi. Lisäksi valmistelutyössä tunnistettiin toimenpiteitä, joilla parannetaan Suomen asemaa kansainvälisesti tunnettuna digitaalisen turvallisuuden tutkimuksen, innovaatiotoiminnan, investointien ja uuden liiketoiminnan edelläkävijänä.

Valmistelutyön tavoitteena oli myös luoda ymmärrystä digitaalisen turvallisuuden toimintakentästä ja osaamisen merkityksestä digitaalisen liiketoiminnan kriittisenä edellytyksenä sekä laajemmin kansalaistaitona. Tätä tukee valmistelutyön yhtenä toimenpide-ehdotuksena esitetty laaja kansalaisportaali, joka antaa julkista tietoa digitaalisesta turvallisuudesta ja luottamuksesta sekä sisältää ajankohtaista tutkimustietoa ja opetuspaketteja. Se on myös kansalaisille suunnattu digitaalisen osaamisen tietopankki.

Tiekartta 2019–2030

Valmistelutyön työpajoissa jalostettu kokonaisvisio *"Maailman luotettavin digitaalinen liiketoiminta ja kattavin digitaalisen turvallisuuden osaaminen tulevat Suomesta "* ja tähän linkittyvät teemakohtaiset visiot antavat suunnan tiekartalle.

Tiekartassa (kuva 5 ja liite 4) kuvatut toimenpiteet on jaoteltu valmistelutyössä käytettyjen neljän pääteeman ympärille: (1) kyberresilienssi, (2) osaaminen ja jatkuva oppiminen, (3) elinkeinoelämän digitalisaatio sekä (4) kasvu ja kansainvälistyminen.

Kyberresilienssi -alueen toimenpiteet keskittyvät huoltovarmuuden edistämiseen parantamalla keskeisten toimijoiden tilannetietoisuutta ja tukemalla kyberuhkiin varautumista ja niistä toipumista yhteiskunnan keskeisillä osa-alueilla. **Osaaminen ja jatkuvan oppiminen** -alueen toimenpiteiden tavoitteena on lisätä kansallista tietoisuutta digitaalisesta turvallisuudesta sekä korostaa digitaalisen turvallisuuden osaamisen roolia ja merkitystä osana uutta digitaalista yhteiskuntaa. **Elinkeinoelämän digitalisaatio** -alueen toiminnot keskittyvät digitaalisen turvallisuuden roolin

kehittämiseen elinkeinoelämän digitaalisen murroksen mahdollistajana ja uuden kasvun ajurina. **Kasvu ja kansainvälistyminen** -alueen toimenpiteet keskittyvät edistämään Suomen asemaa kansainvälisesti tunnettuna digitaalisen turvallisuusalan edelläkävijänä. Teema kattaa myös alan tutkimus- ja innovaatiotyön sekä suomalaisten digitaalisen turvallisuusalan yritysten kansainvälistymisen edistämisen.

Tiekartan 2019–2030 tärkeimmät toimenpiteet ovat seuraavat:

1. Hallinnonaloja yhdistävä **digitaalisen turvallisuuden kasvutiekartan ohjausryhmän perustaminen**
2. **Digitaalisen turvallisuuden liiketoiminnan ekosysteemin rakentaminen ja käynnistäminen**
3. Yhteiskunnan toiminnan suojaamiseen ja varmistamiseen liittyvien **digitaalisen turvallisuuden perusratkaisujen ja -palveluiden systematisointi, tuotteistaminen ja yhteistyömallien rakentaminen yritysten TKI-toiminnan vauhdittamiseksi**
4. Digitaalisen turvallisuuden ja luottamuksen **opetussuunnitelman laatiminen**
5. Suomen **”Digital Trust & Safety” -maabrändin rakentaminen ja markkinointi**

Tarvittavat portaalit ja tietokannat:

6. **Digitaalisen turvallisuuden kansalaisportaali**
7. Yritysten ja julkisten toimijoiden käyttöön tarkoitettu digitaalisen turvallisuuden **hanke- ja toimijaportaali**

Toimeenpano

Tässä raportissa kuvatussa valmistelutyössä tarkasteltiin digitaaliseen turvallisuuteen liittyvien kasvumahdollisuuksien hyödyntämiseen tähtäävän ohjelmatoiminnan käynnistämisen edellytyksiä ja tavoitteita**. Yritysten, julkisten toimijoiden ja tutkimuslaitosten sitoutuminen tiekartan toimenpiteiden laajamittaiseen**

toteuttamiseen on ensiarvoisen tärkeää. Tämä työ on aloitettu valmistelun työpajoissa ja vaikuttaa vahvasti siltä, että yhteinen tarve ja tahtotila ohjelmatoiminnan käynnistämiselle on olemassa. Tämän valmistelutyön tulokset ja toimenpidesuositukset tarjoavat hyvän pohjan ohjelmatoiminnan käynnistämiselle ja jatkotoimenpiteiden suunnittelulle ja toteutukselle.

Johdanto, tavoitetila ja tulevaisuuskuva

Johdanto

Digitaalinen turvallisuus[1] muodostaa perustan kehittyvälle digitaaliselle yhteiskunnalle. Digitaalisen murroksen edetessä ja digitaalisten ratkaisujen tullessa kiinteäksi osaksi yksilöiden ja yhteiskunnan toimintaa kansallisen digitaalisen turvallisuuden merkitys nousee keskeiseksi yhteiskunnan kokonaisturvallisuuden ja elintärkeiden toimintojen turvaamisen kannalta. Digitaalisella turvallisuudella ja siihen liittyvällä osaamisella on tärkeä merkitys myös suomalaisen elinkeinoelämän digitalisaation mahdollistajana: korkealaatuisten ja luotettavien ratkaisujen ja palveluiden tarjoaminen edellyttää digitaalisen turvallisuuden kokonaisvaltaista huomioon ottamista. Ilman tarvittavaa digitaalisen turvallisuuden osaamista vientiyrityksemme eivät pysty luomaan uusia ratkaisuja ja niihin perustuvaa uutta liiketoimintaa. Lisäksi digitaalisen turvallisuuden merkityksen globaali kasvu avaa merkittäviä uusia kansainvälisiä liiketoimintamahdollisuuksia suomalaisille digitaalisen turvallisuuden alan osaajille. Suomi tunnetaan digitaalisen turvallisuuden vahvana toimintaympäristönä. Esimerkiksi Microsoftin Security Intelligence -raporteissa[iii] Suomi on vuodesta toiseen ollut kärkisijoilla, kun tarkastellaan maita, joiden verkoissa on vähiten haittaohjelmia. Digitaalisen turvallisuuden liittämiseksi osaksi Suomen maabrändiä on siis olemassa hyvät lähtökohdat.

1 Termillä ”**kyberturvallisuus**” viitataan luotettaviin ja toiminnaltaan turvattuihin digitaalisiin tietojärjestelmiin (lähde: *Kyberturvallisuuden sanasto*, Turvallisuuskomitea, 2018). Tässä raportissa käytetty termi ”**digitaalinen turvallisuus**” on laajempi, sillä se kattaa turvallisesti toteutettujen yhteyksien, laitteiden ja ohjelmistojen lisäksi myös käyttäjien osuuden eli ymmärryksen siitä, miten digitaalisessa toimintaympäristössä toimitaan vastuullisesti ja turvallisesti. Digitaaliseen turvallisuuteen panostavassa toimintakulttuurissa hyödynnetään systemaattisesti ja kattavasti sekä turvallista tekniikkaa että käyttäjien korkeatasoista tietotaitoa.

Maailman talousfoorumin (World Economic Forum, WEF) arvioiden mukaan kyberrikollisuudesta johtuvat taloudelliset menetykset nousevat maailmanlaajuisesti 3000 miljardiin dollariin vuoteen 2020 mennessä[iv]. Jo kuluvan vuoden aikana kaksi kolmasosaa kaikista yrityksistä voivat odottaa joutuvansa hakkeroinnin kohteeksi. Kyberhyökkäykset ovat usein luonteeltaan maailmanlaajuisia, esimerkiksi vuonna 2017 tapahtunut Wannacry-hyökkäys tapahtui 150 maassa ja kohdistui mm. Britannian terveydenhuoltosektoriin ja moniin muihin yhteiskunnan kannalta kriittisiin toimintoihin. Maailman talousfoorumi onkin nimennyt kyberuhat yhdeksi aikamme suurimmista riskeistä.

Digitaalinen turvallisuus ja alueellisen kyberosaamisen kehittäminen ovat keskeisessä asemassa EU:ssa ja ne ovat yksi painopistealueista myös EU:n tulevassa tutkimuksen ja innovoinnin puiteohjelmassa. Omien digitaalisten voimavarojen ja sisämarkkinoiden turvaamisen lisäksi unioni haluaa olla kilpailukykyinen toimija maailmanlaajuisilla digitaalisen turvallisuuden markkinoilla. Vuonna 2013 hyväksytyssä EU:n digitaalisen turvallisuuden strategiassa pyritään edistämään luotettavaa, turvallista ja avointa kybertoimintaympäristöä. Näiden tavoitteiden saavuttamiseksi EU:n komissio on syyskuussa 2018 laatinut ehdotuksen keskitetyn digitaalisen (kyber-) turvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen sekä kansallisten koordinointikeskusten verkoston perustamisesta[v]. Mikäli ehdotus hyväksytään, näiden toimielinten perustaminen tapahtuu 2021–2027 rahoituskaudella. Osaamiskeskusta ehdotetaan eurooppalaisena kumppanuutena, mikä helpottaisi unionin, jäsenvaltioiden ja/tai teollisuuden yhteisiä investointeja. Ehdotuksessa esitetään, että jäsenvaltiot osallistuvat osaamiskeskuksen ja verkoston toiminnan rahoitukseen unionin rahoitusosuutta vastaavalla määrällä.

Tulevaisuuden turvallisuus edellyttää, että unioni on suojattava paremmin kyberuhilta, sillä sekä siviili-infrastruktuurit että sotilaalliset valmiudet ovat riippuvaisia turvallisista digitaalisista järjestelmistä. Lähtötilanne on kuitenkin haastava, sillä digitaalisen turvallisuuden alueella 20 maailman johtavan maan joukossa on vain kuusi EU:n jäsenvaltiota.

Suomessa on runsaasti digitaalisen turvallisuusalan osaamista ja kokemusta. Mikäli pystyisimme muuntamaan tämän osaamisen markkinoitaviksi tuotteiksi ja ratkaisuiksi, voisimme kattaa merkittävän osan alan arvoketjusta. Tutkimus- ja teollisuusyhteisöjen toimet ovat kuitenkin hajanaisia, lyhytkestoisia ja epäyhtenäisiä ja niiltä

puuttuu yhteinen missio, mikä heikentää mahdollisuuksia menestyä kansainvälisillä markkinoilla. Pitkäaikaisten tutkimussuunnitelmien puute rajoittaa tällä hetkellä teollisten haasteiden ratkaisemista.

Myöskään digitaalisen turvallisuuden siviili- ja puolustusalojen välisiä synergioita ei toistaiseksi hyödynnetä täydessä mitassa. Kattavampi lähestymistapa mahdollistaisi digitaalisen turvallisuuden tukemisen koko arvoketjussa, tutkimuksesta aina keskeisten teknologioiden ja ratkaisujen käyttöönoton tukemiseen.

Digitaalisen turvallisuuden merkitys kasvaa vahvasti riskien ja uhkien kasvaessa. Sekä julkisella sektorilla että yrityksillä on kasvava tarve investoida kyberriskeihin varautumiseen. Forbes ennustaa, että pelkästään globaali tietoturvamarkkina kasvaa vuoden 2015 75 miljardista dollarista 170 miljardiin dollariin vuonna 2020[vi]. Esineiden internet, älykkäät autot ja yleinen ”elämän digitalisoituminen” ovat tärkeimmät kasvun moottorit. EU-alueella digitaalisen turvallisuuden markkinan kasvuksi ennustetaan noin 10 % vuosittain[vii]. Tietoturvapalvelut, uhkien älykäs tunnistaminen ja torjunta kasvavat kuitenkin huomattavasti keskiarvoa nopeammin.

Suomen digitaalisen turvallisuusalan yrityksistä[2] yli 60 % vie palveluita EU-alueelle ja noin kolmannes myös EU:n ulkopuolisiin maihin[viii] . Kokonaismarkkinan kasvu lisää myös suomalaisten yritysten liiketoimintamahdollisuuksia. Pk-sektorilla viennin suurimpana haasteena on kokonaisratkaisujen puuttuminen. Sen parantamiseksi tarvitaan enemmän yhteistyötä yritysten välillä. Lisäksi haasteena on osaajien puute ja yritykset joutuvatkin kouluttamaan osaajia esimerkiksi erilaisilla oppisopimusjärjestelyillä. Digitaalisen turvallisuuden huomioon ottaminen on myös tärkeä kilpailutekijä muiden teollisuudenalojen viennissä (valmistava teollisuus, terveysteknologia, finanssialan palvelut, jne.).

Valtioneuvoston raportti ”Kyberosaaminen Suomessa – nykytila ja tiekartta tulevaisuuteen”[ix] nosti esille puutteita Suomen kyberomavaraisuudessa. Digitaalisen turvallisuuden osaajien tarpeesta on olemassa erilaisia arvioita, mutta varovaisimmissakin arvioissa puhutaan kymmenien tuhansien uusien osaajien tarpeesta

2 Suomen tieto- ja kyberturva-alan yritysten järjestöön (Finnish Information Security Cluster, FISC) kuuluu noin 70 yritystä. Niiden yhteenlaskettu liikevaihto on yli 5 miljardia euroa ja ne työllistävät yli 28.000 henkilöä.

lähivuosina. ”Kyberturvallisuuden strateginen johtaminen Suomessa” -raportin[x] mukaan merkittävä osa tietoyhteiskunta-alan parissa tehtävästä huoltovarmuustyöstä koostuu yritysten jatkuvuudenhallinnan kehittämisestä. Varautumista yhteiskunnalle välttämättömien tietoteknisten järjestelmien ja rakenteiden toimivuuteen kyberuhka- ja häiriötilanteissa tuleekin tehostaa jo normaalioloissa.

Jotta digitaaliseen turvallisuuteen liittyvät mahdollisuudet pystytään hyödyntämään täysimääräisesti, tarvitaan systeemisiä, kaikki yhteiskunnan toimijat samaan suuntaan saattavia toimenpiteitä kansallisen digitaalisen turvallisuuden kasvun viitekehyksen luomiseksi ja toteuttamiseksi. Suomessa ei ole tällä hetkellä yhtenäistä kansallista puiteohjelmaa tai merkittävää hankekantaa digitaalisen turvallisuuden osaamisen systemaattiselle kehittämiselle tai alan liiketoiminnan kasvun mahdollistamiselle. Valmistelutyön tavoitteena olikin määritellä edellytykset ja tavoitteet laaja-alaiselle, digitaalisen turvallisuuden kasvumahdollisuudet haltuun ottavalle ohjelmatoiminnalle. Valmisteluhankkeen konkreettisina tavoitteina oli:

- luoda viitekehys sekä tarkempi tiekartta ja keskeiset toimenpide-ehdotukset kansalliselle digitaalisen turvallisuuden osaamisen ja liiketoiminnan kehittämiselle sekä
- tunnistaa ja sitouttaa keskeiset toimijat kansalliseen digitaalisen turvallisuuden kasvumahdollisuuksiin liittyvään ohjelmatoimintaan.

Toteutuessaan digitaalisen turvallisuuden koordinoitu ohjelmatoiminta:

- luo mahdollisuudet osaamisen kasvattamiselle,
- nostaa kansallista tietoisuutta digitaalisen turvallisuuden aiheista ja korostaa niiden roolia osana uutta, digitaalista yhteiskuntaa,
- tuo esille digitaalisen turvallisuuden osaamisen merkityksen kansallisena voimavarana ja uuden kasvun mahdollistajana,
- nostaa Suomen asemaa kokonaisvaltaisen digitaalisen turvallisuuden osaamisen edelläkävijämaana, sekä
- vahvistaa kansallista, systeemistä varautumista kyberuhkiin.

Digitaalisen turvallisuuden osaaminen edellyttää poikkitieteellisyyttä ja ohjelmatoiminnan rakentamista usean eri sidosryhmän yhteistyönä. Valmistelutyöhön tulee sitouttaa mukaan opetus- ja koulutusalan toimijat (yliopistot, ammattikorkeakoulut, peruskoulut, kansalaisjärjestöt, kunnat ja kaupungit), digitaalisen elinkeinoelämän keskeiset toimijat ja yhteistyöekosysteemit, yhteiskunnan kriittiseen infrastruktuuriin liittyvät toimijat (kaupungit, tietoliikenne, sähkönjakelu, sairaalat ja terveydenhuolto, puolustusministeriö) sekä digitaalisen turvallisuusalan yritykset ja toimijat.

Digitaalisen turvallisuuden kasvun tiekartan lähtökohtana on edistää toimialan yritysvetoista kehitystä, osaamisen kehittämistä, kyberresilienssiä sekä kansainvälistymistä ja kasvua. Lähestymistapana on ekosysteeminen ajattelu, jossa julkisen ja yksityisen sektorin sekä tutkimuslaitosten yhteisvoimin luodaan tavoitteiden saavuttamista tukeva systemaattinen toimintatapa. Tiekartassa luodaan alan yhteinen tavoitetila ja visio vuoteen 2030, kuvataan alan osaaminen ja toimintaympäristö, määritetään keskeiset toimenpiteet ja välitavoitteet lähivuosille sekä organisoidaan ohjelman edistymisen aktiivinen seuranta. Tiekartan valmistelu on ollut laaja-alaista ja avointa, työpajoissa tai muuten työssä mukana on ollut mukana lähes 150 eri henkilöä. Valmistelun aikana on järjestetty yhteensä kuusi työpajaa (aloitustilaisuus, neljä teematyöpajaa ja yhteenvetotilaisuus), muita tapaamisia ja haastatteluja sekä työskentelyä sähköisellä ryhmätyöalustalla eri alojen toimijoiden näkemysten kokoamiseksi.

Tiekartan valmistelutyössä digitaalisen turvallisuuden kokonaisuutta on lähestytty neljän teeman kautta, pyrkimyksenä muodostaa kokonaisvaltainen lähestyminen aihepiiriin. Teemat ovat **kyberresilienssi**, **osaaminen ja jatkuva oppiminen**, **elinkeinoelämän digitalisaatio** sekä **kasvu ja kansainvälistyminen**. Teemat esitellään tarkemmin ”Valmistelutyön teemat”-osiossa.

Nykytilanne: SWOT-analyysi

Valmistelutyön aikana järjestetyissä työpajoissa analysoitiin teemakohtaisten visioiden lisäksi myös nykytilannetta perinteisen SWOT-nelikentän (vahvuudet, heikkoudet, mahdollisuudet ja uhat) avulla. Tässä esitetty SWOT-analyysi on yhteenveto

työpajoissa kirjatuista näkemyksistä, joiden pohjalta myös keskeiset tavoitteet ja toimenpiteet on määritelty.

Vahvuudet

- Suomessa on **selkeä julkinen tahtotila** ja **avaintoimijoiden vahva sitoutuminen** digitaalisen turvallisuuden ja sen osaamisen kehittämiseksi kansalliseksi osaamisalueeksi.
- Suomessa on **hyvin toimiva ja turvallinen yhteiskunta ja luotettava infrastruktuuri** (energia, tietoliikenne, rahoituslaitokset, logistiikka, terveydenhuolto, koulutus, jne.).
- Suomi on **digitalisaation kärkimaa maailmassa**: meillä on useita digitaalisia tuotteita ja palveluita tarjoavia yrityksiä, erityisesti suuret yritykset panostavat digitalisaatioon ja keskeisiä julkisia palveluita on jo digitalisoitu (verotus, luvat, terveystiedot, jne.).
- Suomessa on **vahva tekninen osaamispohja** (koneenrakennus, automaatio, mobiiliteknologiat) ja korkea teknologian yleinen arvostus.
- Suomi on **kansainvälisesti tunnettu ja neutraali toimija**, jonka on mahdollista toimia välittäjän ja sillanrakentajan rooleissa.
- Suomessa on **yhteistyön kulttuuri** ja valmiina testattuja ja hyväksi havaittuja **yhteistoimintamalleja** erilaisten toimijoiden välillä (yhteishankkeet ja tutkimusyhteistyö).
- Suomessa on **aktiivisia digitaalisen turvallisuuden osaamisen verkostoja** (FISC ja PIA, startup-ekosysteemejä) sekä arvostettu ja joustava **regulaattori** (FICORA).

