VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalliselvitys

Julkisen hallinnon ICT

Valtiovarainministeriön julkaisuja – 2022:76

Valtiovarainministeriön julkaisuja 2022:76

Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalliselvitys

Valtiovarainministeriö Helsinki 2022

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Julkaisumyynti
Beställningar av publikationer

Valtioneuvoston verkkokirjakauppa

Statsrådets
nätbokhandel

vnjulkaisumyynti.fi

ISBN pdf: 978-952-367-201-7
ISSN pdf: 1797-9714

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2022

Kuvailulehti

1.12.2022

Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalliselvitys

Valtiovarainministeriön julkaisuja 2022:76		**Teema**	Julkisen hallinnon ICT
Julkaisija	Valtiovarainministeriö		
Yhteisötekijä	Valtiovarainministeriö		
Kieli	suomi	**Sivumäärä**	83

Tiivistelmä

Selvityksessä on kuvattu julkisen hallinnon digitaalisen turvallisuuden nykytila, tavoitetila sekä keskeisiä ehdotuksia ja kehittämistarpeita. Nykytilassa yhteistoimintaa rajoittavat yhteistoimintakulttuuri, rajalliset resurssit ja osaaminen, turvallisten palvelujen saatavuus, käyttöönotettavuus ja käytettävyys sekä tietojen luokitteluun, jakamiseen ja käyttöön liittyvät lainsäädännölliset ja tekniset rajoitukset.

Digitaalisen turvallisuuden yhteistoiminta edellyttää jatkossa yhä vahvempaa osaamista ja yhtenäisempiä toimintatapoja, sekä vahvempaa strategia-, normi-, resurssi- ja informaatio-ohjausta. Digitaalisen turvallisuuden keskeisten vastuiden ja yhteisten toimintamallien tulee olla velvoittavia. Digitaalisen turvallisuuden palvelujen määrittely ja kehittäminen on toteuttava yhdessä. Toimijoiden välistä keskustelua digitaalisen turvallisuuden tutkimuskohteista tulee kehittää ja tutkimustuloksia on jaettava yhteiskunnassa laajasti.

Asiasanat	julkisen hallinnon ICT, valtio työnantajana, keskustelualoitteet, lautakunnat, tietoturva, digitalisaatio, julkinen hallinto, kyberturvallisuus		
ISBN PDF	978-952-367-201-7	**ISSN PDF**	1797-9714
Julkaisun osoite	https://urn.fi/URN:ISBN:978-952-367-201-7		

Presentationsblad

1.12.2022

Utredning om samarbets- och hanteringsmodellen för digital säkerhet inom den offentliga förvaltningen

Finansministeriets publikationer 2022:76		**Tema**	Offentliga förvaltningens ICT
Utgivare	Finansministeriet		
Utarbetad av	Finansministeriet		
Språk	finska	**Sidantal**	83

Referat

I utredningen beskrivs nuläget och målbilden för digital säkerhet inom den offentliga förvaltningen. Dessutom redogörs det för centrala utvecklingsbehov och de viktigaste förslagen. I nuläget begränsas samarbetet av samarbetskulturen, begränsade resurser och begränsat kunnande, tillgången till trygga tjänster, tjänsternas användbarhet och möjligheten att använda dem samt lagstiftningsmässiga och tekniska begränsningar som gäller klassificering, utbyte och användning av uppgifter.

Samarbete inom digital säkerhet förutsätter i fortsättningen mer kunnande, enhetligare arbetssätt och starkare strategi-, norm-, resurs- och informationsstyrning. De ansvar och gemensamma handlingsmodeller som hänför sig till digital säkerhet ska vara bindande. Tjänsterna för digital säkerhet bör definieras och utvecklas tillsammans. Dialogen mellan aktörerna om forskningsobjekt som anknyter till digital säkerhet bör utvecklas och forskningsresultaten spridas brett i samhället.

Nyckelord	offentliga förvaltningens ICT, datasäkerhet, digitalisering, offentlig förvaltning, cybersäkerhet		
ISBN PDF	978-952-367-201-7	**ISSN PDF**	1797-9714
URN-adress	https://urn.fi/URN:ISBN:978-952-367-201-7		

Description sheet

1 December 2022

Report on cooperation and management models for digital security in public administration

Publications of the Ministry of Finance 2022:76		**Subject**	Public Sector ICT
Publisher	Ministry of Finance		
Group author	Ministry of Finance		
Language	Finnish	**Pages**	83

Abstract

The report describes the current state, desired state and key proposals and development needs of digital security in public administration. In the current state, cooperation is limited by the culture of cooperation, limited resources and skills, the availability, adoptability and usability of secure services, and the legislative and technical restrictions on sharing and using information.

In the future, cooperation in digital security will require stronger skills and more uniform modes of operation, as well as stronger strategic, normative, resource and information guidance. The key obligations and joint modes of operations related to digital security must be mandatory. The definition and development of digital security services must be implemented jointly. Dialogue between involved parties concerning digital security research topics should be developed and the results of research should be shared widely in society.

Keywords public sector ICT, data security, digital transformation, public administration, cyber security

ISBN PDF	978-952-367-201-7	**ISSN PDF**	1797-9714
URN address	https://urn.fi/URN:ISBN:978-952-367-201-7		

Sisältö

TIIVISTELMÄ

Toimintaympäristön muuttuminen ja digitalisaation edistyminen ovat kasvattaneet turvallisuusuhkia. Meistä kaikista on tullut digitaalisen rikollisuuden kärkikohteita. Toimintamme on alttiina digitaalisten järjestelmien, palvelujen ja tietoverkkojen globaalien toimitusketjujen haavoittuvuuksille. Digitaalisesta turvallisuudesta huolehtiminen edellyttää organisaatiossa riskienhallinnan, jatkuvuudenhallinnan, tietoturvallisuuden, kyberturvallisuuden ja tietosuojan sekä informaatioturvallisuuden toteuttamista vaatimustenmukaisesti kaikessa toiminnassa.

Julkisen hallinnon digitaalisessa turvallisuudessa keskeisiä ministeriöitä ovat valtiovarainministeriön ohella liikenne- ja viestintäministeriö, työ- ja elinkeinoministeriö, valtioneuvoston kanslia, ulkoministeriö, sisäministeriö ja puolustusministeriö. Jokaisen julkisen hallinnon organisaation tehtävänä on lakisääteisten tehtäviensä lisäksi niihin liittyvien palveluiden ja tietojen digitaalisesta turvallisuudesta huolehtiminen. Keskitettyjä poikkihallinnollisia julkisen hallinnon digitaalisen turvallisuuden tehtäviä hoitavia keskeisiä virastoja ovat Digi- ja väestötietovirasto (DVV), Liikenne- ja viestintävirasto (Traficom), Suomen Erillisverkot Oy sekä valtiotoimijoiden näkökulmasta Valtion tieto- ja viestintätekniikkakeskus (Valtori).

Selvityksessä on kuvattu julkisen hallinnon digitaalisen turvallisuuden yhteistoiminnan nykytila, tiivistelmä kansainvälisestä vertailusta ja tavoitetila. Nykytilan kuvauksessa on keskitytty laaja-alaiseen digitaalisen turvallisuuden yhteistoimintaan ja siihen liittyviin toimintamalleihin. Kuvauksessa on tunnistettu koko julkisen hallinnon kattavaa digitaalisen turvallisuuden yhteistoimintaa, valtionhallinnon, hyvinvointialueiden ja kuntien yhteistoimintaa sekä tutkimustoiminnan ja yksityissektorin kanssa toteutettavaa digitaalisen turvallisuuden yhteistoimintaa.

Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminnan kehittämiselle tuovat haasteita niin sääntelyn ja toimivallan hajautuminen usealle eri toimijalle kuin digitaalisen turvallisuuden yhteistoiminnan erilaiset toimintamallit. Digitaalisen turvallisuuden yhteistoimintaryhmiä on lukuisia ja eri tarkoituksiin on rakentunut lukuisia erilaisia yhteistoiminnan muotoja. Yhteistoiminta eri toimijoiden välillä toteutuu vain osittain. Toimintaa rajoittavat yhteistoimintakulttuuri, rajalliset resurssit ja osaaminen, turvallisten palvelujen saatavuus, käyttöönotettavuus ja käytettävyys sekä tietojen luokitteluun, jakamiseen ja käyttöön liittyvät lainsäädännölliset ja tekniset rajoitukset. Nykytilakuvauksen perusteella

muodostunut kuva julkisen hallinnon digitaalisen turvallisuuden yhteistoiminnasta tuo esiin tarpeen vahvalle tehtävien organisoinnille ja selkeyttämiselle, uudelleen resursoinnille ja voimavarojen keskittämiselle, osaamisen kehittämiselle, tiedon jakamiselle sekä yhteiselle tilannekuvalle.

Tavoitetilan kuvauksessa on tuotu esille digitaalisen turvallisuuden yhteistoiminta- ja hallintamalliin toivottuja muutoksia. Digitaalisen turvallisuuden yhteistoiminta edellyttää jatkossa yhä vahvempaa ohjausta sekä koko julkisessa hallinnossa, että hallinnon eri alueilla: ministeriöissä, valtionhallinnon toiminnallisella ja operatiivisilla tasoilla, hyvinvointialueilla ja kunnissa. Ohjausta on toteuttava strategia-, normi-, resurssi- ja informaatio-ohjauksena. Digitaalisen turvallisuuden keskeisten vastuiden ja yhteisten toimintamallien tulee olla velvoittavia. Digitaalisen turvallisuuden palvelujen määrittely ja kehittäminen on toteuttava yhdessä. Toimijoiden välistä keskustelua digitaalisen turvallisuuden tutkimuskohteista tulee kehittää sekä varmistaa tutkimukselle riittävä rahoitus. Tutkimustuloksia on jaettava yhteiskunnassa laajasti ylläpitämällä jatkuvaa ja aktiivista keskustelua digitaalisen turvallisuuden tilasta ja kehittämisestä. Digitaalisen turvallisuuden varmistaminen, välttämättömän tiedon jakaminen ja nopea poikkeamiin reagointi edellyttää osaamista ja yhtenäisempiä toimintatapoja toimijoiden välillä. Selvityksen viimeisessä luvussa on kuvattu tavoitetilakuvauksen perusteella valittuja keskeisiä ehdotuksia ja kehittämistarpeita vastuutahoineen. Ehdotusten sisällön perusteella niiden jatkovalmistelu on ohjattu linjatyöksi, osaksi Haukka-ohjelmaa tai laajimpien ehdotusten osalta arvioitaviksi digitoimistossa.

1 Johdanto

1.1 Raportin lähtökohdat

Valtioneuvosto teki 8.4.2020 periaatepäätöksen julkisen hallinnon digitaalisesta turvallisuudesta (VM 2020:23). Sen mukaan digitaalisen turvallisuuden viitekehykseen sisältyy riskienhallintaan, toiminnan jatkuvuuden hallintaan ja varautumiseen sekä kyberturvallisuuteen, tietoturvallisuuteen ja tietosuojaan liittyviä asioita. Periaatepäätöksessä on kuvattu julkisen hallinnon digitaalisen turvallisuuden kehittämisalueet ja kehittämisen periaatteet sekä keskeisiä hallinnon toimintaa ja prosesseja tukevia digitaalisen turvallisuuden palveluja.

Valtioneuvoston periaatepäätöksen 8.4.2020 linjauksia toteuttaa Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka) (VM 2020:33). Yhtenä Haukka-toimeenpanosuunnitelman tehtävänä on julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalli. Tavoitteena on, että ”Valtiovarainministeriö yhdessä muiden ministeriöiden, kuntien ja yhteisöjen kanssa toimivat julkisen hallinnon digitaalista turvallisuutta tehostavan yhteistoiminta- ja hallintamallin mukaisesti.” Valtiovarainministeriön Haukka-hankkeessa tehtävän toteuttaminen aloitetiin selvittämällä digitaalisen turvallisuuden kunta-valtio-yhteistoimintamallia. Esiselvityksen tuloksena[1] todetaan, että nykytilassa digitaalisen turvallisuuden yhteistoiminta valtion ja kuntien välillä rakentuu usealla eri tavalla ja selkeä yhteistoiminnan malli puuttuu.

Valtiovarainministeriö on asettanut 23.9.2021 Haukka-hankkeeseen kaudeksi 15.9.2021–31.12.2022 julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamallin koordinaatioryhmän. Sen tehtävänä on tuottaa esiselvityksen perusteella julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamallia koskeva selvitysraportti, joka luo perustan mahdolliselle säädösvalmistelulle. Selvityksessä huomioidaan valtioneuvoston periaatepäätösten 10.6.2021: Kyberturvallisuusstrategian kehittämisohjelman (KEHO) ja tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla (Titukri) toimenpiteet. Samoin on huomioitu EU:n direktiivi kyberturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella ja verkko- ja tietoturvadirektiivin

1 Esiselvitys Digitaalisen turvallisuuden kunta-valtio yhteistoimintamalli, valtiovarainministeriö 11.6.2021

(EU) 2016/1148 kumoamisesta, eli niin sanottu NIS2[2]. Koordinaatioryhmän jäsenet ovat liitteessä 1.

NIS2-direktiivin mukaan jäsenvaltioiden tulee määrittää yksi tai useampi valvova viranomainen, joka on vastuussa laajamittaisten kyberturvallisuushäiriöiden ja -kriisien operatiivisesta johtamisesta. Jäsenvaltioiden tulee varmistaa, että valvovilla viranomaisilla on näihin tehtäviin riittävät resurssit. Jokaisen jäsenvaltion tulee lisäksi tunnistaa valmiudet, resurssit ja prosessit, jotka voidaan käynnistää ja ottaa käyttöön direktiivin mukaisissa tilanteissa. NIS2-direktiivin kansallisen toteutuksen yhteydessä on tarkoitus tarkastella direktiiviin liittyvä julkishallinnon sektoria koskeva lainsäädäntö.

1.2 Työn toteutus ja rajaukset

Selvitys on valmisteltu julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamallin koordinaatioryhmässä. Tietohallintoneuvos Tuija Kuusisto valtiovarainministeriöstä toimi koordinaatioryhmän puheenjohtajana ja selvityksen pääkirjoittajana. Selvitys aloitettiin haastattelemalla koordinaatioryhmän jäseniä ja heidän nimeämiään henkilöitä. Haastattelijoina toimi valtiovarainministeriön Haukka-ohjelman jäseniä. Haastatteluissa kartoitettiin digitaalisen turvallisuuden valtio-hyvinvointialue-kunta-yhteistoiminnan nyky- ja tavoitetilaa sekä yhteistoiminnan toteutumisen merkittäviä haasteita. Haastattelut toteutettiin lokakuun 2021 ja helmikuun 2022 välisenä aikana. Haastatteluja oli yhteensä 26. Haastatellut organisaatiot ovat liitteenä 2.

Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamallin nyky- ja tavoitetilan kuvaukset perustuvat haastatteluihin ja koordinaatioryhmän näkemyksiin. Nykytilan kuvauksessa on keskitytty laaja-alaiseen digitaalisen turvallisuuden yhteistoimintaan ja siihen liittyviin toimintamalleihin valtionhallinnossa, hyvinvointialueilla ja kunnissa. Kuvauksessa on tunnistettu koko julkisen hallinnon kattavaa digitaalisen turvallisuuden yhteistoimintaa, valtionhallinnon yhteistoimintaa, hyvinvointialueiden yhteistoimintaa, kuntien yhteistoimintaa sekä tutkimustoiminnan ja yksityissektorin kanssa toteutettavaa digitaalisen turvallisuuden yhteistoimintaa.

Valtioneuvoston periaatepäätöksen Kyberturvallisuuden kehittämisohjelma 10.6.2021 yhtenä tehtävänä on kehittää edelleen poikkihallinnollisesti viranomaisten varautumista kyberhäiriötilanteisiin. Periaatepäätöksen toteuttaminen on aloitettu käynnistämällä selvitystyö, jossa arvioidaan viranomaisten toimintaedellytyksiä kansallisen

2 COM(2020) 823 final NIS2 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823

kyberturvallisuuden varmistamisessa, kyberrikollisuuden torjunnassa, kyberpuolustuksessa sekä nopeasti kehittyvissä yhteiskunnan kyberturvallisuutta uhkaavissa tilanteissa. Selvitystyössä otetaan huomioon kansallisen ja kansainvälisen uhkaympäristön jatkuva kehittyminen. Työn perusteella määritetään käynnistettävät toimenpiteet ja aloitetaan tarvittava säädösvalmistelu. Tässä selvitystyössä toteutetaan myös Haukka-toimeenpanosuunnitelmassa esitettyä tavoitetta määritellä operatiivisen johtamisen vastuut ja järjestelyt huomioiden viranomaisten toimivaltuudet. Titukrin yhtenä toimenpiteenä on lisäksi luoda yhtenäinen säädöspohja viranomaisten väliselle yhteistyölle tietoturvaloukkaustilanteissa (ns. kyber-PTR-valmistelu). Vuoden 2022 aikana valmistellut kyber-PTR ehdotukset ovat jo käsittelyssä eduskunnassa. KEHO- ja Titukri-tehtävien toteuttamisen johdosta operatiivisen johtamisen vastuut ja järjestelyt on rajattu tämän selvitystyön ja Haukka-ohjelman ulkopuolelle.

Selvitystyön aikana valmisteltiin digitaalisen turvallisuuden tehtäviä koskeva kansainvälinen vertailu, joka on saatavilla valtiovarainministeriön verkkosivuilla[3]. Vertailun tarkoituksena oli selvittää, miten verrokkivaltioissa on organisoitu digitaaliseen turvallisuuteen liittyviä toiminnallisen tason keskitettyjä tehtäviä. Verrokkivaltiot olivat Alankomaat, Australia, Iso-Britannia, Israel, Ruotsi, Saksa, Venäjä ja Viro. Vertailu perustui julkisesti saatavilla oleviin kirjallisiin lähteisiin. Vertailussa käsiteltiin organisaatioita, joilla on sektorikohtaisia vastuita laajempia digitaalisen turvallisuuden toiminnallisen tason tehtäviä.

Selvityksen viimeisenä tehtävänä koordinaatioryhmässä valmisteltiin merkittävimmät kehittämistoimenpiteet. Selvitysraportti oli julkisesti lausuttavana lausuntopalvelussa 4.5.–3.6.2022 välisenä aikana. Koordinaatioryhmä viimeisteli selvityksen lausuntopalautteiden perusteella.

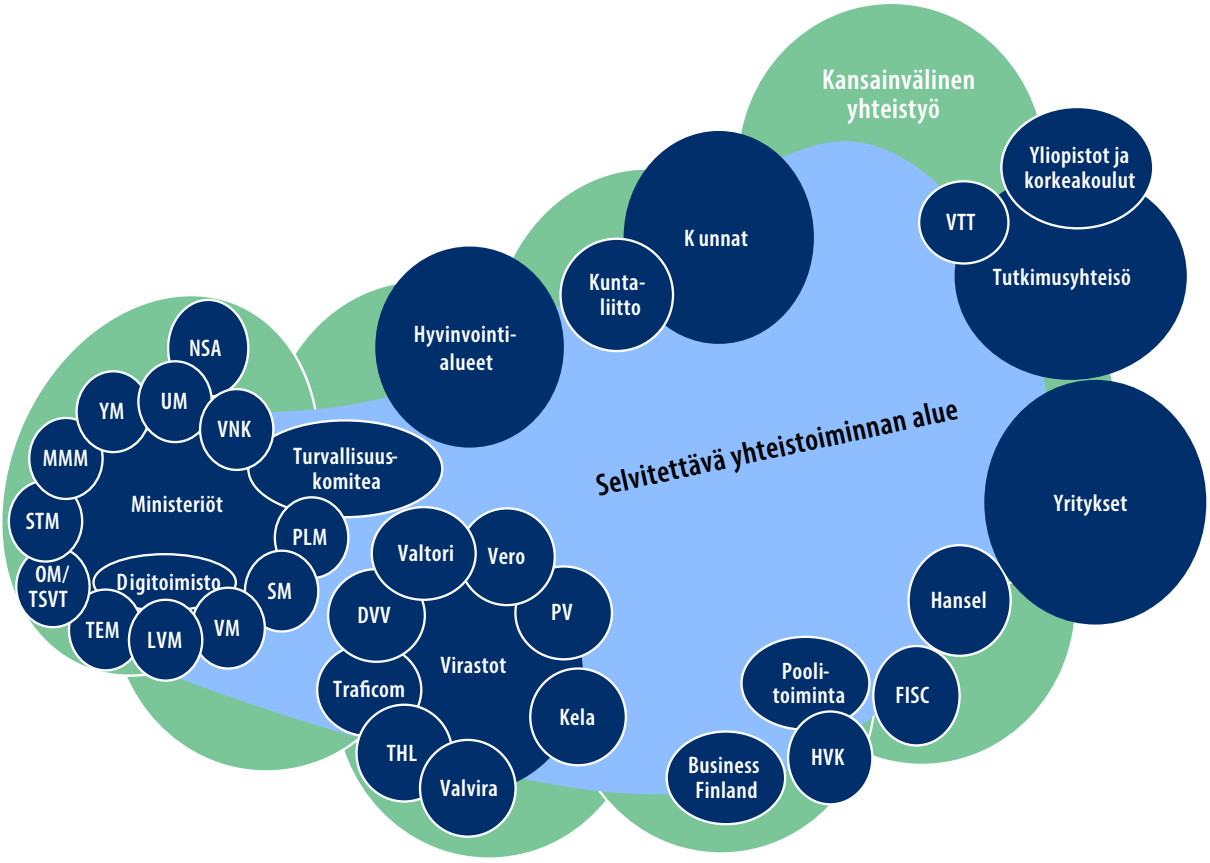
3 Digitaalisen turvallisuuden yhteistoiminta- ja hallintamallien kansainvälinen vertailu, valtiovarainministeriö 25.4.2022

2 Nykytilan kuvaus

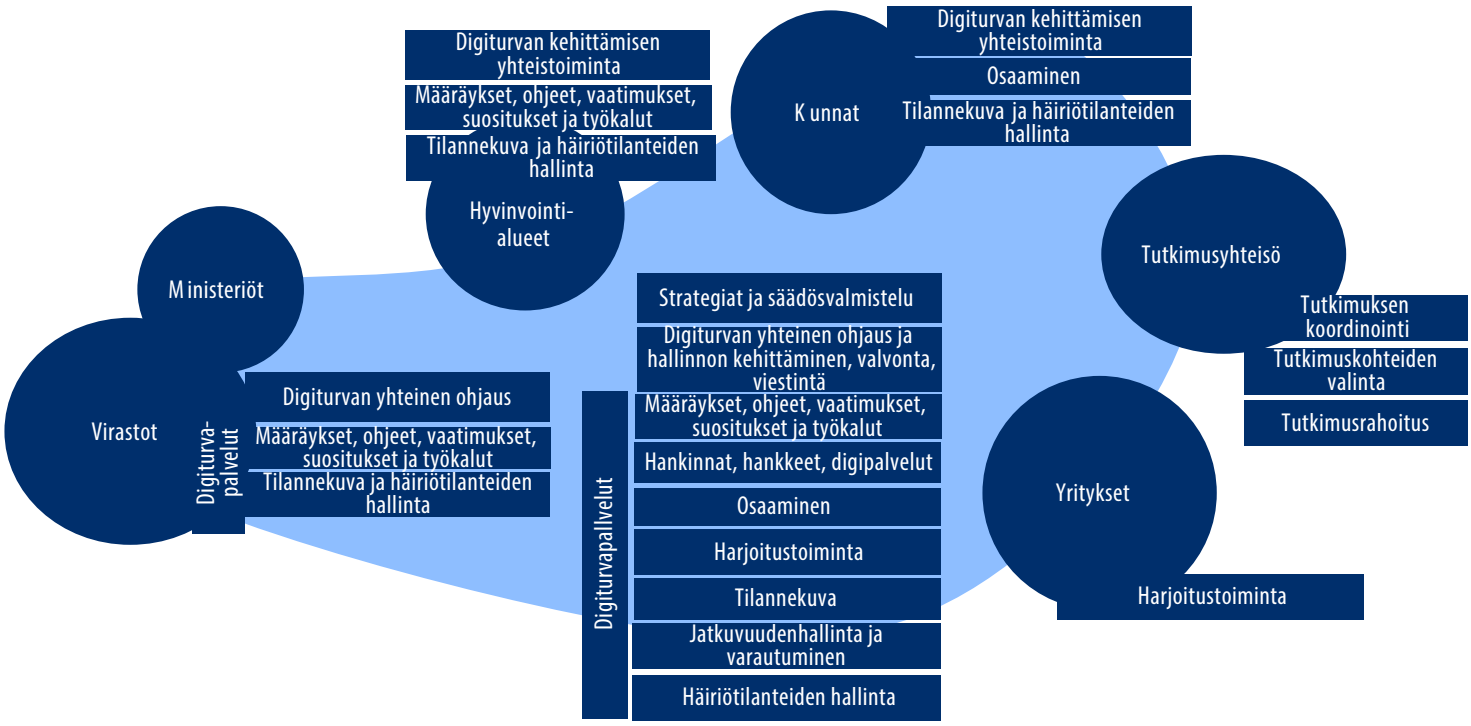
2.1 Julkisen hallinnon laaja-alainen digitaalisen turvallisuuden yhteistoiminta

Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminnan nykytilan kuvaus valtionhallinnossa, hyvinvointialueilla ja kunnissa pyrkii kattamaan eri toimijoiden laajoihin yhteistoiminnan tehtäväkenttiin liittyvät digitaalisen turvallisuuden kokonaisuudet. Tätä on havainnollistettu kuvassa 1.

Kuva 1. Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminnan kokonaisuus.



Kuva 2. Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta-alueet/teemat.



Yhteistoiminnan hallinnan parantamisen tavoitteena on löytää kustannustehokkaita ratkaisuja riittävän digitaalisen turvallisuuden ylläpitämiseksi julkisessa hallinnossa. Yhteistoiminnan ja sen hallinnan jäsentämiseksi on nykytilasta tunnistettu sellaisia yhteistoiminnan osa-alueita ja teemoja, joilla tapahtuvaa yhteistoiminnan hallintaa olisi mahdollista yhtenäistää eri toimijoiden kesken. Kuvaan 2 on kirjattu tunnistetut julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta-alueet ja teemat.

Taulukossa 1 on kuvattu tunnistettuihin yhteistoiminta-alueisiin liittyvät nykytilaa koskevat havainnot. Nykytilan kartoituksen yhteydessä havaittiin, että julkisen hallinnon digitaalisen turvallisuuden yhteistoiminnan kehittämiselle tuovat haasteita niin sääntelyn ja toimivallan hajautuminen usealle eri toimijalle kuin digitaalisen turvallisuuden yhteistoiminnan erilaiset toimintamallit. Yhteistoimintaa toteutetaan eri hallinnonaloilla ja maantieteellisillä alueilla sekä digitaalisen turvallisuuden eri osa-alueilla laajuudeltaan ja sisällöltään vaihtelevasti ja eri muodoissa. Digitaalisen turvallisuuden yhteistoimintaryhmiä on lukuisia, ja eri tarkoituksiin on rakentunut lukuisia erilaisia yhteistoiminnan muotoja. Yhteistoiminta eri toimijoiden välillä toteutuu vain osittaisena. Toimintaa rajoittavat yhteistoimintakulttuuri, rajalliset resurssit ja osaaminen, turvallisten palvelujen saatavuus, käyttöönotettavuus ja käytettävyys sekä tietojen luokitteluun, jakamiseen ja käyttöön liittyvät

lainsäädännölliset ja tekniset rajoitukset. Kaikki virastot ovat keskenään erilaisia ja eri kokoisia, joten suuremmilla virastoilla on usein enemmän resursseja käytettävissään kuin pienemmillä.

Julkisen hallinnon digitaalisen turvallisuuden ja siihen liittyvien säädösten ohjausta ja valvontaa on edelleen syytä selkeyttää. Tällä hetkellä ohjaus- ja valvontatehtäviä hoitavat valtiovarainministeriö (JulkICT-osasto) ja sen yhteydessä toimiva tiedonhallintalautakunta. Ohjauksen ja valvonnan tueksi sekä julkisen hallinnon digitaalisen turvallisuuden edistämiseksi on perustettu VAHTI-verkosto, jota ylläpitää nykyisin Digi- ja väestötietovirasto (DVV). Verkosto on julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja keskeisten palveluiden tuottamisesta vastaavien organisaatioiden laajapohjainen yhteistyö-, valmistelu- ja koordinaatioelin[4]. Lisäksi DVV kehittää ja tarjoaa erilaisia julkisen hallinnon digitaalisen turvallisuuden kehittämistä tukevia palveluja ja tuotteita valtiovarainministeriön ohjaamissa kehittämisohjelmissa, joista esimerkkinä on Haukka-ohjelma.

Liikenne- ja viestintävirasto (Traficom) ja virastoon sijoitettu Kyberturvallisuuskeskus (KTK) vastaavat valtiohallinnon turvallisuusluokitellun tiedonkäsittelyyn tarkoitettujen tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista ja hyväksynnästä. KTK tarjoaa arviointipalvelua viranomaisen määräämisvallassa oleville tai hankittavaksi suunnittelemille tietojärjestelmille, joista viranomainen on tehnyt sille arviointipyynnön. Lisäksi se tarjoaa arviointipalvelua erikseen valtiovarainministeriön pyynnöstä tehtäviin selvityksiin valtionhallinnon viranomaisen määräämisvallassa olevan tietojärjestelmän tai tietoliikennejärjestelyn yleisestä tietoturvallisuuden tasosta. Keskus tarjoaa tietoturvaneuvontaa valtionhallinnolle sekä huoltovarmuuskriittisille toimijoille sekä tuottaa ohjeita ja oppaita yleisesti käytettäväksi organisaatioissa. DVV:n tavoin KTK:kin kehittää ja tarjoaa erilaisia julkisen hallinnon digitaalisen turvallisuuden kehittämistä tukevia palveluja ja tuotteita valtiovarainministeriön ohjaamissa kehittämisohjelmissa, kuten esimerkiksi Haukka-ohjelmassa.

KTK kehittää ja tarjoaa erilaisia palveluja ja tuotteita huoltovarmuuskriittisille toimijoille Huoltovarmuuskeskuksen (HVK) kehittämisohjelmissa ja rahoittamana. Monet näistä huoltovarmuuskriittisille toimijoille tarjotuista ja kehitetyistä palveluista ja tuotteista ovat julkisesti saatavilla ja siten myös muiden kuin huoltovarmuuskriittisten toimijoiden hyödynnettävissä. Suomen Erillisverkot Oy, Valtion tieto- ja viestintätekniikkakeskus (Valtori), DigiFinland Oy, Kuntien Tiera Oy, Istekki Oy ja muut kuntien, kuntayhtymien ja hyvinvointialueiden omistamat ICT-yhtiöt tarjoavat keskitetysti ICT-palveluja, mukaan lukien ICT-laitteita, valtiohallinnon toimijoille, kunnille ja sairaanhoitopiireille sekä jatkossa hyvinvointialueille.

4 https://dvv.fi/vahti

Taulukko 1. Julkisen hallinnon digitaalisen turvallisuuden tunnistetut yhteistoiminta-alueet sekä niihin liittyvät nykytilaa koskevat havainnot

Yhteistoiminta-alue/teema	Koordinaatioryhmän näkemys nykytilasta
Digitaalisen turvallisuuden strategiat ja säädösvalmistelu	Digitaalisen turvallisuuden näkökulmia on sisällytetty moniin eri strategioihin, valtioneuvoston periaatepäätöksiin ja kehittämisohjelmiin, joiden valmistelusta ja esittelystä vastaavat useat eri ministeriöt. Keskeisiä digitaalisen turvallisuuden asioita käsitteleviä strategioita ovat Yhteiskunnan turvallisuusstrategia ja Kyberturvallisuusstrategia. Ne ovat Turvallisuuskomitean valmistelemia. Lisäksi digitaalisen turvallisuuden asioita käsitellään 8.4.2020 annetussa valtioneuvoston periaatepäätöksessä julkisen hallinnon digitaalisesta turvallisuudesta, 10.6.2021 annetuissa päätöksissä kyberturvallisuuden kehittämisohjelmasta (KEHO) sekä tietoturvan ja tietosuojan parantamisesta yhteiskunnan kriittisillä toimialoilla (Titukri). Sisäministeriön koordinoimaan Suomen kansalliseen riskiarvioon sisältyy digitaalisen turvallisuuden riskien arviointia. Julkisen hallinnon digitaalista turvallisuutta ohjaavat useat säädökset, ohjeet ja suositukset. Niiden valmistelusta vastaavat useat eri ministeriöt ja virastot. Valmistelun aikaista eri toimijoiden välistä yhteistyötä ei ole aina pidetty riittävänä. Yleislakien lisäksi julkisen hallinnon toimijoiden tulee huomioida myös toimintaan vaikuttavat monet sektorikohtaiset säädökset, ohjeet ja suositukset. Digitaalisen turvallisuuden ja siihen läheisesti liittyvien käsitteiden, kuten kyberturvallisuus ja tietoturvallisuus, merkityksestä ja käsitehierarkiasta puuttuu yhteinen ymmärrys. Säädökset eivät tunne termiä digitaalinen turvallisuus. Säädöksissä käytetään samoista tai samankaltaisista asioista eri termejä, kuten tiedonhallintayksikkö ja rekisterinpitäjä. Yhteinen käsitteistö on välttämätön sekä eri toimijoiden strategia-asiakirjojen valmistelua että erityisesti digitaalista turvallisuutta koskevien toimintapolitiikkojen ja säädösten valmistelua varten. Valtioneuvosto asetti 2.9.2021 uuden ministerityöryhmän ohjaamaan digitalisaation, datatalouden ja julkisen hallinnon kehittämistä sekä koordinoimaan näihin liittyviä toimenpiteitä ja tilannekuvaa (DDH).[5] Ryhmä jatkaa julkisen hallinnon uudistamisen poliittiselle johtoryhmälle asetettujen tehtävien edistämistä. Ryhmä sovittaa yhteen kehittämishankkeita ja tekee tarvittavia poliittisia linjauksia keskeisistä toimialansa kehittämiseen liittyvistä toimista. Ministerityöryhmän vastuulle annettiin 10.3.2022 myös kyberturvallisuuden ja julkisen hallinnon varautumisen ohjaaminen.[6] Ryhmä tekee tarvittavat poliittiset linjaukset toimista, joilla taataan yhteiskunnan toimintakyky ja digitaalinen toimintaympäristö kyberhäiriöissä ja kybervaikuttamisessa. Se tekee myös päätökset julkisen hallinnon varautumisesta turvallisuuspoliittisen tilanteen muutoksessa, joka johtuu Venäjän hyökkäyksestä Ukrainaan. Samassa yhteydessä selkeytettiin kyberturvallisuuden johtamista: • Kyberturvallisuuden johtamisen ylimmän tason muodostaa valtioneuvosto. • Yhdistetyn kyberturvallisuuden tilannekuvan tuottamisesta ja ylläpitämisestä vastaa Liikenne- ja viestintäviraston Kyberturvallisuuskeskus. Liikenne- ja viestintäministeriöön sijoitetun kyberturvallisuusjohtajan tehtävänä on välittää tietoa kyberturvallisuuden ajantasaisesta tilanteesta, kytkeä yhteen kyberturvallisuuden eri toimijoita sekä tulkita ja analysoida tietoa kyberturvallisuuden tilannekuvasta päättäjille, medialle ja muille toimijoille. Tällä toiminnalla luodaan tietoa päätöksenteon pohjaksi ja lisätään kyberturvallisuuden ymmärrystä. • Normaalitilanteessa kyberturvallisuusjohtaja tukee julkisen hallinnon digitaalisen turvallisuuden hallintaa. Vakavassa kyberhäiriötilanteessa liikenne- ja viestintäministeriö koordinoi kyberturvallisuusjohtajan rinnalla tarpeen mukaan niitä ministeriöitä, joita asia koskee.

5 https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f80751b54

6 https://www.lvm.fi/-/ministerityoryhma-vastaamaan-kyberturvallisuudesta-ja-julkisen-hallinnon-varautumisesta-1684814

Yhteistoiminta-alue/teema	Koordinaatioryhmän näkemys nykytilasta
	Valtioneuvoston asettaman ministerityöryhmän yhteyteen perustettiin digitalisaation ja datatalouden vastuualuetta koskeva yhteistyöryhmä eli Digitoimisto. Digitoimisto on pysyvä yhteistyöryhmä, jonka tehtävänä on vahvistaa ministeriöiden välistä yhteistyötä, koordinaatiota ja tiedonkulkua digitalisaatiossa ja datataloudessa. Digitoimisto tukee työllään digitalisaation, datatalouden ja julkisen hallinnon kehittämisen sekä kyberturvallisuuden ja julkisen hallinnon varautumisen ohjaamisen ministerityöryhmän toimintaa. Siten digitoimiston tehtäviin liittyy myös julkisen hallinnon digitaalisen turvallisuuden kehittäminen. Digitoimisto ylläpitää digi-, data- ja tietopolitiikan tilannekuvaa eli digisalkkua. Tavoitteena on, että liikenne- ja viestintäministeriön, valtiovarainministeriön ja työ- ja elinkeinoministeriön digitalisaation ja datatalouden kehittämisen toimet muodostavat yhtenäisen kokonaisuuden ja jaetun tilannekuvan. Tämä auttaa priorisoimaan hankkeita ja lisää Suomen vaikuttavuutta EU-tasolla. Julkisen hallinnon digitaalisen turvallisuuden kehittäminen on organisoitu hankkeisiin, joita ovat KEHO, Titukri, julkisen hallinnon digitaalisen turvallisuuden Haukka-ohjelma ja Huoltovarmuuskeskuksen Digitaalinen turvallisuus 2030 -ohjelma. Näissä on kuvattu laajasti toimenpiteitä ja tehtäviä seuraaviksi vuosiksi. Kehittämisohjelmissa määritettyjen tehtävien toteuttamisessa voi tulla vastaan toimivaltakysymyksiä, jotka rajoittavat tehtävien toteuttamista merkittävästi. Hankkeiden lisäksi viranomaiset toteuttavat lakisääteisiä digitaalisen turvallisuuden tehtäviä normaalioloissa ja häiriötilanteissa. Yksi keskeinen digitaalisen turvallisuuden säädös on laki julkisen hallinnon tiedonhallinnasta (906/2019, jatkossa tiedonhallintalaki). Sen mukaan tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Siten kunkin tiedonhallintoyksikön tehtävänä on tietoturvallisuuden ja sen hallinnan kehittäminen.
Digitaalisen turvallisuuden yhteinen informaatio-ohjaus ja hallinnon kehittäminen, valvonta ja viestintä	Julkisen hallinnon digitaalisen turvallisuuden kehittämistä koordinoidaan valtiovarainministeriön kaudelle 2020–2024 asettamassa digitaalisen turvallisuuden strategisessa johtoryhmässä sekä DVV:n kaudelle 2020–2024 asettamassa VAHTI-johtoryhmässä. Digitaalisen turvallisuuden strategisen johtoryhmän puheenjohtajana on valtiovarainministeriön alivaltiosihteeri ja jäseninä on ministeriöiden ylintä- ja keskijohtoa, DVV:n pääjohtaja, Vantaan kaupunginjohtaja, Kuntaliiton, yliopistojen, Huoltovarmuuskeskuksen ja Turvallisuuskomitean edustajat sekä kyberturvallisuusjohtaja. Johtoryhmä on kokoontunut säännöllisesti ja sen kokousten aineisto on julkaistu hankeikkunassa (VM025:00/2020). VAHTI on julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja keskeisten palveluiden tuottamisesta vastaavien organisaatioiden laajapohjainen yhteistyö-, valmistelu- ja koordinaatioelin. VAHTI-johtoryhmässä on noin 70 jäsentä ja varajäsentä julkisen hallinnon virastoista, korkeakouluista ja keskeisistä sidosryhmistä. VAHTI-asiantuntijaverkostoihin osallistuu lisäksi satoja henkilöitä julkisesta hallinnosta, korkeakouluista ja sidosryhmistä. Tiedonhallintalain nojalla on valtiovarainministeriön yhteyteen perustettu tiedonhallintalautakunta. Se arvioi valtion ja kuntien viranomaisten tiedonhallinnan toteuttamista sekä edistää tiedonhallinnan ja tietoturvallisuuden menettelytapojen toteuttamista. Sen tehtävänä on edistää tiedonhallintalaissa säädettyjen tiedonhallinnan ja tietoturvallisuuden menettelytapojen ja tiedonhallintalain vaatimusten toteuttamista. Lautakunta on kokoontunut säännöllisesti ja julkaissut mm. asiakirjojen ja tiedon turvallista käsittelyä tukevaa ohjeistusta. Tiedonhallintalautakunnan pääsihteerinä ja sihteereinä toimivat valtiovarainministeriön määräämät valtiovarainministeriön virkamiehet. Tiedonhallintalautakunnan toteuttama informaatio-ohjaus tapahtuu käytännössä lautakunnan asettamissa väliaikaisissa jaostoissa. Niiden jäseninä toimii kunkin jaoston tehtäväalueen asiantuntijoita. Tiedonhallintalautakunnan toiminnalta toivotaan vahvempaa roolia digitalisaatioon liittyvän teknologisen kehityksen ja sen mahdollisuuksiin tarttumisen mahdollistajana. Nykytilassa tiedonhallintayksiköt joutuvat yksin harkitsemaan soveltuvan riskitason ja teknologioiden tarjoamat hyödyntämismahdollisuudet tietoturvan toteuttamisessa. Tämä on voinut vaikuttaa varovaiseen teknologioiden hyödyntämiseen.

Yhteistoiminta-alue/teema	Koordinaatioryhmän näkemys nykytilasta
	Kuntakentässä haasteeksi onkin noussut hankkeitten tuotosten ja hyvien käytäntöjen jalkauttaminen organisaatioissa. Tiedonhallintayksiköitä on kuntakentässä noin 420, ja ne ovat sekä rakenteeltaan että resursseiltaan erilaisia toiminnallisia kokonaisuuksia. Tiedonhallintamalli on tiedonhallintalain määrittelemä päivittyvä nykytilakuvaus. Tiedonhallintalaki velvoittaa tiedonhallintayksiköitä viranomaisina kuvaamaan toimintaansa ja toimintaympäristöään mallin avulla kuvaamalla ja esittämällä toimintaprosessien, tietoaineistojen, tietovarantojen, tietojärjestelmien sekä tietojärjestelmien tietoturvallisuuskäytäntöjen välisiä suhteita ja riippuvuuksia. Kuntakenttää kokonaisuutena tarkasteltaessa tämä työ on kesken. Koko kuntakenttää tarkasteltaessa on tarkentamatta lisäksi se, miten digitaalisen turvallisuuden vastuuhenkilöt osallistuvat tiedonhallintayksikkötyöhön muuten kuin erityisasiantuntijoina. Toiminta ja käytössä olevat resurssit kohdennetaan arjen tekemiseen, mutta erilaisista lähtökohdista aloittavat kuntatoimijat ovat eri tasoilla. Puolustusvoimilla on kokonaisvaltainen kyberpuolustuskyky lakisääteisiä tehtäviään varten osana yhteiskunnan elintärkeiden toimintojen turvaamista. Kyberpuolustuksella tarkoitetaan digitaalisen turvallisuuden maanpuolustuksellista osa-aluetta, joka muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä. Kyberpuolustuksen suorituskyvyillä tuotetaan tiedustelutietoa valtionjohdon ja puolustusvoimien johdon päätöksenteon tueksi sekä tuetaan puolustusvoimien operaatioita suojaamalla oman päätöksenteon edellytykset. Maa- ja metsätalousministeriön hallinnonalalla Ruokavirasto tekee EU:n maatalouden ohjaus- ja tukivarojen kansallisessa hallinnoinnissa yhteistyötä kuntien muodostamien yhteistoiminta-alueiden kanssa (maksajavirastotoiminta). Maksajavirastotoimijoiden tietoturvallisuutta hallitaan yhteisen ISO/IEC 27001 -standardiin perustuvan hallintajärjestelmän avulla, keskinäisellä yhteistyöllä, johon sisältyy yhteisiä koulutuksia, tietoturvatyöpajoja ja auditointeja sekä yhteiseen käyttöön sovitettuja työkaluja. Sosiaali- ja terveysministeriön tehtäviin kuuluu hallinnonalan virastojen ja laitosten ohjauksen lisäksi yksityisten palveluntuottajien ohjaus. Ministeriön toteuttamassa digitaalisen turvallisuuden ohjauksessa on siten huomioitava sekä valtiovarainministeriöstä että liikenne- ja viestintäministeriöstä annetut ohjeet ja kehittämishankkeet. Ne ovat ajoittain olleet päällekkäisiä tai keskenään kilpailevia. Sosiaali- ja terveysministeriön hallinnonala, kuntien ja kuntayhtymien omistamat yhtiöt ja Huoltovarmuuskeskus tekivät yhteistyötä Kyber-terveys-hankkeessa, jossa käsiteltiin erityisesti huolto- ja toimintavarmuutta erilaisissa häiriötilanteissa, tehtiin yhteisiä uhka-arvioita ja turvallisuushankintoja sekä järjestettiin koulutusta. Julkisen hallinnon digitaalisen turvallisuuden kehittämisen yhteistoimintaa toteutuu myös KEHOn, Titukrin, Digitaalinen turvallisuus 2030 (DT2030) ja Haukan toimeenpanon työryhmissä. Työryhmien haasteena on ollut jäsenten sitoutuminen poikkihallinnolliseen työhön sekä jatkuva uudelleenorganisoituminen ryhmiä perustettaessa. Vastaavasti kuntien välistä digitaalisen turvallisuuden kehittämisen yhteystoimintaa on toteutettu Kuntaliiton järjestämässä kuntien tietoturvan verkostoitumistyössä, joka on tukenut kuntien onnistumista tietoturvan toteuttamisessa. Yhteiset harjoitukset, kuten TIETO-, KYHA- ja TAISTO-harjoitukset, ovat hyviä esimerkkejä laajasti vaikuttavasta yhteistyöstä. Ministeriöiden välisessä toimivallanjaossa valtiovarainministeriön toimialaan kuuluvat julkisen hallinnon tiedonhallinnan yleiset perusteet, mikä sisältää myös tietoturvallisuuden. Valtioneuvoston kanslian toimialaan puolestaan kuuluvat valtioneuvoston yhteinen tilannekuva, varautuminen ja turvallisuus, häiriötilanteiden hallinnan yleinen yhteensovittaminen sekä ministeriöiden yhteinen tietohallinto. Kukin ministeriö käsittelee oman toimialansa tietohallintoasiat. Julkisessa hallinnossa on toimialakohtaisen lainsäädäntöön perustuvia tietoturvallisuuden sektorikohtaisia valvontaviranomaisia, kuten Valvira. Lisäksi yksityisellä sektorilla on sektorikohtaisia valvontaviranomaisia (esimerkiksi ns. NIS-viranomaiset) sekä Liikenne- ja viestintävirasto NIS-direktiiviä koordinoivana viranomaisena.