Heikkoudet

- Suomen **kotimarkkinat ovat pienet** ja monilla aloilla ei ole riittävää kriittistä massaa (asiakkaat, markkinat, yritykset, osaajat).
- **Alustatalouden** kehittyminen on Suomessa vasta alkuvaiheessa.

- Kansallisen **julkisen innovaatiorahoituksen määrä on liian alhainen** – viimeaikaiset lisäykset ovat oikeansuuntaisia, mutta määrältään riittämättömiä.
- Suomessa painotetaan **teknologialähtöistä lähestymistapaa**, jolloin muiden näkökulmien painoarvo jää liian pieneksi (mm. poikkitieteellisyys, markkinointi, sosiotekninen ajattelu, loppukäyttäjät).
- **Koulutettujen ohjelmisto-osaajien puute** – jopa alemman tason tutkinnon suorittaminen jää usein kesken, sillä ohjelmistoalan opiskelijat rekrytoidaan jo ensimmäisten opiskeluvuosien aikana.

Mahdollisuudet

- Uuden digitaalisen (kyber-) turvallisuusstrategian laadinnan yhteydessä Suomeen voidaan määritellä hallinnonalojen yli ulottuva **strategisen kyberjohtamisen malli** (vastuut, resursointi, rahoitus, jne.).
- **Julkisia hankintoja** voidaan hyödyntää paremmin uusien, innovatiivisten ratkaisujen kokeilemiseen, jolloin yritykset saavat arvokkaita asiakasreferenssejä.
- **Digitaalinen turvallisuus on uusi liiketoiminta-alue**, joka skaalautuu helposti digitaalisuuden ansiosta, joten pienenkin toimijan on mahdollista päästä merkittävään kansainväliseen rooliin (regulaatio, standardointi).
- Digitaalinen turvallisuus ja luottamus voidaan ottaa osaksi **Suomen maabrändiä** ja hyödyntää niitä kattavasti markkinoinnissa: suomalaiset yritykset ottavat digitaalisen turvallisuuden huomioon tuotteissaan ja palveluissaan. Kyberresilienssin alueella Suomi voisi erikoistua esimerkiksi kriisitilanteisiin ja kyberrikollisuuteen liittyvän tarkan tilannekuvan muodostamiseen, analysointiin ja jakamiseen. Myös kriisiajan toiminta- ja johtamismallien tuotteistaminen vientituotteeksi voitaisiin ottaa osaksi maabrändiä.
- Digitaalisen turvallisuuden kokonaisnäkemystä tukevan **opetusmateriaalin kehittäminen ja käyttöönotto** kaikilla

opetustasoilla (peruskoulu, ammatillinen koulutus, ammattikorkeakoulut, yliopistot, vapaaehtoistoiminta, reserviläistoiminta, järjestöt, jne.).

- **Professoreiden määrän lisääminen** digitaalisen turvallisuuden eri osa-alueilla nostaisi ja laajentaisi tieteellistä osaamista ja houkuttelisi kansainvälisiä yrityksiä investoimaan Suomeen.
- **Kansallisen ja kansainvälisen (EU, USA, Aasia) verkostoitumisen ja yhteistyön tukeminen** suuntaamalla tutkimusrahoitusta yritysten ja tutkimuslaitosten yhteisiin hankkeisiin.

Uhat

- Suuri osa suomalaisista **pk-yrityksistä** on vielä digitalisaation ulkopuolella – pääsevätkö ne mukaan vai jäävätkö ne lopullisesti kehityksen ulkopuolelle?
- **Hallitsematon globalisoituminen**, jonka seurauksena pienet toimijat marginalisoituvat. Ei-eurooppalaiset eettiset arvot normiutuvat ja erityisesti Kiinan käyttämä aggressiivisen taloudellisen vaikuttamisen malli yleistyy. Väärin ja liiallisesti käytettynä **ulkoistamisen kulttuuri** voi johtaa kansallisen osaamispohjan näivettymiseen.
- **Digi-infrastruktuurin siirtyminen ulkomaiseen omistukseen ja hallintaan**. Kansainvälisten pilvipalveluiden alustat ovat jo nyt osa Suomen kriittistä digitaalista infrastruktuuria ja niiden kyberresilienssin hallinta on ongelmallista. Toistaiseksi meillä ei ole uskottavia kotimaisia vaihtoehtoja, jotka pystyisivät tarjoamaan vastaavan palvelutason kilpailukykyisillä ehdoilla.
- **Kansainväliset investoinnit eivät kohdistu Suomeen**. Suomea ei koeta houkuttelevana opiskelu- tai asumispaikkana eikä hyvänä toimintaympäristönä yritystoiminnalle, joten tänne ei haluta myöskään perustaa yrityksiä. Ilman lisäpanostuksia Suomen kansainvälinen kilpailukyky alenee, uusiutumiskyky heikkenee ja riskinottokyky pienenee.

- **Kyberrikollisuus** on globaalia liiketoimintaa, joka leviää nopeasti helposti saatavilla olevien hyökkäystyökalujen ansiosta. **Hybridiuhat** (eli internetin ja digitaalisten työkalujen käyttäminen poliittisten vaikutusperien edistämiseen) yleistyvät ja verkottuvat.

Tavoitetila ja tulevaisuuskuva 2030

Suomen tavoitetilaa ja tulevaisuuskuvaa vuodelle 2030 työstettiin teemakohtaisissa työpajoissa. Niiden perusteella digitaalisen turvallisuuden tiekartan kokonaisvisioksi ehdotetaan: *"Maailman luotettavin digitaalinen liiketoiminta ja kattavin digitaalisen turvallisuuden osaaminen tulevat Suomesta"*. Teemakohtaiset visiot linkittyvät kokonaisvisioon kuvan 1 mukaisesti.

Kuva 1. Kokonaisvisio ja siihen liittyvät teemakohtaiset visiot.

Kyberresilienssi -teeman visiossa *Suomi tunnetaan yhtenä maailman kärkimaista digitaaliseen yhteiskuntaan kohdistuvien kriisien ja uhkien sieto- ja toipumiskyvyssä.* Tärkeimpinä tekijöinä tämän aseman saavuttamisessa ovat panostukset eri toimijoiden yhteistyöhön ja jatkuvaan oppimiseen, tilannetietoisuuden kehittämiseen ja jakamiseen sekä oikea-aikaiseen ja -tasoiseen johtamiseen. Säännölliset yhteistoimintaharjoitukset auttavat johtamismallien kehittämisessä ja omaksumisessa, ja saatuja kokemuksia hyödynnetään myös tavanomaisen operatiivisen toiminnan

kehittämisessä. Käytössä oleva yhteinen malli tilanne- ja uhkatietojen keräämiseen, analysointiin ja jakamiseen mahdollistaa nopean ja joustavan reagoinnin häiriötilanteissa. *Kriittisen digitaalisen infrastruktuurin suhteen Suomi on "selektiivisesti omavarainen" eli kansainvälisten alustapalveluiden tarjoajien rinnalla on tarjolla myös uskottavia ja kilpailukykyisiä kotimaisia toimijoita ja ratkaisuja.*

Osaaminen ja jatkuva oppiminen -teeman visiossa *Suomi on koulutuksen ja oppimisen mallimaa, jossa digitaalisen turvallisuuden peruskäsitteet ja kokonaisnäkemys omaksutaan jo nuorena ja osaamisen kehittymistä tuetaan jatkuvalla oppimisella läpi elämän.* Digitaalisen turvallisuuden ymmärtäminen on kansalaistaito ja -velvollisuus, ja siihen liittyvät opetuksen ja osaamisen kehittämisen periaatteet ja menetelmät on tunnustettu parhaiksi maailmassa. Kokonaisnäkemykseen sisältyvät teknisten taitojen ja osaamisen ohella myös esimerkiksi etiikka, psykologia, systeeminen ajattelu ja liiketoimintaosaaminen. Jokaisella asukkaalla on yhdenvertaiset mahdollisuudet digitaalisten taitojen hankkimiseen ja oman osaamisensa jatkuvaan kehittämiseen. Digitaalinen luottamus ja turvallisuus nähdään yleisesti tulevaisuuteen suuntaavina investointeina, kansakunnan tukijalkoina sekä keskeisinä viennin ja kansainvälisen yhteistyön mahdollistajina. Koulutuksen ja tutkimuksen rahoitukselle on löydetty kestävä malli, joka mahdollistaa pitkäjänteisen osaamisen kehittämisen.

Elinkeinoelämän digitalisaatio -teeman visiossa *Suomessa toimii digitaalisen turvallisuuden yritysvetoinen innovaatioekosysteemi, joka aktiivisesti edistää toimivan ja luotettavan data- ja tekoälypohjaisen yhteiskunnan ja elinkeinoelämän kehittymistä.* Vuonna 2030 Suomessa on data- ja tekoälypohjaisen elinkeinoelämän toimintaa ja menestystä tukeva laitekanta, infrastruktuuri, regulaatio ja lainsäädäntö. Suomi tunnetaan luottamusyhteiskuntana, jossa asioita edistetään ja kehitetään yhdessä ja rakentavasti myös kilpailijoiden kesken. Hyvän koulutusjärjestelmän osana meillä on korkeatasoista, digitalisaatioon ja turvallisuuteen liittyvää tutkimusta ja TKI-toimintaa, jota yritykset ja tutkimuslaitokset tekevät läheisessä yhteistyössä. Suuret yritykset ovat valmiita kokeilemaan pienten toimijoiden innovatiivisia ratkaisuja omassa toiminnassaan. Pienet yritykset hyötyvät suurten yritysten kanssa tehtävän yhteistyön kautta saatavista asiakasreferensseistä. Edelläkävijän asema koulutuksessa, tieteessä sekä teknologian alueilla ja datataloudessa on johtanut merkittävään kansainväliseen kasvuun ja lisännyt kasvuyritysten määrää Suomessa.

Kasvu ja kansainvälistyminen -teeman visiossa *digitaalinen luottamus ja turvallisuus ovat kiinteä osa Suomen maabrändiä, jota viedään maailmalle toimialakohtaisten liiketoimintaekosysteemien avulla yhteistyössä kansainvälisten yhteistyökumppanien kanssa.* Suomessa on digitaalisen turvallisuuden alueella useita liiketoimintaekosysteemejä, joiden avulla yritykset voivat toimia osana suurempaa yrityskonsortiota ja sen avulla ylittää tai kiertää kasvun ja kansainvälistymisen esteitä. Houkuttelevimmat ekosysteemien painopistealueet löytyvät esimerkiksi teollisen internetin kehitystarpeista sekä yksityisen sektorin palvelutarpeista.

Tämän raportin teemakohtaisissa osioissa kerrotaan tarkemmin niistä toimenpiteistä, joilla nykytilanteesta edetään kohti vuoden 2030 tavoitetilaa.

VUONNA 2030 DIGITAALISEN TURVALLISUUDEN TOIMIALA ON SUOMESSA:

- digitaalisen yhteiskunnan kriittisten alojen **häiriöttömän toiminnan suojaaja ja varmistaja**.
- **merkittävä kasvutoimiala**, jolla toimii useita vientiin ja kansainväliseen kasvuun tähtääviä yritysvetoisia liiketoiminta- ja innovaatioekosysteemejä.
- **dynaaminen toimintaympäristö** toimintaansa aloittaville ja kasvua hakeville yrityksille.
- **ennakkoluuloton edelläkävijämarkkina** uusien teknologioiden ja palveluiden pilotoinnissa sekä houkutteleva testialusta ja investointien kohde.
- **maabrändin tärkeä elementti**, joka houkuttelee kansainvälisiä yrityksiä investoimaan ja siirtämään investointejaan Suomeen.
- **monitieteellisen ja korkeatasoisen** tutkimuksen, koulutuksen, osaamisen ja innovaatioiden lähde ja hyödyntäjä.

Valmistelutyön teemat

Kyberresilienssi

Johdanto

Yhteiskunnan digitaalinen resilienssi (eli kriisitilanteiden sietokyky ja niistä toipuminen) koskettaa kaikkia: viranomaisia, kaikenkokoisia ja -tyyppisiä organisaatioita sekä jopa yksittäisiä kansalaisia. Digitalisoitunut yhteiskunta on riippuvainen katkeamattomasta energiansyötöstä, luotettavasta ja nopeasta tietoliikenteestä sekä ajan tasalla olevista, varmennetuista ja 365/24/7-käytettävissä olevista reaaliaikaisista tietovarannoista.

Lisääntyvän digitalisaation myötä yritysten tarjoamien ratkaisujen ja palveluiden arvoketjut pirstoutuvat edelleen ja muuttuvat aikaisempaa dynaamisemmiksi, kansainvälisemmiksi ja monimutkaisemmiksi. Uusien toiminta-alustojen, teknologioiden ja liiketoimintamallien käyttöönottoon liittyy kuitenkin merkittäviä luottamusoletuksia ja -haasteita. Esimerkiksi suurten kansainvälisten toimijoiden (Google, Amazon, Microsoft, jne.) tarjoamien globaalien ja suljettujen toiminta-alustojen häiriönsiedon hallinta ja varmistaminen voivat olla ongelmallisia suomalaisille yrityksille (miten alusta ottaa huomioon pienen kansallisen markkinan erityistarpeet? kuinka se priorisoi palvelinkeskusten kapasiteettia kansainvälisissä häiriötilanteissa?).

Uhkakuvien monimuotoisuus kasvaa. Kyberrikollisuus leviää nopeasti verkottuneen toiminnan ja digitaalisten hyökkäystyökalujen helpon saatavuuden myötä. Teollisuusvakoilu ja valtiollinen hyökkäystoiminta lisääntyvät samoista syistä. Nopeiden langattomien yhteyksien käytön lisääntymiseen liittyy merkittäviä häiriöihin,

häirintään ja käytön estoon liittyviä haasteita. Myös inhimilliset tekijät ovat vaikeasti hallittavissa oleva uhka.

Yhteiskunnan toiminnan kannalta kriittisen infrastruktuurin järjestelmissä yksittäisen kohteen lamautuminen tai vaurio ei saa lamauttaa koko järjestelmää. Kaikkein kriittisimmät järjestelmät ja tietovarannot on pyrittävä varmistamaan myös tilanteissa, joissa kansainväliset tietoliikenneyhteydet eivät ole käytössä. Infrastruktuurin toiminnan suojaamisen ja varmentamisen lisäksi on tärkeää varautua mahdollisten häiriö- ja pulatilanteiden aiheuttamiin poliittisiin reaktioihin ja muihin ääri-ilmiöihin. Sosiaalisen median kautta leviävät uudet uhkat, kuten valesivustot, vaihtoehtoiset uutiset ja uutislähteet, valeprofiilit ja muu peitetty kansalaismielipiteeseen vaikuttaminen nopeuttavat, kärjistävät ja vahvistavat äärimielipiteiden muodostumista ja leviämistä. Myös näihin uhkiin varautuminen ja niiden vaikutusten minimointi ovat olennainen osa digitaalisen yhteiskunnan toimintaedellytysten suunnittelua ja varmistamista. Valtioneuvosto on valmistellut uutta päätöstä huoltovarmuuden tavoitteista (ns. HUOVA-päätös) vuonna 2018 ja se tulee linjaamaan myös Huoltovarmuuskeskuksen toimintaa.

CGI:n kokoaman ”Kyberturvallisuuden tila suomalaisissa yrityksissä 2018”-raportin[xi] mukaan yritykset kokevat, että ne ovat varautuneet kyberuhkiin riittämättömästi. Tuloksissa ei ole havaittavissa merkittävää muutosta vuoteen 2016 verrattuna. Yrityksissä uhat tiedostetaan, mutta oma rooli koetaan usein sivustaseuraajaksi. Raportin mukaan suurimmat puutteet liittyvät johtamiseen, strategioihin ja investointeihin: vain noin puolella vastanneista yrityksistä oli erikseen nimetty tieto- tai kyberturvallisuusjohtaja tai -osasto, alle 40 prosenttia yrityksistä oli laatinut digitaalisen turvallisuuden strategian ja vain noin joka kolmas yritys ilmoitti tekevänsä merkittäviä investointeja tai parannuksia digitaaliseen turvallisuuteen. Kuitenkin lähes 90 prosenttia CGI:n tutkimukseen vastanneista koki yritykseensä kohdistuvien digitaalisten turvallisuusuhkien kasvaneen.

Haasteita: Kyberresilienssin ylläpitoon ja kehittämiseen liittyy olennaisena osana riittävän tarkan uhka- ja tilannekuvan muodostaminen ja sen jakaminen eri toimijoiden kesken. Tässä toiminnassa keskeisinä haasteina ovat mm. yritysten ja muiden toimijoiden haluttomuus paljastaa ongelmatilanteita esimerkiksi liiketoiminnallisiin syihin ja yrityssalaisuuksiin vedoten. Myös GDPR:n ja muun tietojen jakamiseen

liittyvän lainsäädännön tuomat rajoitteet sekä kansallisen tahtotilan ja selkeän vastuunjaon puuttuminen vaikeuttavat kattavan tilannekuvan muodostamista.

Eri toimijoiden riittävä kybertietoisuus ja -ymmärrys ovat välttämättömiä edellytyksiä tulokselliselle yhteistoiminnalle, mutta osaamisen tasoerot ovat suuria ja kehittämisaktiviteetit siiloutuneita. Uudet digitaaliset liiketoimintamallit, kuten esimerkiksi pilvipalvelut, voivat olla ongelmallisia, sillä niiden keskeiset teknologia- ja alustayhtiöt ovat globaaleja toimijoita, joita on vaikea saada muuttamaan toimintamallejaan yksittäisen maan vaatimusten ja tarpeiden perusteella. Tällä hetkellä Suomessa ei kuitenkaan ole riittävästi uskottavia kotimaisia toimijoita, jotka pystyisivät tarjoamaan vastaavan palvelutason kilpailukykyisillä ehdoilla.

Mahdollisuuksia: Suomessa on runsaasti digitaalisen yhteiskunnan turvallisuuden ja toimintakyvyn säilyttämiseen liittyvää systeemistä osaamista ja kokemusta. Viranomaiset on valmiuslaissa velvoitettu huolehtimaan poikkeustilanteisiin varautumisesta oman toimintansa osalta. Huoltovarmuuskeskuksella on lakiin perustuva tehtävä huoltovarmuuden turvaamiseen liittyvistä erityistoimenpiteistä. Lisäksi kriittisillä aloilla toimivilta yrityksiltä edellytetään toiminnan jatkuvuuden turvaamista ja varmistamista myös poikkeustilanteissa: digitaalisten palveluiden häiriöiden hallinta tulee voida toteuttaa normaaliajan prosesseilla ja toimintamalleilla.

Tämän osaamisen ja siihen liittyvien käytäntöjen ja toimintamallien (johtamismallit, uhkakuvan muodostaminen, analysointi ja jakaminen, viranomaisten ja yritysten yhteisharjoitukset, jne.) paketoiminen yhtenäiseksi kokonaisuudeksi tarjoaa merkittäviä mahdollisuuksia kansainväliseen resilienssiyhteistyöhön. Toisaalta, testattujen ja hyväksi havaittujen osaratkaisuiden tuotteistamisen kautta voidaan saada aikaan myös vientiä ja muuta kansainvälistä liiketoimintaa. Huoltovarmuuskeskuksella ja erityisesti sen digipoolilla on tässä merkittävä rooli. Resilienssitoimijoiden aktiivinen yhteydenpito asiakasyritysten kanssa tuo myös esille tarpeita, jotka voivat parhaimmillaan toimia ponnahduslautana uusille kasvuyrityksille.

Digitaalisen yhteiskunnan toiminnan suojaamiseen ja varmistamiseen liittyvistä ratkaisuista ja palveluista on mahdollista rakentaa Suomeen merkittävä liiketoiminta-alue sekä voimakkaasti kasvava vientiala. Suomeen voidaan myös muodostaa

eri alueita ja erilaisia toimijoita yhdistävä ja kaikki olennaiset osa-alueet kattava, aktiivinen ja toimintakykyinen **kyberresilienssin ekosysteemi,** jolla on valmiutta ja halukkuutta viedä tiekartan toteutusta eteenpäin.

Teemakohtainen visio 2030

VUONNA 2030 SUOMI TUNNETAAN YHTENÄ MAAILMAN KÄRKIMAISTA DIGITAALISEEN YHTEISKUNTAAN KOHDISTUVIEN UHKIEN SIETO- JA TOIPUMISKYVYSSÄ.

Mitä tämä edellyttää? Suomessa panostetaan eri toimijoiden (yritysten, viranomaisten, järjestöjen, kansalaisten, jne.) jatkuvaan oppimiseen, tilannetietoisuuden kehittämiseen ja jakamiseen sekä oikea-aikaiseen ja -tasoiseen johtamiseen. Osaamista ja tilannetietoutta kehitetään jatkuvasti, ”security and sustainability by design” -periaate on omaksuttu kaikilla tahoilla ja saatuja kokemuksia hyödynnetään aktiivisesti myös yritysten tavanomaisen, operatiivisen toiminnan kehittämisessä. Säännölliset, ohjatut yhteisharjoitukset auttavat johtamismallien kehittämisessä ja omaksumisessa.

Tilanne- ja uhkatietojen keräämiseen ja analysointiin on käytössä yhteinen, myös uudet uhkakuvat kattava malli. Vuonna 2030 suuret, globaalit ICT-toimijat muodostavat edelleen merkittävän osan Suomen kriittisestä digitaalisesta infrastruktuurista, mutta niiden rinnalla on tarjolla myös uskottavia ja kilpailukykyisiä kotimaisia toimijoita ja ratkaisuja. Kansainvälisten toimijoiden rooli ja kansainvälinen lainsäädäntö otetaan huomioon tilannetiedon muodostamisessa ja jakamisessa. Kriittisen digitaalisen infrastruktuurin suojaamisen ja turvaamisen lisäksi tilannetietoa hyödynnetään myös kolmansien osapuolten häiriötilanteiden hallinnassa.

Keskeiset tavoitteet vuosille 2021, 2025 ja 2030

Välitavoitteet 2021

- Määritelty yhteinen **tilanne- ja uhkatietojen rakenteellinen tietomalli**, analysointiprosessi, jakeluperiaatteet sekä kansallinen tietoturvarikkomusten käsittelyprosessi.
- Poikkeustilanteiden **harjoitustoimintaa on systematisoitu ja laajennettu** kattamaan kaikki olennaiset teollisuudenalat.
- **Oikeantasoisella regulaatiolla** on määritelty ja varmistettu eri toimijoiden (julkiset organisaatiot, yritykset, jne.) kyberresilienssille minimi- ja tavoitetasot.
- **Julkisiin hankintoihin** on määritelty kyberresilienssiin liittyvät perusvaatimukset.
- Yritysvetoisen **kyberresilienssiekosysteemin** toiminta on käynnistynyt.
- **Kyberresilienssiyhteistyön** vientimahdollisuuksien kartoittaminen on käynnistetty.

Välitavoitteet 2025

- Kaikki keskeiset kansalliset toimijat ja toimialat ovat ottaneet käyttöön yhteisen **tilanne- ja uhkatiedon tietokannan, tietojen jakamisen mallin ja käsittelyprosessin, jotka ovat yhteensopivia EU:n säännösten ja direktiivien kanssa.**
- Poikkeustilanteiden **harjoitustoiminnan tuotteistaminen** on saatu valmiiksi.
- Keskeisten digitaalisten liiketoiminta-alustojen tarjoajilla on käytössään **toimintamalli**, joka on yhteensopiva Suomen resilienssivaatimusten kanssa.
- Kyberhyökkäyksiin liittyvien **aineellisten ja muiden vahinkojen määrä** on kasvanut Suomessa selvästi verrokkimaita hitaammin.
- **Julkisista hankinnoista** on muodostunut merkittävä tekijä kyberalan uusien teknologioiden ja innovatiivisten ratkaisujen kehittämisessä ja käyttöönotossa.

- **Kyberresilienssiekosysteemin** toimijat välittävät ennakoivasti ja aktiivisesti tietoa tarpeistaan, innovatiivisista ratkaisuista ja uusista kyvykkyyksistä.
- **Kansainvälinen kyberresilienssiyhteistyö** on käynnistetty ensimmäisten kumppanien kanssa.

Tavoitteet 2030

- Digitaalisen yhteiskunnan toiminnan suojaamiseen ja varmistamiseen liittyvät ratkaisut ja palvelut ovat Suomessa **merkittävä liiketoiminta-alue** sekä **voimakkaasti kasvava vientiala**.
- **Kansainväliset yritykset** ovat siirtäneet keskeisiä toimintojaan Suomeen turvallisen, stabiilin ja toimintavarman yhteiskunnan ja toimintaympäristön houkuttelemina.
- Kyberhyökkäyksiin liittyvien **aineellisten ja muiden vahinkojen määrä** on Suomessa kääntynyt selvään laskuun.
- Suomi on kokoaan suurempi toimija **kyberrauhanturvaajana**. Suomalaiset viranomaiset kouluttavat kriisitilanteiden kokonaisturvallisuuden toimintamallia myös ulkomailla.

Ehdotukset mittareiksi ja KPI:ksi

- Ohjelmatoimintaan valittavat kehityshankkeet: projektointi ja toteutuksen seuranta
- Yhteiskunnan toiminnan suojaamisen ja varmistamisen mittarit (esim. kyberhyökkäyksiin liittyvät vahingot, uhkien tunnistamisaika, toipumisaika, jne.)
- Kansainvälisen yhteistyön kehittyminen

Keinovalikoima

- Kansallisen kyberturvallisuusstrategian tehokas toteuttaminen
- Kansallinen kampanja verkkosivustojen haavoittuvuuksien siivoamiseksi ja poistamiseksi (esimerkiksi www.hackr.fi)

- Digitaaliseen turvallisuuteen keskittynyt julkinen palvelu tai jaettu tietokanta (+ API:t), jota yritykset voivat käyttää
- Havainnollinen ja kansantajuinen ohjeistus kyberuhkien tunnistamiseksi ja arvioimiseksi sekä yleisen tilannekuvan rakentamiseksi
- Yritysten, palveluntuottajien ja media-alan toimijoiden kyberresilienssin auditointi- ja sertifiointiohjelma

Osaaminen ja jatkuva oppiminen

Johdanto

Nykyaikainen yhteiskunta on yhä riippuvaisempi digitaalisista ratkaisuista, kun kasvavaa osaa sen jokapäiväisistä ja kriittisistä toiminnoista tuotetaan ja ohjataan tietoverkkojen avulla. Viranomaisten ja yritysten lisäksi myös yksittäiset kansalaiset käyttävät digitaalisia palveluja päivittäin. Digitaalisessa toimintaympäristössä turvallisuus ja luottamus määräytyvät kaikkien toimijoiden yhteisvaikutuksesta. Kattavaa digitaalista turvallisuutta ei saavuteta ilman palveluiden kehittäjien, tuottajien ja käyttäjien – työntekijöiden ja yksittäisten kansalaisten – vahvaa kyberalan perusosaamista, joka kattaa yksityisen ja julkisen sektorin keskeiset tarpeet. Teknisen digitaalisen turvallisuuden osaamisen kehittäminen on tärkeä osa-alue, mutta se ei ole yksin riittävä. Digitaaliset taidot ja käsitteet kokonaisvaltaisesti osaavat ja ymmärtävät kansalaiset ovat olennainen osa nykyaikaista hyvinvointiyhteiskuntaa. Samalla tuo osaamispohja luo myös kestävän alustan, jonka avulla voidaan rakentaa yhä laajempaa ja syvempää digitaalista luottamusta.

Digitaalisen turvallisuuden tiekartta tarjoaa mahdollisuuden tukea koulutuspolitiikasta päättäviä tahoja digitaaliseen turvallisuuteen liittyvien taitojen kehittämisessä (esim. digitaalisen turvallisuuden opetussuunnitelma ja tutkinnot, alan kansalaisportaali, jne.). Lisäksi sen puitteissa voidaan kehittää alalle koordinoidusti ajantasaista perus-, jatko- ja täydennyskoulutusmateriaalia. Osaavan työvoiman saatavuus on olennainen voimavara alan toimijoille (viranomaiset, järjestöt, yritykset, yliopistot, korkeakoulut, tutkimuslaitokset) sekä muille digitaalisen turvallisuuden kanssa tekemisissä oleville teollisuudenaloille.

Koulutuksen rooli kansallisissa digitaalisen turvallisuuden strategioissa: Useissa kansallisissa strategioissa koulutus ja sen kehittäminen on nähty tärkeäksi tekijäksi (ks. tarkemmin liite 1). Euroopan maista erityisesti Alankomaat, Itävalta ja Ranska ovat asettaneet strategioissaan yksityiskohtaisia, koulutukseen liittyviä tavoitteita. Euroopan ulkopuolella aktiivisia koulutuksen kehittäjiä ovat Australia ja Yhdysvallat.

Edellä mainituissa strategioissa mainitaan usein koulutuksen merkitys kaikilla koulutusasteilla. Alankomaat on tehnyt konkreettisen päätöksen siitä, että kyberturvallisuuden koulutusta sisällytetään peruskoulun opetusohjelmaan jo lähivuosina. Itävalta ja Ranska ovat tunnistaneet hyvin tarkasti kyberturvallisuuden koulutukseen liittyviä tasoja ja näissä maissa digitaalinen turvallisuus nähdään koko yhteiskuntaa tukevana kompetenssina. Yhteistä edellä mainituissa esimerkeissä on myös voimakas yhteiskunnallinen tuki esim. opetusministeriön taholta. Australia luottaa digitaalisen turvallisuuden osaamisen kehittämisessä keskitettyihin osaamiskeskuksiin. Yhdysvaltojen tavoite on lähinnä lisätä työvoimaa kompetenssisiirroilla eri toimijoiden välillä.

ESIMERKKI: KANSALLINEN DIGITAALISEN TURVALLISUUDEN OSAAMISEN OPPIMATERIAALI JA OPPIMISYMPÄRISTÖ

Luodaan kansalliseen käyttöön **skaalautuva oppimisympäristö** (esim. Moodle, Eliademy, Canvas, tms.), joka sisältää **opetusmateriaalin**, **tehtävät** ja **toimintaohjeet**. Oppimisympäristöön on integroitu pedagoginen malli, jonka avulla opetusta voidaan skaalata oppimistavoitteiden ja koulutettavan ryhmän mukaan.

Opetettava asiakokonaisuus jaetaan osiin, joissa on teorian lisäksi myös harjoituksia ja tehtäviä. Opiskelumateriaalina käytetään monipuolisesti ja vaihtelevasti videoita ja luettavaa materiaalia. Tehtävät ovat erityyppisiä: monivalintatehtäviä, kirjoitelmia, laboratorioharjoituksia, pelejä (esim. Kahoot) tai oppitunneilla tehtäviä harjoituksia. Järjestelmään luodaan useita vaihtoehtoisia tapoja sisältöjen oppimisen tueksi. Kysymykset ja tehtävät ovat monivalinta-, tunnistus-, raahaus- tai siirtotehtäviä ruudulla – tai jopa pieniä, pelin kaltaisia, oivallusta vaativia tehtäviä. Opettaja tai ohjaaja valitsee tehtävät (henkilökohtaisen) oppimistavoitteen perusteella.

Opetusmateriaalin kielinä ovat ainakin **suomi ja ruotsi**, joten alan keskeiselle sanastolle on kehitettävä myös kotimaiset vastineet. Turvallisuuskomitean alaisuudessa terminologiatyötä onkin jo aloitettu.

Haasteita: Digitaaliseen turvallisuuteen liittyvä tieto kehittyy jatkuvasti ja nopeasti. Opetusmateriaalin ja -menetelmien on kehityttävä samaa vauhtia, jotta niiden avulla luotava osaaminen olisi hyödyllistä, mielekästä ja ajan tasalla olevaa. Tämä asettaa erittäin kovat vaatimukset opetusalustalle, sillä sen on tuettava dynaamisesti päivittyvän digitaalisen oppimateriaalin käyttöä. Sen on myös tuettava erilaisia oppimistapoja ja oppimisen eri tasoja (ks. liite 1). Myös opettajien, kouluttajien, valmentajien ja ohjaajien sisällölliseen ja menetelmälliseen kouluttamiseen sekä heidän osaamisensa ylläpitämiseen ja kehittämiseen on panostettava merkittävästi ja pitkäjänteisesti. Tuoreimpien Pisa-tulosten perusteella koulutukseen kohdistuvat säästötoimet ja väärin mitoitetut tai joustamattomat opetussuunnitelmat vaikuttavat nopeasti yleisen osaamispohjan kehittymiseen.

Digitaalinen turvallisuus ja siihen liittyvät aiheet ovat monimutkaisia käsitteitä. Niihin liittyvät termit ja konseptit ovat pääosin teknisiä ja edellyttävät usein hyviä taustatietoja ja asioiden perusteellista ymmärtämistä. Kattavan osaamispohjan luomiseksi digitaalinen turvallisuus olisi kuitenkin saatava osaksi normaalia toimintaa selvällä ja ymmärrettävällä kielellä ja ajantasaisella tiedolla.

Mahdollisuuksia: Koulutusjärjestelmämme on arvioitu ja arvostettu kansainvälisesti korkealle tasolle perinteisten aineiden opetuksessa. Hyvä menestyksemme on rakentunut hyvin laadittujen opetussuunnitelmien ja korkeasti koulutettujen opettajien varaan. Näitä samoja tekijöitä voidaan hyödyntää myös digitaalisen turvallisuuden ja kyberosaamisen opettamisessa.

Kaikki opetustasot ja koulutussuunnat kattavan opetussuunnitelman lisäksi tarvitsemme digitaalisen turvallisuuden kokonaisnäkemystä ja kansallisia toimintamalleja tukevan opetusmateriaalin sekä sen käyttöä tukevan digitaalisen, skaalautuvan oppimisympäristön. Oppimateriaaliin tuotetaan ja tuodaan digitaalista sisältöä eri lähteistä. Oppimisympäristön käyttö mahdollistaa opetuksen ja materiaalien joustavan jakamisen osaamistavoitteiden mukaisesti.

Opettajan, kouluttajien, valmentajien ja ohjaajien sisällöllinen ja pedagoginen koulutus voidaan toteuttaa ns. ”*train-the-trainer*” -mallilla, jossa opettajia koulutetaan mentoreiksi, jotka jakavat osaamistaan eteenpäin.

Monipuolinen ja korkeatasoinen digitaalisen turvallisuuden koulutustarjonta tukee hyvin nykyistä korkeatasoista insinöörikoulutustamme. Sen lisäksi tarvitaan poikkitieteellistä (kotimaista ja kansainvälistä) tutkimusyhteistyötä yrityksien ja tutkimuslaitosten kanssa sekä lisää professoreita digitaalisen turvallisuuden eri osa-alueille.

Teemakohtainen visio 2030

VUONNA 2030 SUOMI ON KOULUTUKSEN JA OPPIMISEN MALLIMAA, JOSSA DIGITAALISEN TURVALLISUUDEN PERUSKÄSITTEET JA KOKONAISNÄKEMYS OMAKSUTAAN JO NUORENA JA OSAAMISEN KEHITTYMISTÄ TUETAAN JATKUVALLA OPPIMISELLA LÄPI ELÄMÄN.

Mitä tämä edellyttää? Vuonna 2030 lähes kaikki Suomessa asuvat ihmiset osaavat toimia turvallisesti ja vastuullisesti digitaalisessa maailmassa. Digitaalisen turvallisuuden ymmärtäminen on kansalaistaito ja -velvollisuus, ja siihen liittyvät opetuksen ja osaamisen kehittämisen periaatteet ja menetelmät on tunnustettu parhaiksi maailmassa. Näiden taitojen oppiminen aloitetaan jo peruskoulussa, ja niitä kehitetään ja syvennetään ylemmän tason koulutuksen, työelämän sekä henkilökohtaisten oppimisratkaisujen avulla. Digitaalisen turvallisuuden kokonaisnäkemykseen sisältyvät teknisten taitojen ja osaamisen ohella myös esimerkiksi etiikka, psykologia, systeeminen ajattelu ja liiketoimintaosaaminen. Suomessa jokaisella asukkaalla on yhdenvertaiset mahdollisuudet digitaalisten taitojen hankkimiseen ja oman osaamisensa jatkuvaan kehittämiseen.

Poliitikoiden, viranomaisten, yritysten ja kansalaisten piirissä digitaalinen luottamus ja turvallisuus nähdään yleisesti tulevaisuuteen suuntaavana investointina, kansakunnan tukijalkana sekä keskeisenä viennin ja kansainvälisen yhteistyön mahdollistajana. Koulutuksen ja tutkimuksen rahoitukselle on löydetty kestävä malli, joka mahdollistaa pitkäjänteisen osaamisen kehittämisen.

Suomessa toimivat kotimaiset ja kansainväliset yritykset hyötyvät täällä tarjolla olevasta, digitaaliseen osaamiseen liittyvästä laajasta ja korkealaatuisesta

osaamispohjasta. Suomalaiset yritykset, tutkimuslaitokset, yliopistot ja korkeakoulut ovat haluttuja kumppaneita kansainvälisten tutkimushankkeiden konsortioihin.

Keskeiset tavoitteet vuosille 2021, 2025 ja 2030

Välitavoitteet 2021

- **Digitaalisten kansalaistaitojen nykytilanne** on kartoitettu laaja-alaisesti ja sen jatkuvalle mittaamiselle on kehitetty systemaattinen prosessi.
- Digitaalisen turvallisuuden kaikki opetuksen tasot kattava **opetussuunnitelma on valmis**.
- **Digitaalisen oppimisalustan** ensimmäistä versiota on jo kokeiltu. Alustan jatkokehittämisestä on tehty päätös.
- Digitaalisen turvallisuuden ja kyberosaamisen **oppimateriaalista** on valmiina ensimmäiset versiot kaikille opetuksen tasoille ja opettajien (täydennys)koulutus on käynnistetty.
- Digitaalisen turvallisuuden **kansalaisportaalin** kokeiluversio on testikäytössä. Portaali sisältää ajan tasalla olevaa materiaalia mm. jokamiehen digitaalisista oikeuksista ja velvollisuuksista.
- Kansallista tutkimusta tuetaan vahvistamalla yliopistojen tutkimusryhmiä ja kannustamalla niitä yhteistyöhön yritysten kanssa.

Välitavoitteet 2025

- Mittausten perusteella kehitetty **kansalaistaitojen osaamisindeksi** osoittaa yleisen osaamistason nousua.
- **Opetussuunnitelma on otettu käyttöön** kaikilla opetusasteilla.
- **Oppimisalusta on laajamittaisessa käytössä**.
- Opetussuunnitelman mukaiset **oppimateriaalit ovat käytössä** kaikilla opetusasteilla. Lisäksi on tuotettu räätälöityä koulutusmateriaalia erikseen valituille kohderyhmille (esimerkiksi työttömät, aikuiset, vanhukset, maahanmuuttajat, jne.).