Yhteistoiminta-alue/teema	Koordinaatioryhmän näkemys nykytilasta
	Kansainvälisten tietoturvallisuusvelvoitteiden toimivaltaisia ovat ulkoministeriö, puolustusministeriö, pääesikunta, suojelupoliisi ja Liikenne- ja viestintävirasto, jolla on tehtävinä myös tietoturvallisuuden arviointi sekä arviointilaitosten hyväksyminen. Turvallisuusselvityksissä toimivaltaisia ovat suojelupoliisi ja pääesikunta sekä Liikenne- ja viestintävirasto, joka laatii yritysturvallisuusselvityksen osana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen. Valtiovarainministeriö vastaa hallinnon yhteisten tieto- ja viestintäteknisten palvelujen sekä hallinnon yhteisten sähköisen asioinnin tukipalvelujen yleishallinnollisesta, strategisesta, taloudellisesta ja tieto- ja viestintäteknisen varautumisen ja valmiuden sekä turvallisuuden ohjauksesta. Lisäksi valtiovarainministeriölle on säädetty erikseen turvallisuusverkon valvontatehtävä. Valtiovarainministeriö vastaa myös Valtorin strategisesta ohjauksesta, tieto- ja viestintäteknisen varautumisen, valmiuden ja turvallisuuden ohjauksesta sekä liiketoiminnallisten periaatteiden ohjauksesta. Tietosuojan valvontaviranomainen on tietosuojavaltuutetun toimisto.
Yhteiset määräykset, ohjeet, vaatimukset, suositukset ja työkalut	Digitaaliseen turvallisuuteen liittyvät määräykset, ohjeet, vaatimukset ja suositukset muodostavat laajan kokonaisuuden. Tiedonhallintalautakunnan jaostot laativat ja ylläpitävät tiedonhallintalaissa säädettyjen vaatimusten toteuttamista koskevia julkisen hallinnon toimijoille tarkoitettuja suosituksia, jotka on julkaistu valtiovarainministeriön julkaisusarjassa ja joiden tarkoituksena on auttaa tiedonhallintayksiköitä täyttämään tiedonhallintalaissa asetettuja vaatimuksia. Suositukset eivät ole sitovia. Ministeriöt ja virastot antavat julkisen hallinnon toimijoita koskevia sitovia toimialakohtaisia digitaalisen turvallisuuden määräyksiä ja ohjeita sekä ohjeita ja suosituksia, jotka eivät ole sitovia. VAHTI-asiantuntijaverkostossa tuotetaan digitaalisen turvallisuuden hyvät käytänteet -tukimateriaaleja. Aikaisemmin VAHTI tuotti julkisen hallinnon toimijoita koskevia VAHTI-ohjeita, jotka eivät ole sitovia ja joita voi edelleen hyödyntää soveltaen ottaen huomioon muun muassa muuttunut lainsäädäntö. Myös muut viranomaiset, kuten DVV ja KTK tuottavat julkisen hallinnon toimijoita koskevia ohjeita, tukimateriaalia ja työkaluja. Digitaaliseen turvallisuuteen liittyviä erilaisia määräyksiä, ohjeita, vaatimuksia, suosituksia ja työkaluja on paljon ja niissä on tunnistettu ristiriitaisuuksia ja päällekkäisyyksiä. Esimerkiksi hyvinvointialueet ja kunnat vastaanottavat usealta ministeriöltä ja virastolta ohjeistusta, jossa sivutaan digitaalisen turvallisuuden osa-alueita, mutta koottu ja koordinoitu tiedottaminen määräyksistä, ohjeista, vaatimuksista ja suosituksista on jäänyt vajavaiseksi. Käytännön työssä erityisesti tietosuojanäkökulmasta on kuitenkin näkynyt positiivisesti VAHTI-työryhmän tekemä työ ja tiedottaminen. Kokonaiskuvan saaminen määräyksistä, ohjeista, vaatimuksista ja suosituksista on vaikeaa ja lopputulos jää pitkälti yksittäisten asiantuntijoiden ja näiden omassa organisaatiossaan tekemän tiedottamisen varaan. Kokonaiskuvaa tulisi ehdottomasti kyetä konsolidoimaan. Ohjeistuksesta ei useimmiten myöskään käy ilmi, onko se julkisen hallinnon toimijaa sitovaa, vai julkisen hallinnon toimijan tueksi tarkoitettua ohjeistusta, jota toimija voi haluamallaan tavalla soveltaa. Nykyinen sekava tilanne johtaa epävarmuuteen siitä, toteutetaanko kaikki lainsäädännön asettamat vaatimukset ja sovelletaanko varmasti oikeita ohjeita ja vaatimuksia. Epävarmuudesta seuraa riskien lisääntyminen esimerkiksi ICT-hankkeiden viivästymisenä ja samalla kustannukset nousevat merkittävästi. Ohjeiden ja suunnitelmien toteutumista erilaisissa poikkeustilanteissa ja -tapauksissa on harjoiteltava esimerkiksi sellaista tilannetta varten, jossa palveluun tai tietojärjestelmään tulee jokin häiriö ja tiedot joudutaan palauttamaan järjestelmiin.

Yhteistoiminta-alue/teema	Koordinaatioryhmän näkemys nykytilasta
	Osa määräyksistä, ohjeista, vaatimuksista ja suosituksista perustuu edelleen liian voimakkaasti kansallisiin tai jopa toimialakohtaisiin kriteeristöihin tai käytäntöihin, joskin EU:n työlistalla on jo yhteiseurooppalaisia kriteeristöjä tukevia aloitteita. Palvelu- ja tuoteratkaisujen toimittajien näkökulmasta ristiriitainen ja kapea-alainen vaatimuskehys luo sekä kannattavuushaasteita että lisääntyviä kustannuksia hankintayksiköille. Organisaatiot tarvitsevat digitaalisen turvallisuuden kypsyyden arvioimiseksi, ylläpitämiseksi, kehittämiskohteiden määrittämiseksi ja kehittämiseksi työkaluja. Yleisesti tarjolla olevia työkaluja, jotka ottaisivat huomioon kansallisen ja toimintaa Suomessa ohjaavan EU-lainsäädännön vaatimukset, on rajoitetusti saatavilla. Yksi tällainen työkalu on KTK:n tarjoama kyberturvallisuuden arviointi- ja kehittämistyökalu Kybermittari, joka on kaikkien hyödynnettävissä. Sen käytön on kuitenkin havaittu vaativan organisaatiolta erityisosaamista, resursointia ja päättäväisyyttä hyödyntää työkalua organisaation kyvykkyyden arvioimisessa ja kehittämisessä. Vastaavasti tietosuojavaltuutetun toimisto julkaisi yhteistyössä Tietoyhteiskunnan kehittämiskeskus TIEKE ry:n tietosuojatyökalun pk-yritysten käyttöön. Vaikka Kybermittari ja tietosuojatyökalu on ensisijaisesti kehitetty huoltovarmuuskriittisille organisaatiolle ja pk-yrityksille näiden toiminnan arvioimiseksi, niitä voidaan hyödyntää myös julkisessa hallinnossa ja kuntien omistamissa yrityksissä. Hyödynnettävyyden kannalta julkisen hallinnon toimijoille tarkoitettujen työkalujen kehittäminen voi olla perusteltua, ja vähintäänkin olemassa olevien työkalujen sovellettavuutta julkisen hallinnon toimijoiden käytettäväksi tulisi selvittää. Lisäksi muiden yhteisten työkalujen kehittämistä tulisi selvittää.
Digitaalisen turvallisuuden hankinnat, hankkeet ja digipalvelut	Yhteistoiminta hankinnoissa helpottaa digitaalisen turvallisuuden palvelujen hankintaa, lisää hankintatoimen tuottavuutta ja vähentää kokonaisuudessaan hankintoihin liittyvää työmäärää. Erityisesti kaupallisiin sopimuksiin ja digitaaliselle turvallisuudelle asetettaviin vaatimuksiin liittyvä yhteistoiminta nähdään hyödylliseksi. Yhteishankinnat mahdollistavat tehokkaan keinon tehdä hankintoja ilman, että jokaisen organisaation olisi erikseen hankittava hankinta-asiakirjojen laatimista varten digitaalisen turvallisuuteen ja/tai hankintoihin liittyvää osaamista. Suuret ostovolyymit mahdollistavat lähtökohtaisesti myös hyvät hinta- ja sopimusehdot. Hansel on yhteishankintayksikkö, jonka asiakkaat voivat osallistua asiakastyöryhmissä kilpailutusten valmisteluun tai vaatimusmäärittelyyn. Vaatimusmäärittely nojaa kuitenkin edelleen liian voimakkaasti kansallisiin tai jopa toimialakohtaisiin kriteeristöihin tai käytäntöihin, joskin EU:n työlistalla onkin jo yhteiseurooppalaisia kriteeristöjä tukevia aloitteita. Pistemäinen ja ennakoimaton vaatimusmäärittely luo ratkaisujen toimittajille kannattavuushaasteita ja kasvattaa hankintayksiköiden kustannuksia. Yhteishankintoja on mahdollista tehdä myös yhteistyössä eri viranomaisten kesken. Hansel on julkaissut tiedonhallinnan ja digitaalisen turvallisuuden asiantuntijapalveluiden sekä tietoturvallisuuden arviointilaitosten arviointipalvelujen dynaamiset hankintajärjestelyt. Hanselin dynaamiset hankintajärjestelyt kattavat laaja-alaisesti digitaalisen turvallisuuden toteuttamisessa tarvittavia asiantuntijapalveluja.
Digitaalisen turvallisuuden palvelut	Julkisen hallinnon digitaalisen turvallisuuden palveluilla tarkoitetaan ihmisistä, prosesseista, tiedosta ja teknologisista ratkaisuista muodostuvaa kokonaisuutta, jonka pääasiallinen tarkoitus on organisaation toiminnan ja toimintaympäristön digitaalisen turvallisuuden varmistaminen ja mahdollistaminen tarkoituksenmukaisella tavalla. Tämä sisältää tarvittavan tuen organisaatioille palveluitten käyttämiseksi ja käyttöönottamiseksi. Julkisen hallinnon toimijat voivat hankkia palveluita, joita voivat tuottaa yksityiset yritykset, kolmannen sektorin toimijat tai julkisen hallinnon kansalliset ja kansainväliset toimijat. Kun digitaalisen turvallisuuden palvelutuotanto on yhteisesti ohjattua ja rahoitettua, puhutaan julkisen hallinnon digitaalisen turvallisuuden yhteisistä palveluista. Tällainen yhteinen palvelu on esimerkiksi TAISTO-harjoitus.

Yhteistoiminta-alue/teema	Koordinaatioryhmän näkemys nykytilasta
	Palvelualueena tai palveluna voidaan pitää myös julkisen hallinnon digitaalista turvallisuutta ohjaavien viranomaisten säädösvalmistelua, viranomaisten laatimia vaatimuksia ja suosituksia sekä viranomaisten mahdollistamia kehittämisverkostoja ja rahoitusta. Digitaalisen turvallisuuden palveluihin liittyvää olemassa olevaa yhteistoimintaa tunnistettiin yhteisiin kehittämisohjelmiin sekä useimmiten maantieteellisesti lähellä toisiaan sijaitsevien toimijoiden välillä. Palveluita kehitetään yhteistoiminnassa KEHO-, Titukri-, DT2030- ja Haukka-ohjelmien toimenpiteissä. Valtori sekä kuntien ja kuntayhtymien omistamat ICT-yhtiöt tarjoavat yhteistoiminnassa kehitettyjä digitaalisen turvallisuuden palveluita. KTK:ssa on käynnissä esiselvitys, jossa selvitetään kuntien havainnointikyvyn rakentamiseen liittyviä kysymyksiä teknologian, toimittajien, juridiikan, kunnille aiheutuvien kustannusten, aikataulun sekä palvelun mahdollisen liiketoimintamallin näkökulmista. Esiselvitys toimii alustavana toimenpidesuunnitelmana myöhemmin käynnistyvälle pilottihankkeelle. Esiselvityksen tavoitteena on selvittää, onko suunnitellun mukainen palvelu mahdollista jalkauttaa kuntiin parantamaan kuntien havainnointikykyä. Esiselvitys sekä mahdollisesti myöhemmin käynnistyvä kuntien havainnointikyvyn kehittämisen palvelun pilotointi ovat osa Haukka-ohjelmaa. KTK:ssa on lisäksi käynnissä kyberturvallisuusuhkien kartoituspalvelun ympäristön kehittäminen ja tuotantokäytön aloittaminen. Kartoituspalvelun kehittämisessä tavoitteena on tuottaa tuotantojärjestelmä ja palvelu, joka tuottaisi KTK:lle kuntien sekä kuntayhtymien julkiseen internetiin näkyvistä haavoittuvuuksista ja mahdollisista konfiguraatiovirheistä automatisoidun ja jatkuvan tilannekuvan. Hankkeen pääkokonaisuuksina ovat uhkatiedon keräämisen automatisointi, uhkatiedon sisällyttäminen KTK:n muuhun tilannetietoon, tilannekuvan muodostaminen, asiakkuudenhallinta ja kokonaisuuteen liittyvät toimintaprosessit. Palvelun hyödyntäminen kunnissa vaatii kuntaa ylläpitämään ja päivittämään omiin tietojärjestelmäympäristöihinsä liittyviä tietoja niin, että ne ovat helposti saatavilla esimerkiksi kartoitusten tekemiseksi. Kartoituksesta saatavien tulosten tulkinta ja hyödyntäminen kunnan kyberturvallisuuden kehittämisessä vaati kunnissa riittävää osaamista. Kartoituspalvelun kehittäminen on osa Haukka-ohjelmaa. Kartoituspalvelun tarjoaminen julkiselle hallinnolle sekä tuotantojärjestelmän ylläpitäminen ja kehittäminen edellyttävät tulevaisuudessa jatkuvaa rahoitusta. Kuntien ja kuntayhtymien omistamien ICT-yhtiöiden digitaalisen turvallisuuden palveluita ovat muun muassa riskienhallintaan, havainnointiin ja valvontaan sekä häiriötilanteiden hallintaan liittyvät palvelut.
Digitaalisen turvallisuuden osaaminen	Digitaalisen turvallisuuden osaaminen julkisessa hallinnossa on epäyhtenäistä.[7,8] Alan ammattilaisten osaaminen ja sijoittuminen eri organisaatioihin sekä henkilöstön ja johdon osaaminen vaihtelevat. Digitaaliseen turvallisuuteen liittyvää koulutusta on rakennettu eri kohderyhmille, joita ovat kansalaiset, julkisen hallinnon henkilöstö, digitaalisen turvallisuuden asiantuntijat ja johto. Koulutusta ja koulutukseen sopivaa materiaalia tuotetaan eri organisaatioissa. Tuotanto on kuitenkin osittain hajanaista, eikä olemassa olevia resursseja kenties käytetä täysin tarkoituksenmukaisesti tai tehokkaasti. DVV:n tuottamat digitaalisen turvallisuuden seminaarit ja koulutusmateriaalit[9] julkisen hallinnon henkilöstölle, asiantuntijoille ja johdolle koetaan hyödyllisiksi. Ammattilaisten osaamisen syventämiseen tähtäävää koulutusta ei ole riittävästi tarjolla. Yhteistoimintaa on hyödynnetty koulutusaiheiden tunnistamisessa sekä esimerkiksi eOppivassa julkaistujen materiaalien koulutusmateriaalien toteutuksessa.

7 Digiturvabarometri 10/2021

8 Organisaation digiturvakysely (8/2021)

9 https://digiturvallinenelama.fi

Yhteistoiminta-alue/teema	Koordinaatioryhmän näkemys nykytilasta
	Lisäksi organisaatioiden järjestämät asiantuntijatilaisuudet ja seminaarit ovat luonnollinen tapa kasvattaa osaamista ja luoda yhteistoimintaan tarvittavia verkostoja. Osaamisen kehittämiseksi ja tietoisuuden lisäämiseksi yhteistyö ja tiedonvaihto erilaisissa verkostoissa on tärkeää. Erityisen hyödyllisiksi on koettu digitaaliseen turvallisuuteen liittyvät julkisen hallinnon yleiseen tarpeeseen sopivat DVV:n verkkotapahtumat, ohjatut TAISTO-harjoitukset sekä itseopiskelun verkkokurssit. Ne ovat lisänneet kuntatoimijoiden digiturvaosaamista merkittävästi. Kyberturvallisuusstrategian kehittämisohjelman toimeenpanossa on menossa kyberturvallisuuden koulutus- ja opetustarjonnan nykytilan ja tarpeiden selvitys. Kehittämisohjelmassa EU:n elpymisvälineen rahoituksella kehitetään kansalaisille kyberturvallisuuden koulutuspakettia, joka tulee saataville kaikilla EU:n virallisilla kielillä. Vuodelle 2022 on päätetty luoda 2300 korkeakoulujen aloituspaikkaa, joista 40 % on tekniikan ja ICT:n koulutusohjelmissa. Uusia tekniikan koulutusvastuita myönnettiin tammikuussa sekä yliopistoille että ammattikorkeakouluille. Tämä myönteinen kehitys kohdistunee kuitenkin vain osittain digitaalisen turvallisuuden segmenttiin ja vaikuttaa parhaimmillaankin vasta vuosien kuluttua. Osaamisen kehittäminen edellyttää tutkintokoulutuksen lisäksi osaamisen kypsymistä alan asiantuntijatehtävissä. On siis välttämätöntä, että nykyisten digitaalisen turvallisuuden tehtävissä työskentelevien osaamista kehitetään edelleen yhteistyössä elinkeinoelämän toimijoiden kanssa. Aalto-yliopiston tutkijat kehittävät vuodesta 2022 alkaen kyberkoulutuspakettia kaikkiin EU-maihin. Suomi on saanut EU:n elpymisvälineestä viisi miljoonaa euroa kolmivuotiseen hankkeeseen.
Digitaalisen turvallisuuden harjoitustoiminta	Julkisen hallinnon harjoitustoiminnassa tunnistettiin eri yhteistoiminnan tasoja. Kansallisen tason harjoitustoimintaa koordinoi KTK yhdessä DVV:n ja HVK:n, huoltovarmuusorganisaation ja sen poolien kanssa. Keskeisiä harjoituksia ovat esimerkiksi DVV:n TAISTO-harjoitukset, HVK:n Digipoolin Tieto-harjoitukset sekä liikenne- ja viestintäministeriön johdolla järjestettävät kansalliset teknis-toiminnalliset kyberturvallisuusharjoitukset, jotka ovat osa KEHOa ja EU:n elvytyspakettia. Lisäksi alueellista harjoitustoimintaa koordinoi ja suunnittelee aluehallintoviranomainen yhdessä alueen kuntien kanssa. Näissä harjoituksissa painopiste on digitaalisen turvallisuuden edistämiseen sijaan lähinnä huoltovarmuuskysymyksissä. KTK tukee huoltovarmuuskriittisten organisaatioiden kyberharjoittelua viranomaispalveluna. Huoltovarmuuskriittisille organisaatiolle tarjottu harjoitusmateriaali on kaikkien organisaatioiden saatavilla ja hyödynnettävissä niiden omien harjoitusten järjestämiseksi. Harjoitusmateriaali sisältää harjoitusten järjestäjille harjoitusohjeen ja harjoitusskenaariot. Harjoitukset tukevat hyvin osaamisen kehittämistä, mutta kaikki julkisen hallinnon toimijat eivät harjoittele säännöllisesti. Esimerkiksi TAISTO-harjoituksiin osallistui vuosina 2018 ja 2019 noin 130 kuntaa, mikä tarkoittaa alle puolta kaikista kunnista. Vastaavasti valtionhallinnon organisaatioita osallistui näihin harjoituksiin 74 ja 55, kun tulosohjattuja virastoja oli samaan aikaan yli 170.[10, 11] Kyberturvallisuuden kehittämisohjelman 10.6.2021 mukaan kyberturvallisuuden harjoitustoimintaa vahvistetaan. Muun muassa valtiotoimijoiden KYHA-kyberturvallisuusharjoitusten suunnittelun ja toteuttamisen avulla on edistetty laajamittaisten kyberhäiriötilanteiden ohjaus- ja johtamismallin määrittelyä ja toteuttamista.

10 https://dvv.fi/documents/16079645/17634906/6-2020+TAISTO19+raportti.pdf

11 https://www.tutkihallintoa.fi/valtionhallinnon-abc/

Yhteistoiminta-alue/teema	Koordinaatioryhmän näkemys nykytilasta
Tilannekuva[12]	DVV on ylläpitänyt syksystä 2022 lähtien hallinnollista digitaalisen turvallisuuden tilannetta verkkopalvelussa, jossa organisaatiot arvioivat ja raportoivat hallinnollisen digitaalisen turvallisuuden tilanteensa. Palvelua kutsutaan kokonaiskuvapalveluksi ja se kuvaa sitä, miten hyvin organisaatio on tunnistanut, kuvannut ja ottanut käyttöön digitaaliseen turvallisuuteen liittyvät menettelytavat, prosessit ja ohjeet. Palvelu sisältää tietoja digitaalisen turvallisuuden tason kehityksestä, henkilö- ja taloudellisista resursseista, koulutuksesta, osaamisesta, kehittämiskohteista ja näkemyksistä riskiväittämiin. Se mahdollistaa organisaation oman tilanteen kehittymisen seurannan sekä vertailun muiden organisaatioiden tilanteeseen. Palvelu tuottaa raportteja ja seurantatietoa digitaalisen turvallisuuden kehittymisestä koko julkisessa hallinnossa. Digitaalisen turvallisuuden häiriötilanteissa valtioneuvoston kanslia tuottaa tilannekuvaa yhteiskunnasta ja tietojärjestelmien häiriöistä sekä jakaa sitä valtion johdolle ja viranomaistoimijoille yhteistyön puitteissa. Hyvinvointialueiden tai kuntien kokonaisuudesta ei ole saatavilla tilannekuvaa. Valtioneuvoston tilannekuvatiedon jakamisen periaatteet ovat osin epäselvät ja osa toimijoista kokee, etteivät ne saa kattavasti tilannekuvatietoja. Tähän vaikuttaa osittain se, että osa tilannekuvatiedosta on turvaluokiteltua tai salassa pidettävää, mikä rajoittaa tiedon jakamista organisaatioiden välillä ja jopa organisaatioiden sisällä. Erityisesti turvaluokitellun tiedon jakamiseen liittyvät rajoitukset voivat kuitenkin olla monelta osin perusteltuja. Valtioneuvoston kanslian digitaalisen turvallisuuden tilannekuva koostuu pääosin KTK:n erilaisista kansallisista ja kansainvälisistä julkisista ja ei-julkisista lähteistä sekä yhteisöjen ja muiden viranomaisten eri lähteistä keräämästä ja tuottamasta tiedosta ja materiaalista. KTK:n digitaalisen turvallisuuden tilannekuvan lisäksi huoltovarmuusorganisaation poolit keräävät ja tuottavat huoltovarmuuden tilannekuvaa, joka sisältää myös digitaalisen turvallisuuden ulottuvuuksia. Huoltovarmuuskeskus ja huoltovarmuusorganisaatio tuottavat lisäksi tilannekuvaa kyberturvallisuuden nykytilasta huoltovarmuuskriittisiltä sektoreilta. Keskusrikospoliisiin sijoitettu Poliisin kyberrikostorjuntakeskus tuottaa tilannekuvaa kyberrikollisuudesta eli tietoverkkosidonnaisista ja tietoverkkoavusteisista rikoksista sekä näihin liittyvistä ilmiöistä. Määritetyille osa-alueille kohdentuvaa tilannekuvatietoa jaetaan myös KTK:n ylläpitämissä tiedonvaihto- ja yhteistyöryhmissä (Information Sharing and Analysis Centre, ISAC), joita on perustettu eri toimialoilla toimivien organisaatioiden välisen, ennen kaikkea luottamuksellisen tiedonvaihdon lisäämiseksi. Julkisen hallinnon kannalta keskeisiä ISAC-tiedonvaihtoryhmiä ovat muun muassa valtiohallinnon ISAC, SOTE-ISAC ja vesihuollon ISAC. Kunta-alan toimijoille ollaan myös perustamassa omaa tiedonvaihto ja -yhteistyöryhmää vuosille 2022–2025. Tilannekuvatietoa on myös saatavilla KTK:n tilannekuvatuotteiden kautta. Tilannekuvatuotteet ovat suurimmaksi osaksi kaikkien käytettävissä, mutta osittain saatavuutta on rajoitettu ja kohdistettu vain tietyille ryhmille, mikä johtuu pääasiassa tuotettavan tilannekuvatiedon luokittelusta. Julkisen hallinnon toimijat ylläpitävät toimijakohtaisia, sisällöiltään vaihtelevia tilannekuvia. Toimijakohtaisten ja eri hallinnonalojen tilannekuvien muodostamisen haasteena koetaan olevan etenkin palvelukeskuksiin ja palvelutoimittajiin liittyvän tiedon kokoaminen. Lisäksi tilannekuvien päivittämisessä on tunnistettu puutteita. Tilannekuvatietoa jaetaan sidosryhmien kanssa rajatusti ja tilanteen niin edellyttäessä. Varsinainen yhteistoiminta tilannekuvan kehittämiseksi ja ylläpitämiseksi koetaan vajavaiseksi.