- **Kansalaisportaali on laajamittaisessa käytössä** ja myös yksittäiset kansalaiset tuottavat sinne korkeatasoista sisältöä.
- Kansainvälisten vertailujen mukaan digitaalisen turvallisuuden ja kyberalan **tutkimuksen taso on noussut** Suomessa. Yritysten kanssa tehty tutkimusyhteistyö on tuottanut tieteellisesti ja liiketaloudellisesti merkittäviä tuloksia.

Tavoitteet 2030

- Suomi on kouluttanut **uuden sukupolven digitaalisia moniosaajia**, jotka määrittelevät, kehittävät ja soveltavat digitaalisen turvallisuuden menetelmiä ja työkaluja monipuolisesti ja tehokkaasti eri osa-alueilla.
- Kansalaistaitojen osaamisindeksiä vastaavia mittauksia on otettu käyttöön myös muissa maissa. Suomi on verrokkiryhmässään paras.
- Kansainvälisissä vertailuissa Suomi on kärjessä digitaalisten taitojen opetuksessa ja oppimistuloksissa.
- Suomessa on saavutettu ainakin **yksi kansainvälinen läpimurto** digitaalisen turvallisuuden ja kyberalan tutkimuksessa.

Ehdotukset mittareiksi ja KPI:ksi

- Digitaalisen oppimisalustan käyttöaste ja sen kurssisisällön kattavuus
- Digitaalisen turvallisuuden kansalaisportaalin käyttöaste ja sen sisällön kattavuus
- Uusien digitaalisen turvallisuuden alan professorien ja tutkimusryhmien määrä
- Tärkeimpien tutkimusryhmien koko ja tieteellinen taso
- Kansalaistaitojen osaamisen ja omaksumisen indeksi

Keinovalikoima

- Kansalaistaitojen ja kansalaisten osaamisen kartoittaminen, osaamisindeksi

- Opetussuunnitelma, oppimateriaalit ja niitä tukeva digitaalinen oppimisalusta
- Kyberalan valmentajien pedagoginen koulutus
- Suomen- ja ruotsinkielisen termistön ja määritelmien luominen
- Uusien professuurien ja tutkimusryhmien perustaminen
- Tutkimusryhmien kriittisen massan varmistaminen, tutkimusrahoituksen ja tohtoriopiskelijoiden rahoituksen vahvistaminen

Elinkeinoelämän digitalisaatio

Johdanto

Elinkeinoelämän digitalisaatio -teeman osalta keskeistä on, kuinka digitaalinen turvallisuus saadaan nykyistä vahvemmin myös muiden kuin varsinaisten alan yritysten liiketoimintaan innovaation ja kasvun lähteeksi.

Digitaaliseen turvallisuuteen liittyviä palveluita ja ratkaisuja tarjoavien yritysten määrä on Suomessa maan kokoon suhteutettuna suuri – alan yhteistoimintaorganisaatiossa (FISC, Finnish Information Security Cluster) on jäseniä lähes 70. Tämän teeman kannalta merkittävämmässä roolissa ovat ne yritykset, joiden varsinainen liiketoiminta on digitaalisen turvallisuusalan ulkopuolella, mutta joiden toimintaan digitaalinen turvallisuus ja erityisesti siihen liittyvät häiriöt vaikuttavat merkittävästi. Tällaisia aloja ovat esimerkiksi tietoliikenne, energian tuotanto ja jakelu, finanssi- ja vakuutusala ja terveydenhuolto. Yritysten varautuminen digitaalisen turvallisuuden uhkiin koetaan kuitenkin riittämättömäksi ja uusien haasteiden ymmärtäminen vaatii toimialakohtaista osaamista.

Haasteita: Eräänä keskeisenä uhkakuvana nähdään ulkoistamisen kulttuuri, sillä sen seurauksena kansallinen osaamispohja kapenee ja näivettyy. Pitemmällä tähtäimellä tämä voi johtaa kokonaisten toimialojen marginalisoitumiseen tai jopa katoamiseen Suomesta osaamis- ja osaajapulan vuoksi. Myös kasvava riippuvuus globaaleista digitaalisen infrastruktuurin toimijoista koetaan ongelmaksi, erityisesti silloin, kun kriittistä kansallista digi-infrastruktuuria siirtyy ulkomaiseen omistukseen.

Yritysten kokemusten mukaan liian tiukka ja hajanainen regulaatio ja säädösten joustamaton soveltaminen hankaloittavat innovointia ja uusien ratkaisujen pilotointia. Yritykset kokevat, että Suomi integroituu muihin EU-maihin verrattuna liian aikaisin sääntelyn piiriin. Kansallisella tasolla julkinen TKI-rahoitus keskittyy liikaa valmistelutyöhön, jolloin tulosten jalkauttaminen jää tekemättä. Lisäksi julkista TKI-rahoitusta on leikattu eikä jatkuvuutta ja ketterää kehitystyötä edistäneelle ICT/SHOK-rahoitusmallille ole vielä kehitetty korvaavaa instrumenttia.

Elinkeinoelämän digitalisaatio ei etene Suomessa tasaisesti, sillä noin 60 % pienistä ja keskisuurista yrityksistä ei ole edes käynnistänyt toimintansa digitalisoimista. Lisäksi yritysten tietojärjestelmien kehittämistä hidastavat käytössä olevien järjestelmien jäykkyys ja suljetut rajapinnat, mikä heikentää yritysten kykyä innovoida ja ottaa käyttöön uusia digitaalisia ratkaisuja. Digitaalisten järjestelmien auditoinnin ja sertifioinnin puute nähdään myös merkittävänä haittatekijänä. Digitaalisen turvallisuuden alalla yritysten ja tutkimuslaitosten välinen yhteistyö on vähäistä. Yritysten yhteistoiminnassa luottamus ja yhteistyö ovat keskeisessä asemassa, joten jos luonteva vuorovaikutus vähenee, siitä voi aiheutua ongelmia esimerkiksi datan jakamisessa ja hyödyntämisessä.

Mahdollisuuksia: Suomessa on vahva ja laaja teknisen digitalisaation osaamispohja ja lisäksi koulutusjärjestelmämme on maailman kärjessä. Yritysten ja tutkimuslaitosten välinen esikilpailullinen yhteistyö on perinteisesti ollut läheistä ja tiivistä jopa markkinoilla keskenään kilpailevien yritysten kesken. Tällaisia hankkeita on käynnistetty esimerkiksi standardoinnin, pilotoinnin, tutkimuksen ja ekosysteemien ympärille. Myös digitaalisen turvallisuuden ohjelmatoiminnan valmistelutyötä voidaan tehdä yhdessä suurenkin toimijajoukon kanssa. Asiakastarpeita, palvelunkehitystä ja huippuosaamista yhdistelemällä voidaan synnyttää poikkileikkaavia innovatiivisia kokonaisuuksia. Tällä hetkellä digitaalinen turvallisuus on liiketoiminnassa usein irrallinen komponentti, joka pyritään integroimaan jälkikäteen mukaan.

Suomeen kannattaisi muodostaa eri yrityksiä, tutkimuslaitoksia ja julkisen hallinnon toimijoita yhdistävä ja kaikki olennaiset osa-alueet kattava, aktiivinen ja toimintakykyinen digitaalisen turvallisuuden yritysvetoinen ekosysteemi, jolla on valmiutta ja halukkuutta viedä eteenpäin yhteistoiminnan kautta ohjelmatoiminnan valmistelua ja toteutusta TKI-toiminnan alueella. Tällaisen innovaatioekosysteemin synnyttäminen mahdollistaisi olemassa olevien huippuideoiden ja -toimijoiden löytämisen,

monitieteellisen osaamisen ja koulutuksen tehokkaamman hyödyntämisen sekä motivaation kasvattamisen. Yritysten kasvun ja kansainvälistymisen tueksi tarvitaan joustavia rahoitusmalleja (pääomittaminen, kasvuyritysten hautomot ja kiihdyttämöt, jne.) sekä kokeilukulttuurin tehokkaampaa hyödyntämistä. Kansallisen kyberalueen testipenkin luominen tukisi TKI-toimintaa ja kannustaisi toimijoita yhteistoimintaan.

Digitaalinen turvallisuus tulisi kytkeä paremmin muihin käynnissä oleviin hankkeisiin, kuten esimerkiksi tekoälyohjelmaan. Julkisella sektorilla esimerkiksi Turvallisuuskomitean ylläpitämä Kyberverstas -toimintamalli kokoaa ansiokkaasti eri toimijoita yhteen, mutta sen verkostossa yrityselämän edustus on vielä vähäistä, poikkeuksena kyberturvayritykset.

Suomen maabrändiä pitäisi vahvistaa liittämällä osaksi sitä digitaalisen turvallisuuden elementti ("*puhdas, turvallinen ja vakaa toimintaympäristö, kaikki toimii, kukaan ei pelkää, kukaan ei eksy*"). Suomalaisten yritysten digitaalisen turvallisuuden ratkaisut tunnetaan siitä, että ne palvelevat koko yhteiskuntaa ja poikkeavat siten esimerkiksi Kiinan ja USA:n itsekkäistä ja protektionistisista toimintatavoista. Suomi voisi myös toimia EU-markkinoiden pilottialueena, myyntivaltteinaan turvallisuus, luottamus ja eettisyys.

Teemakohtainen visio 2030

SUOMESSA TOIMII DIGITAALISEN TURVALLISUUDEN YRITYSVETOINEN INNOVAATIOEKOSYSTEEMI, JOKA AKTIIVISESTI EDISTÄÄ TOIMIVAN JA LUOTETTAVAN DATA- JA TEKOÄLYPOHJAISEN YHTEISKUNNAN JA ELINKEINOELÄMÄN KEHITTYMISTÄ.

Mitä tämä edellyttää? Vuonna Suomessa on 2030 data- ja tekoälypohjaisen elinkeinoelämän toimintaa ja menestystä tukeva laitekanta, infrastruktuuri, regulointi ja lainsäädäntö. Suomi tunnetaan luottamusyhteiskuntana, jossa asioita edistetään ja kehitetään yhdessä ja rakentavasti myös kilpailijoiden kesken. Hyvän

koulutusjärjestelmän osana meillä on korkeatasoista, digitalisaatioon ja turvallisuuteen liittyvää tutkimusta ja TKI-toimintaa.

Suurilla suomalaisilla yrityksillä on kyky ja halu kokeilla ja soveltaa pienten toimijoiden ja startup-yritysten innovatiivisia teknologioita ja ratkaisuja omassa toiminnassaan, ja ne suuntautuvat aktiivisesti kansainvälisille markkinoille. Pienet yritykset hyötyvät suurten yritysten kanssa tehtävän yhteistyön ansiosta saatavista asiakasreferensseistä. Kansainväliset yritykset panostavat yhteistyöhön Suomen ja suomalaisten yritysten ja tutkimuslaitosten kanssa.

Suomen elinkeinoelämä on hyötynyt osaamispohjan kokonaisvaltaisesta kasvamisesta digitalisaation ja digitaalisen turvallisuuden alueilla sekä viisaasta regulaation ja sääntelyn mukauttamisesta uusien palveluiden mahdollistamiseksi. Tätä on edistänyt tehokas elinkeinoelämän ja tutkimuslaitosten yhteistyö TKI-toiminnassa. Suomi on tehnyt tärkeitä sovellusaluevalintoja, jotka ovat johtaneet merkittäviin läpimurtoihin. Edelläkävijyys koulutuksessa, tieteessä sekä teknologian alueilla ja datataloudessa on johtanut merkittävään kansainväliseen kasvuun ja lisännyt kasvuyritysten määrää Suomessa.

Keskeiset tavoitteet vuosille 2021, 2025 ja 2030

Välitavoitteet 2021

- **Digitaalisen turvallisuuden tiekartan ja ohjelmatoiminnan ohjausryhmän** toiminta on jo vakiintunut. Ohjausryhmä tukee tämän alueen strategista kehittämistä toimimalla eri ministeriöitä ja muita toimijoita yhdistävänä koordinaattorina.
- **Digitaalisen turvallisuuden innovaatioekosysteemin** puitteissa on laaja sitoutuminen yhteiseen tiekarttaan, yhteisiin tavoitteisiin ja keinoihin, joilla tavoitteisiin päästään.
- **Innovaatiotoiminnan julkisen rahoituksen instrumentit** ovat aktiivisessa käytössä ja ne vauhdittavat yritysten ja tutkimuslaitosten monivuotisia, esikilpailullisia yhteishankkeita ja TKI-ohjelmia myös digitaalisen turvallisuuden alueella. Business Finlandin ”Digital Trust” -ohjelma on eräs käynnissä olevista tutkimusohjelmista, mutta ei ainoa.

- Suomeen on muodostumassa merkittäviä kasvuhakuisia **sovellusaluekeskittymiä** (esimerkiksi Autonomous Maritime-ekosysteemi, data- ja alustatalous, teollinen internet, jne.).

Välitavoitteet 2025

- Ohjelmatoiminnan ohjausryhmän toiminnan ansiosta Suomi on pystynyt merkittävästi tehostamaan digitaaliseen turvallisuuteen liittyvien aktiviteettien **lisäarvoa** ja luomaan **synergioita** eri toimijoiden ja toimintojen välille.
- Suomen digitaalisen turvallisuuden liiketoimintaekosysteemi on kansainvälisesti tunnettu ja se on kasvattanut jäsenmääräänsä merkittävästi myös Suomen ulkopuolella.
- Parhaat sovellusaluekeskittymät ovat jo tuottaneet merkittäviä innovaatioita, lisäarvoa ja liiketoiminnan kasvua. Uusia kasvuyrityksiä on syntynyt näille sovellusalueille.
- Toimintansa digitalisoineiden pk-yritysten määrä on noussut huomattavasti: enää 30 % pk-yrityksistä on digitalisaation ulkopuolella.
- **Kansallinen kybertestipenkki** on mahdollistanut tehokkaan digitaalisten turvallisuusuhkien ennakoinnin, havainnoinnin ja torjunnan sekä tukenut uusien tuotteiden kehittämistä ja testausta.

Tavoitteet 2030

- Pitkäjänteinen ja suunnitelmallinen työ digitaalisen turvallisuuden kehittämisessä on synnyttänyt Suomeen innovatiivisen ympäristön ja globaalisti ainutlaatuisen, data- ja alustatalouteen pohjautuvan toimintamallin.
- Digitaalisen turvallisuuden innovaatioekosysteemin onnistuneen toiminnan pohjalta Suomessa on käynnistetty vastaavanlaisia yhteistoimintamalleja myös muille keskeisille toimialoille.
- Vain 10 % suomalaisista pk-yrityksistä on digitalisaation ulkopuolella.

Ehdotukset mittareiksi ja KPI:ksi

- Digitalisaatiota hyödyntävien pk-yritysten määrä (osuus kokonaismäärästä)
- Digitaalisen turvallisuuden alueelle tehdyt patenttihakemukset ja myönnetyt patentit
- Liiketoimintaekosysteemin puitteissa syntyneiden kasvuyritysten lukumäärä
- Kansallisen kybertestipenkin käyttöaste

Keinovalikoima

- Uusien liiketoimintamallien kehittämisen ja käyttöönoton mahdollistava regulaatio, esimerkiksi dataoperaattori-toimijat (elinkeinoelämä, tutkimuslaitokset ja kansalaiset tuottavat dataa yhteiselle alustalle, mikä mahdollistaa uutta liiketoimintaa)
- Digitaaliset turvallisuussertifikaatit ja standardisointi (esimerkiksi JAMKissa kehitetty Finnish Cyber Security Certificate, FINCSC)
- Digitaalisen turvallisuuden hankeportaali, josta näkee valtionhallinnon, tutkimuslaitosten ja yritysten hankkeet yhdestä paikasta.
- Digitaalisen turvallisuuden kasvuohjelman rahoitus esimerkiksi Business Finlandin ”Digital Trust” ohjelman puitteissa.
- Kansainvälisten toimijoiden ottaminen mukaan tukemaan elinkeinoelämän ja kansalaisten toimintaa (esim. maatason yhteistyösopimukset Googlen, Microsoftin ja/tai Amazonin kanssa)

Kasvu ja kansainvälistyminen

Johdanto

Digitaaliset palvelualustat, palvelut ja data eivät noudata kansallisia rajoja, vaan ne jäsentyvät asiakkaiden tarpeiden ja asiakkaille tarjottavien hyötyjen perusteella.

Toimialatasolla tämä tarkoittaa sitä, että markkinoille tulon ja sieltä poistumisen esteet ovat madaltuneet, uudet liiketoimintamallit ovat tulleet mahdollisiksi ja erilaiset yhteistyömahdollisuudet ovat lisääntyneet. Samaan aikaan globaali kilpailu on kiristynyt innovaatioiden leviämisen nopeuduttua. **Yritystasolla** digitalisaatio mahdollistaa kansainvälistymisen aloittamisen jo lähes yrityksen perustamisvaiheessa, maantieteellisen etäisyyden roolin pienenemisen, virtuaalisen läsnäolon kansainvälisillä markkinoilla, yhtäaikaisen menon useille kansainvälisille markkinoille, sekä helpomman verkottumisen yhteistyökumppanien kanssa.

Perinteisesti kansainvälistymisen haasteiksi listataan yrityksen pienuudesta johtuva resurssien puute, tarjonnan uutuudesta johtuva vähäinen tunnettuus markkinoilla, kokemattomuus kansainvälisestä liiketoiminnasta, sekä heikot suhteet keskeisiin, kansainvälisen liiketoiminnan rakentamisessa tarvittaviin verkostoihin ja ekosysteemeihin. Uusilla liiketoiminta-alueilla, kuten esimerkiksi digitaalisen turvallisuuden ratkaisuissa ja palveluissa, näihin voidaan kehittää ja soveltaa uudenlaisia ratkaisuja, joita voidaan löytää ja edistää ekosysteemiajattelun avulla.

Ekosysteemien muodostuminen ei tapahdu toimijoita ulkopuolelta toisiinsa liittäen, vaan ne syntyvät toimijoiden löytäessä **yhteiseen ongelmaan ratkaisun**, joka ylittää yksittäisen toimijan kyvykkyydet ja edellyttää usean toimijan tarjoomien yhdistämistä toimivaksi kokonaisuudeksi. Yhteisen ratkaisun perustana voi olla esimerkiksi teknologinen alusta, joka tarjoaa resursseja tai toimintoja, joita muut ekosysteemin jäsenet voivat hyödyntää. Ekosysteemi voi myös perustua myynti- tai jakelukanavaan, joka tarjoaa pääsyn muuten suljetuille tai vaikeapääsyisille markkinoille. Keskeistä on, että ratkaisu perustuu alan toimijoiden tunnistamiin haasteisiin ja että se koetaan riittävän houkuttelevaksi, jotta toimijat haluavat liittyä ekosysteemiin. Menestyvän liiketoimintaekosysteemin on lisäksi oltava kooltaan riittävän suuri ja jäsenistöltään riittävän monimuotoinen ja dynaaminen (= riittävästi uusia ja poistuvia toimijoita), jotta se pystyy joustavasti tuottamaan ja tarjoamaan kilpailukykyisiä ratkaisuja. Toimijoiden välillä on myös oltava tarpeeksi yhteisiä, ekosysteemiä yhteen sitovia ja sen lisäarvoa kasvattavia aktiviteetteja.

Teknologian kehityksen myötä olennaiseksi kilpailueduksi tulee muodostumaan turvallisen digitaalisen liiketoiminnan perusperiaatteiden ymmärtäminen ja niiden ylivoimainen hyödyntäminen: yrityksen kokonaistarjooma muodostuu sen **tuotteiden ja palveluiden lisäksi datasta ja sen pohjalta asiakkaalle syntyvästä**

lisäarvosta. Tämänkaltaisen liiketoiminnan menestyminen on vahvasti kytköksissä digitaaliseen turvallisuuteen infrastruktuuriin, dataan, ohjelmistoihin ja palveluihin liittyen. Tämä monimuotoisuus asettaa alan yritysten liiketoimintaosaamisen ja kansainvälistymisen kehittämiselle uusia haasteita. Digitaalisten palvelualustojen ja niiden päälle rakennettujen palvelujen keskittyminen ja ryhmittyminen liiketoimintaekosysteemeiksi on yksi esimerkki näistä haasteista – ja samalla mahdollisuuksista.