12 tilannekuva on ”koottu kuvaus vallitsevista olosuhteista, käsillä olevan tilanteen synnyttäneistä tapahtumista, tilannetta koskevista taustatiedoista ja tilanteen kehittymistä koskevista arvioista sekä eri toimijoiden toimintavalmiuksista” (Kokonaisturvallisuuden sanasto (TSK 50, 2017)

Yhteistoiminta-alue/teema	Koordinaatioryhmän näkemys nykytilasta
	Valtionhallinnosta puuttuu yhteinen ja hyväksytty tietojärjestelmäratkaisu, jonka avulla viranomaiset voisivat vaihtaa salassa pidettävää ja turvallisuusluokiteltua tietoa. Tilannekuvan kokoamisen prosessi koetaan yksisuuntaiseksi, eikä tarvittavaa dialogia uhkamalleista tai niiden vaikutuksista käydä. Tilannekuva ja sen kokoamiseen liittyvä yhteistyö ja tiedonjako tukisivat yhteisten hallintatoimenpiteiden määrittämistä ja keskinäisriippuvuuksien ymmärtämistä. Näin ollen esimerkiksi sidosryhmien riskienhallintatoimenpiteet olisivat yhtenäisiä. Häiriöhallinnan tilannekuvien lisäksi ylläpidetään digitaalisen turvallisuuden kehittämishankkeiden tilannetietoja. Kehitysohjelmien tilannetietojen ajantasaisuudessa on puutteita, eikä esimerkiksi digitaalisen turvallisuuden toimenpiteistä ja niiden tilanteesta ole kerätty keskitetysti tietoa yleisesti saataville. Organisaatiot hyödyntävät tilannekuvaa hyvin eri tavoin. Osassa organisaatioita on eri lähteistä kerätyn digitaalisen turvallisuuden tilannekuvan jalostamiseksi selkeät toimintamallit, joiden avulla ylin johto saa kokonaistilannekuvaa organisaation toiminnasta, jota se voi hyödyntää organisaation päätöksenteossa. Toisissa organisaatioissa digitaalisen turvallisuuden tilannekuva jää sen sijaan vain asiantuntijatason henkilöstön hyödynnettäväksi.
Digitaalisen turvallisuuteen liittyvä toiminnan jatkuvuuden hallinta ja varautuminen	Jokainen viranomainen vastaa omiin lakisääteisiin tehtäviinsä ja toimialavastuisiinsa kuuluvien yhteiskunnan elintärkeiden toimintojen kannalta tärkeiden tietojen, tietojärjestelmien, ICT-infrastruktuurin ja palveluntoimittamisen ketjujen toiminnan varmistamisesta. Vastuu yhteisistä palveluista ja infrastruktuurista on palveluiden järjestämisestä vastaavalla viranomaisella tai julkista tehtävää hoitavalla tai sen järjestämisestä vastaavalla palveluntuottajalla. Yhtenäinen tapa turvata toiminnan jatkuvuus varmistetaan normaalioloissa kunkin viranomaisen antamilla toiminnan jatkuvuuden ja digitaalisen turvallisuuden ohjeilla sekä kunkin viranomaisen laatimilla suunnitelmilla. Hallitus on 19.9.2022 esittänyt tiedonhallintalakiin seuraavan päivityksen: *”Viranomaisen on viipymättä tiedotettava sen tietoaineistoja hyödyntäville, jos sen tiedonhallintaan kohdistuu häiriö, joka estää tai uhkaa estää viranomaisen tietoaineistojen saatavuuden. Viranomaisen on tiedotettava häiriön tai sen uhkan arvioidusta kestosta, mahdollisuuksien mukaan korvaavista tavoista hyödyntää viranomaisen tietoaineistoja sekä häiriön tai uhkan päättymisestä.* *Viranomaisen digitaalisten palvelujen ja muiden sähköisten tiedonsiirtomenetelmien käyttökatkoista tiedottamisesta yleisölle säädetään digitaalisten palvelujen tarjoamisesta annetun lain (306/2019) 4 §:n 2 momentissa.* *Tiedonhallintayksikön on selvitettävä sen tietoaineistojen käsittelyn, tietojärjestelmien hyödyntämisen sekä niihin perustuvan toiminnan jatkuvuuteen kohdistuvat olennaiset riskit. Tiedonhallintayksikön on riskiarvioinnin perusteella valmiussuunnitelmin ja häiriötilanteissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muilla toimenpiteillä huolehdittava, että sen tietoaineistojen käsittely, tietojärjestelmien hyödyntäminen ja niihin perustuva toiminta jatkuvat mahdollisimman häiriöttömästi normaaliolojen häiriötilanteissa sekä valmiuslaissa (1552/2011) tarkoitetuissa poikkeusoloissa.* *Viranomaisten yleisestä varautumisvelvollisuudesta poikkeusoloihin sekä valtion tietohallinnon, tiedonkäsittelyn, sähköisten palveluiden, tietoliikenteen ja tietoturvallisuuden järjestämisestä poikkeusoloissa säädetään valmiuslaissa.”* Suomessa varautuminen ja yhteiskunnan kriittisten toimintojen varmistaminen ovat laajasti yksityisten toimijoiden varassa, mikä koskee myös digitaalisia palveluja. Euroopan unionin tasolla on meneillään sääntelyhankkeita, jotka vaikuttavat suoraan sekä tilannekuvan muodostamiseen että toiminnan jatkuvuuden hallintaan, jossa vaikutus kohdistuu muun muassa varautumiseen ja häiriöilmoitusvelvoitteisiin. Toiminnan jatkokehittämisessä nämä seikat tulee huomioida aiempaa selkeämmin.

Yhteistoiminta-alue/teema	Koordinaatioryhmän näkemys nykytilasta
	Julkisessa hallinnossa on olemassa toimintamalli, jossa varautuminen häiriötilanteisiin erityisesti erikoistilanteissa tehdään huolellisesti jo ennakolta. Esimerkiksi vaalien järjestämiseen on liittynyt korotettu valmius informaatiovaikuttamisen ja informaatiohäirinnän sekä digitaalisen turvallisuuden häiriöiden torjumiseksi. Vaalien aikana seurataan tehostetusti mahdollista informaatiovaikuttamista ja informaatiohäirintää sekä digitaalisen turvallisuuden mahdollisia häiriöitä.
Digitaaliseen turvallisuuteen liittyvä häiriötilanteiden hallinta	Häiriötilanteiden hallinnan ennalta ehkäisevät ja korjaavat toimenpiteet ovat toimijoiden vastuulla. Häiriötilanteiden hallinnassa keskeinen yksikkö on kunkin toimijan tai usean toimijan yhteinen häiriöhallintakeskus (SOC). KTK tukee organisaatioita ohjeistuksen ja neuvonnan avulla, ja poliisi tutkii häiriötilanteisiin mahdollisesti liittyviä tietoverkkosidonnaisia ja -avusteisia rikoksia. Yhteistyö KTK:n kanssa koetaan hyödylliseksi ja tarpeelliseksi. Vakavan kyberloukkauksen kohteeksi joutuneella organisaatiolla pitää kuitenkin olla riittävä osaaminen, jotta se voi hyödyntää KTK:n tarjoamia palveluja. Useissa tapauksissa vakavan kyberloukkauksen selvittämiseen otetaan mukaan tieturvallisuuden konsultointipalveluja tarjoava yritys ja näidenkin palvelujen hankkiminen ja hyödyntäminen vaativat organisaatiolta riittävää osaamista ja tarpeen mukaan riittäviä, etukäteen toteutettuja palvelusopimusjärjestelyjä. Lisäksi häiriötilanteessa toimijan on pystyttävä itse tekemään korjaavia toimenpiteitä, mikä edellyttää riittävää digitaalisen turvallisuuden osaamista ja resursseja. Operatiivista ”kyberpalokuntaa” ei ole eikä yleisesti valmiiksi kilpailutettuja häiriönhallinnan palveluja ole saatavilla. Poliisitutkinnankin kannalta on eduksi, jos organisaatiolla itsellään on riittävästi osaamista tuottaa ja tarjota rikostutkinnan kannalta olennaista tietoa sekä hankkia tarvittaessa ulkopuolista osaamista tietoturvallisuuden konsultointipalveluja tarjoavalta yritykseltä. Valtioneuvoston kanslian johtama ministeriöiden valmiuspäälliköiden verkosto ja Turvallisuuskomitean johtama ministeriöiden valmiussihteerien verkosto käsittelevät säännöllisesti myös digitaalisen maailman turvallisuuskysymyksiä. Vapaaehtoisten verkostona toimiva KyberVPK voi neuvoa kyberloukkausten kohteeksi joutuneita. Verkostossa on mukana kokeneita kyberturvallisuusammattilaisia niin tietoturvayrityksistä kuin julkisesta hallinnosta ja se toimii yhteistyössä viranomaisten kanssa. KyberVPK ei voi ottaa vastuuta yhteiskunnan kriittisten tietojärjestelmien ja infrastruktuurin toimivuudesta, vaan ne ovat viranomaisten vastuulla. KyberVPK:n rooli onkin viranomaistoimintaa täydentävä.

2.2 Valtionhallinnon yhteistoiminta

Perinteiset valtion ohjauksen keinot ja toimintatavat, kuten talous- ja tulosohjaus, perustuvat hallinnonalakohtaiselle ja toimivaltaisuutta korostavalle yksittäisten toimijoiden, toimintojen ja järjestelmän osien ohjaukselle. Nämä perinteiset ohjausmallit eivät yksin riitä digitaalisen turvallisuuden ohjaamiseen. Digitaalinen turvallisuus nähdään valtiotoimijoiden välillä hankalasti hallittavana ja monitahoisena haasteena, joka edellyttää kattavaa kokonaiskuvaa ja toimijoiden välistä yhteistyötä yli organisaatiorajojen. Digitaaliseen turvallisuuteen liittyvät kokonaisuudet nähdään toisinaan ainoastaan teknisenä kysymyksenä ilman syvällistä näkökulmaa niiden yhteiskunnallisesta vaikutuksesta. Nykytilassa valtionhallinnon toimijat ratkovat esimerkiksi koulutukseen, järjestelmiin, tilannekuvaan, varautumiseen ja tiedonvaihtoon liittyviä haasteita siiloissa, mikä ei ole resurssinäkökulmasta kestävää. Taulukossa 2 on kuvattu tunnistetut valtiotoimijoiden digitaalisen turvallisuuden yhteistoiminta-alueet sekä näihin liittyvät nykytilaa koskevat havainnot.

Taulukko 2. Valtiohallinnon digitaalisen turvallisuuden tunnistetut yhteistoiminta-alueet sekä niihin liittyvät nykytilaa koskevat havainnot

Yhteistoiminta-alue/teema	Koordinaatioryhmän näkemys nykytilasta
Digitaalisen turvallisuuden yhteinen ohjaus	Valtioneuvoston asettama ministerityöryhmä ohjaa digitalisaation, datatalouden ja julkisen hallinnon kehittämistä sekä koordinoi näihin liittyviä toimenpiteitä ja tilannekuvaa. Ryhmä sovittaa yhteen kehittämishankkeita ja tekee tarvittavia poliittisia linjauksia keskeisistä toimialansa kehittämiseen liittyvistä toimista. Ryhmä vastaa kyberturvallisuuden ja julkisen hallinnon varautumisen ohjaamisesta ja tekee tarvittavat poliittiset linjaukset toimista, joilla taataan yhteiskunnan toimintakyky ja digitaalinen toimintaympäristö kyberhäiriöissä ja kybervaikuttamisessa. Ryhmän työtä tukee Digitoimisto. Ryhmä ja Digitoimisto olivat olleet toiminnassa vasta noin puoli vuotta haastattelujen ajankohtana, joten toiminnan tuloksia ei ollut mahdollisuutta arvioida haastatteluissa, joita tämän raportin valmistelua varten tehtiin. Valtioneuvoston kanslia koordinoi ministeriöiden tietoturvallisuuden ohjaus- ja yhteistyöryhmiä. Neljä kertaa vuodessa kokoontuva valtioneuvoston tietoturvallisuuden ohjausryhmä on strategisen tason ryhmä, joka johtaa, suunnittelee ja seuraa tietoturvallisuuden toimenpiteitä. Viidesti vuodessa kokoontuva valtioneuvoston tietoturvallisuuden yhteistyöryhmä on operatiivisen tason ryhmä, joka tukee valtioneuvoston kansliaa ministeriöiden tietoturvallisuuden ja ICT-varautumisen yhteensovittamisessa sekä tiedonkulun parantamisessa ja häiriöhallinnassa. Kuukausittain kokoontuvan tietosuojaverkoston tehtävänä on kehittää ja koordinoida EU:n yleisen tietosuoja-asetuksen (EU) 2016/679 ja muun tietosuojalainsäädännön velvoitteiden toteutumista valtioneuvoston piirissä. Valtionhallinnon digitaalisen turvallisuuden yhteistoimintaa koordinoidaan hallinnonaloittain ministeriöissä. Nämä rakenteet ovat osittain päällekkäisiä. Eri toimijoiden digitaalisen turvallisuuden roolit ovat epäselviä muille julkisen hallinnon toimijoille, kuten kunnille. Digitaalista turvallisuutta käsitellään tilanteen mukaisesti ja korjaavat toimenpiteet ovat tapauskohtaisia. Toimintaympäristön nopean muuttumisen takia tehtäviä koskevat säädökset ovat jatkuvasti osin vanhentuneita tai epätarkkoja. Tämä tulisi ottaa huomioon säädösvalmistelussa ja pyrkiä joustavuuteen sekä tilanteen mukaisen toiminnan mahdollistamiseen. Vastuiden on kuitenkin aina oltava selkeitä. Toimijat ovat sopineet keskenään digitaalisen turvallisuuden tarkemmasta tehtäväjaosta myös muistioin ja sopimuksin. Esimerkiksi yhteistyöstä ja työnjaosta DVV:n ja KTK:n sekä KTK:n ja HVK:n välillä on sovittu sopimuksin. Tällä on pyritty välttämään päällekkäistä toimintaa, ohjeistusta ja oppaita. Ministeriöiden ja virastojen tietoturvapäälliköiden välinen verkosto toimii puutteellisesti. Toiminnan parantamiseksi VAHTI perusti syksyllä 2022 uuden valtionhallinnon tietoturvan vastuuhenkilöiden verkoston. Digitaalisen turvallisuuden osa-alueilla yhteinen ohjaus toteutuu seuraavasti: Tietosuoja: Tietosuojavaltuutetun toimisto antaa tietosuojan toteuttamista koskevia ohjeita. Tietosuojaverkosto kehittää ja koordinoi EU:n yleisen tietosuoja-asetuksen (EU) 2016/679 ja muun tietosuojalainsäädännön velvoitteiden toteutumista valtioneuvoston piirissä. Riskienhallinta: Valtiovarainministeriön controller-toiminto antaa yleisiä ohjeita riskienhallinnan toteuttamisesta valtionhallinnossa. Digitaalisen turvallisuuden strategisessa johtoryhmässä on edustus keskeisistä ministeriöistä. DVV tuottaa strategisten digiturvariskien analyysejä, joita on käytetty digitaalisen turvallisuuden kehittämisen ohjauksessa.

Yhteistoiminta-alue/teema	Koordinaatioryhmän näkemys nykytilasta
	Tieto- ja kyberturvallisuus: Tiedonhallintalaki asettaa vaatimukset tiedonhallintayksiköiden tietoturvallisuudelle. Muualla lainsäädännössä on sektorikohtaisia vaatimuksia, esimerkiksi laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä. Valtioneuvosto antaa ministeriöille tieto- ja kyberturvallisuuteen liittyviä ohjeita. Kukin ministeriö ohjaa hallinnonalaansa ohjeilla ja määräyksillä. Jatkuvuudenhallinta: Huoltovarmuuskeskus ohjeistaa huoltovarmuuskriittisten toimijoiden varautumista, mutta toiminnan jatkuvuuden yhteistä ohjausta ei ole.
Määräykset, ohjeet, vaatimukset, suositukset ja työkalut	Valtioneuvoston kanslian tietoturvallisuusohjeistus on koettu hyväksi ja tarpeelliseksi, mutta se koskee ainoastaan ministeriöitä. Ohjeistus on myös hyvin yleistä ja se edellyttää rinnalleen ministeriö- ja hallinnonalakohtaisia, yksityiskohtaisempia linjauksia. Toisaalta substanssinäkökulmaan perustuvaa hallinnonalakohtaista ohjeistusta tarvitaan aina täydentämään yleisiä ohjeita. Hallinnonalakohtaisen ohjeistuksen lähtökohta on tunnistaa suojattavat kohteet. Joillakin valtion virastoilla, esimerkiksi ulkoministeriöllä, on ISO27001-tietoturvasertifikaatti. ISO27001-tietoturvasertifiointia ei ole juuri lainkaan toteutettu valtionhallinnossa, mikä nähdään puutteena. Virastojen tulisi arvioida toimintaansa ja toteuttaa tämän perusteella tietoturvasertifiointi tai muu vaatimuksenmukaisuuden toteuttamisen arviointi. Tiedonhallintalain mukaan tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Joillekin ministeriöille on epäselvää, miten valtioneuvoston kanslian ohjeistoa voitaisiin kattavasti ja helposti saattaa koskemaan ministeriöiden alaista hallintoa soveltuvin osin. Digitaalisen turvallisuuden osa-alueilla yhtenäiset suositukset, ohjeet ja vaatimukset toteutetaan seuraavasti: Tietosuoja: Tietosuojavaltuutetun toimisto antaa tietosuojan toteuttamista koskevia ohjeita. Riskienhallinta: Valtiovarainministeriön controller-toiminto antaa yleisiä riskienhallinnan ohjeita. Tiedonhallintalautakunnan suositukset koskevat tietoriskien hallintaa. Tieto- ja kyberturvallisuus: Valtioneuvosto antaa ministeriöille tieto- ja kyberturvallisuuteen liittyviä ohjeita. Kukin ministeriö ohjaa hallinnonalaansa ohjeilla ja määräyksillä. Tiedonhallintalautakunnan suositukset koskevat tietoturvallisuusvaatimusten toteuttamista. Jatkuvuudenhallinta: Valtionhallinnon varautumiseen ja toiminnan jatkuvuuden hallintaan on olemassa osin vanhentuneita VAHTI-ohjeita. Toiminnan jatkuvuutta koskevia vaatimuksia on annettu sektorikohtaisesti, mutta yhtenäistä ohjeistusta ei ole. Normaaliaikojen toiminnan jatkuvuutta koskevia vaatimuksia ei ole. Valmiuslaki asettaa poikkeusoloja koskevia yleisiä vaatimuksia.
Digitaalisen turvallisuuden palvelut	Valtionhallinnon toimijat eivät tyypillisesti itse tuota digitaaliseen turvallisuuteen liittyviä palveluja, vaan ne hankitaan palvelukeskuksista tai palvelutarjoajilta. Valtiotoimijoiden digitaalisen turvallisuuden palvelut ovat tyypillisesti osa toimialariippumattomia palveluita, joita Valtori tuottaa keskitetysti. Osa toimialariippumattomista palveluista kuuluu Valtorin TUVE-toimintaan, joka keskittyy korkean varautumisen ja turvallisuuden vaatimukset täyttävien tieto- ja viestintäteknisiin ratkaisuihin ja integraatiopalveluihin. Valtorin asiakasneuvottelukunta tukee asiakasohjausta ja toiminnan kehittämistä. Valtorin ohjausrakenne on suunniteltu strategiseen ohjaukseen sopivaksi. Yksittäisten palvelujen digitaalisen turvallisuuden kehittämiseen soveltuvaa toimintamallia ei ole. Valtorin keskitetysti tuottamien palveluiden asiakkaiden näkökulmasta vastaukset digitaalisen turvallisuuden kysymyksiin koostuvat eri osapuolten ja toimijoiden näkemyksistä. Valtorin rooli ei ole selkeä näiden vastausten kokoamisessa tai digitaalisen turvallisuuden kehittämisessä.

Yhteistoiminta-alue/teema	Koordinaatioryhmän näkemys nykytilasta
	Valtorin tuottamien keskitettyjen palvelujen tietoturvallisuuden arviointi on yksi valtiohallinnon digitaalisen turvallisuuden yhteistoiminnan näkökulma. Valtorin palvelujen turvallisuudesta ei ole kaikilta osin ollut varmuutta ja toimintavarmuus ei ole ollut riittävä. Valtorissa onkin parhaillaan menossa usean vuoden kestävä tietoturvallisuuden kehittämisen hanke, jonka yhteydessä toteutetaan kattava Valtorin palvelujen tietoturvallisuuden arviointi. Digitaalisen turvallisuuden osa-alueilla digitaalisen turvallisuuden palvelut toteutetaan seuraavasti: Tietosuoja: Yhteisten palvelujen tietosuojan toteutumisesta vastaavat rekisterinpitäjänä toimivat palveluiden käyttäjät tai palveluiden tarjoajat. Riskienhallinta: Palvelujen hankintaan ja käyttöönottoon liittyvät riskiarviot ovat käyttäjäorganisaatioiden vastuulla. Tieto- ja kyberturvallisuus: Digitaalisen turvallisuuden palveluiden yleistä hyväksymiskäytäntöä ei ole, vaan palveluiden käyttäjät tekevät omat arvionsa tieto- ja kyberturvallisuuden toteutumisesta. Tiedonhallintalautakunnan julkisen hallinnon tietoturvallisuuden arviointikriteeristön (Julkri) tavoitteena on toimia jatkossa tieto- ja kyberturvallisuuden, tietosuojan sekä varautumisen ja jatkuvuudenhallinnan toteutumisen arviointikriteeristönä. Palveluiden vaatimusten tulisi rakentua riskiperustaisesti. Puolustusvoimat näkee tarpeelliseksi kasvattaa maanpuolustukseen liittyvien järjestelmien ja ratkaisujen auditointitoiminnan valtuuksiaan. Valtuuksien kasvattaminen edellyttää puolustusvoimien arviointikyvykkyyden edelleen kehittämistä sekä muun muassa arviointilain[13] muutosta. Jatkuvuudenhallinta: Yhteisten digitaalisen turvallisuuden palvelujen jatkuvuuden hallinta on palveluntuottajien vastuulla. Asiakaskohtaisten jatkuvuudenhallinnan tarpeiden huomioimiseksi ei ole yleistä menettelyä.
Tilannekuva ja häiriötilanteiden hallinta	Valtionhallinnossa on laajavaikutteisten kyberhäiriöiden hallintaryhmä (VIRT). VIRT-ryhmässä ovat mukana kaikki ministeriöt ja osa virastoista, ja niiden välillä voidaan sopia tehtävistä ja käytännön toimenpiteistä häiriön hallitsemiseksi. Ryhmän toiminnalla on kaksi tarkoitusta: 1) häiriötilanteen hallinta ja tilannekuvan jakaminen ja 2) kyberturvallisuuden kehittäminen. Lisäksi KTK ja valtiohallinnon toimijat jakavat tilannetietoa valtionhallinnon tiedonvaihto- ja yhteistyöryhmässä (ISAC). Digitaalisen turvallisuuden osa-alueilla tilannekuva ja häiriötilanteiden hallinta toteutetaan seuraavasti: Tietosuoja: Erityistä tietosuojan tilannekuvaa ei ole tunnistettu. Riskienhallinta: Digitaalisen turvallisuuden strategisessa johtoryhmässä arvioidaan julkisen hallinnon strategisia riskejä. Sisäministeriön johdolla on laadittu kansallinen riskiarvio. Tieto- ja kyberturvallisuus: KTK tuottaa kyberturvallisuuden tilannekuvatuotteita erilaisista lähteistä ja jakaa niitä. KTK neuvoo toimijoita häiriötilanteiden hallinnassa. Poliisi tutkii häiriöihin mahdollisesti liittyviä tietoverkkosidonnaisia ja -avusteisia rikoksia. Jatkuvuudenhallinta: Valtionhallinnon toimijoilla on vastuu oman toimintansa jatkuvuuden toteuttamisesta ja häiriötilanteiden hallinnasta. VIRT-ryhmässä voidaan sopia tehtävistä ja käytännön toimenpiteistä häiriön hallitsemiseksi.