Digitaalisten infrastruktuurien ja ekosysteemien digitaalista turvallisuutta voi tarkastella kahdesta näkökulmasta. Yhtäältä on ensiarvoisen tärkeää turvata digitaalinen kriittinen infrastruktuuri yhdessä muiden kriittisten infrastruktuurien kanssa (ks. Kyberresilienssi-teema). Toisaalta on olennaista luoda tuotteita ja ratkaisuja, jotka turvaavat yritysten liiketoiminnan edellytykset eli investoinnit, resurssit ja kyvykkyydet sekä myös asiakkaiden toimintaedellytykset. Liiketoiminnan näkökulmasta katsottuna suomalaisilla digitaalisen turvallisuuden alalla toimivilla yrityksillä on hyvät menestymisen mahdollisuudet kansainvälisillä markkinoilla – erityisesti, kun otetaan huomioon Suomen vahva osaaminen kone- ja laitevalmistuksessa ja langattomassa tietoliikenteessä.

Teollisen internetin kehittyminen avaa suomalaisille yrityksille merkittäviä mahdollisuuksia. Eräs mahdollinen lähestymistapa voisi olla liitteessä 2 esimerkkinä kuvattu "*Internet of Safe Things*" -liiketoimintaekosysteemi, joka kokoaisi yhteen monipuolisesti digitaalisen turvallisuuden, teollisen liiketoiminnan, tietoliikenteen ja tutkimuslaitosten toimijoita.

Kuten jo aiemmin todettiin, Euroopan unioni on lisäämässä panostuksiaan kyberturvallisuuteen. EU:n komissio on ehdottanut Euroopan unionin verkko- ja tietoturvaviraston (ENISA) vahvistamista, unionin laajuisen vapaaehtoisen kyberturvallisuuden sertifiointikehyksen luomista digitaalisten tuotteiden ja palvelujen kyberturvallisuuden parantamiseksi sekä suunnitelman tekemistä nopeasta ja koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin.

Euroopan komission ehdottama kyberturvallisuuden osaamiskeskus täydentäisi valmiuksien kehittämistä unionissa ja kansallisella tasolla. Kansalliset osaamiskeskukset toimisivat mekanismina, jonka avulla voidaan rakentaa pysyviä valmiuksia, yhdistää toimia, koota osaamista ja edistää sellaisten innovatiivisten ratkaisujen kehittämistä, jotka vastaavat kyberturvallisuuden teollisiin haasteisiin uusien

teknologioiden alalla (esim. tekoäly, kvanttilaskenta, lohkoketju ja turvalliset digitaaliset identiteetit) samoin kuin kriittisillä sektoreilla (esim. liikenne, energia, terveydenhuolto, rahoitusala, hallinto, televiestintä, valmistus, puolustus ja avaruus). Suomen tuleekin ottaa aktiivinen ja merkittävä rooli EU:n puiteohjelman teemojen ja sisällön valmistelussa ja suunnittelussa.

Teemakohtainen visio 2030

DIGITAALINEN LUOTTAMUS JA TURVALLISUUS OVAT KIINTEÄ OSA SUOMEN MAABRÄNDIÄ, JOTA VIEDÄÄN MAAILMALLE TOIMIALAKOHTAISTEN LIIKETOIMINTAEKOSYSTEEMIEN AVULLA YHTEISTYÖSSÄ KANSAINVÄLISTEN YHTEISTYÖKUMPPANIEN KANSSA.

Mitä tämä edellyttää? Digitaalisen turvallisuuden alueelle on syntynyt useita toimijoita yhdistäviä **liiketoimintaekosysteemejä**, joiden avulla yritykset voivat toimia osana suurempaa yrityskonsortiota ja sen avulla ylittää tai kiertää kasvun ja kansainvälistymisen esteitä. Suomelle luonnollinen kehityssuunta ekosysteemin kasvuun voisi löytyä esimerkiksi **teollisen internetin kehitystarpeista** sekä yksityisen sektorin palvelutarpeista – joskin uskottavuuden pohjana tulee olla riittävä kriittisen digitaalisen infrastruktuurin turvallisuus.

Keskeiset tavoitteet vuosille 2021, 2025 ja 2030

Välitavoitteet 2021

Suomalaiset, digitaalisen turvallisuuden palveluita ja ratkaisuja tarjoavat toimijat, niiden tarjoomat, hankkeet ja suunnitelmat on kartoitettu. Kartoituksen pohjalta on toteutettu syntynyt **toimija- ja hankeportaali** eli verkkosivusto, jonne eri toimijat voivat luoda ja päivittää tietonsa. Portaali on jäsennelty teemoittain niin, että sen avulla on helppo etsiä yhteistyökumppaneita, kartoittaa päällekkäisiä hankkeita ja kilpailijoita sekä viestittää omista avauksista kohdennetusti relevantille yleisölle.

Portaalin kantaviin voimiin kuuluu muutaman julkisen toimijan lisäksi myös suuria teollisuusyrityksiä sekä innovatiivisia startup-toimijoita ja niiden yhteenliittymiä.

Portaalissa on myös oma osionsa avoimesti julkaistaville tutkimustuloksille, jonka avulla yliopistojen, tutkimuslaitosten ja yritysten asiantuntijat pystyvät tiivistämään ja syventämään yhteistyötään sekä nopeuttamaan kilpailua.

- Suomalaiset organisaatiot osallistuvat aktiivisesti digitaalisen turvallisuuden kansainvälisten **standardointi- ja regulaatioelimien** toimintaan. Seuraavassa EU-puiteohjelmassa digitaalinen turvallisuus ja kyberturvallisuus ovat selkeästi edustettuina.
- Suuret suomalaiset teolliset toimijat (esim. KONE, Wärtsilä, Metso, Valmet ja Nokia) ovat aloittaneet **korkean profiilin yhteistyön** digitaalisen turvallisuuden alalla. Yhteistyön pohjalta on syntynyt useita ekosysteemiaihioita.
- Suomessa käynnissä oleva pitkäaikainen ja kooltaan merkittävä **tutkimusohjelma** toimii sateenvarjona useille tutkimus- tai liiketoimintavetoisille hankkeille, joiden erityinen painopiste on digitaalisessa turvallisuudessa.
- Suomi on aloittanut **merkittävät markkinointiponnistukset** maabrändin laajentamiseksi kattamaan myös Suomen roolin digitaalisen turvallisuuden edelläkävijänä sekä turvallisena kansainvälisten yritysten sijoittumispaikkana.

Välitavoitteet 2025

Suomen aktiivisiin **liiketoimintaekosysteemeihin perustuva toimintamalli** herättää kansainvälistä kiinnostusta. Erityisesti kone- ja laitevalmistajien ja digitaalisen turvallisuuden startup-sektorin yhteistyö on kantanut hedelmää, ja kansainvälisillä markkinoilla on käytössä tästä ekosysteemistä peräisin olevia ratkaisuja.

- Suomalaisten organisaatioiden edustajilla on **useita keskeisiä rooleja** digitaalisen turvallisuuden kansainvälisissä standardointi- ja regulaatioelimissä, verkostoissa ja yhteistyöelimissä.
- Ekosysteemiaihioista on syntynyt useita **toimialakohtaisia liiketoimintaekosysteemeitä**.

- Jo päättyneestä digitaalisen turvallisuuden kansallisesta tutkimusohjelmasta saatujen hyvien kokemusten perusteella alalle ollaan käynnistämässä **uusi monivuotinen puiteohjelma**.
- Suomella on aktiivinen ja merkittävä rooli **EU:n seuraavan puiteohjelman teemojen ja sisällön valmistelussa ja suunnittelussa**.
- Suomen maabrändiä on laajennettu kattamaan uusia digitaalisen turvallisuuden ja kybervaikuttamisen toimialoja.

Tavoitteet 2030

Tiivis digitaalisen turvallisuuden palveluntarjoajien ja teollisuusyritysten läheinen ja menestyksekäs yhteistyö on luonut Suomeen toimintaympäristön, jossa turvallisuus ja luotettavuus ovat itsestään selvä osa kaikkea uutta innovaatiotoimintaa.

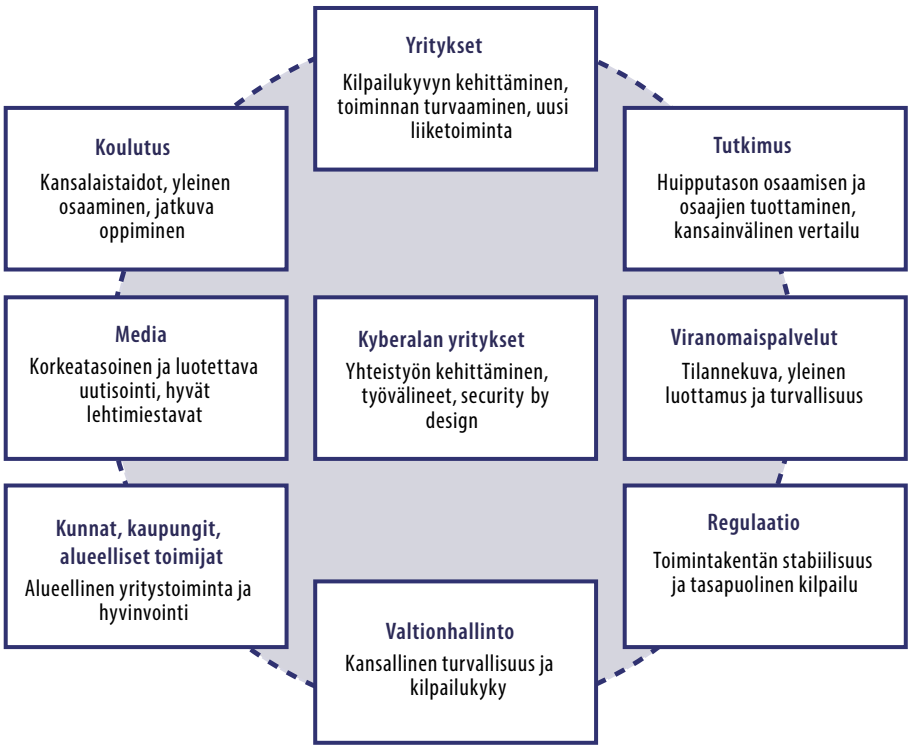
- Digitaaliseen turvallisuuteen liittyvän liiketoiminnan **globaalit markkinajohtajat** ovat Suomessa toimivia yrityksiä, konsortioita ja/tai liiketoimintaekosysteemejä.
- Kasvavan vientitoiminnan tukena on **Suomen vahva maabrändi**: Suomi on tunnustettu kärkimaa mm. tietoturvallisen digitaalisen teknologian ja palvelujen suunnittelussa, toteuttamisessa, operoinnissa ja hyödyntämisessä.

Sidosryhmät

Valmistelutyön aikana tunnistettiin yhdeksän erilaista sidosryhmää (kuva 3), jotka ovat:

- **Valtionhallinto** (ministeriöt, teollisuuden järjestöt, FICORA, jne.)
- **Alueelliset toimijat** (kunnat, kaupungit, maakunnat, sekä keskitetyt julkiset palveluorganisaatiot kuten Valtori, Kuntien Tiera, Palkeet, jne.)
- **Regulaatiotoimijat** (ministeriöt, valvontaviranomaiset, EU:n komissio)
- **Viranomaiset ja julkiset palvelut** (tiedusteluviranomaiset, turvallisuusviranomaiset, Huoltovarmuuskeskus, Kyberturvallisuuskeskus, Valtioneuvoston tilannekeskus, Puolustusvoimat, poliisi, tuomioistuimet, vankeinhoitolaitos)
- **Media** (suuret mediatalot, perinteinen painettu media, sosiaalisen median palveluntuottajat, verkon keskustelupalstat, markkinointiyritykset, Journalistiliitto)
- **Koulutus** (yliopistot, korkeakoulut, ammattikorkeakoulut, peruskoulut, ammatillinen koulutus, kansalaisjärjestöt ja työväen opistot, puolustusvoimat, reserviläiskoulutus)
- **Tutkimus** (yliopistot, korkeakoulut, tutkimuslaitokset)
- **Yritykset** (huoltovarmuuden kannalta kriittiset infrastruktuuritoimijat, tietotekniikkaa hyödyntävät yritykset, yritysten verkkokaupat, Teknologiateollisuus)
- **Digitaalisen turvallisuusalan (kyberalan) yritykset** (FISC-verkoston toimijat, PIA-verkoston toimijat, ICT- ja internetpalveluiden tuottajat, ohjelmistoalan yritykset, sähköisten identiteettien luojat ja palveluntarjoajat)

Liitteessä 3 on esitelty tarkemmin näiden keskeisten sidosryhmien haasteita, mahdollisuuksia ja mahdollisia toimenpiteitä.



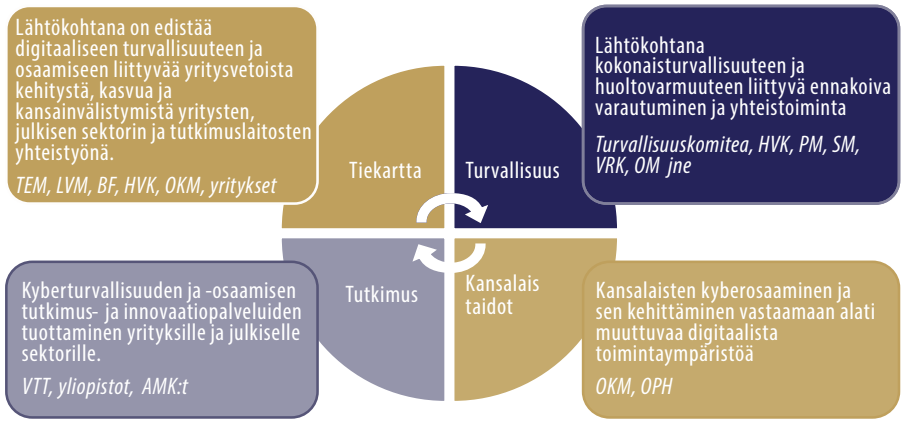
Kuva 3. Digitaalisen turvallisuuden toimialan keskeiset sidosryhmät ja niiden tavoitteet.

Toimeenpano, mittaaminen ja seuranta

Digitaalisen turvallisuuden tiekartan tarkoituksena on edistää digitaaliseen turvallisuuteen ja osaamiseen liittyvää yritysvetoista kehitystä, kasvua ja kansainvälistymistä yritysten, julkisen sektorin ja tutkimuslaitosten yhteistyönä. Kuva 4 kuvaa digitaalisen turvallisuuden ympäristöä, jossa muut keskeiset alueet ovat:

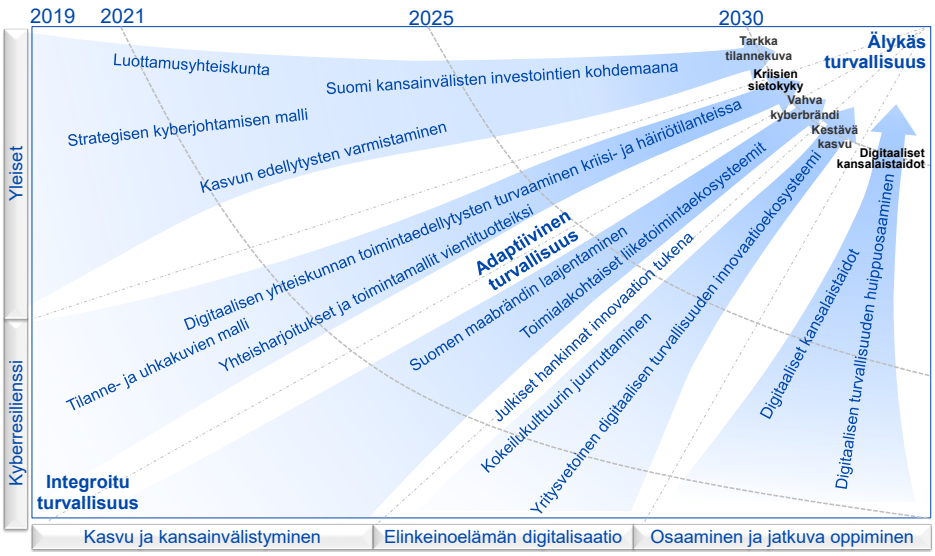
- **turvallisuus**, joka käsittää kokonaisturvallisuuteen ja huoltovarmuuteen liittyvän ennakoivan varautumisen ja yhteistoiminnan,
- **tutkimuslaitokset**, jotka tuottavat kyberturvallisuuden ja -osaamisen tutkimus- ja innovaatiopalveluita yrityksille ja julkiselle sektorille, sekä
- **kansalaistaidot**, jotka kattavat kansalaisten digitaalisen turvallisuuden osaamisen ja sen kehittämisen vastaamaan alati muuttuvaa digitaalista toimintaympäristöä.

Toteutuessaan digitaalisen turvallisuuden tiekartta linkittyisi tiiviisti yhteen näiden muiden toimintojen kanssa. Tärkeimmät yhteisen vaikuttamisen alueet ovat yritysten investointien kiihdyttäminen (Turvallisuus), poikkitieteellisen yhteistyön tiivistäminen tutkimuslaitosten ja julkisen sektorin turvallisuustoimijoiden kanssa (Tutkimus) sekä osaamisen kehittäminen yritysten henkilökunnan ja kansalaisten osalta (Kansalaistaidot).



Kuva 4. Digitaalisen turvallisuuden tiekartan asemointi

Ohjelmatoiminnan toimeenpanon tueksi on laadittu ylätason tiekartta (kuva 5), jonka yksityiskohtaisempi versio on liitteessä 4.



Kuva 5. Kasvuohjelman ylätason tiekartta 2019–2030

Tiekartassa kuvatut toimenpiteet on jaoteltu kasvuohjelman valmistelutyössä käytettyjen neljän pääteeman ympärille: (1) kyberresilienssi, (2) osaaminen ja jatkuva oppiminen, (3) elinkeinoelämän digitalisaatio sekä (4) kasvu ja kansainvälistyminen.

Kyberresilienssi -alueella olevat toimenpiteet keskittyvät kriisien ja häiriötilanteiden sietokyvyn ja niistä toipumisen edistämiseen digitaalisen yhteiskunnan keskeisillä osa-alueilla. **Osaaminen ja jatkuvan oppiminen** -alueen toimenpiteiden tavoitteena on lisätä kansallista tietoisuutta digitaalisesta turvallisuudesta ja korostaa kansalaisten kyberosaamisen roolia ja merkitystä osana uutta digitaalista yhteiskuntaa. **Elinkeinoelämän digitalisaatio** -alueen toiminnot keskittyvät digitaalisen turvallisuuden roolin kehittämiseen elinkeinoelämän digitaalisen murroksen mahdollistajana ja uuden kasvun ajurina. **Kasvu ja kansainvälistyminen** -alueen toimenpiteet keskittyvät edistämään Suomen asemaa kansainvälisesti tunnettuna kyberturvallisuusalan edelläkävijänä. Teema kattaa myös alan tutkimus- ja innovaatiotyön sekä suomalaisten kyberalan yritysten kansainvälistymisen edistämisen.

Digitaalisen turvallisuuden perusratkaisut ja -palvelut ovat tärkeä osa kriisinsietokyvyn saavuttamista. Tiekartta sisältää myös **johtamismallien vastuiden määrittelyt** ja käyttöoton, yhteisten arvojen ja toimintamallien määrittelyt sekä **tilanne- ja uhkatietojen tietokannan** luomisen. **Digitaalisen turvallisuuden liiketoiminnan ekosysteemin** luominen on esimerkki mahdollisesta sovellusalueesta, jolla luodaan uutta liiketoiminnallista kasvua jo nyt vahvoilla teollisuusalueilla.