13 Lakiviranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011)

2.3 Hyvinvointialueiden välinen yhteistoiminta

Hyvinvointialueiden digitaalisen turvallisuuden hallintaan liittyviä toimintatapoja luodaan alueiden palvelukokonaisuuksien näkökulmasta. Tavoitteena on palvelujen yhteentoimivuus ja saumattomuus. Hyvinvointialueiden digitaalisten palveluiden tulee olla helppokäyttöisiä riippumatta siitä, millaisella alustalla tai päätelaitteella niitä käytetään. Tietoturvasta ja asiakkaan tietosuojasta on huolehdittava palvelun koko elinkaaren ajan. Hyvinvointialueella on tietoturvan kannalta erilaisia osa-alueita, kuten julkista päätöksentekoa, julkisia ohjeita, sosiaali- ja terveysalan asiakas- ja potilastietoa sekä turvallisuustoiminnan piirissä olevaa pelastusalan tietoa. Hyvinvointialueet huolehtivat itsenäisesti palveluihin liittyvästä digitaalisesta turvallisuudesta.

Hyvinvointialueille tuodaan yhteen erittäin laajoja kokonaisuuksia, mikä aiheuttaa haasteita digiturvallisuuden, koulutuksen ja ohjeistusten yhtenäisyydelle. Myös luovuttajaorganisaatioiden digiturvallisuuden lähtötasot voivat olla hyvin erilaisia. Tietoturvan ja tietosuojan roolit korostuvat nykyään voimakkaasti terveydenhuollossa. Havaittujen kehittämistarpeiden vuoksi onkin erittäin tärkeää, että hyvinvointialueiden rahoituksessa huomioidaan tietosuoja- ja tietoturvaosaamisen korostunut tarve. Digiturvallisuus ei voi perustua pelkkään tekniseen toteutukseen, vaan tärkeitä ovat myös substanssiasiantuntijat, jotka kykenevät viestimään tietoturvasta ja tietosuojasta henkilökunnalle ja asiakkaille.

Vaikka hyvinvointialueille on laadittu referenssiarkkitehtuurimalleja, kokevat toimijat tärkeäksi yhteistyön ja hyvien toimintamallien jakamisen riittävän turvallisuuden varmistamiseksi. Tietojärjestelmien suuri määrä sekä tietoverkkojen rakenteet lisäävät digitaaliseen turvallisuuteen liittyviä riskejä. Toimintaympäristön yhtenäistäminen ja tavoitteen mukainen yhteentoimivuuden ja joustavuuden rakentaminen on vaikea ja pitkäkestoinen tehtävä. Laajat investointitarpeet koskevat kaikkia hyvinvointialueita, mutta investoinnit toteutetaan hyvinvointialueittain. Yhtenäiset linjaukset digitaalisen turvallisuuden kehittämisessä edesauttavat palvelujen yhteentoimivuuteen ja saatavuuteen liittyvien tavoitteiden saavuttamista. Esimerkkinä yhtenäisistä linjauksista sekä vaatimuksista toimii hyvinvointialueiden yhteinen referenssiarkkitehtuuri. Siinä otetaan kantaa muun muassa valtiovarainministeriön tiedon hyödyntämisen ja avaamisen linjauksiin. Ne on tarkoitettu koko julkisen hallinnon tarpeisiin yhteisten periaatteiden ja suositusten ohjelmointirajapintakehityksestä sekä digitalisaation edistämisestä. Myös hyvinvointialueiden tulisi arvioida kattavasti toimintaansa ja toimialojaan (terveydenhuolto, sosiaalihuolto ja pelastustoimi) sekä toteuttaa tämän perusteella tietoturvasertifiointi, kuten esimerkiksi ISO27001-tietoturvasertifointi tai muu vaatimuksenmukaisuuden toteuttamisen arviointi. Vaatimuksia toimialakohtaisten arvioinnin tekemiseen tai teettämiseen ulkopuolisella toimijalla tulee suoraan myös sektorikohtaisesta lainsäädännöstä.

Taulukko 3. Hyvinvointialueiden väliseen digitaalisen turvallisuuden yhteistoimintaan nykytilassa liittyviä havaintoja

Yhteistoiminta-alue/teema	Koordinaatioryhmän näkemys nykytilasta
Digitaalisen turvallisuuden kehittämisen yhteistoiminta	Yhteistoiminta hyvinvointialueiden välillä rajoittuu olemassa oleviin rakenteisiin, kuten SOTE ISAC-tiedonvaihtoryhmiin, joissa jaetaan esimerkiksi tilannekuvatietoa. KTK onkin tunnistettu hyvinvointialueilla keskeiseksi tahoksi tietoturvallisuuden kehittämisessä. Sairaanhoitopiirit ovat osallistuneet aktiivisesti DVV:n toteuttamien palveluiden hyödyntämiseen muun muassa osallistumalla TAISTO-harjoituksiin ja hyödyntämällä DVV:n toteuttamia digitaalisen turvallisuuden kyselyitä. Lisäksi Huoltovarmuuskeskus koordinoi Alue 2030 -ohjelmaa, jossa aluehallintovirastot ja ELY-keskukset ovat mukana suunnittelemassa ja toteuttamassa kehittämistoimenpiteitä toimintaa uhkaavien riskien pienentämiseksi.
Määräykset, ohjeet, vaatimukset, suositukset ja työkalut	Hyvinvointialueiden toimialoja (terveydenhuolto, sosiaalihuolto ja pelastustoimi) koskevat erilaiset sektorikohtaiset digitaalisen turvallisuuden säädökset. Tämä on perusteltua, koska eri toimialoilla käsiteltävän tiedon luonne on erilainen. Hyvinvointialueiden vastuulle siirtyvien erilaisten potilastietojärjestelmien tietoturvallisuudelle on asetettu vaatimukset, mutta niiden tietoturvallisuuden vaatimustenmukaisuuden ylläpitämistä on haastavaa arvioida, koska toimintaympäristö on kompleksinen. Yhtenäisen digitaalisen turvallisuuden tason saavuttaminen edellyttää sekä hyvinvointialueiden välistä yhteistyötä että kuntien digitaalisen turvallisuuden kaikkien osa-alueitten huomiointia. Huomiota on kiinnitettävä sekä tiedonantovelvoitteisiin että tiedonsaantioikeuksiin. Kunnille kuuluvat jatkossakin ennalta ehkäisevä hyvinvointi ja tämän edellyttämät riippuvuudet hyvinvointialueen tehtävistä ja palveluista. Sosiaali- ja terveyspalvelujen tarjoajille erityisesti asetettujen vaatimusten tulisi olla ristiriidattomia. Tällä hetkellä tämä ei toteudu, minkä seurauksena resursseja haaskataan vaatimusten tulkintaan ja toteuttamiseen. Esimerkiksi potilastietojärjestelmä on lääkinnällinen laite ja sitä koskevat tietosuojaa, tietoverkkoja ja potilastietojärjestelmiä koskevat EU:n ja kansalliset lakisääteiset vaatimukset sekä standardit. Näiden ristiriitaistenkin vaatimusten ratkaiseminen kansallisesti ei ole mahdollista.
Tilannekuva ja häiriötilanteiden hallinta	Sosiaali- ja terveysministeriön hallinnonalalla yliopistollisten sairaaloiden ympärille muodostetut yhteistoiminta-alueet tukevat kootusti hyvinvointialueitaan tietoturvallisuuteen ja häiriönhallintaan liittyvissä asioissa. Kansaneläkelaitoksen valvomon on tarkoitus jatkossa toimia yhteistoiminta-alueiden yhteisenä häiriönhallintakeskuksena (SOC). Yhteistoiminta-alueiden omien keskusten muodostamista selvitetään. KTK neuvoo toimijoita häiriötilanteiden hallinnassa. Poliisi tutkii häiriöihin mahdollisesti liittyviä tietoverkkosidonnaisia ja -avusteisia rikoksia.

2.4 Kuntatoimijoiden välinen yhteistoiminta

Kuntatoimijoiden välisellä digitaalisen turvallisuuden yhteistoiminnalla on monta muotoa. Kuntaliitolla on merkittävä rooli osaamisen kasvattamisessa ja yhteistoiminnan koordinoinnissa kuntien suuntaan. Toisaalta yhteistoiminta digitaalisen turvallisuuden alueella toteutuu tyypillisesti laajimmin maantieteellisesti lähekkäin sijaitsevien kuntien välillä. Tämä vaikuttanee jatkossa kunkin hyvinvointialueen kuntien yhteistyöhön. Alueellisesti toteutettu yhteistyö erityisesti kasvukeskuksissa on koettu hyödylliseksi muun muassa kustannustason hallinnan sekä osaamisen kehittämisen näkökulmista. Toimiva yhteistyö edellyttää vastavuoroisuutta, jotta yhteistoimintaa koordinoiva taho ei joudu tekemään asioita yksin muiden hyötyessä tuloksista. Kuntatasolla digitaaliseen turvallisuuteen liittyviä kokonaisuuksia tarkastellaan käytännön ratkaisujen näkökulmasta. Kuntien toimialat ratkaisevat usein digitaaliseen turvallisuuteen liittyviä ongelmia omaan toimintaan liittyvien käytännön toteutusten kautta ilman laajempaa digitaalisen turvallisuuden kehityssuunnitelmaa.

Digitaalisen turvallisuuden kokonaisuus ja sen ohjaaminen ei ole kunnissa toiminnan kehittämisen kannalta suunnitelmallista eikä järjestelmällistä. Myöskään toimintaa tai toimintaympäristöä ei kehitetä järjestelmällisesti. Usein digitaaliseen turvallisuuteen liittyvät linjaukset ja tekniset toiminnallisuudet tehdään irrallaan laajemmasta kokonaisuudesta. Kuntakentän arjessa vähäisillä resursseilla tulisi saada enemmän aikaan, mikä edellyttää julkisen hallinnon valtio-hyvinvointialue-kunta digitaalisen turvallisuuden yhteistoiminta- ja hallintamallilta kiinteää, osallistavaa ja käytännön ratkaisuja tukevaa kansallista ohjausta. Oman haasteensa digitaalisen turvallisuuden määrätietoiselle kehittämiselle luovat kunnan eri toimialoja, kuten kunnan hallintoa ja konsernihallintoa, ympäristötoimialaa, sivistystoimialaa, sosiaalihuoltoa, terveydenhuoltoa, vesihuoltoa sekä energiahuoltoa koskevat lukuisat sektorikohtaiset säädökset ja niiden eroavaisuudet. Tosin osittain digitaalisesta turvallisuudesta vastaavat kuntien omistamat liikelaitokset, kuten vesi- ja energiayhtiöt, eikä kunnan ja kunnan johdon tarvitse huolehtia siitä.

Tämän hetken kunnalle mahdollisesti sopivien digipalveluiden ongelmana on nykyaikaisten ja markkinoilta kilpailutettavien digipalveluiden laadun epävarmuus. Kunnat joutuvat hakemaan kompromissia tosiasiallisen palvelutarjooman ja julkishallinnon digitaalisen turvallisuuden ja muiden vaatimusten suhteen, mikä koskee esimerkiksi pilvipalveluita.

Kuntien ja yksityisen sektorin välinen yhteistoiminta on vähäistä. Yhteistoiminta rajoittuu pitkälti yhteisiin projekteihin, joissa keskitytään yksittäisen järjestelmä- tai palvelukokonaisuuden kehittämiseen. Kuntien rajalliset resurssit sekä esimerkiksi tiedon omistamisen hajautuminen eri toimialoille lisäävät yhteistoimintaan liittyvää tehottomuutta. Taulukkoon 4 on koottu erityisiä kuntien yhteistoimintaan liittyviä havaintoja digitaalisen turvallisuuden yhteistoiminta-alueittain. Tämän lisäksi kuntia koskevat kaikki julkisen hallinnon

digitaalisen turvallisuuden nykytilan yhteiset havainnot, jotka on kirjattu kappaleessa 2.2. Erityisesti esille on nostettava määräyksiin, ohjeisin, vaatimuksiin ja suosituksiin sekä työkaluihin liittyvät havainnot sekä tiedonhallintalain ja sektorikohtaisten säännösten muodostamaan kompleksiseen kokonaisuuteen liittyvät havainnot.

Taulukko 4. Kuntien väliseen digitaalisen turvallisuuden yhteistoimintaan nykytilassa liittyviä havaintoja.

Yhteistoiminta-alue/teema	Koordinaatioryhmän näkemys nykytilasta
Digitaalisen turvallisuuden kehittämisen yhteistoiminta	Kuntaliiton digitaalisen turvallisuuden yhteistyöryhmiä ovat kuntakentän tietosuojavastaavien verkosto, kuntakentän tietoturvavastaavien verkosto (Kun-TVV) sekä Turvallinen ja kriisinkestävä kunta -verkosto. Kuntaliiton tavoitteena on huolehtia kuntien toimintaedellytyksistä tarjoamalla ja järjestämällä kunnille asiaan liittyviä tilaisuuksia ja antaa näkyvyyttä julkisen hallinnon digitaalisen turvallisuuden kehittämiseen. Tähän sisältyvät Kuntaliiton eri yksiköitten asiantuntija- ja tietopalveluitten käytettävyys ja kannanotot. Kuntaliitto toimii yhteistyössä KTK:n kanssa väylänä, joka tarjoaa yhteys- ja tiedottamiskanavan KTK:n ja kuntakentän tietoturvavastaavien välille. Kaupunkien välinen tiedonhallinnan kehittämisen yhteistyö on säännöllistä. Yliopistojen ja sairaanhoitopiirien kanssa tehdään yhteistyötä vaihtelevasti. Kuntien ja yksityisen sektorin välinen yhteistoiminta on vähäistä. Yhteistoiminta rajoittuu pitkälti yhteisiin projekteihin, joissa keskitytään yksittäisen järjestelmä- tai palvelukokonaisuuden kehittämiseen. Haasteena on saada tulevaisuudessa ylemmän tason kansallisten ryhmien keskiöihin mukaan kuntien vahva edustus. Esimerkiksi valtionhallinnon VIRT-ryhmässä ja ISAC-toiminnassa kuntien edustus on nyt vähäinen. KTK:n toiminta tulisi kytkeä lähemmäksi kuntien arjen toimintaa, mikä onkin lähdössä liikkeelle KTK:n esittelemän kunta-ISAC-yhteistyömallin mukaisesti. Tampereen kaupunki koordinoi yhteistyötä alueen kuntien kesken. Yhteisillä palvelukokonaisuuksilla on omat hallintamallinsa sekä koordinaatio- ja työryhmät, joissa yhteistyö konkretisoituu. Yhtenäiset tietosuoja- ja tietoturvapolitiikat sekä niihin liittyvät ohjeet ovat onnistuneen yhteistyön keskeinen tekijä. Yhteistyön etuja ovat olleet alhaisempi kustannustaso sekä osaamisresurssien jakaminen kuntien välillä. Palvelut hankitaan markkinatoimijoilta, jotka ovat soveltuvin osin mukana yhteisissä työryhmissä. Oulun kaupunki on kehityshankkeissaan pyrkinyt ohjaamaan digitaalisen turvallisuuden kehitystä Digiohjausryhmällä, joka ohjaa palvelutoiminnan kehitystä. Ohjausryhmässä yhdistyvät kaupungin sekä tutkimus- ja yksityissektorin edustus. Yksittäisissä hankkeissa pyritään yhdistämään tutkimus- ja kehitystyö yksityisen sektorin tarjoamien palveluiden kanssa käytäntöön siten, että kaikki toimijat hyötyvät yhteistyöstä.
Digitaalisen turvallisuuden osaaminen	Kuntien digitaalisen turvallisuuden resursoinnissa ja osaamisen tasossa on suurta vaihtelua. Kunnat ovat ulkoistaneet ICT-toimintojaan ja digitaaliseen turvallisuuteen liittyvää osaamista ulkopuolisille palveluntarjoajille. Tämä on voinut vähentää kunnan omaa kykyä osallistua digitaaliseen turvallisuuteen liittyvään keskusteluun eri osapuolten välillä. Ulkoistaminen on lisäksi voinut heikentää kunnan kykyä vastaanottaa, käsitellä ja hyödyntää tilannekuvatietoa, tarjolla olevia palveluita ja työkaluja, joita turvallisuusuhkilta suojautumiseen ja turvallisuuden kehittämiseen tarvitaan. Vastavuoroisesti ulkoistamisella voidaan tuottaa kustannushyötyjä ja eritysosaamista, kuten esimerkiksi tietojärjestelmien tietoturva-arviointia, jota kunnan ei välttämättä kannata hankkia itselleen. Tärkeintä olisi varmistaa riittävä oma osaaminen.

Yhteistoiminta-alue/teema	Koordinaatioryhmän näkemys nykytilasta
	Joissain kunnissa digitaalisen turvallisuuden resurssit ja osaaminen ovat olleet jo lähtökohdiltaan vähäisiä, eivätkä ne ole mahdollistaneet kehittämistä vastaamaan nykyisiä tai tulevia turvallisuusuhkia. Niukat resurssit ja osaaminen vaikuttavat myös palveluiden hankintaan ja vaatimusten asettamiseen hankinnoille, jolloin hankittu palvelu ei välttämättä tue kunnan digitaalisen turvallisuuden ylläpitämistä ja kehittymistä. Oman haasteensa luo digitaalisen turvallisuuden osaajien rajallinen saatavuus Suomessa. Niukkojen resurssien ja osaamisen vallitessa olisi tarpeen tiivistää yhteistyötä osaamisen hankkimiseksi, kehittämiseksi ja ylläpitämiseksi entisestään. Digitaalisen turvallisuuden kannalta olisi kustannustehokkaampaa ylläpitää esimerkiksi yksittäisten tietojärjestelmien kuin lukuisten tietojärjestelmien turvallisuutta. Mitä enemmän kunnissa käytetään yhteisiä tai samoja tietojärjestelmiä sitä paremmin voidaan hyödyntää yhteisiä resursseja ja osaamista tietojärjestelmien turvallisuuden ylläpitämiseksi ja kehittämiseksi.
Tilannekuva ja häiriötilanteiden hallinta	Kunta-alalla ei ole tällä hetkellä yhteistä tilannekuvan muodostamista tai tuottamista eikä foorumia, jossa jakaa digitaalisen turvallisuuden tilannekuvatietoa. Kunta-alan toimijoille ollaan kuitenkin perustamassa KTK:n ylläpitämä oma tiedonvaihto ja -yhteistyöryhmä vuosille 2022–2025. Kunta vastaa itse niin digitaalisen turvallisuuden häiriöiden hallinnasta kuin palveluiden jatkuvuudenkin hallinnasta. Kunta hankkii tarvittaessa ulkopuolista osaamista häiriötilanteiden hoitamiseksi konsultointia tarjoavilta tietoturvayrityksiltä. KTK neuvoo toimijoita häiriötilanteiden hallinnassa. Poliisi tutkii häiriöihin mahdollisesti liittyviä tietoverkkosidonnaisia ja -avusteisia rikoksia.

2.5 Julkisen hallinnon ja tutkimustoiminnan välinen yhteistoiminta

Suomessa tutkimusorganisaatioiden välinen yhteistyö on koko 2000-luvun ollut alle EU:n keskiarvon, vaikka elinkeinoelämän ja tutkimusorganisaatioiden välinen yhteistoiminta on ollut erityisen toimivaa ja tuottavaa.[14] Julkisen hallinnon ja tutkimustoiminnan väliseen yhteistoimintaan on luotu erilaisia malleja, joita koordinoivat useat toimijat.

Business Finlandin tavoitteena on vahva yritysten kansainvälistyminen sekä elinkeinojen auttaminen kehittymään ja uudistumaan teknologian ja innovaation keinoin. Vaikuttavuussäätiön perustehtävänä on tukea elinkeinoelämän ja tutkimuksen yhteistyötä. Valtion tutkimuslaitokset edistävät omalla toiminnallaan tutkimuksen ja teknologian laaja-alaista hyödyntämistä.

Ammattikorkeakoulut nähdään alueellisina, soveltavaa tutkimusta tekevinä tahoina, joiden tutkimustuloksia voidaan hyödyntää esimerkiksi kunnissa. Myös yksityisen sektorin tekemät selvitykset ja nykytila-analyysit nähdään kuntia hyödyttävinä tuotoksina, joiden pohjalta voidaan määrittää kuntien toimintaan sopivia kehitystoimenpiteitä.

Digitaalisen turvallisuuden alueella korkeakoulut tekevät ja kehittävät yhdessä muun muassa opiskelijavalinnan ja opintojen turvallisuutta edistäviä toimintamalleja. Korkeakoulujen keskinäisen yhteistyön muotoja ovat esimerkiksi korkeakoulujen SEC-työryhmä, CSC/Funet sekä FUCIO-verkosto. Lisäksi korkeakoulut osallistuvat julkisen hallinnon digitaalisen turvallisuuden yhteistyöryhmiin. Parhaillaan pohdinnassa on yliopistojen yhteisen 24/7 kyberhyökkäysten valvonta- ja havaitsemistoiminnon (SOC eli security operations center) perustamismahdollisuudet.

Tutkimusten tavoiteasetantaa, tutkimuksia ja niiden tuloksia ei nykyisin kuitenkaan hyödynnetä riittävästi digitaalisen turvallisuuden kehittämiseksi. DVV kerää tietoa digitaalisen turvallisuuden tilasta. Aineiston hyödyntämistä tutkimustyössä arvioidaan parhaillaan.