Digitaalisen turvallisuuden **tietämyksen, osaamisen ja koulutustason** kohottamiseksi tarvitaan kaikki opetustasot kattavan opetussuunnitelman ja sitä tukevan alustan luomista. Alusta mahdollistaa muuttuvan tiedon ja opetusmateriaalien skaalautuvan luomisen mukaan lukien jatkuvan oppimisen sekä kyberkansalaistaidot. Tietoa kerätään kattavasti eri lähteistä (mukaan lukien alan keskeiset tutkimustulokset), mikä mahdollistaa tietokannan jatkuvan ajankohtaisuuden.

Innovaatioekosysteemi perustuu tehokkaaseen elinkeinoelämän ja tutkimuslaitosten väliseen yhteistyöhön, jossa hyödynnetään Suomen tasolla myös EU-puiteohjelmia niihin aktiivisesti vaikuttamalla. Kotimaisen tutkimuksen vahvistamiseksi on investoitava uusien professuurien ja riittävän suurten tutkimusryhmien muodostamiseksi poikkitieteellisille kyberturva-alueille.

Tärkeimmät toimenpiteet ja niiden toteuttamisesta vastaavat tahot ovat seuraavat:

1. **Hallinnonaloja yhdistävä digitaalisen turvallisuuden tiekartan ohjausryhmän perustaminen**
    a. Vahva mandaatti ja aktiivinen rooli.
    b. Kattavan asiantuntijaryhmän tuominen mukaan jatkotoimenpiteiden suunnitteluun ja toteuttamiseen.
    c. Mittarit ja seuranta: valittavien kehityshankkeiden projektointi ja niiden seuranta. Eri toimijoiden konsolidointiin tähtäävät mittarit.
2. **Digitaalisen turvallisuuden liiketoiminnan ekosysteemin rakentaminen ja käynnistäminen**
    a. Mukana: yritykset, tutkimuslaitokset, julkinen sektori. Tavoitteena digitaalisen turvallisuuden TKI-toiminnan pystyyn laittaminen ja vauhdittaminen. Sisältää myös alaekosysteemejä, esim. kyberresilienssin alueella.
    b. Mittarit ja seuranta: Ekosysteemin toimintaan liittyvät KPI:t (hankekanta, uudet jäsenet, kansainvälinen yhteistyö, investoinnit, vienti).
3. Yhteiskunnan toiminnan suojaamiseen ja varmistamiseen liittyvien **digitaalisen turvallisuuden perusratkaisujen ja -palveluiden systematisointi, tuotteistaminen ja yhteistyömallien rakentaminen yritysten TKI-toiminnan vauhdittamiseksi**
    a. Mukana: johtamismallit ja -vastuut, yhteinen arvopohja sekä harjoitustoiminnan systematisointi ja tuotteistaminen (mahdollista vientitoimintaa varten).
    b. Mittarit ja seuranta: Yhteiskunnan toiminnan suojaamisen ja varmistamisen mittarit. Yhteiskunnan toimintaedellytysten suojaamiseen ja turvaamiseen liittyvät johtamismallit ja -vastuut on toteutettu eri toimialoilla. Resilienssitoimijoiden osaamisen skaalaaminen yritysten käyttöön.

4. **Digitaalisen turvallisuuden ja luottamuksen opetussuunnitelman laatiminen**
    a. Mukana: kaikki opetustasot (peruskoulu, toinen aste, ammattikoulut, ja korkeakoulut), sisältää myös systemaattisen prosessin kansalaisten digiosaamistason kartoittamiseksi ja seuraamiseksi.
    b. Mittarit ja seuranta: Oppimisympäristön luominen (esim. Moodle), skaalautumisen seurannan mittarit. Uusien professorien määrä (minimitavoite 10), tutkimusryhmien kriittinen taso ja koko. Kansalaisten kyberosaamistason kartoitus ja edistymisen seuranta.
5. Suomen **"Digital Trust & Safety" -maabrändin rakentaminen ja markkinointi**
    a. Mittarit ja seuranta: Suomen ranking sijoitus kyberbränditutkimuksissa. Ulkomaalaisten kyberalan toimijoiden houkuttelu Suomeen (määrä) ja investointien kasvu Suomessa.

Tarvittavat portaalit ja tietokannat:

6. **Digitaalisen turvallisuuden kansalaisportaali**
    a. Sisältää ajan tasalla olevaa materiaalia mm. jokamiehen digitaalisista oikeuksista ja velvollisuuksista, koulutuksesta, opetuksesta
    b. Mittarit ja seuranta: kävijämäärä, opetusvideoiden tms. katsojamäärät
7. Yritysten ja julkisten toimijoiden käyttöön tarkoitettu digitaalisen turvallisuuden **hanke- ja toimijaportaali**
    a. Mukana: käynnissä olevat julkishallinnon hankkeet
    b. Mittarit ja seuranta: hankkeiden määrä, toimijoiden määrä

Liitteet

Liite 1. Osaamisen teoriasta

Liite 2. Esimerkki kansallisen painopistealueen valinnasta: Internet of Safe Things (IoST)

Liite 3. Sidosryhmät, keskeiset haasteet ja mahdollisuudet

Liite 4. Digitaalisen turvallisuuden tiekartta 2019–2030

Liite 5. Käynnissä olevat, digitaaliseen turvallisuuteen liittyvät hankkeet

Liite 6. Listaus valmistelutyöhön osallistuneista asiantuntijoista

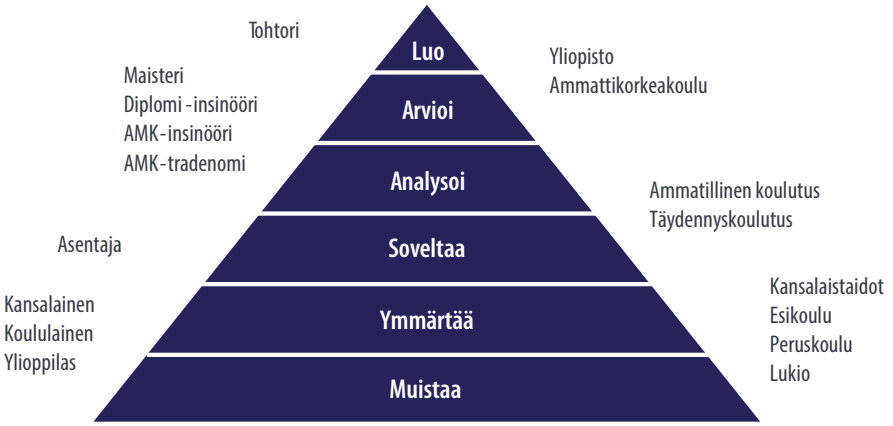
Liite 1. Osaamisen teoriasta

(Pasi Kämppi, Laurea)

Osaamisen tasot voidaan mallintaa esimerkiksi Bloomin taksonomian[xii] avulla. Bloomin taksonomia tunnistaa kuusi erilaista oppimisen tasoa: 1) muistaminen, 2) ymmärtäminen, 3) soveltaminen, 4) analysointi, 5) arviointi ja 6) luominen. Digitaalisen turvallisuuden tietoisuuden osalta riittää, kun asiat tai termit ymmärretään. Pienetkin muutokset arjen toiminnassa koulussa tai kotona voivat itse asiassa olla myös yhteiskunnallisesti merkittäviä. Parhaimmillaan ymmärryksen lisääminen voi johtaa syvällisempiin osaamispolkuihin. **Muistamisen ja ymmärtämisen taso** on riittävä esimerkiksi kansalaistaidoksi, peruskouluihin tai lukioihin.

Ammatillisessa koulutuksessa vaaditaan **soveltavaa osaamista**, jotta yksilöt osaavat toimia työyhteisön jäsenenä oikeassa työympäristössä. *Digitaalisen turvallisuuden* soveltavalla osaamisella on suora välitön vaikutus organisaation tehokkuuteen ja tuloksellisuuteen. Ammattikorkeakouluissa ja yliopistoissa voidaan pyrkiä oppimisen kolmelle ylimmälle tasolle, joilla **analysoidaan**, **arvioidaan** ja myös **luodaan** uusia innovaatioita. Analysointi- ja arviointiosaamisella voidaan kehittää organisaation toimintaa, arvioida organisaatioon liittyviä uhkia ja tehdä tilannekuvaan liittyvää analyysia.

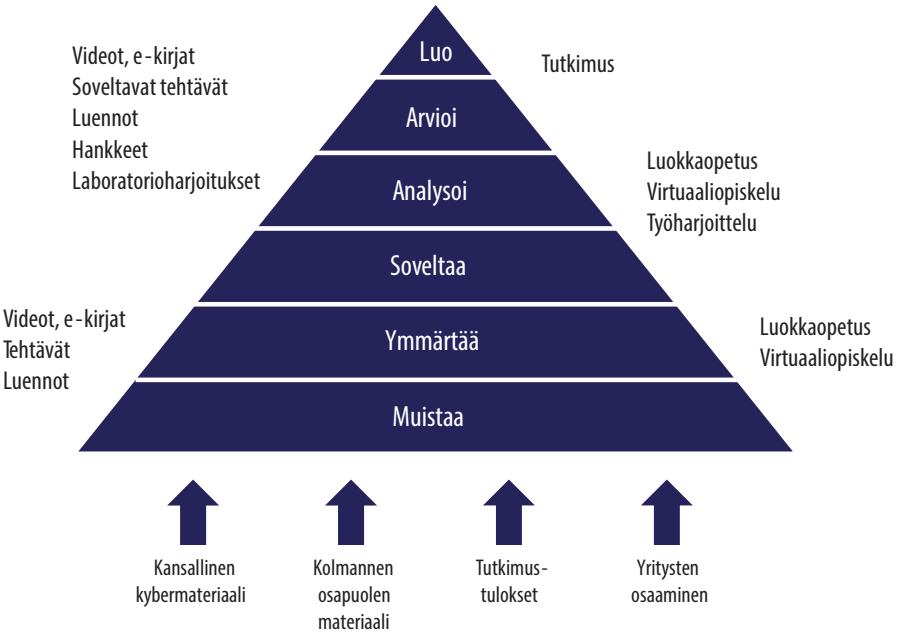
Osaamisen huipulla on uuden kehittäminen ja luominen. Yliopistoissa tutkimustyö voi olla teoreettisempaa, mutta ammattikorkeakouluissa pyritään käytännön sovelluksiin. Osaamisen tasot yhdistettynä oppilaitosten tuottamaan osaamiseen on esitetty kuvassa a.



Kuva a. Skaalautuva koulutuksen toteutus

Koulutus toteutetaan skaalautuvalla mallilla osaamistavoitteiden mukaan. Tietoisuuden osalta (muistaminen, ymmärtäminen) riittävät luennot, tietoiskut ja jopa itsenäinen virtuaaliopiskelu. Opiskeluun voidaan liittää myös tehtäviä osaamistavoitteiden mukaan tai osaamisen kehittymisen seurantaa varten. Tehtäviksi käyvät esimerkiksi helpohkot monivalintatehtävät. Soveltavassa osaamisessa tietoperusta voidaan rakentaa virtuaalisessa oppimisympäristössä, jota syvennetään luokkaopetuksessa tai oppimisympäristöissä. Luokkaopetuksessa voidaan tehdä erilaisia ymmärrystä lisääviä analyyttisia tehtäviä tai digitaaliseen turvallisuuteen ja sen osana kyberturvallisuuteen liittyviä laboratorioharjoituksia (esim. haavoittuvuustestaus).

Soveltavaan oppimiseen käy hyvin myös työharjoitteluympäristö, jossa opiskelija tutustuu ”oikeaan työhön”. Osaamisen kolme ylintä tasoa (analysointi, arviointi, luominen) voidaan saavuttaa erilaisissa tutkimushankkeissa, joissa opiskelijat, opettajat, tutkijat ja työelämän edustajat tekevät tutkimustyötä yhteisen tavoitteen saavuttamiseksi. Tutkimustavoitteena voi olla käytännön sovellus tai teoreettinen malli. Erilaiset pedagogiset mallit yhdistettynä osaamistavoitteisiin on esitetty kuvassa b.



Kuva b. Pedagogiset mallit ja osaamistavoitteet

Osaamisen kehittäminen nojautuu jatkuvan ja elinikäisen oppimisen malliin. Mallissa mahdollistetaan erimuotoisten ja erilaisista taustoista tulevien ihmisten osaamisen kehittäminen. Myös tämä osaamismalli tulee olla skaalautuva ja erilaiset osaamistarpeet huomioon ottava.

Digitaalinen toimintaympäristö on alati muuttuva ja siihen liittyvän opetus- ja koulutusmateriaalin tuottaminen sekä jakaminen on kyettävä toteuttamaan siten, että kaikilla on yhtäläinen mahdollisuus tarvittavan tiedon omaksumiseen. Oleellisena osana skaalautuvaa oppimiskokonaisuutta on **yhtenäinen digitaalinen alusta**, joka mahdollistaa muuttuvan tiedon ja siihen liittyvän materiaalin jakamisen kouluille ja oppilaitoksille. Alustan kautta pystytään tuottamaan työkaluja sekä opettajille että oppilaille, heidän tarpeistaan riippuen. Sellainen voisi olla esimerkiksi verkkopohjainen oppimistyökalu. Digitaalisen alustan lisäksi digitaalisen turvallisuuden kokonaisuus vaatii sisällön tuottamisen sekä jatkuvan oppimisen tuen muuttuvassa ympäristössä. Digitaaliset taidot sekä digitaalinen turvallisuus nähdä uutena oppimiskokonaisuutena nykyisten jo vakiintuneiden perusaineiden rinnalla.

Kansainvälisiä vertailukohtia

Alankomaat näkee kyberturvallisuuteen liittyvän koulutuksen työllistymistä edistävänä ja ylläpitävänä tekijänä. Strategiassa huomioidaan tarve sekä tieteelliselle että soveltavalle tutkimukselle ja koulutuksen tarve on kaikilla koulutuksen tasoilla. Alankomaat pyrkii laajentamaan koulutustarjontaa etenkin peruskouluille ja koulutus tulee lakisääteiseksi vuonna 2019 koulutus, kulttuuri- ja tiedeministeriön tukemana. Alankomailla on myös pitkäjänteinen kehitysohjelma akateemisen yhteisön kanssa.[xiii]

Itävallalla on hyvin voimakas painotus koulutukseen ja strategia jakaa koulutustarpeen seitsemään osa-alueeseen: 1) koulutusta jo peruskoulussa turvalliseen median käyttöön, 2) tietoturvallisuus pakolliseksi osaksi opettajakoulutusta, 3) kolmannen sektorin koulutus yhteistyössä koululaitosten kanssa, 4) aikuis- ja seniorikoulutus, 5) tietoturvallisuuteen liittyvän koulutuksen lisääminen osana kansallista osaamispääomaa, 6) poikkitieteellisen tutkimuksen lisääminen osana tietoturvallisuuteen liittyvää tutkimusta ja 7) Itävallan saaminen osallistujaksi kansainvälisissä tutkimusohjelmissa (EU).[xiv]

Ranska on jakanut koulutukseen liittyvät tavoitteet neljään osa-alueeseen: 1) kouluikäisten tietoturvallisuustietoisuuden kohottaminen, 2) kyberturvallisuuteen liittyvän korkeakoulutuksen lisääminen, 3) ammatillisen jatkokoulutuksen lisääminen ja 4) kansalaisten tietoturvatietoisuuden lisääminen internet-ajokortin muodossa. Koulutusministeriö on hankkeissa voimakkaassa roolissa ja aluksi kyberturvallisuuden integrointi pyritään toteuttamaan integroimalla koulutus jo olemassa oleviin opintojaksoihin. Julkisen sektorin osaamistarve on myös huomioitu koulutustarpeissa.[xv]

Australiassa koulutus nähdään tarpeellisena kaikilla koulutustasoilla. Keskitettyjen osaamiskeskusten vastuulla on kehittää laadukasta koulutusta kaikille koulutusasteille. Osaamiskeskukset auttavat myös opiskelijoita etsimään itselleen sopivia urapolkuja ja hakeutumaan kyberturvallisuuden opintojen pariin.[xvi]

USA:n kyberstrategian lähtökohtana on lisätä osaamista kybersektorilla kolmella tavalla; 1) koulutusputket kaikille kouluasteille, 2) jatko- ja lisäkoulutus ja 3) huippuosaajien palkitseminen kansallisella tasolla. Osaamisen arviointi perustuu "National

Initiative for Cybersecurity Education (NICE)" -viitekehykseen, joka on standardoitu menettely työvoiman osaamisen tunnistamiseen.[xvii]

Koulutustarpeet Suomessa

Suomessa koulutustarpeet ovat pääosin yhteneväisiä edellä kuvattujen esimerkkimaiden kanssa, mutta kuitenkin siten, että *kyberturvallisuus* nähdään meillä osana laajempaa *digitaalisen turvallisuuden* kokonaisuutta. Digitaaliseen turvallisuuteen liittyy myös muita kuin teknisiä taitoja. Näitä ovat muun muassa monilukutaito, digitaalisen toimintaympäristön lainalaisuuksien ymmärtäminen sekä informaatiovaikuttaminen.

Digitaaliseen turvallisuuteen liittyvä osaaminen tulisi nähdä kansalaistaitona – tai jopa kansalaisvelvollisuutena. Tätä taustaa vasten jokaisella kansalaisella tulisi olla mahdollisuus kartuttaa digitaaliseen turvallisuuteen liittyvää osaamistaan äidinkielellään. Merkittävänä haasteena on tällä hetkellä se, että alan keskeinen sanasto on englanninkielistä. Digitaaliseen toimintaympäristöön ja informaatiovaikuttamiseen liittyvää opetusta tulisi tarjota jo peruskoulun ensimmäiseltä luokalta alkaen ja opetuksen tulisi jatkua myös yläasteella ja lukiossa.

Ammatillisessa koulutuksessa digitaalisen osaamisen taidot kannattaa integroida osaksi ammattiin oppimista siten, että kaikilla aloilla opiskellaan ainakin perusoppimäärä riittävän perustaidon takaamiseksi. Ammattikorkeakouluissa ja yliopistoissa opiskelevien näkökulmaa tulisi laajentaa niin, että heille tarjotaan digitaaliseen turvallisuuteen liittyviä suurempia opintokokonaisuuksia. Niiden lisäksi tulisi tarjota soveltaviin tutkintoihin johtavaa koulutusta sekä aiheeseen liittyvää täydennyskoulutusta siten, että kaikkiin tutkintoon johtaviin koulutuksiin on sisällytetty ainakin digitaalisen turvallisuuden perusteet.

Yleisen kansalaistaidon tai kansalaisvelvollisuuden tason saavuttaminen edellyttää, että oppilaitosten ja yleissivistävän koulutuksen lisäksi kaikille kansalaisille on tarjolla avoin oppimisympäristö, jossa digitaalisen turvallisuuden perusteita on mahdollisuus opiskella myös ilman oppilaitokseen kirjoittautumista. Tällaisen oppimisympäristön kautta pystytään tarvittaessa jakamaan nopeasti ja tehokkaasti ajan tasalla olevaa tietoa.

Liite 2. Esimerkki kansallisen painopistealueen valinnasta: Internet of Safe Things (IoST)

Painopistealueen visio: Vuonna 2030 Suomi tunnetaan **teollisen internetin turvallisuuden edelläkävijänä, digitaalisen identiteetin ja varmistamisen mallimaana, sekä turvallisimpana digitaalisen liiketoiminnan toimintaympäristönä**. Suomalaiset toimijat ovat kansainvälisen, liiketoimintaorientoituneen digitaalisen turvallisuuden ekosysteemin ytimessä tuotteillaan ja palveluillaan, ja vaikuttavat aktiivisesti toimialan standardien, regulaation ja lainsäädännön kehittymiseen.

Keinovalikoima: (vastuuorganisaatioina DIMECC, BF, FISC r.y. sekä alan yritykset ja tutkimusorganisaatiot)

- **Kasvumahdollisuuksien systemaattinen kartoitus ja priorisointi**:
  - Asiakasnäkökulman valinta (valtiolliset toimijat vs. yksityiset yritykset vs. kuluttajat)
  - Tarjoomanäkökulman valinta (tuote- ja palvelukeskeinen vs. toimiala- tai teknologiakeskeinen)
  - Julkisen tuen panostuskohteiden valinta
- **Kansallisen yhteistyön tiivistäminen:**
  - Digitaalisen turvallisuuden hanke- ja toimijaportaalin hyödyntäminen relevanttien kontaktien ja kytkentöjen muodostamisessa
- **Kansainvälisen tunnettuuden ja näkyvyyden lisääminen:**
  - Jokavuotinen kansainvälinen digitaalisen turvallisuuden IoST-foorumi ja/tai konferenssi
  - Kansallisten ja kansainvälisten verkostojen hyödyntäminen (esim. SLUSH, IIC, IFIP, jne.)

- **Kansallinen ekosysteeminen TKI-ohjelma kansainvälistymisen edistämiseen:**
  - Tavoitteena liiketoiminnan kasvun ja viennin kiihdyttäminen yritystasolla
  - Vertaistukiverkosto ja ohjausryhmä edistämään oikea-aikaisten ja oikein kohdistettujen toimenpiteiden valmistelua ja käyttöä
  - Yritystasolla kohteena on erityisesti ylin johto sekä muut yrityksen avainhenkilöt

Keskeiset tavoitteet:

2021: Suomalaisten **toimijoiden ja hankkeiden kartoitus** on tehty ja sen pohjalta on rakennettu **hanke- ja toimijaportaali**, jonne toimijat voivat ilmoittaa tietonsa, etsiä yhteistyökumppaneita, kartoittaa päällekkäisiä hankkeita sekä viestittää omista avauksistaan. Sivustolla julkaistaan myös **tutkimustuloksia** ja sen avulla yliopistot, tutkimuslaitokset ja yritykset pystyvät tiivistämään ja syventämään yhteistyötään, sekä nopeuttamaan kilpailua. Sivuston **keskustelufoorumi** aktivoituu, kun ensimmäisessä kansainvälisessä **IoST-konferenssissa** toisensa tavanneet asiantuntijat huomaavat sen arvon.

2025: **IoST-konferenssi** järjestetään viidennen kerran. Esineiden internetin yleistymiseen liittyneiden ongelmien myötä Suomen teollisen internetin kyberturvallisuusekosysteemi herättää kansainvälistä kiinnostusta. Konevalmistuksen ja digitaalisen turvallisuuden startup-sektorin yhteistyön ansiosta suomalaiset ovat vakiinnuttamassa asemaansa **kansainvälisissä standardointi- ja regulointielimissä**. IoST alkaa olla globaalisti tunnistettu ja tunnustettu brändi.

2030: Kymmenes **IoST-konferenssi** kokoaa yhteen alan kansainväliset huippuosaajat, lainsäätäjät, palveluntarjoajat ja teollisuusyritykset. Sen ympärille on muodostunut kansainvälinen IoST -ekosysteemi, joka on alan merkittävin asiantuntijoiden yhteenliittymä. Erilaiset **digitaalisen turvallisuuden liiketoimintaan** perustuvat uudet avaukset ovat lähteneet liikkeelle Suomesta. Suomalaiset konevalmistajat ovat vallanneet kansainvälisiä markkinoita tarjoamalla toimintaympäristön, jossa kyberturvallisuus on itsestään selvä, kokonaisuuteen kiinteästi integroitu osa innovaatiotoimintaa.

Mittarit ja KPI:t:

- **Hanke- ja toimijaportaaliin** liittyneiden toimijoiden määrä, vierailijamäärä, keskustelufoorumin aktiivisuus
- **Konferenssin** osallistujamäärä, kumppanien määrä, kansallinen ja kansainvälinen julkisuus, kävijäpalaute
- **Maabrändin** tunnettuustutkimus, kansainväliset luotettavuus/turvallisuusraportit ja listaukset, ”invest in” -kansainvälistyminen (eli kuinka moni kansainvälinen toimija valitsee Suomen liiketoimintansa tukikohdaksi)
- **Kasvu:** uudet ja kansainvälistyvät alan toimijat, uudet tuotteet ja palvelut, uudet kansainväliset asiakkaat
- **Vaikutusvalta:** Suomeen jäljitettävien standardien ja patenttien määrä, edustukset kansainvälisissä regulaatio- ja lainsäädäntöelimissä.

Liite 3. Sidosryhmät, keskeiset haasteet ja mahdollisuudet

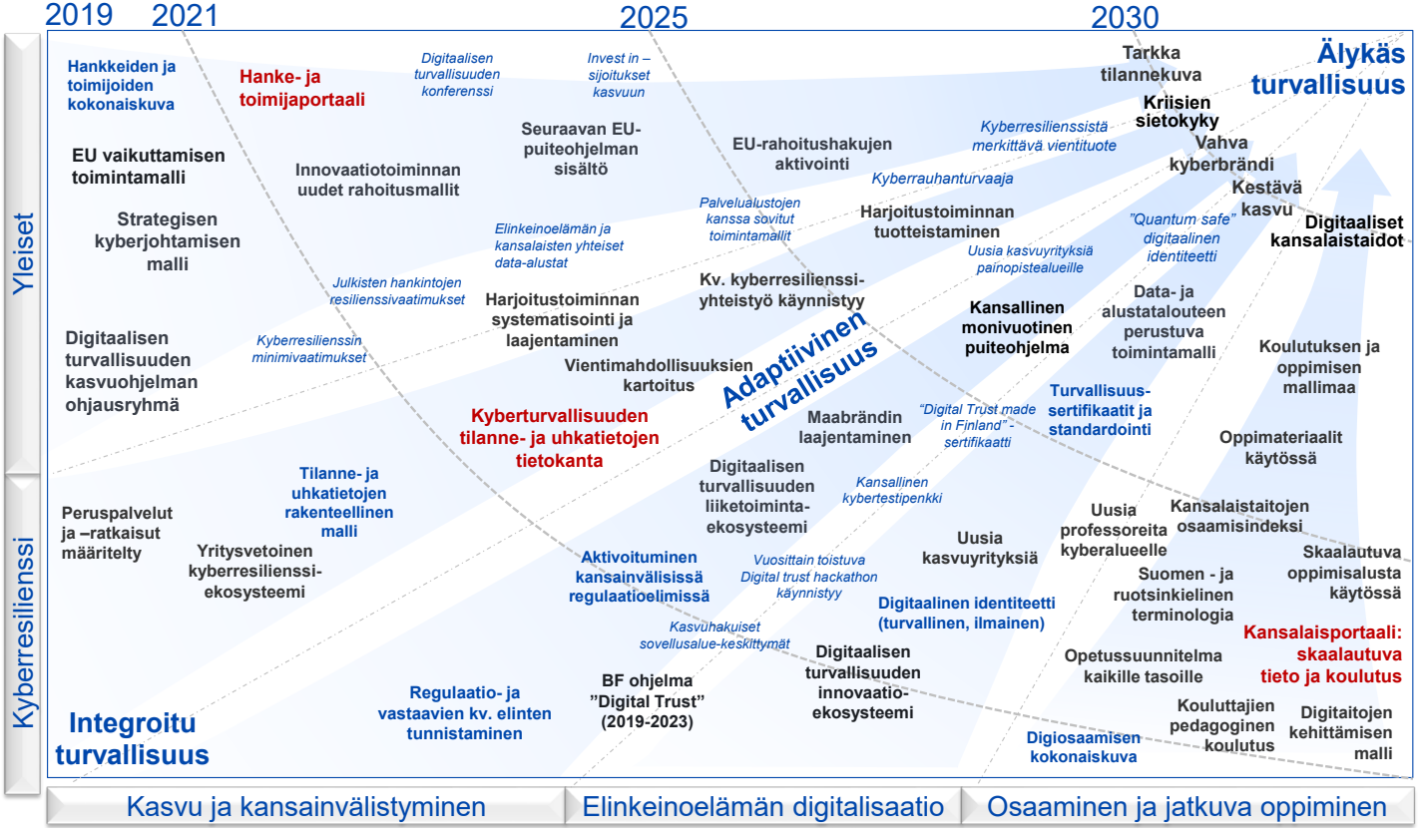
Sidosryhmät	Keskeiset haasteet	Mahdollisuudet	Toimenpide-ehdotukset	Esimerkkejä
Yritykset (kyberala)	Kyberrikollisuus (hyökkäykset, vakoilu, tietojen kalastelu, hybridiuhat, jne.) Kustannushaasteet (miten saadaan asiakas ymmärtämään, että digitaalinen turvallisuus on tärkeää ja että siitä kannattaa maksaa) Huonon tietoturvan aiheuttamat taloudelliset ja muut vahingot sekä mainehaitta Osaavien ohjelmistokehittäjien huono saatavuus	Toimialan ekosysteemi, jonka puitteissa jaetaan tietoa, osaamista ja riskejä Turvalliset työvälineet ja ”security and sustainability by design” Yhteistyön kehittäminen Henkilöstön osaamisen ylläpito ja kehittäminen Digitalisaation edistymisen myötä ICT- ja kyberosaamisen merkitys kasvaa (uusi liiketoimintapotentiaali)	Yhteisten toimintamallien ja de-facto standardien luominen ja juurruttaminen käyttöön Yhteinen markkinointi, valistus ja tiedottaminen Asiakkaiden osaamisen ja ymmärryksen kehittäminen Auktorisointi- ja varmennuspalvelut Kattavan, luotettavan ja ilmaisen digitaalisen identiteettipalvelun luominen	FISC-verkoston toimijat PIA-verkoston toimijat ICT- ja internetpalveluiden tuottajat, esimerkiksi Security Operations Center (SOC) ja Network Operations Center (NOC) Ohjelmistoalan yritykset Sähköisten identiteettien luojat ja palveluntarjoajat
Yritykset (muut)	Toiminnan häiriintyminen poikkeusoloissa Globaalien alustatalouden yritysten (Amazon, Google, Microsoft, jne.) merkittävä rooli Suomen elinkeinoelämän toiminnassa	Sieto- ja toipumiskyvyn jalkauttaminen osaksi normaalia (rauhanajan) toimintaa Huoltovarmuuden kehittämisestä vientituote Suomelle Alustatalouden yritysten roolin vähentäminen	Yhteiset toimintaharjoitukset Haavoittuvuuksien, uhkatietojen ja parhaiden käytäntöjen jakaminen Uskottavien kotimaisten alustavaihtoehtojen luominen Digitaalisten alustojen ”oikean” käytön arkkitehtuuri ja periaatteet (kerrokset, rajapinnat)	Huoltovarmuuden kannalta kriittiset toimijat ja toimialat, kuten: energia-ala (tuotanto ja jakelu) logistiikka-ala finanssiala elintarviketeollisuus terveydenhoito
	Digitaalisesti turvallisen tarjooman ja toimintamallien kehittäminen Tietoturvalliset tuotteet ja palvelut Digitaalisen turvallisuuden käytettävyys	Kilpailuetu ja/tai kilpailukyvyn säilyttäminen (toimialasta riippuen) Uudet liiketoiminta-alueet, esimerkiksi digitaalisten riskien vakuuttaminen	Kattavan, luotettavan ja ilmaisen digitaalisen identiteettipalvelun luominen	Tietotekniikkaa hyödyntävät yritykset Yritysten verkkokaupat Vakuutusalan yritykset
	Kokonaiskuvan hahmottaminen ja ymmärtäminen PK-yritysten digitalisaation ja kyberhallinnan eriarvoistuminen	Jäsenyritysten määrän lisääminen Jäsenyritysten toiminnan volyymi kasvaa	Jäsenyritysten neuvonta Informoitu edunvalvonta	Teknologiateollisuus, FISC, PIA ja muut vastaavat toimijat

Sidosryhmät	Keskeiset haasteet	Mahdollisuudet	Toimenpide-ehdotukset	Esimerkkejä
Media	Ulkomailta lähtöisin oleva vaikuttaminen (sosiaalisessa) mediassa Uutislähteiden luotettavuus, lähdekritiikin puute, nimettömien lähteiden käyttö, valeprofiilit Painetun median hitaus online-tarjontaan verrattuna Huomiotalous (kilpailu kuluttajien ajankäytöstä ja huomiosta) Mainostuottojen siirtyminen verkkoon	Korkeatasoisten ja luotettavien uutisten tuottaminen (todenperäisyyden varmistaminen, kestävä taustoitus) Alan sisäinen kontrolli: ”hyvien lehtimiestapojen” kehittäminen ja noudattaminen Sisällön tuotannon joukkoistaminen	Mielipidevaikuttajien hyödyntäminen resilienssiajattelun levittämiseksi Konkreettiset toimittajien informointitempaukset	Suuret mediatalot (YLE, Sanoma, Alma, jne.) Perinteinen painettu media Sosiaalisen median palveluntuottajat Verkon keskustelupalstat Markkinointiyritykset Journalistiliitto
Viranomaiset ja julkiset palvelut	Hallitsematon maahanmuutto Ulkovaltiolliset toimijat Ulkomailta lähtöisin oleva kyberrikollisuus ja järjestäytyneet rikollisryhmät	Yleisen luottamuksen ja turvallisuuden tunteen edistäminen Kattavan, tarkan ja ajantasaisen tilannekuvan luominen ja välittäminen sidosryhmille Kyberrikosten tehokas tutkinta ”Valkohattuhakkerien” hyödyntäminen (tilannekuvan muodostaminen, pro bono hakkerointi, haavoittuvuuksista raportointi, jne.)	Tiedustelulaki ja sen toimeenpano Selvitys julkisten toimijoiden (valtio ja kunnat, virastot, liikelaitokset) resilienssitasosta Defensiivinen ja hyökkäävä puolustus Monialainen varautuminen kyberuhkiin Lisää resursseja talous- ja kyberrikosten tutkintaan Kansallinen ”bug bounty”	Tiedusteluviranomaiset Turvallisuusviranomaiset Huoltovarmuuskeskus Kyberturvallisuuskeskus Valtioneuvoston tilannekeskus Puolustusvoimat Poliisi, tuomioistuimet, vankeinhoitolaitos

Sidosryhmät	Keskeiset haasteet	Mahdollisuudet	Toimenpide-ehdotukset	Esimerkkejä
Regulaatiotoimijat	Liian tiukka regulaatio hidastaa yritysten ja toimialojen kehitystä Regulaatio johtaa alueellisiin ja/tai toimialakohtaisiin monopoleihin Tarve kansainväliselle regulaatiolle (normit, standardit)	Regulaatio tukee yhteiskunnan toiminta-edellytysten varmistamista myös kriisitilanteissa Ennustettavuuden ja kattavuuden lisääminen Kansallinen vastuutaho ja kestävä rahoitus	Aktiivinen osallistuminen relevantteihin kansainvälisiin verkostoihin Kansainvälisten verkostojen hyödyntäminen regulaation valmistelussa Vastuiden selkeä määrittely	Valvontaviranomaiset, kuten FICORA EU:n komissio (Connect pääosasto) Ministeriöt
	European Digital Single Market (https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market)	EU-tason harmonisointi luo pohjan yhteismarkkinan toiminnalle	Koordinoitu yritysten ja tutkimuslaitosten osallistuminen uusien työohjelmien ja hankkeiden valmisteluun	EU-komissio, EU-parlamentti, EU-neuvosto Kansainväliset verkostot, kuten EU:n ECSO ja ENISA
Valtionhallinto	EU:n horisontaalisen regulaation kommunikointi teollisuudelle ja kuluttajille on haasteellista	Kansallisten ja kansainvälisten yhteistyöverkostojen luominen ja ylläpito Keskustelukanavien avaaminen, yhteisymmärryksen ja pelisääntöjen luominen Uskottava sertifiointijärjestelmä tukee yritystoimintaa Yhteistyö tilannetiedon vaihdossa ja kokonaiskuvan muodostamisessa.	Usean maan väliset poikkeustilanteiden yhteisharjoitukset. Keskustelukanavien avaaminen, yhteisymmärrys, pelisääntöjen luominen Lisää resursseja FICORAlle sertifikaattijärjestelmien pyörittämiseen Kohdennettu kommunikointi sidosryhmille	Ministeriöt FICORA Teollisuuden järjestöt Potentiaalisiksi riskeiksi katsottavat ulkovallat ja ulkovaltiolliset toimijat Kumppaneiksi katsottavat ulkovallat
	Vaalikausien yli ulottuva, pitkäaikainen ja ennustettavissa oleva yritysten ja tutkimuslaitosten innovaatiotoiminnan rahoitus	EU-rahoituksen täydentäminen kansallisella rahoituksella	Business Finlandin ”Digital trust” -ohjelman käynnistäminen Yritysten tutustuttaminen kv. rahoitusmahdollisuuksiin, mm. kehitysaluerahoittajat ja YK:n hankinnat	Business Finland, FINNVERA Muut kansalliset rahoittajat Valtiotalouden tarkastusvirasto EU

Sidosryhmät	Keskeiset haasteet	Mahdollisuudet	Toimenpide-ehdotukset	Esimerkkejä
Kunnat, kaupungit, maakunnat, ym. alueelliset toimijat	Kuntakentän kyberalan regulaation ja ohjeistuksen puute Monimutkaisen regulaation ymmärtäminen Tarve ymmärtää mitä kybermaailma tarkoittaa paikallisemmalla tasolla, liikenne, infra, SoTe	”Älykkäät kaupungit” Paikalliset ratkaisut Alueellisen elinkeinopolitiikan vahvistaminen Paikallinen harjoitustoiminta ja koulutus	Korkealaatuiset ja (kyber) turvalliset palvelut julkisille toimijoille Kuntien/kaupunkien järjestelmien ulkopuolinen auditointi Parhaiden toimintatapojen tunnistaminen ja jakaminen Alueelliset yhteistoimintaharjoitukset	Kunnat Keskitetyt julkiset palveluorganisaatiot (Valtori, Kuntien Tiera, Palkeet, jne.)
Tutkimus	Julkisen tutkimusrahoituksen saatavuus ja ennustettavuus vaikeaa Kova kilpailu rajallisista resursseista Koulutusta jo perustasolta alkaen	Eettinen ja teknologinen edelläkävijyys Yhteiskuntarauhan turvaaminen Salaus- ja koodausosaamisen korkean tason varmistaminen	Kansainvälinen vertailu (benchmarking)	Korkeakoulut Tutkimuslaitokset Kryptograafikot
Koulutus	Miten pystytään tuottamaan oikean alan osaajia nopeasti? (esim. koodarit) Miten toteutetaan tutkintokoulutusta nopeamman syklin koulutustarjonta?	Tutkimuksen ja uuden tiedon ja vaikutuksen tutkimiseksi Informaation hyödyntämisen opettaminen ja sen analysointi Kyberkansalaistaidot	Elinkeinoelämää tukevat, muuttuvan toimintaympäristön tarpeiden mukaiset joustavat koulutuspaketit	Yliopistot, korkeakoulut, AMK:t Päiväkodit, peruskoulut, ammatillinen koulutus Kansalaisjärjestöt ja työväenopistot Puolustusvoimat (varusmies- ja reserviläiskoulutus)

Liite 4. Digitaalisen turvallisuuden tiekartta 2019–2030



Liite 5. Käynnissä olevia, digitaaliseen turvallisuuteen liittyviä hankkeita ja toimijoita