14 Tutkimusyritysyhteistyö, https://www.vaikuttavuussaatio.fi/wp-content/uploads/2021/02/vaikuttavuussaatio_selvitys.pdf

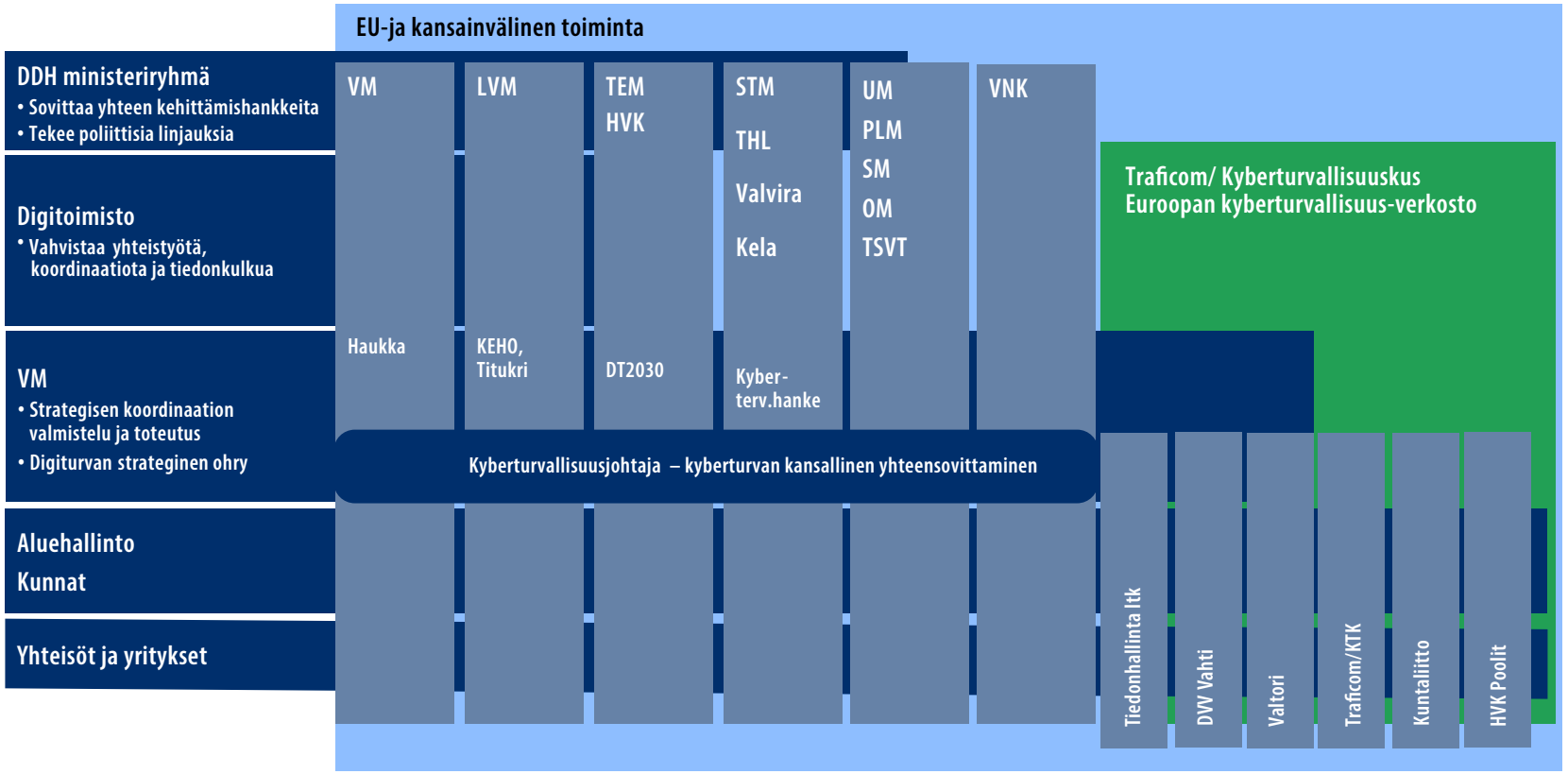
Taulukko 5. Julkisen hallinnon ja tutkimustoiminnan yhteistoimintaan nykytilassa liittyviä havaintoja

Yhteistoiminta-alue/teema	Koordinaatioryhmän näkemys nykytilasta
Tutkimuksen koordinointi	Valtioneuvoston kanslian koordinoimalla valtioneuvoston yhteisellä selvitys- ja tutkimustoiminnalla (VN TEAS) tuotetaan tietoa päätöksenteon, tiedolla johtamisen ja toimintakäytäntöjen tueksi. Toiminnan puitteissa toteutetaan tilaustutkimuksia sekä soveltavaa tutkimusta. Vaikka toimintamallin kautta on toteutettu joitakin digitaalisen turvallisuuden tutkimuksia, sitä ei erityisesti ole tarkoitettu digitaalisen turvallisuuden tutkimukseen ja näin ollen malli on riittämätön tutkimusyhteistyön koordinoimiseksi. Julkisen hallinnon panostukset digitaalisen turvallisuuden tutkimukseen nähdään tavoitteisiin nähden vajavaisina. Suomen tavoitellessa asemaa turvallisena maana sekä johtavana tekijänä kybertutkimuksessa panostusten tutkimukseen tulisi tukea näitä tavoitteita. Vuoden 2021 lopussa voimaan tulleen Euroopan kyberturvallisuuden kompetenssikeskusta ja kyberturvallisuusverkostoa koskevan asetuksen tavoitteena on syventää julkisen sektorin, yksityisen sektorin ja tutkimusmaailman välistä yhteistyötä kyberturvallisuustutkimuksen, -tuotekehityksen ja -innovoinnin saralla. Asetuksen myötä Suomessa Liikenne- ja viestintäviraston Kyberturvallisuuskeskukseen ollaan perustamassa kansallista kyberturvallisuuden koordinointikeskusta, joka muun muassa osallistuu Euroopan kyberturvallisuuden kompetenssikeskuksen ja kansallisten kyberturvallisuuden koordinointikeskusten verkoston työhön sekä edistää kansallisesti eri sektorit ylittävää kyberturvallisuuden tki-toimintaa ja osallistumista EU-laajuisiin tki-hankkeisiin.
Tutkimuskohteiden valinta	Säännöllinen yhteistyö tutkimuskohteiden ja -tavoitteiden määrittämiseksi puuttuu. Keskustelu valtiotoimijoiden, kaupunkien ja kuntien sekä tutkimuslaitosten välillä on puutteellista. Tutkimuslaitokset kokevat, ettei niille tarjota tutkimuskohteita tai tutkimukseen tarvittavaa tietoa. Toisaalta kunnat ja kaupungit kokevat, että niille ei tarjota tutkimusta, joka kehittäisi heidän digitaalista turvallisuuttaan. Esimerkiksi erilaiset nykytila-analyysit ja osaamiskartoitukset sekä näiden tietojen vertaisarviointi kuntien välillä nähdään mielenkiintoisena ja tarpeellisena tutkimusalueena.
Tutkimusrahoitus	Merkittävin tutkimusrahoituksen lähde yliopistoissa ja valtion tutkimuslaitoksissa on ulkopuolinen, kilpailutettu rahoitus; yli puolet tutkimuksesta perustuu tällaiseen rahoitukseen. Tämä nähdään nykyisen toimintamallin heikkoutena, sillä rahoitus keskittyy hankkeisiin, jotka ovat jo aikaisemmin saaneet rahoitusta. Lisäksi ulkopuolinen rahoitus sitoo asiantuntijoita ja tutkijoita kehityshankkeisiin, jotka heikentävät tutkimuksen ja ylimmän tason opetuksen suhdetta. Digitaalisen turvallisuuden tutkimukselta puuttuu vahva ja pitkäjänteinen rahoitus ja kehityspolku tavoitteineen. Vahvaa ja osaavaa tutkijapoolia ei ole syntynyt, sillä tutkijat toimivat vain rahoituksen saaneissa tutkimushankkeissa. Hankkeen päättymisen jälkeen tutkijoilla ei ole palkkarahoitusta, ja he ovat usein siirtyneet jo muihin tehtäviin ennen mahdollisen seuraavan tutkimushankkeen alkamista. Jatkossa on siten syytä painottaa pitkäjänteistä tutkimusta. Maakuntien ja hyvinvointialueiden resurssit ja rahoitus tutkimukseen ovat rajalliset. Kuntatason tutkimusyhteistyö tapahtuu yksittäisten ja tarkasti kohdennettujen tutkimuskohteiden ja opinnäytetöiden kautta. Esimerkkeinä yksittäisistä hankkeista ovat kaupunki- ja tapahtumaturvallisuutta kehittävä hanke sekä kuntien opetussektoreiden kyberosaamiseen liittyvä tutkimus.

2.6 Toimijoiden tehtävät digitaalisen turvallisuuden yhteistoiminnassa nykytilassa

Kuvassa 3 on digitaalisen turvallisuuden yhteistoiminta- ja hallintamalli nykytilassa. Kuva sisältää keskeisiä toimijoita ja tehtäviä. Tarkempi nykytilan kuvaus on edellisissä luvuissa. Taulukkoon 6 on kuvattu vapaamuotoisesti toimijoiden tehtäviä digitaalisen turvallisuuden yhteistoiminnassa nykytilassa.

Kuva 3. Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalli nykytilassa



Taulukko 6. Toimijoiden roolit digitaalisen turvallisuuden yhteistoiminnassa nykytilassa.

Toimija	Tehtävät
Valtioneuvoston kanslia	• valtioneuvoston yhteiset hallinto- ja palvelutoiminnot • tietoturvallisuuden ohjaus- ja yhteistyöryhmät • kyberturvallisuuden EU-asioiden koordinointi
Digitalisaation, datatalouden ja julkisen hallinnon kehittämisen ministerityöryhmä ja Digitoimisto	• ohjaa julkisen hallinnon, digitalisaation, datatalouden ja tietopolitiikan kehittämistä • vastaa kyberturvallisuudesta ja julkisen hallinnon varautumisesta • Digitoimisto huolehtii ministeriöiden välisestä yhteistyöstä sekä digitalisaation ja datatalouden edistämisestä • Digitoimisto on yhden luukun yhteyspiste yhteydenotoille, jotka liittyvät data-, digi- ja tietopolitiikan toimialaan
Ulkoministeriö	• kansallinen turvallisuusviranomainen (NSA) • kyber- ja hybridilähettilästoiminta kv-verkostoissa
Tietosuojavaltuutetun toimisto	• tietosuojalainsäädännön noudattamisen valvonta • edustaa Suomea Euroopan tietosuojaneuvostossa
Puolustusministeriö ja Puolustusvoimat	• kyberturvallisuuden tilannekuvan muodostaminen erityisesti valmiudessa ja varautumisessa • muiden viranomaisten tukeminen kyberpuolustuksen suorituskyvyillä • kyberpuolustuksen kehittämiseen liittyvien harjoitusten järjestäminen ja niihin osallistuminen • digitaaliseen turvallisuuteen liittyvän tiedustelutiedon tuottaminen
Sisäministeriö	• kyberrikostorjunnan ministeriöohjausvastuu • kansallisen turvallisuuden kyberuhkien torjunnan ja kybertiedustelun ministeriöohjausvastuu • valtionhallinnon hybridiuhkaverkoston koordinaatio
Valtiovarainministeriö	• julkisen hallinnon tietopolitiikan, tiedonhallinnan ja sähköisen asioinnin yleiset perusteet • julkisen hallinnon digitaalisen turvallisuuden linjausten, säädösten ja kehittämisohjelmien valmistelu sekä toimeenpanon ohjaus • Digitoimisto • digitaalisen turvallisuuden strateginen johtoryhmä • tiedonhallintalautakunta

Toimija	Tehtävät
Digi- ja väestötietovirasto	• VAHTI-johtoryhmä ja VAHTI-toiminta • digitaalisen turvallisuuden nykytilan ja riskien kokonaiskuvan ylläpito • harjoitustoiminnan koordinointi • julkisen hallinnon digitaalisen turvallisuuden kehittämishankkeet • julkisen hallinnon digiturvaosaamisen ja -kulttuurin kehittäminen • digiturvan hallinnollisen tilannekuvan kerääminen ja raportointi • digiturva-arkkitehtuurin kehittäminen
Liikenne- ja viestintäministeriö	• Digitoimisto • kyberturvallisuuden EU-asiat
Liikenne- ja viestintävirasto Traficom ja Kyberturvallisuuskeskus	Kyberturvallisuuskeskus: • kerää ja tuottaa kyberturvallisuuden tilannekuvaa • ylläpitää kansallisia tiedonvaihtoryhmiä (ISAC) ml. valtiohallinnon tiedonvaihtoryhmä • tukee ennen kaikkea huoltovarmuuskriittisiä organisaatioita kyberturvallisuuden kehittämisessä • tukee ennen kaikkea huoltovarmuuskriittisten organisaatioiden kyberturvallisuuden harjoittelua • auttaa organisaatioita havaitsemaan niihin kohdistuvia tietoturvaloukkauksia ja resurssiensa puitteissa loukkausten selvittämisessä • tarjoaa tietojärjestelmien turvallisuusarviointia ja -hyväksyntäpalveluja sekä ohjaa hyväksyttyjen arviointilaitosten toimintaa • toimii Euroopan kyberturvallisuuden kompetenssikeskuksen ja kyberturvallisuusverkoston kansallisena koordinaatiokeskuksena
Poliisi	• tutkii tietoverkkosidonnaisia ja -avusteisia rikoksia • tuottaa tilannekuvatietoa tietoverkkosidonnaisista ja -avusteisista rikoksista ja niihin liittyvistä ilmiöistä
Sosiaali- ja terveysministeriö	• sektorilainsäädännön mukaiset vastuut • ei erityisiä digitaalisen turvallisuuden poikkihallinnolliseen yhteistoimintaan liittyviä vastuita
Valvira	• valvoo yleisesti sosiaali- ja terveydenhuollon yksiköiden toimintaa ja osana tätä valvontaa yksiköiden tietoturvallisuussuunnitelmia ja niiden noudattamista

Toimija	Tehtävät
Maa- ja metsätalousministeriö	• sektorilainsäädännön mukaiset vastuut • ei erityisiä digitaalisen turvallisuuden poikkihallinnolliseen yhteistoimintaan liittyviä vastuita
Työ- ja elinkeinoministeriö	• Digitoimisto • sektorilainsäädännön mukaiset vastuut • Business Finland, VTT digiturvallisuuteen liittyvien koko yhteiskuntaa koskevien asioiden ohjaus
Huoltovarmuuskeskus	HVK:n koordinoimien sektorien tehtäviä: • seurata, selvittää, suunnitella ja valmistella huoltovarmuutta • tehdä selvityksiä korvaavien toimintojen kehittämiseksi • hankkia ja ylläpitää toimialojen toimintoja ja toimintaedellytyksiä koskevia tietoja • järjestää valmiuden ylläpitämiseksi tarpeellisia tiedotus-, koulutus- ja harjoitustilaisuuksia
Aluehallintovirastot	• edistää peruspalvelujen saatavuutta sekä sisäistä turvallisuutta ja turvallista elin- ja työympäristöä omilla alueillaan
Suomen Kuntaliitto	Kuntaliiton yhteistoimintaan liittyviä tehtäviä: • vapaaehtoisten yhteistyöryhmien koordinointi • kuntien neuvonta ja tiedottaminen • toiminnan kehittäminen
Kunnat	• säädetyt tehtävät, joihin sisältyvät tiedonhallintalain velvoitteiden mukaiset tehtävät • vapaaehtoiseen yhteistyöhön osallistuminen
Hansel	• yhteishankintojen koordinointi • hankintojen yhteistoiminnan järjestäminen
Kuntayhtymät ja kuntien omistamat yritykset	• osaamisverkoston ylläpito • yhteistoiminta palvelujen kehittämiseksi
Yliopistot	• digitaalisen turvallisuuden opetus- ja tutkimustoiminnan yhteistoiminta julkisen hallinnon toimijoiden kanssa
VTT Oy	• digitaalisen turvallisuuden palveluja yrityksille sekä julkiselle hallinnolle
Finnish Information Security Cluster – Kyberala ry.	• kyber- ja tietoturvallisuusalan organisaatioiden edunvalvoja ja verkostoitumisalusta

3 Kansainvälisestä yhteistoiminnan vertailusta

Digitaalisen turvallisuuden yhteistoiminta- ja hallintamallien kansainvälisen vertailun tarkoituksena oli selvittää, mitä julkisen hallinnon digitaalisen turvallisuuden toiminnallisen tason keskitettyjä tehtäviä verrokkivaltioissa on tunnistettavissa ja miten ne on organisoitu. Valtioneuvoston periaatepäätöksen 8.4.2020 julkisen hallinnon digitaalisesta turvallisuudesta taustatyönä valmistui helmikuussa 2020 selvitys[15], jossa vertailtiin kahdeksan verrokkivaltion ja Suomen digitaalisen turvallisuuden rakenteita ja toteutuksia. Verrokkivaltiot olivat Alankomaat, Australia, Iso-Britannia, Israel, Ruotsi, Saksa, Venäjä ja Viro. Tämän selvitysraportit tiedot on kansainvälisessä vertailussa ajantasaistettu ja tarkennettu ottaen erityisesti huomioon kussakin verrokkivaltiossa keskitetysti toiminnallisella tasolla, lähinnä virastoissa, toteutettuja tieto- ja kyberturvallisuustehtäviä. Vertailun tulokset on julkaistu tämän selvityksen taustamuistiossa[16]. Muistion keskeiset näkökulmat on kuvattu tässä luvussa.

3.1 EU:n digitaalinen turvallisuus ja kyberturvallisuus

Digitaalisen turvallisuuden varmistamiseksi EU-valtioissa on yhteisiä käytäntöjä:

- yleinen tietosuoja-asetus (General Data Protection Regulation, GDPR[17])
- verkko- ja tietoturvadirektiivi (Directive on Security of Network and Information Systems, NIS (EU) 2016/1148[18]

15 https://vm.fi/documents/10623/307681/Digitaalisen+turvallisuuden+kansainv%C3%A4linen+vertailu/7aafe82e-86e7-7450-358c-f1adfeecb3e5/Digitaalisen+turvallisuuden+kansainv%C3%A4linen+vertailu.pdf?t=1583343825000

16 Digitaalisen turvallisuuden yhteistoiminta- ja hallintamallien kansainvälinen vertailu, valtiovarainministeriö 25.4.2022

17 (EU) 2016/679 GDPR https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

18 (EU) 2016/1148 NIS https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

- Euroopan Parlamentin ja Neuvoston direktiivi kyberturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella ja verkko- ja tietoturvadirektiivin (EU) 2016/1148 kumoamisesta, eli niin sanottu NIS2[19]
- akkreditointi- ja markkinavalvonta-asetus (New Legislative Framework, NLF) [20]
- kyberturvallisuusasetus[21]
- Euroopan kyberturvallisuuden kompetenssikeskusta ja kyberturvallisuusverkostoa koskeva asetus (Regulation of European Cybersecurity Competence Centre and the Network of National Coordination Centres)[22]
- EU:n radiolaitedirektiivin delegoidut asetukset (Delegated Act supplementing the Radio Equipment Directive).

Yleisessä tietosuoja-asetuksessa asetetaan organisaatioille henkilötietojen keräämistä, säilytystä ja hallinnointia koskevat tarkat vaatimukset. NIS-direktiivissä asetetaan yleisiä tietoturvavaatimuksia erikseen määritellyille kriittisille toimialoille sekä velvoite ilmoittaa merkittävistä tietoturvaloukkauksista. NIS2-direktiivillä säädetään tiukempia tietoturvavaatimuksia, laajennetaan lainsäädännön soveltamisalaa uusille toimialoille ja toimintoihin, kuten julkishallinnon sektorille, sekä annetaan uusia valvontamenetelmiä kansallisten valvontaviranomaisten käyttöön. NLF-asetuksella on säädetty akkreditointitoiminnasta ja markkinavalvonnan vaatimuksista Euroopan unionin tasolla, mukaan lukien kansallisten akkreditointielimien velvollisuudet tehtävissään. Lisäksi digitaaliseen turvallisuuteen suoraan vaikuttavia säädöshankkeita ovat mm. EU:n kyberkestävyyssäädös (Cyber Recilience Act) sekä kriittisiä toimijoita koskeva direktiivi (Directive of the Resilience of Critical Entities).

Vuonna 2019 annettuun asetukseen Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 (kyberturvallisuusasetus) liittyen valmistellaan asiakohtaisia sertifiointimalleja ja -skeemoja, kuten esimerkiksi eurooppalainen kyberturvallisuuden sertifiointikehys, jossa vahvistetaan tärkeimmät horisontaaliset vaatimukset kehitettäville eurooppalaisille kyberturvallisuuden sertifiointijärjestelmille. Määritellyn kehyksen ansiosta tieto- ja viestintätekniikan tuotteita ja palveluja koskevat sertifikaatit voidaan tunnustaa ja ottaa käyttöön kaikissa jäsenvaltioissa. Uuteen kehykseen sisältyy kattava joukko sääntöjä, teknisiä

19 COM(2020) 823 final NIS2 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823

20 (EC) No 765/2008 NLF https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008R0765

21 (EU) 2019/881 https://eur-lex.europa.eu/eli/reg/2019/881/oj

22 (EU) 2021/887 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R0887

vaatimuksia, standardeja ja menettelyjä, joiden avulla pyritään rakentamaan luottamusta, lisäämään kyberturvallisuusmarkkinoiden kasvua sekä helpottamaan EU:n laajuista kauppaa. Parhaillaan valmistellaan esimerkiksi EU:n yhteistä mallia (skeema) pilviteknologioiden turvallisuuden sertifioimiseksi (European Cybersecurity Certification Scheme for Cloud Services). EU:n vuonna 2004 perustetun kyberturvallisuusviraston (The European Union Agency for Cybersecurity, ENISA) tehtävänä on valmistella malliluonnos komission ja jäsenmaiden käsiteltäväksi. Asetuksella ENISAlle annettiin lisäksi entistä vahvempi mandaatti tukea jäsenmaita, EU:n toimielimiä ja muita sidosryhmiä kyberhyökkäysten torjumisessa. ENISAn määräaikainen rooli muutettiin pysyväksi samalla, kun sen tehtäväkenttää laajennettiin EU:n verkko- ja tietoturvavirastosta (European Network and Information Security Agency) EU:n kyberturvallisuusvirastoksi.[23,24]

Euroopan Kyberturvallisuuden kompetenssikeskusta ja kyberturvallisuusverkostoa koskeva asetus (EU 2021/887) tuli voimaan 28.6.2021. Asetuksen tavoitteena on syventää julkisen sektorin, yksityisen sektorin ja tutkimusmaailman välistä yhteistyötä kyberturvallisuuden tutkimuksen, tuotekehityksen ja innovoinnin alueilla. KTK on nimitetty Suomen kansalliseksi kyberturvallisuuden koordinointikeskukseksi, ja se hoitaa Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen ja kansallisten koordinointikeskusten verkoston perustamisesta annetun Euroopan parlamentin ja neuvoston asetuksen 6. artiklassa tarkoitetun kansallisen koordinointikeskuksen tehtäviä.[25]

Digitaalista turvallisuutta koskevan yhteisen lainsäädännön lisäksi EU:ssa on valmisteltu kyberturvallisuusstrategia. EU:n uuden kyberturvallisuusstrategian tarkoituksena on vahvistaa Euroopan sietokykyä kyberuhkia vastaan ja varmistaa, että kaikki kansalaiset ja yritykset voivat hyötyä täysimääräisesti luotettavista palveluista ja digitaalisista välineistä. Strategia kuvaa kolme instrumenttia (sääntely, investoinnit ja politiikat), joiden avulla ohjataan EU:n toimenpiteitä kolmella alueella:[26]

- resilienssi sekä teknologinen riippumattomuus ja johtajuus,
- operatiivinen kyky häiriöiden havainnointiin ja hallintaan (prevent, deter, respond)
- avoimen globaalin kybertoimintaympäristön edistäminen yhteistyön avulla.

23 https://www.consilium.europa.eu/fi/policies/cybersecurity/

24 https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

25 Laki sähköisen viestinnän palveluista (2014/917) §304

26 https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

3.2 Keskitetyistä tieto- ja kyberturvallisuustehtävistä

Suomen tavoin jokaisessa verrokkivaltiossa on muodostettu keskitetty kyberturvallisuustoimija, johon on koottu koko yhteiskuntaa palvelevia digitaalisen turvallisuuden ja kyberturvallisuuden tehtäviä. Kyberturvallisuustoimijalle keskitetyt tehtävät palvelevat tyypillisesti yhteiskunnan teknisiä tieto- ja kyberturvallisuuden operatiivisia tarpeita. Kyberturvallisuustoimijalle annetut tehtävät ja se, miten paljon ja mitä tehtäviä on keskitetty yhdelle toimijalle, vaihtelevat maittain. Osassa vertailun maista julkisen hallinnon digitaaliseen turvallisuuteen liittyviä tehtäviä ja ohjausta ei ole erotettu muista kyberturvallisuuteen liittyvistä tehtävistä ja ohjauksesta samalla tavoin kuin Suomessa. Toisaalta Suomessa KTK vastaa monista sellaisista kyberturvallisuuden tehtävistä, jotka eivät kuulu esimerkiksi Ruotsin tai Iso-Britannian kyberturvallisuuskeskusten tehtäviin.

Kyberturvallisuudesta vastaavan toimijan organisointi noudattaa verrokkivaltioissa yleensä kahta eri tapaa. Alankomaissa, Australiassa ja Isossa-Britanniassa kyberturvallisuustoimija kuuluu osaksi keskitettyä turvallisuusvirastoa, jonka tehtäviin voi kuulua esimerkiksi sisäinen turvallisuus tai terrorismin torjunta. Israelin, Saksan ja Viron keskitetty toimija on puolestaan suoraan jonkin ministeriön alaisuudessa: Israelissa pääministerin, Saksassa sisäministeriön ja Virossa talous- ja viestintäministeriön.

Keskitetyn toimijan tehtäviin kuuluvat mm. kyberturvallisuushäiriöiden hallinta (CERT- ja CIRT-toiminta), tietoverkkojen valvonta, ympärivuorokautisen tilannekeskuksen operointi sekä kyberturvallisuuden uhka-arvion muodostaminen ja sen jakaminen. Kyberturvallisuuskeskukset antavat lisäksi neuvontaa ja tuottavat digitaalisen toimintaympäristön turvallisuutta koskevia ohjeita hallinnolle, yrityksille ja yksityishenkilöille. Lisäksi kansalliset kyberturvallisuuskeskukset tukevat muita viranomaisia kyberhäiriötilanteiden selvittämisessä ja tutkinnassa.