Hankkeen nimi	Kuvaus
Euroopan komission Digital Europe -aloite (2021–2027)	Tarkoituksena on kasvattaa digitalisaatiosta Euroopan kansalaisille ja yrityksille koituvia hyötyjä sekä tukea EU:n digitaalisten sisämarkkinoiden tavoitteita. http://digitaleurope.org/Welcome
Horizon Europe-puiteohjelma (2021–2027)	Eurooppalaisen innovaatioyhteistyön kytkeminen kansalliseen työhön 100+ Meur rahoitusta innovaatioyhteistyöhön https://ec.europa.eu/info/designing-next-research-and-innovation-framework-programme/what-shapes-next-framework-programme_en
ECSO (European Cyber Security Organization)	Vuonna 2016 perustettu yksityinen, voittoa tavoittelematon yritys, joka edistää kyberturvallisuuteen liittyvien hankkeiden käynnistämistä ja toteuttamista https://ecs-org.eu/
EU:n kyberturvallisuuden osaamiskeskus ja kansalliset koordinaatiokeskukset (2021–2027)	Syyskuussa 2018 tehty ehdotus EU:n kyberturvallisuuden osaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamisesta. Osaamiskeskus toimisi täytäntöönpano- ja koordinaatioelimenä unionin kyberturvallisuutta tukeville ohjelmille (Digitaalinen Eurooppa ja Euroopan horisontti). https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52018PC0630&qid=1537349553647&from=EN
Suomen tietoturvallisuusstrategia: ”Maailman luotetuinta digitaalista liiketoimintaa” (2016)	Strategian keskeiset tavoitteet: 1) Suomessa on digitaalisen liiketoiminnan kannalta kilpailukykyinen ja edistyksellinen lainsäädäntö; 2) EU:n sisämarkkinat toimivat nykyistä luotettavammin; 3) suomalaiset yritykset hyötyvät kansainvälisistä standardeista ja markkinoilla on saatavilla digitaalisia hyödykkeitä, joiden tietoturva on sisäänrakennettua; 4) tietoturvaa ja siihen liittyvää osaamista tutkitaan, mitataan, seurataan ja kehitetään; 5) Viranomaiset auttavat yhteisöjä ja kansalaisia tietoturvan parantamisessa. http://julkaisut.valtioneuvosto.fi/handle/10024/78106
Yhteiskunnan turvallisuusstrategia (2017)	Valtioneuvoston periaatepäätös, joka kuvaa kokonaisturvallisuuden yhteistoimintamallin perusperiaatteet. Ohjaa ja yhtenäistää hallinnonalojen varautumista ja antaa tietoa varautumisen perusteista myös muille toimijoille. Strategian seurantaa ja kehittämistä koordinoi Turvallisuuskomitea ministeriöiden valmiuspäällikkökokouksen kanssa. https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia-2017/

Hankkeen nimi	Kuvaus
Suomen uusi kyber-turvallisuusstrategia ja sen toimeenpano-ohjelma (2017–2020)	Kyberturvallisuusfoorumi (TK-jäsenet, yritysten toimitusjohtajat, tutkijat) 1 x vuosi Asiantuntijatason seminaarit 2 x vuosi Seurantamittaristo vuosittain Harjoitustoiminta: Järjestetyt harjoitukset: hallitus, TK, VP; KYHA, TIETO18 https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia/
Digitaalisen infra-struktuurin strategia	Strategiassa määritellään Suomelle teknologianeutraalit laajakaistatavoitteet vuodeksi 2025 sekä keinot näiden saavuttamiseksi. Strategiassa on huomioitu niin elinkeinoelämän kuin kuluttajienkin tarpeet. http://julkaisut.valtioneuvosto.fi/handle/10024/161066
Tekoälyaika-ohjelma	Kytkökset datan ja AI:n kautta kyberturvallisuuteen, luotettavuuteen ja saatavuuteen Kontaktihenkilöinä Pekka Ala-Pietilä (pj), Jussi Nissilä (TEM, pääsihteeri), Mika Klemettinen (BF, data- ja alustatalous) www.tekoalyaika.fi
Business Finland: ”Digital Trust”-innovaatio-rahoitusohjelma (2019-2023/2024)	Visiona on digitaalisten palveluiden ja ratkaisujen turvallinen kehittäminen ja käyttö, lisäksi keskeisenä teemana on digitaalinen identiteetti (sekä Suomessa että Euroopan laajuisesti) Alustava toteutusaikataulu 2019–2023 (tai 2024) ja budjetti 100 Meur (50+50 tai 100+100)
Aurora AI (VM)	Julkisten palvelujen tekoälyistäminen, keskeisinä teemoina turvallisuus, luotettavuus ja saavutettavuus. Kontaktihenkilönä Aleksi Kopponen (VM).
Sitran hankkeet	IHAN®, MyData ja palveluoperaattoritoiminta, keskeisinä teemoina turvallisuus ja luotettavuus. Kontaktihenkilönä Jaana Sinipuro (SITRA)
Huoltovarmuuskeskuksen aktiviteetit	Huoltovarmuuskeskuksen Kyber2020-ohjelma on käynnissä v. 2017–2020. Ohjelmaa toteutetaan läheisessä yhteistyössä Viestintäviraston Kyberturvallisuuskeskuksen ja kriittisestä infra-struktuurista vastaavien yritysten kanssa. Kontaktihenkilö Kalle Luukkainen (HVK).
Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma (”JUDO”)	Painopistealueet: digiturvallisuuden johtamisen ja riskienhallinnan kehittäminen, osaava henkilöstö sekä uuden teknologian hyödyntäminen palveluiden ja turvallisuuden toteuttamisessa. Digiturvallisuuden osa-alueet: riskienhallinta, tietoturvallisuus, kyberturvallisuus, toiminnan jatkuvuus (valmius-, varautumis- ja jatkuvuussuunnittelu) sekä tietosuoja https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=0b6ad318-f343-4e39-98db-b0f13fe7d498
Tampereesta turvallisuus-osaamisen keskittymä -aloite	Tampereen kaupunkiseutu haluaa profiloitua turvallisuusalan osaamiskeskittymänä. Toimijat: Business Tampere, Tampereen kauppakamari ja Itämeri-instituutti https://www.sttinfo.fi/tiedote/tehdaan-tampereen-kaupunkiseudusta-kansainvalisesti-tunnustettu-turvallisuusosaamisen-keskittyma?publisherId=54555086&releaseId=69843834
From Failand to Winland	Tutkimushanke pureutuu Suomen energia- ja ruokaturvaan yhteiskehittämisen sekä tulevaisuusskenaarioiden avulla Toimijat: Demos Helsinki, Finland Futures Research Centre, Turun yliopisto, Aalto yliopisto, Helsingin yliopisto, Itä-Suomen yliopisto, Maanpuolustuskorkeakoulu ja Suomen ympäristö-keskus https://winlandtutkimus.fi/

Hankkeen nimi	Kuvaus
JAMKin hankkeet	Mm. CyberSec4Europe, CybeRDI, CinCan (Continuous Integration for the Collaborative Analysis of Incidents), Kyberosaaminen 2020, EDA/Cyber Ranges, Tekoälyn käyttö poikkeamapohjaisten tunkeutumisten havainnointiin verkkoliikenteestä, Thematic Partnerships to Pilot Interregional Innovation Partnerships, Data-analytiikasta uutta kasvua ja liiketoimintaa ja IoT:sta liiketoimintaa FINCSC / FINCSC PLUS -sertifikaatti: JAMK /JYVSECTEC, EK, Suomen Yrittäjät, Viestintävirasto, Telia, Helsingin seudun kauppakamari, Keski-Suomen Liitto
Laurean hankkeet	Kyberuhkien torjunnan tutkimushanke (EU Horisontti 2020)
Kyberturvaaja	Kehitetään kyberturvallisuuteen liittyvää, työelämälle tarjolla olevaa koulutusta olemassa olevien tutkintokoulutusten pohjalta (työelämäkoulutuksia, ohjeita ja suosituksia, testaus- ja pilotointiympäristöjä ja osaajaverkosto). Toimijat: Tampereen AMK (koordinaattori), Metropolia AMK, Turku AMK, Oulun yliopisto ja Tampereen teknillinen yliopisto, päärahoittajana Euroopan sosiaalirahasto (ESR) http://kyberturvaaja.blogs.tamk.fi
Reaaliaikatalouden ekosysteemi (RTECO), Teknologiateollisuus	Tavoitteena on käynnistää ja viedä käytännön toteutuksiksi ekosysteemejä, jotka edistävät rakenteisen taloustiedon käsittelyä. Konkreettisesti käynnissä on kaksi hanketta: RTECO eKuitti ja RTECO eYritys. Ohjausryhmässä ovat edustettuina mm. valtiovarainministeriö, Verohallinto, Patentti- ja rekisterihallitus, Rakennusteollisuus r.y., Palvelualojen työnantajat r.y., Suomen Taloushallintoliitto r.y. ja Teknologiateollisuus r.y. https://www.teknologiateollisuus.fi//////fi/rteco

Liite 6. Listaus valmistelutyöhön osallistuneista asiantuntijoista

Kasvuohjelman valmistelutyön ohjausryhmä:

Jussi Nissilä	Työ- ja elinkeinoministeriö
Kalle Luukkainen	Huoltovarmuuskeskus
Jarkko Moilanen	Opetus- ja kulttuuriministeriö
Maija Rönkä	Liikenne- ja viestintäministeriö
Mika Klemettinen	Business Finland

Ohjausryhmä järjesti valmistelutyön aikana yhteensä 3 kokousta.

Kasvuohjelman valmistelutyön vastuuorganisaatio: DIMECC Oy

Antti Karjaluoto, DIMECC
Ülo Parts, DIMECC
Tapio Frantti, Oulun yliopisto
Risto Lehtinen, DIMECC

Kasvuohjelman valmistelutyön teematiimien vetäjät:

Markku Korkiakoski, Bittium Oyj	Osaaminen ja jatkuva oppiminen
Mika Grundström, Tampereen teknillinen yliopisto	Osaaminen ja jatkuva oppiminen
Pasi Kämppi, Laurea	Osaaminen ja jatkuva oppiminen
Petri Ahokangas, Oulun yliopisto	Kasvu ja kansainvälisyys
Milla Wirén, Turun yliopisto	Kasvu ja kansainvälisyys
Matti Mäntymäki, Turun yliopisto	Kasvu ja kansainvälisyys
Jarno Salonen, VTT	Kasvu ja kansainvälisyys
Sasu Tarkoma, Helsingin yliopisto	Elinkeinoelämän digitalisaatio
Pekka Abrahamsson, Jyväskylän yliopisto	Elinkeinoelämän digitalisaatio
Harri Happonen, Cargotec Oyj	Elinkeinoelämän digitalisaatio
Henri Paukku, Cargotec Oyj	Elinkeinoelämän digitalisaatio
Reijo Savola, VTT	Kyberresilienssi
Marko Koukka, Telia Oyj	Kyberresilienssi
Mika Karjalainen, JAMK	Kyberresilienssi

Kasvuohjelman työpajoihin ja valmistelutyöhön osallistuneet asiantuntijat:

Aapo Cederberg, Cyberwatch
Aimo Pellinen, JAMK
Alexey Kirichenko, F-Secure Oyj
Andrei Lauren, ANS Finland
Anniina Autero, Tampereen yliopisto
Antti Eskola, Työ- ja elinkeinoministeriö
Antti Ikonen, Joensuun yliopisto
Antti Kauppinen, Erillisverkot
Antti Kiuru, Nordea Oyj
Antti Nyqvist, Teknologiateollisuus
Ari Laaksonen, Rajavartiosto
Ari Pokka, Gradia
Ari Turunen, Uptopoint Oy
Bengt Sahlin, Ericsson Oyj
Danilo D´Elia, ECSO
Essi Huttu, DIMECC
Hanna Smith, Hybridikeskus
Hanna-Miina Sihvonen, Sisäministeriö
Harri Hyvönen, Sotedigi
Harri Kulmala, DIMECC
Harri Luuppala, Cysec Oy
Harri Mäntylä, Puolustusministeriö
Irina Olkkonen, Puolustusministeriö
Jaakko Wallenius, Elisa Oyj
Jan Melen, Ericsson Oyj
Jan Mickos, CGI
Jan Wirtanen, Valtori
Janne Eskola, Demola Oy
Janne Kankare, Telia Oyj
Janne Kotilahti, Valtori
Janne Kurvinen, Rajavartiosto
Jari Still, F-Secure Oyj
Jari Hautamäki, JAMK
Jari Pirhonen, Tieto Oyj

Jarkko Oksala, Tampereen kaupunki
Jarkko Saarimäki, Viestintävirasto
Jarno Lötjönen, JAMK
Jessikka Aro, Yleisradio
Johan Boije, Kone Oyj
Johanna Järvinen, Oikeusministeriö
Jouni Huotari, JAMK
Jouni Perttula, Tampereen kaupunki
Jorma Mellin, SSH Oyj
Juha Ala-Mursula, Business Oulu
Juha Huhtakangas, Valtori
Juha Kiiski, SOK
Juha Mölkänen, Nokia Oyj
Juha Nieminen, S-Pankki
Juha Remes, FISC ry
Juho Gustafsson, Poliisi
Jukka Märijärvi, TOIP Oy
Jussi Valkiainen, Kone Oyj
Jyri Rajamäki, Laurea
Jyrki Heinonen, 112
Jyrki Kaipanen, Suojelupoliisi
Jyrki Pennanen, Fingrid
Kai Valonen, Oikeusministeriö
Kaisa Olkkonen, SSH Oyj
Kim Westerlund, Nixu Oyj
Kimmo Rousku, Väestörekisterikeskus
Kirsi Kokko, Business Finland
Laura Juvonen, Teknologiateollisuus
Lauri Frank, Jyväskylän yliopisto
Lauri Karppinen, Oikeusministeriö
Maikki Sipinen, Työ- ja elinkeinoministeriö
Marja Hamilo, Teknologiateollisuus
Markku Kivistö, Business Finland
Markku Kutvonen, F-Secure Oyj
Markku Raitio, Helsingin kaupunki
Marko Komssi, F-Secure Oyj

Marko Sjöroos, Valtioneuvoston kanslia
Martti J. Lehto, Jyväskylän yliopisto
Matti Parviainen, Espoon kaupunki
Miika Valtonen, Remion Oy
Mika Susi, Elinkeinoelämän keskusliitto
Mikko Soikkeli, Puolustusvoimat
Olli Joronen, Valtori
Panu Vesterinen, Helsingin kauppakamari
Pasi Eronen, Foundation for Defence of Democracies
Pasi Hakkarainen, Kansaneläkelaitos
Pasi Paunu, Suojelupoliisi
Pasi Vilja, Konecranes Oyj
Paul Kinnunen, Liikennevirasto
Pauli Wihuri, KPMG
Pekka Ala-Pietilä, Tekoälyaika-ohjelma
Pekka Iivonen, Opetushallitus
Pekka Kuittinen, Erillisverkot
Pentti Olin, Puolustusministeriö
Petri Nykänen, Business Tampere
Petri Holopainen, Suomen Yrittäjät
Petri Kuurma, Ulkoministeriö
Petri Puhakainen, Valtioneuvoston kanslia
Pyry Heikkinen, Tulli
Raimo Kantola, Aalto yliopisto
Rami Raulas, SSH Oyj
Riikka Heikinheimo, Elinkeinoelämän keskusliitto
Roberto Cascella, ECSO
Sami Kilkkilä, Erillisverkot
Sami Suokas, Sarlin Oy
Samuli Bergström, Verohallinto
Sauli Savisalo, Huoltovarmuuskeskus
Simo Mäkipaja, Patria
Teemu Anttila, Puolustusministeriö
Terho Rintanen, JAMK
Tero Huttunen, Opetus- ja kulttuuriministeriö
Tero Kokkonen, JAMK

Tero Toiviainen, Poliisi
Tiina Nurmi, Business Finland
Timo Kekkonen, STEK ry
Timo Lankinen, Viestintävirasto
Tuomas Kokkomäki, Poliisi
Tuukka Laava, JAMK
Ville Haapakangas, TAMK
Ville Peltola, Teknologiateollisuus
Ville Valovirta, VTT

LÄHDEVIITTAUKSET

i Lehto, M., Limnéll, J. & al. "Kyberturvallisuuden strateginen johtaminen Suomessa". Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018.

ii Maailman luotetuinta digitaalista liiketoimintaa. Suomen tietoturvallisuusstrategia. Liikenne- ja viestintäministeriön julkaisuja 7/2016

iii https://www.microsoft.com/en-us/security/intelligence-report

iv World Economic Forum, "WEF Centre of Cybersecurity," https://www.weforum.org/centre-for-cybersecurity, 2018.

v https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52018PC0630&qid=1537349553647&from=EN

vi Forbes, "Cybersecurity market oulook," https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#17ca4bfd30d6 viewed on the 4th of September 2018, 2015.

vii ECSO, "Strategic research and innovation agenda," 2017.

viii VTT ja Cybercom, "Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen," Valtioneuvoston selvitys- ja tutkintatoiminta, 2016.

ix VTT ja Cybercom, "Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen," Valtioneuvoston selvitys- ja tutkintatoiminta, 2016.

x Lehto, Limnéll, Kokkomäki, Pöyhönen ja Salminen, "Kyberturvallisuuden strateginen johtanminen Suomessa," Valtioneuvoston selvitys- ja tutkimustoiminta, 2018.

xi https://www.cgi.fi/fi/lataa/kyberturvallisuuden-tila-suomessa-2018

xii D. R. Krathwohl, "A Revision of Bloom's Taxonomy: An Overview," Theory Into Practice, vol. 41, o. 4, pp. 212–218, 2002.

xiii NCSC, "National Cyber Security Agenda | NCSC," 14-May-2013. [Online]. Available: https://www.ncsc.nl/english/current-topics/national-cyber-security-agenda.html. [Accessed: 29-Nov-2018].

xiv Federal Chancellery of the Republic of Austria, "Austrian strategy for Cyber security - Digital Austria," Mar-2013. [Online]. Available: https://www.digital.austria.gv.at/austrian-strategy-for-cyber-security. [Accessed: 29-Nov-2018].

xv Agence nationale de la sécurité des systèmes d'information's, "The French national digital security strategy: meeting the security challenges of the digital world," ANSSI, Oct-2015. [Online]. Available: https://www.ssi.gouv.fr/actualite/the-french-national-digital-security-strategy-meeting-the-securitychallenges-of-the-digital-world/. [Accessed: 29-Nov-2018].

xvi Department of Home Affairs, "Australia's Cyber Security Strategy," 2016. [Online]. Available: https://cybersecuritystrategy.homeaffairs.gov.au/. [Accessed: 29-Nov-2018].

xvii White House, "The White House National Cyber Strategy: Continuity with a Hint of Hyperbole," Council on Foreign Relations, Sep-2018. [Online]. Available: https://www.cfr.org/blog/white-house-nationalcyber-strategy-continuity-hint-hyperbole. [Accessed: 29-Nov-2018].

Kasvua digitaalisesta turvallisuudesta Tiekartta 2019–2030

Digitaalisen turvallisuuden kasvun tiekartan tavoitteena on edistää digitaaliseen turvallisuuteen ja osaamiseen liittyvää yritysvetoista kehitystä, kasvua ja kansainvälistymistä yritysten, julkisen sektorin ja tutkimuslaitosten yhteistyönä.

Raportissa esitetään digitaalisen turvallisuuden alan yhteinen tavoitetila ja tulevaisuuskuva vuodelle 2030, kuvataan alan osaaminen ja toimintaympäristö, määritetään teemakohtaiset visiot vuodelle 2030 ja keskeiset välitavoitteet vuosille 2021 ja 2025.

Tiekartta voi toimia käytännön työkaluna suunniteltaessa uusia kyberturvallisuusosaamista vahvistavia politiikkatoimia ja niiden toteutusta sekä mahdollistettaessa toimijoiden kasvupolkuja esimerkiksi erilaisten ekosysteemien ja kiihdyttämöjen kautta.

Verkkojulkaisu
ISSN 1797-3562
ISBN 978-952-327-405-1

Sähköinen versio: julkaisut.valtioneuvosto.fi
Julkaisumyynti: julkaisutilaukset.valtioneuvosto.fi