EU-valtioiden kyberturvallisuuskeskukset ovat NIS-direktiivissä määriteltyjä yhteyspisteitä. Verrokkivaltioiden erityispiirteiden takia kyberturvallisuuskeskuksille on näiden lisäksi annettu tehtäväksi digitaalisen turvallisuuden tuotteiden turvallisuuden arviointi (Iso-Britannia, Saksa ja Suomi), digitaalisen turvallisuuden tutkimuksen koordinointi (Alankomaat[27]) ja digitaalisen turvallisuuden henkilösertifiointi (Australia, Iso-Britannia, Israel ja Saksa). Kyberturvallisuuskeskukset toimivat kiinteässä yhteistyössä muiden turvallisuudesta vastaavien viranomaisten kanssa. Ne toimivat tarvittaessa hallitustensa asiantuntijoina toimialueensa asioissa ja osallistuvat kyberturvallisuusstrategioiden laatimiseen.

27 https://english.ncsc.nl/research

Australiassa keskitetyn toimijan (ACSC) alaisuudessa toimii lisäksi yhteisö kyberturvallisuuskeskuksia (Joint Cyber Security Centres, JCSC). Ne tukevat ACSC-kumppanuusohjelmaa, jonka tarkoituksena on tuoda yhteen yrityksiä ja tutkimusyhteisöä sekä osavaltioiden, alueiden ja Australian hallituksen virastoja avoimessa ja yhteistyöhön perustuvassa ympäristössä.

Ruotsissa hallitus on asettanut kansallisen varautumisviranomaisen (MSB), puolustusvoimien, signaalitiedustelun (FRA) ja turvallisuuspoliisin (Säpo) tehtäväksi perustaa Ruotsin kyberturvallisuuskeskus[28]. Keskuksen on tarkoitus käynnistyä vaiheittain 2021–2023 välisenä aikana. Uuden, keskitetyn kyberturvallisuuskeskuksen tavoitteena on koota yhteen ja vahvistaa Ruotsiin kohdistuvien kyberturvallisuusuhkien ennaltaehkäisy-, havainnointi- ja hallintakykyä.[29] Keskuksen toimintaan osallistuvien viranomaisten tehtäviä ei kuitenkaan siirretä perustettavalle Ruotsin kyberturvallisuuskeskukselle, vaan viranomaiset vastaavat edelleen niille lainsäädännössä asetetuista tehtävistä keskuksen toimintaan liittyvien tehtävien rinnalla. Ruotsin kyberturvallisuuskeskuksen ympärille rakennettava kyberturvallisuuden yhteistoimintamalli vastaa osittain Suomen olemassa olevaa yhteistoimintamallia. Ruotsin kyberturvallisuuskeskuksen käynnistymisen jälkeen jokaisessa verrokkivaltiossa on keskitetty, yhden tahon ohjauksessa oleva kyberturvallisuuskeskus.

Venäjällä varsinaista kyberturvallisuusvirastoa ei ole tunnistettu, mutta digitaalisesta kehityksestä, viestinnästä ja joukkoviestimistä vastaavan ministeriön (Минцифры России, ”Mintsifry Rossii”) alle on sijoitettu mm. tietoliikenteen turvaamiseen, teknologioiden seurantaan ja edistämiseen sekä tietosuojaan liittyviä tehtäviä. Lisäksi Venäjän turvallisuuspalvelu (FSB) vastaa turvallisuudesta laajasti.

Digitaalisen turvallisuuden kansainvälisiä yhteistyöryhmiä on useita ja niiden toiminnan painopiste vaihtelee. Suomelle kyberturvallisuuskysymyksissä erityisesti EU on keskeinen toimija ja sitä koskevissa kyberkysymyksissä valtioneuvoston kanslia toimii valtionhallinnon koordinoijana. EU:n ohella kybertoimintaympäristöä koskevaa keskustelua käydään muun muassa YK:ssa, OECD:ssä, NATOssa, ETYJ:ssä, Euroopan neuvostossa ja Pohjoismaiden neuvostossa. Myös monet alueelliset järjestöt käsittelevät kyberturvallisuuskysymyksiä. Suomessa ulkoministeriö, liikenne- ja viestintäministeriö, sisäministeriö ja puolustusministeriö osallistuvat aktiivisesti kybertoimintaympäristöä koskevaan globaaliin, alueelliseen ja kahdenväliseen keskusteluun ja vaikuttavat kansainvälisellä kyberturvallisuuden asialistalla olevien kysymysten edistämiseen Suomen etujen mukaisesti.

28 https://www.regeringen.se/4af5d9/globalassets/regeringen/dokument/forsvarsdepartementet/regeringsbeslut/uppdrag-om-fordjupad-samverkan-inom-cybersakerhetsomradet-genom-ett-nationellt-cybersakerhetscenter.pdf

29 https://www.cfcs.se/om-centret/

Suomen kansainvälistä asemaa digitaalisen turvallisuuden alueella seurataan useiden kansainvälisten indeksien perusteella. Näitä ovat esimerkiksi International Telecommunication Unionin (ITU) Global Cybersecurity Index (GCI) ja Viron e-Governance Academyn National Cyber Security Index (NCSI). GCI mittaa maiden sitoutumista kyberturvallisuuteen kansainvälisellä tasolla tietoisuuden lisäämiseksi ja kyberturvallisuuden merkittävyyden korostamiseksi. Koska kyberturvallisuus ulottuu monille teollisuusaloille, arvioidaan kunkin maan kehitystasoa tai sitoutumista viidestä näkökulmasta: 1) oikeudelliset toimenpiteet, 2) tekniset toimenpiteet, 3) organisatoriset toimenpiteet, 4) valmiuksien kehittäminen ja 5) yhteistyö. NCSI mittaa maiden valmiutta kyberuhkien torjumiseen ja kyberhäiriöiden hallitsemiseen. NCSI on myös tietokanta, joka sisältää työkalun kansallisen kyberturvallisuusvalmiuksien kehittämiseen. Vuonna 2020 Suomi sijoittui GCI-vertailussa sijalle 22, ja 10.3.2022 Suomi oli sijalla 10 NCSI-vertailussa[30].

30 NCSI Finland https://ncsi.ega.ee/country/fi/

4 Tavoitetilan kuvaus

4.1 Julkisen hallinnon laaja-alainen digitaalisen turvallisuuden yhteistoiminta

Digitaalisten palveluiden ja tietojärjestelmien kehitys on muuttanut julkisen hallinnon toimintaa. Digitaaliset ratkaisut ja niissä kerättävä tieto muodostavat perusteen digitaalisen turvallisuudenkin yhteistoiminnalle. Yhteistoiminnan avulla voidaan siirtyä rakentamaan yhteisiä digitaalisen turvallisuuden palvelukokonaisuuksia sekä tiedon jakamisen ja jalostamisen rajapintoja. Yhteisten palvelujen keskeisiä etuja ovatkin osaamisen keskittäminen, yhtenäiset prosessit, järjestelmien yhteensopivuus ja päällekkäisen työn vähentäminen esimerkiksi kilpailutuksissa.[31]

Nykytilakuvauksen perusteella muodostunut kuva julkisen hallinnon digitaalisen turvallisuuden kansallisen tason yhteistoiminnasta tuo esiin tarpeen vahvalle tehtävien organisoinnille ja selkeyttämiselle, uudelleen resursoinnille ja voimavarojen keskittämiselle, osaamisen kehittämiselle, tiedon jakamiselle sekä yhteiselle tilannekuvalle. Monet yhteistoimintaan tarvittavat elementit ovat jo nykyisin toiminnassa, mutta niiden laajentaminen kattamaan kaikki tarvittavat tahot on tekemättä. Nykyisten digitaalisen turvallisuuden yhteistoiminnan ongelmien ratkaiseminen vaatii siten merkittäviä muutoksia yhteistoiminnan hallintaan ja ohjaamiseen sekä resurssien uudelleen järjestämiseen ja lisäämiseen. Raporttia valmisteltaessa näihin ongelmiin vastaamiseksi on osin jo tehty toimenpiteitä, kuten kyberturvallisuuden ja julkisen hallinnon varautumisen ohjaamisen lisääminen digitalisaation, datatalouden ja julkisen hallinnon kehittämisen ministeriryhmän tehtäviin sekä digitoimiston perustaminen. Toimenpiteiden tuomaa muutosta ja vaikuttavuutta ei ole mahdollista vielä täysin arvioida.

Organisaatiot ovat tietoisia toimintaympäristönsä kompleksisuudesta ja omien resurssiensa riittämättömyydestä. Alati muuttuva digitaalisen turvallisuuden toimintaympäristö edellyttää joustavia yhteistoiminnan rakenteita, jotka toimivat ympäristön jatkuvan muutoksen tilassa. Valtionhallinnon, hyvinvointialueiden ja kuntien digitaalisen turvallisuuden yhteistoiminta edellyttää sekä säänneltyjä että epämuodollisia rakenteita,

31 Virasto 2020 loppuraportti, https://vm.fi/documents/10623/3203079/Virasto2020+-loppuraportti+(20.3.2019)/937279ce-799a-f511-ef2b-80845cb73760/Virasto2020+-loppuraportti+(20.3.2019).pdf

entistä tiiviimpää yhteistyötä ja yhteistyön koordinointia rajallisten resurssien tehokkaaksi hyödyntämiseksi.

EU:n verkko- ja tietoturvadirektiivi eli NIS-direktiivi tulee huomioida julkisen hallinnon digitaalisen turvallisuuden ohjaukseen tarvittavien säädösten määrittämisessä ja toimeenpanossa. Direktiivissä säädetään yhteiskunnan kriittisen infrastruktuurin tarjoajien ja toimijoiden tietoturvavelvollisuuksista sekä havaitsemistaan tietoturvauhkista ja -loukkauksista (eli häiriöistä) ilmoittamisesta. NIS-direktiiviä ja direktiivin mukaisesti toteutettua kansallista lainsäädäntöä sekä niissä asetettuja velvoitteita sovelletaan erikseen direktiivissä määritellyillä toimialoilla[32]. Suomessa velvoitteet säädetään kyseisten toimialojen omassa lainsäädännössä ja niitä valvovat toimialojen omat valvontaviranomaiset. Säädetyt velvoitteet koskevat myös kuntia ja hyvinvointialueita siltä osin kuin ne tai niiden omistamat kuntayhtymät tarjoavat NIS-lainsäädännön soveltamisalaan kuuluvia palveluja kuten vesihuoltoa tai sosiaali- ja terveyspalveluja.

Käytännössä NIS-direktiivissä ja siten pääasiassa myös kansallisessa lainsäädännössä asetetut tietoturvavelvoitteet ovat hyvin ylätasoisia ilman konkreettisia tietoturvan toteuttamisen tai häiriöistä ilmoittamisen vähimmäisvaatimuksia. Tämä sallii kansalliselle lainsäätäjälle, valvovalle viranomaiselle ja velvoitteiden kohteena olevalle paljon velvoitteisiin liittyvää tulkinnanvaraa[33], mikä on huomioitu NIS2-direktiivissä. Siihen sisältyy lainsäädännön soveltamisalan selventämistä ja merkittävää laajentamista uusille toimialoille, koska direktiiviä on sovellettu hyvin eri tavoin eri jäsenmaissa ja merkittäviä toimialoja on jäänyt kokonaan sääntelyn ulkopuolelle. Uusiin soveltamisalueisiin kuuluvat julkisen hallinnon sektori sekä jätevesi- ja jätehuolto.

---

32 NIS-direktiivin velvoitteet koskevat sähkönjakeluverkon ja suurjännitteisen jakeluverkon haltijoita, sähkön kantaverkonhaltijaa, maakaasun siirtoverkonhaltijaa, sosiaali- ja terveyspalvelujen tarjoajia, lääkinnällisten laitteiden valmistajia, sosiaali- ja terveyspalveluissa käytettyjen tietojärjestelmien valmistajia, pankkeja, pankkien keskusyksikköjä, EU-pankkien sivuliikkeitä, pörssiä, liikennepalvelujen (ilmailu, merenkulku, rautatieliikenne ja maantieliikenne) tarjoajia, vesilaitoksia, teleyrityksiä (DNS-palvelujen ja yhdysliikennepisteiden tarjonta), .fi-domain -palvelun tarjoajaa, pilvipalveluja, hakukoneita sekä verkon keskitettyjen markkinapaikkojen tarjoajia.

33 Esimerkiksi tietoturvallisuudesta NIS-direktiivissä on säädetty seuraavasti: ”…keskeisten palvelujen tarjoajat toteuttavat asianmukaiset ja oikeasuhteiset tekniset ja organisatoriset toimenpiteet hallitakseen riskejä, joita kohdistuu niiden verkko- ja tietojärjestelmien turvallisuuteen, joita nämä keskeisten palvelujen tarjoajat käyttävät toiminnoissaan. Näillä toimenpiteillä on varmistettava riskiin suhteutettu verkko- ja tietojärjestelmien turvallisuuden taso uusin tekniikka huomioon ottaen.” …keskeisten palvelujen tarjoajat toteuttavat asianmukaiset toimenpiteet, joilla ehkäistään ja minimoidaan tällaisten keskeisten palvelujen tarjoamisessa käytettyjen verkko- ja tietojärjestelmien turvallisuuteen vaikuttavien poikkeamien vaikutus näiden palvelujen jatkuvuuden takaamiseksi”.

Julkisen hallinnon digitaalisen turvallisuuden säädösten tulee olla lähtökohtaisesti yhteneviä muiden kriittisten toimialojen säädösten kanssa. Siten niiden kohteena oleva julkisen hallinnon toimija ei joudu tarpeettomasti soveltamaan erilaisia ja ristiriitaisia vaatimuksia toiminnassaan. Esimerkiksi hyvinvointialue toimii sekä yleisenä julkisen hallinnon toimijana että NIS-direktiivin alaisena sosiaali- ja terveyspalvelujen tarjoajana, jolloin sekä julkisen hallinnon toimijoille yleisesti että sosiaali- ja terveyspalvelujen tarjoajille erityisesti asetettujen vaatimusten tulisi olla ristiriidattomia. Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminnan tavoitetilaan liittyviä odotuksia on kuvattu tarkemmin taulukossa 7.

Taulukko 7. Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminnan tavoitetilaan liittyviä odotuksia

Yhteistoiminta-alue/palvelu	Kehitysehdotus
Digitaalisen turvallisuuden ohjaus	Digitaalista turvallisuutta on tuettava, ohjattava, seurattava ja arvioitava aiempaa vahvemmin koko julkisessa hallinnossa ja sen eri alueilla: ministeriöt, valtionhallinnon toiminnallinen ja operatiivinen taso, hyvinvointialueet ja kunnat. Ohjausta tulee toteuttaa strategia-, resurssi-, normi- ja informaatio-ohjauksena. • Ohjaukseen tarvitaan vastuutaho, joka ei ole sidottu hallinnonalojen operatiiviseen toimintaan. Vastuutaholla on oltava olla riittävät valtuudet ja työkalut (esimerkiksi rahoitusinstrumentti) tehokkaan ohjauksen toteuttamiseksi. Eri alueilla ja tasoilla tapahtuva ohjaaminen tulee sovittaa yhteen. Julkisen hallinnon digitaalisen turvallisuuden yhteisten tehtävien ja palveluiden tarjoamisen keskittämistä on jatkettava (yhden luukun periaate), vaikka taustalla palveluita tuottaa useampi julkinen tai yksityinen toimija. • Julkisen hallinnon digitaalisen turvallisuuden ohjausta, valvontaa ja toimeenpanon seurantaa sekä niihin liittyviä vastuita on selkeytettävä ja viestintää niistä on lisättävä. Digitalisen turvallisuuden vahvempi ohjaaminen mahdollistaisi yhteistoiminnan lisäämisen useilla eri alueilla. Ohjaamisen keinona voitaisiin vahvemmin käyttää koko julkisessa hallinnossa yhteisten tavoitteiden ja tarpeiden määrittämisen pohjalta toteutettuja yhteishankintoja ja -hankkeita. Tavoitteena on entistä yhtenäisempi toiminta läpi julkisen hallinnon, mikä vaatii entistä enemmän yhteisten järjestelmien ja sovellusten käyttämistä huomioiden kuitenkin varautumisen, toimintavarmuuden, tietoturvallisuuden ja tietosuojan näkökulmat. Vahvemman ohjaamisen avulla on mahdollista toteuttaa niin valtiotoimijoille kuin hyvinvointialuille ja kunnille enemmän yhteisiä palveluja. Lisäksi esimerkiksi yhteishankintayksikön Hanselin avulla on mahdollista toteuttaa enemmän yhteisiä kilpailutuksia, jotka eivät vaadi toimijakohtaisia minikilpailutuksia. Näin voidaan huomioida esimerkiksi huoltovarmuusvaatimuksia ja niiden toteutumista entistä paremmin. Lisäksi hankintojen tietoturvallisuusvaatimuksia ja sopimusehtoja koskevilla suosituksilla voidaan yhtenäistää julkisen hallinnon tietoturvallisuusvaatimusten toteutumista. Yhteisillä malleilla voidaan myös helpottaa yksittäisen organisaation tietojärjestelmien hankintaa.

Yhteistoiminta-alue/palvelu	Kehitysehdotus
	On esitetty, että Suomessa hyvinvointialueilla tulisi tulevaisuudessa olla käytössä muutama toistensa kanssa yhteentoimiva ydinasiakas- ja potilastietojärjestelmä, mikä mahdollistaisi järjestelmien ja niiden digitaalisen turvallisuuden tason kustannustehokkaan ylläpidon ja kehittämisen sekä varautumisen kannalta riittävän hajauttamisen. Muutaman järjestelmän ja niiden digitaalisen turvallisuuden ylläpitäminen Suomessa on helpompaa ja kustannustehokkaampaa kuin nykyisten lukuisten järjestelmien. Eri järjestelmiä tulee kuitenkin olla riittävä määrä, jotta koko Suomessa ei toimita yhden järjestelmän varassa. Järjestelmät voivat lisäksi olla hyvinvointialueittain toisistaan eriytettyjä, vaikka niissä olisikin samat ja yhdessä kehitetyt ohjelmistot. Yhtäkin järjestelmää voidaan käyttää, mutta tällöin on huolehdittava riittävästä palvelinympäristöjen maantieteellisestä eriyttämisestä ja häiriötilanteissa käyttöönotettavista 1–2 varajärjestelmästä eli tuotantojärjestelmän kopiosta. Toisaalta on todettu, että tämä lähestymistapa on ongelmallinen muun muassa kilpailun rajoittamisen vuoksi. Muutaman järjestelmän malli voi johtaa siihen, että vain suuret tietojärjestelmätoimittajat voivat toimittaa järjestelmiä hyvinvointialueille. Tämä voi puolestaan johtaa vanhojen teknologioiden ja prosessien käyttämiseen, mikä voi edelleen altistaa erilaisille vaikeasti hallittaville haavoittuvuuksille sovelluskoodin määrän kasvaessa ja teknologioiden vanhetessa. Tietoturvallisuutta ja tietosuojaa voidaan toteuttaa ketterästi ja riskilähtöisesti arvioimalla, teknisellä testauksella ja asianmukaisilla tietoturvaa ja henkilötietojen käsittelyä koskevilla sopimuksilla. Lisäksi on huomioitava, että vaikka hyvinvointialueilla olisi käytössään vain yksi järjestelmä, liitettäisiin siihen kymmeniä muita järjestelmiä (laboratorio, radiologia, sosiaalihuolto, jne.), joiden tietoturvasta tulisi myös huolehtia. Yksityiset ja työterveydenhuollon toimijat tuottavat ison osan kertomusdatasta. Lisäksi on otettava huomioon, että yhteentoimivuuden kannalta järjestelmien sisältöjä vakioivat Kanta-palvelut, jotka ovat hyvinvointialueille erittäin keskeisiä tietolähteitä. Hyvinvointialueitten todetaan tarvitsevan tukea vastuutaholta. Hallintamalleissa tätä osiota on syytä tarkastella yksityiskohtaisemmin ja käytännönläheisesti. Yliopistojen ja ammattikorkeakoulujen näkökulmasta on tärkeää, että viranomaistoimijoiden ja korkeakoulujen välinen yhteistyö on toimivaa ja kokonaisturvallisuuden tilannekuva on helposti hyödynnettävissä ja ajantasaista. Toisaalta on epäselvää miten ehdotetun ohjausmallin ja korkeakoulujen yhteensovittaminen tapahtuu. Esitetty vastuutaho ohjausvaltuuksineen ei sovi yhteen korkeakoulujen autonomian kanssa. Lainsäädäntöön ja asetuksiin nojautuva malli vaikuttaa myös jäykältä. Ohjauksen tulevina haasteina ovat lisäksi rahoitus ja resursointi; miten varmistetaan, että organisaatiot osoittavat riittävän määrän resursseja ohjausmekanismien osoittamien kohteiden toteuttamiseen? Valtioneuvoston periaatepäätöstä 8.4.2020 julkisen hallinnon digitaalisesta turvallisuudesta ei ole toistaiseksi tarvetta ajantasaistaa. Se kuvaa edelleen hyvin julkisen hallinnon digitaalisen turvallisuuden linjaukset ja kehittämisen painopistealueet. Sen toteuttamisohjelma Haukka päättyy vuonna 2023.

Yhteistoiminta-alue/palvelu	Kehitysehdotus
	• Vuodesta 2023 alkaen tarvitaan Haukka-ohjelmaa seuraava julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma toimeenpanosuunnitelmineen. Sen tulee sisältää tärkeimmät tavoitteet, kehitystoimenpiteet ja aikataulut. Toimeenpano-ohjelman tavoitteiden asettaminen ja tavoitteista johdettujen kehitystoimenpiteiden on pohjauduttava mitattuun ja analysoituun tietoon digitaalisen turvallisuuden tilasta julkisessa hallinnossa sekä riskiarvioon digitaalisen turvallisuuden nykyisistä ja tulevaisuuden uhkista. Tavoitteita tulee tarkastella ja päivittää vuosittain. Kehitystoimenpiteitä suunnitellaan, suunnataan uudelleen ja toteutetaan tavoitteisiin pohjautuen. • Digitaalisen turvallisuuden kehittämisohjelman yhteisten tavoitteiden toteutumista on seurattava aktiivisesti. Kehitystoimenpiteiden vaikutuksia ja vaikuttavuutta tulee mitata ja arvioida säännöllisesti. Mittaustulokset ja arvioinnit tulee jakaa keskeisille julkisen hallinnon toimijoille vaarantamatta kuitenkaan yksittäisen organisaation tai yhteiskunnan kannalta kriittisiä, salassa pidettäviä tai turvallisuusluokiteltuja tietoja. • Tulee määrittää taho tai yhteistoimintaelin, joka koordinoi turvallisuuden kehitystoimenpiteitä ja seuraa niiden toteutumista. Digitaalisen turvallisuuden ohjauksen vastuutahon tulee olla tiiviissä vuorovaikutuksessa ja yhteistyössä kyseessä olevan tahon tai yhteistyöelimen kanssa. Omaehtoisten kyselyiden lisäksi mittaamisen ja arvioinnin tulee perustua todelliseen tilanteeseen ja todennettuihin mittareihin. **Hyvinvointialueille** tarvitaan joustava yhteistoimintamalli, jossa digitaalisen turvallisuuden hallintaan liittyviä periaatteita ja rakenteita on mahdollista suunnitella ja linjata. Hyvinvointialueiden joustava yhteistoimintamalli edesauttaa alueellista ja seudullista digitaalisen turvallisuuden hallinnan kehittymistä. Hyvinvointialueiden ja kuntien tarkoituksenmukaista varautumisen, häiriöitten hallinnan ja toiminnan jatkumisen yhteistoimintaa on tuettava. Arjen turvallisuus edellyttää yhteisten tavoitteiden yhteentoimivia käytäntöjä ja yhdenmukaista ohjeistusta. Tämän toteutuminen edellyttää kansallisen tason kiinteää ohjausta. Hyvinvointialueet haluavat vapaaehtoisuuteen perustuvaa epämuodollista yhteistyötä, jossa on mahdollista keskustella digitaalisen turvallisuuden teemoista ja vaihtaa tietoa toimivista käytännöistä. Hyvinvointialueilla on vastuullaan infrastruktuurit, joiden ylläpito ja digitaalisen turvallisuuden kehittäminen edellyttävät osaamista ja resursseja. Hyvinvointialueet tarvitsevat osaavaa henkilöstöä, joka ymmärtää kriittiseen infrastruktuuriin liittyvät turvallisuusvaatimukset sekä tavat, joilla ne voidaan toteuttaa. Vastuiden kuvaaminen sekä infrastruktuurien digitaalisen turvallisuuden vaatimukset ovat kokonaisuuksia, joihin hyvinvointialueet odottavat apua viranomaisilta. Hyvinvointialueitten irtautuminen kuntapohjaisista ICT-toimintaympäristöistä on käynnissä. Kuitenkin esimerkiksi olemassa olevien sopimussuhteiden ja toiminnallisten riskien takia on syytä varautua yhteistoiminnan jatkumiseen erityisesti infrastruktuuriin liittyvissä hankinnoissa, käyttäjähallinnassa, muutostenhallinnassa sekä häiriötilanteiden hallinnassa.

Yhteistoiminta-alue/palvelu	Kehitysehdotus
	Hyvinvointialueitten ja kuntien välistä yhteistyötä tarvitaan lisäksi turvallisuusasioissa, häiriötilanteisiin varautumisessa sekä työllisyyden hoitamisessa, koska näillä alueilla on paljon yhteisiä tavoitteita. Lainsäädäntö määrittää tehtävät ja ohjaa yhteistyön toteuttamista ja niin hyvinvointialueiden kuin kuntienkin tulisi nimetä eri yhteistyön osa-alueille vastuutahot. Yhteistoiminnan avulla tulisi varmistaa esimerkiksi varautumisen ja toiminnan jatkuvuuden tiedonantovelvoitteiden ja tiedonsaantioikeuksien yhdenmukaisuus. Lisäksi yhteisesti sovittujen käytäntöjen ja poikkeamien hallinnan tavoitteet ja niiden seuranta on dokumentoitava. • Hyvinvointialueiden digitaalisen turvallisuuden yhteistoimintamalli tulee valmistella ja ottaa käyttöön. Hyvinvointialueille tulee tarjota tukea, johon sisältyy muun muassa suosituksia, ohjeita sekä digitaaliseen turvallisuuteen liittyvien vastuiden kuvaamisen ja infrastruktuureihin liittyvien digitaalisen turvallisuuden vaatimusten määrittämisen vaatimuslistoja. • Hyvinvointialueiden tuen antamiseen tarvitaan vastuutaho, joka ymmärtää operatiivista toimintaa ja kykenee toimimaan strategisen ja operatiivisen toiminnan välimaastossa näitä yhdistävänä tekijänä. Vastuutaho vastaa siitä, että annettava tuki on ajan tasalla. – Vastuutaho vastaisi lisäksi annettavien määräysten, ohjeiden, vaatimuslistojen, suositusten ja työkalujen ylläpidosta ja päivittämisestä. Vastuutaho voisi antaa velvoittavia määräyksiä lainsäädännön rajoissa, jolloin digitaalisen turvallisuuden uhkiin olisi mahdollista reagoida nopeammin. Vastuutaho voisi käyttää alihankkijoita esimerkiksi suosituksen tai ohjeen valmistelussa ja valmistelutyön fasilitoinnista, mutta se vastaisi aina lopputuloksesta. – Vastuutaho voisi koota tilannekuvaa hyvinvointialueiden tietoturvallisuuden ja tietosuojan tilanteesta sekä tunnistaa ja priorisoida kansallisia kehityshankkeita ja selvittää näiden rahoitusta kansallisesti. Hyvinvointialueiden yhteistoiminta on haasteiden ratkaisemista yhdessä. Se ei saa olla esimerkiksi ministeriön, viraston tai Kelan sanelua. Hyvinvointialueet tuntevat tietoturvallisuuteen, tietosuojaan ja regulaatioon liittyvät käytännön haasteet ja ne ovat itse parhaat tahot ratkaisemaan näitä haasteita.
Yhteiset määräykset, ohjeet, vaatimukset, suositukset ja työkalut	Yleisiä julkisen hallinnon digitaalisen turvallisuuden normeja on tarpeen selkeyttää. Nykytilan kuvauksen perusteella julkisen hallinnon digitaalista turvallisuutta koskevia säädöksiä ja ohjeistusta annetaan eri tahoilta ja nämä ovat osittain keskenään ristiriitaisia. Ohjeistusta annetaan sekä toimijoita sitovana että suosituksina ja ohjeina, joita toimijat voivat tahtoessaan noudattaa tai soveltaa. Sitovaa ohjeistusta nimitetään useimmiten määräyksiksi ja joskus ohjeiksi. Julkisen hallinnon digitaalisen turvallisuuden kokonaisvaltainen kehittyminen edellyttää yhtenäistä ohjeistusta, joka olisi saatavissa yhdestä paikasta. Vaikka erilaista ohjeistusta tuotettaisiin jatkossakin eri lähteistä, tulisi näiden sisältämien määräysten, ohjeiden, vaatimusten ja suositusten olla keskenään ristiriidattomia.

Yhteistoiminta-alue/palvelu	Kehitysehdotus
	Määräysten, ohjeiden tai suositusten soveltaminen voi olla vaikeaa toimijalle, jolla ei ole riittävästi osaamista tai resursseja. Siksi olisi tuotettava ja ylläpidettävä soveltamisohjeita, jotta määräysten ja ohjeiden käyttöönotto sujuisi mahdollisimman ketterästi. Soveltamisohjeiden pitäisi kuitenkin jättää riittävästi liikkumavaraa erilaisille toteutuksille. Yhteisten määräysten, ohjeiden ja suositusten sekä mahdollisten soveltamisohjeiden keskittämistä riittävän laajapohjaiselle toimijalle tulisi arvioida. Norminomaiseksi tulkittavia ohjeita tai suosituksia tulee välttää ja niiden tulee ennen kaikkea antaa vain esimerkkiohjeistusta siitä, miten säädösten vaatimukset ja velvoitteet on mahdollista täyttää. Jos esimerkiksi säännöstö velvoittaa organisaatiota mittaamaan digitaalisen turvallisuuden hallinnan kypsyystasoa ja tunnistamaan kehitysalueet, voisi organisaatio yhtenä vaihtoehtona täyttää vaatimuksen käyttämällä suosituksessa määriteltyä työkalua, kuten KTK:n kehittämää Kybermittaria, julkisen hallinnon tietoturvallisuuden arviointikriteeristöä Julkria tai DVV:n kehittämää kokonaiskuvapalvelua. Säännösten vaatimusten toteuttamisen hyviä käytäntöjä sekä toiminnan kehittämisen toimintamalleja tulee jakaa yhteistoiminnan kautta viestinnän ja vuorovaikutuksen eri keinoin. Lisäksi on tarjottava selkeää koulutusta työpajoissa, tilaisuuksissa ja eOppiva-oppimisympäristössä. Valtiohallinnon tulee korostaa, että suosituksia ei tule valvonnassa tulkita normatiivisina. Lisäksi valtiohallinnon on siirryttävä ohjaamaan ja valvomaan julkisen hallinnon digitaalisen turvallisuuden tuloksia, kuten esimerkiksi palveluiden turvallisuustason parantumista. Valtiohallinnon tulee myös tarjota yhteisiä työkaluja organisaatioiden tueksi ja digitaalisen turvallisuuden ylläpitämiseksi, mittaamiseksi ja kehittämiseksi julkisen hallinnon organisaatioissa. On tärkeää, että annetut määräykset, ohjeet, vaatimukset, suositukset ja yhteiset työkalut pidetään ajan tasalla. Digitaalisen turvallisuuden yhteisten riskienhallintamallien, määräysten, ohjeiden, vaatimusten, suositusten ja käytettävien palveluiden turvallisuuden hyväksyntäkriteerien tulee olla jatkuvasti päivitettyjä, yhteneviä ja pohjautua yleisesti hyväksyttyihin ja käytettyihin periaatteisiin, kuten yleisiin kansainvälisiin standardeihin. Tällöin julkisen hallinnon toimijat voivat hyödyntää jo markkinoilla olevia tuotteita ja palveluita mahdollisimman laaja-alaisesti ja digitaalisen turvallisuuden arviointia voidaan kehittää nykyistä kattavammaksi. Julkisen hallinnon yhteisiä määräyksiä, ohjeita, vaatimuksia ja suosituksia on yhtenäistettävä kansallisesti. Lisäksi niiden velvoittavuus tulee ilmaista selkeästi osana ohjeistusta. Selkeästi on merkittävä, milloin ohjeistuksessa on kyse lainsäädäntöön verrattavasta linjauksesta ja milloin suosituksesta. Sovellettavan yhteisen lainsäädännön, ohjeiden, sopimusmallien ja tarkistuslistojen kokoaminen yhteistyöverkoston käyttöön esimerkiksi tiedotukseen tarkoitetuille verkkosivuille mahdollistaa myös vähemmillä resursseilla toimivia organisaatioita saamaan kokonaiskuvan tärkeimmistä noudatettavista yhteisistä vaatimuksista.

Yhteistoiminta-alue/palvelu	Kehitysehdotus
	Yhtenäiset mallipohjat ja toimintatavat toimijoiden välillä parantavat tietoturva- ja tietosuojatasoa. Yhteisten määräysten, ohjeiden, vaatimusten ja suositusten sekä yhteishankintojen kehittämistoimintaan tulee myös osallistaa käytännön toimijoita siten, että käytännön työn näkökohdat tulevat otetuksi huomioon. Erityinen tarve on jatkuvuudenhallinnan yhteiselle ohjeistukselle, jossa on huomioitava liitynnät riskienhallintaan. Hyvinvointialueeseen sovellettavat digitaalisen turvallisuuden säännökset on yhdenmukaistettava. Hyvinvointialue toimii jatkossa sekä julkisen hallinnon toimijana että sosiaali- ja terveyspalvelujen ja pelastustoimen järjestäjänä. Yhtenäisen ohjauksen ja ”yhden luukun periaatteen” toteuttaminen tiedon jakamisessa on erittäin tärkeää, koska resurssit ovat rajallisia. Määräyksissä, ohjeissa, vaatimuksissa ja suosituksissa tulee ottaa huomioon toimijoiden erilaiset toimintaympäristöt ja riskitasot. Esimerkiksi korkeakouluilta ei voi vaatia samaa tietoturvan tasoa kuin huoltovarmuuskriittisillä toimialoilla. Määräysten, ohjeiden, vaatimusten ja suositusten liitynnät toisiinsa, niiden väliset riippuvuudet ja vaikutukset on viestittävä ymmärrettävästi. • Julkisen hallinnon digitaalista turvallisuutta koskeva yhteinen lainsäädäntö, määräykset, ohjeet, suositukset ja työkalut tulee olla saatavilla yhdestä paikasta ja niistä on viestittävä yhtenä kokonaisuutena. • Tarvitaan vastuutaho, joka vastaa siitä, että yhteiset määräykset, ohjeet, vaatimukset, suositukset ja työkalut ovat ajan tasalla. Riskien arviointi on virastojen, hyvinvointialueiden ja kuntien velvoite, mutta riskiarviointia ei toteuteta systemaattisesti eikä yhteistä mallia riskien arvioimiseksi ja hallinnoimiseksi ole. Lisäksi yhteinen näkymä arvioituihin riskeihin tai riskitiedon jakamisen ja laaja-alaisen hyödyntämisen toimintamalli puuttuu. Reagoiva toimintatapa tulee muuttaa ennakoivaksi, jolloin yhdessä ja yhtenäisesti jatkuvuudenhallinnan kanssa tehtyjä riskianalyyseja ja selvityksiä hyödynnetään johtopäätösten tekemiseksi ja suojaustoimenpiteiden toteuttamiseksi. Yhteistyön koordinointia varten on nimettävä erikseen henkilöt ja varata riittävät resurssit. Tiedonhallintalaki velvoittaa tiedonhallintayksiköitä kuvaamaan toimintaansa ja toimintaympäristöään päivittyvän nykytilakuvauksen kautta. Tätä kuvausta kutsutaan tiedonhallintamalliksi. Se on organisaation staattinen kuvaus, jonka avulla varmistetaan tietojärjestelmien ja tietovarantojen yhteentoimivuus. Muutostenarviointiprosessi auttaa tiedonhallintamallin kehittämistä menetelmänä, joka ohjaa organisaatiota kohdentamaan investointeja mm. digitaalisen turvallisuuden osa-alueilla riskipohjaista päätöksentekoa tukien. Kuntakentän kannalta julkisen hallinnon toiminnan yhteentoimivuuden edistämisen odotukset kohdistuvat valtionvarainministeriön ylläpitämään tiedonhallintakarttaan ja siinä kuvattuihin keskeisiin yhteisiin resursseihin (mm. perustietovarannot ja niiden sidokset sekä riippuvuuden kunnille asetettuihin lakisääteisiin tehtäviin). Yhteentoimivuus tulee huomioida toiminnanohjauksessa tiedonhallintakartan toimiessa välineenä, kun tiedonhallintamalleja kehitetään toimintalähtöisesti.

Yhteistoiminta-alue/palvelu	Kehitysehdotus
	Julkisen hallinnon toimijat tarvitsevat tiedonhallintamallin digitaaliseen turvallisuuteen vahvaa tiedolla johtamista ja sitä tukevia tietokantoja tai tietovarantoja. Valtiotoimijoilta odotetaan konkreettisia ohjeita, tarkastuslistoja ja materiaalipankkia, jotka ovat saatavissa yhdestä paikasta tai yhdeltä viranomaiselta. Tietopankeista löytyy sopimusmalleja ja valmiita vaatimusluetteloita, esimerkiksi listaus järjestelmän ei-toiminnallisista vaatimuksista, valmisohjelman tarkastuslista tai toimenpidelista digitaalisen turvallisuuden hankintojen tekemiseksi ja tarjottujen tuotteiden ja palveluiden arvioimiseksi sekä digiturvallisuuden johtamiseksi ja ylläpitämiseksi esimerkiksi häiriötilanteessa. • Yhteistoiminta digitaalisen turvallisuuden riskien hallinnassa. • Yhteistoiminta ICT-palveluiden tietoturvallisuuden arvioinnissa. • Nimetyt henkilöt, jotka osallistuvat yhteistoimintaan. Tarvitaan mahdollisesti säädös, jossa edellytetään organisaation koko ja tehtävät huomioiva digitaaliseen turvallisuuteen liittyvä rooli jokaisessa julkisen hallinnon organisaatiossa. – Kyseessä olisi lähinnä samankaltainen koordinoiva tehtävä kuin tietosuojavastaavankin tehtävä. [34] – Koordinointivastuu voi sisältää esimerkiksi vastuun organisoida tietoturvan hallintajärjestelmät ja tietoturvaan liittyvien riskien hallinta. Rooli ei kuitenkaan voi vastata esimerkiksi yksittäisten järjestelmien, rekisterien tai sovelluskehityksen tietoturvallisuudesta tai tietosuojasta. – Ylin vastuu tietoturvallisuudesta on organisaation ylimmillä viranhaltijoilla tai johtajilla, jotka voivat päättää rahoituksesta ja siten aidosti vaikuttaa riskien hallintaan. On tärkeää, että digitaalisen turvallisuuden roolin luomisella vastuuta ei siirretä organisaatiossa ylimmästä johdosta asiantuntijalle, mikä johtaisi tietoturvallisuuden ja tietosuojan negatiiviseen kehitykseen. • Tunnistettuja työkalutarpeita ovat tiedon luokittelu sekä siihen liittyvät ohjeet ja mallit, jotka ovat saatavissa esimerkiksi ohjeistuksen keskitetyltä sivustolta. • Vastuullinen virasto, joka ylläpitää hankintoihin ja sopimuksiin sekä tietoturvallisuuden arviointiin liittyvää tietopankkia ja jakaa tietoa eri toimijoille.

34 Selvitys organisaation tietoturvatehtävistä ja niiden organisoimisesta, valtiovarainministeriö, 9.3.2022

Yhteistoiminta-alue/palvelu	Kehitysehdotus
Digitaalisen turvallisuuden yhteiset hankinnat, hankkeet ja digipalvelut	Digitaalisen turvallisuuden yhteisiä hankintoja ja hankkeita tulee edistää niihin kannustavalla hallinto- ja rahoitusmallilla. Siten ohjataan valtionhallintoa, hyvinvointialueita, kuntia ja korkeakouluja toimimaan yhdessä digitaalisen turvallisuuden kokonaisvaltaiseksi kehittämiseksi. Yhteisissä hankkeissa ja hankinnoissa on otettava huomioon toimijakohtaiset erot asiakassegmentoinnin avulla. Hyvinvointialueiden näkökulmasta tarvitaan laaja palvelutarjoama, josta hyvinvointialueet voisivat täydentää omaa osaamistaan, resurssejaan ja kyberturvallisuuden sekä tietosuojan palveluitaan. Hankintojen yhteinen kilpailuttaminen vahvistaisi myös tietojärjestelmien yhteentoimivuutta. Turvallisuushankintojen toteuttaminen on erityisesti pienemmissä organisaatioissa haasteellista resurssisyistä. Digitaalisen turvallisuuden alueellisesti yhtenäinen 'perustaso' mahdollistaisi asiakkaan tietoturvan ja tietosuojan tasalaatuisen toteuttamisen. Keinona voi olla rahasto, josta jaettaan rahoitusta hyvinvointialueiden ja kuntien digitaalisen turvallisuuden kehittämishankkeisiin. Rahoituksen ehtona voi olla esimerkiksi se, että vähintään x kuntaa ja/tai x hyvinvointialuetta osallistuu hankkeeseen ja hankkeen tulokset ja tuotokset jaetaan kaikkien julkisen hallinnon organisaatioiden käyttöön. Muutoinkin valtion kunnille osoittamaa rahoitusta ohjataan entistä enemmän siten, että rahoitus ohjaa yhteistyöhön ja yhdessä digitaalisen turvallisuuden kehittämiseen sekä palveluiden hankintaan. Rahoitusmalleja voisi olla useampikin sen mukaan, kuinka moni julkinen toimija hankkeeseen osallistuu. • Rahoitusmalli, joka kohdentaa rahoituksen yhteishankkeisiin ja -hankintoihin yksittäisten kehitystoimenpiteiden sijaan ja ohjaa yhteistyöhön. Kehityshankkeiden rahoittamisen rinnalla on pohdittava keinoja mahdollistaa ja varmistaa digitaalisen turvallisuuden toimintakulujen rahoitus. Rahoitustarve on tyypillisesti kasvanut kaikissa organisaatioissa digitalisoitumisen edistyessä.
Digitaalisen turvallisuuden yhteiset palvelut	Digitaalisen turvallisuuden palvelujen kehittäminen ja ylläpito ovat samankaltaista eri toimijoiden välillä. Niiden määrittely ja kehittäminen tulisi toteuttaa yhdessä. Yhteisille palveluille on yhdessä asetettava tietoturvallisuus-, tietosuoja-, kyberturvallisuus- sekä varautumisen ja jatkuvuudenhallinnan vaatimukset julkisen hallinnon tietoturvallisuuden arviointikriteeristön (Julkri) avulla. Palvelujen vaatimustenmukaisuutta on arvioitava ja palvelujen toimintaa on valvottava niiden koko elinkaaren ajan. Tavoitteena on, että yhteiset palvelut toteuttavat myös yksittäisten organisaatioiden niille asettamat vaatimukset. Mikäli yhteiseen palveluun tulee häiriöitä tai palvelukatkoksia, se vaikuttaa suureen osaan toimijoita, jotka kyseistä palvelua käyttävät ja hyödyntävät.

Yhteistoiminta-alue/palvelu	Kehitysehdotus
	Toimijoiden välisistä eroista aiheutuvat vaatimukset tulisi ottaa huomioon asiakassegmentoinnin avulla. Tällaisia eroja ovat esimerkiksi toimijan hallinnollinen taso, koko ja maantieteellinen sijainti. Palveluiden kehittäminen useissa erilaisissa tai eri pituisissa ohjelmissa tai hankkeissa voi johtaa erilaiseen tai jatkuvasti muuttuvaan ohjeistukseen. Hallinnonalojen tulisi pyrkiä vahvistamaan vuoropuhelua yhtenäisen linjan löytämiseksi. Esimerkkinä yhteisesti kehitettävästä palvelusta on yhteinen organisaation digitaalisen turvallisuuden kypsyystason mittari. Se voi olla tai perustua jo olemassa oleviin kypsyystasojen mittareihin, kuten Kybermittariin tai DVV:n kehittämään kokonaiskuvapalveluun. Niiden avulla kypsyystasoja voitaisiin mitata yhtenevästi ja mittauksen pohjalta voitaisiin määrittää yhteisiä tavoitteita sekä kehityskohteita ja -alueita. Tämä mahdollistaisi ja loisi puitteet muun muassa julkisen hallinnon digitaalisen turvallisuuden tason yhteisen tilannekuvan jakamiselle, digitaalisen turvallisuuden osaamisen jakamiselle, yhteisten hankintojen ja turvallisuusvaatimusten valmistelulle sekä yhteisten, keskeisimpiin kehityskohteisiin ja -alueisiin kohdistuvien harjoitusten valmistelulle ja järjestämiselle. Tämä mahdollistaisi uusien kehityshankeaihioiden esille tuomisen ja toteuttamisen osana koko julkisen hallinnon digitaalisen turvallisuuden kehittämistä seuraavan hallituskauden aikana. Kuntien digitaalisen turvallisuuden varmistamiseksi on kuntien saatavilla oltava hyväksyttävien tietotekniikkapalveluiden palvelutarjooma, josta kunnan suoraviivaisesti ja hankintasäädösten mukaisesti hankkima palvelu on laadultaan varmasti riittävä julkishallinnon käyttöön. Tavoitetilakuvauksen palvelualueiden sisältöä, vastuuorganisaatioita sekä palvelualuekohtaisia yhteistoiminta- ja hallintamalleja on selkeytetty tässä raportissa nykytilan jäsennyksessä käytetyn, kuvassa 2 hahmotellun palvelualuekokonaisuuden perusteella yhteisten palvelujen kehittämisen edistämiseksi. • Tavoitetilassa palveluissa tulee huomioida nykyistä enemmän ennakointi, kyky tunnistaa digitaalisen turvallisuuden toimintaan vaikuttavia ilmiöitä ja trendejä sekä tulkita digitaalisen turvallisuuden uhkasignaaleja. Siten mahdollistetaan muun muassa ennakoivampi koulutus ja oppiminen sekä ennakoivampi häiriöhallinta. • Palveluissa tulee huomioida jatkuvuudenhallinta ja varautuminen, mukaan lukien poikkeusolojen vaikutus tieto- ja kyberturvallisuuden toteuttamiselle. Palvelualueita on kuvattu tarkemmin kappaleessa 4.3.

Yhteistoiminta-alue/palvelu	Kehitysehdotus
Digitaalisen turvallisuuden osaaminen	Henkilöstön, digiturva-asiantuntijoiden ja johdon osaamisen kehittämistä on jatkettava aktiivisesti tarjoamalla jokaiselle kohderyhmälle sille parhaiten sopivia menetelmiä. Vuosittaiselle osaamisen kehittämiselle on asetettava minimitavoitteet, joita organisaatioiden on seurattava. Tämän ohella tulee panostaa teknisen tason tietoturvallisuuden kehittämiseen, jotta voidaan esimerkiksi estää paremmin henkilöille toimitettavia haittaohjelmia tai muita kalasteluviestejä sisältävät yhteydenotot eri digipalveluissa. Jokainen tällainen estetty viesti pienentää riskiä, että organisaatio joutuisi henkilötietojen tietoturvaloukkauksen tai tietomurron kohteeksi. Erityisesti teknisen tietoturvallisuuden kehittäminen pitäisi olla yksi keskeisiä seuraavan hallituskauden kehityskohteita. Eri tutkimusten mukaan yli 80 % erilaisista häiriöistä, hyökkäyksistä ja loukkauksista tapahtuu henkilöstön kautta. Turvalliseen sovelluskehitykseen tarvitaan vastaava panostus, koska pelkästään vuonna 2021 hyödynnettiin useampaa nollapäivähaavoittuvuutta kuin edeltävänä yli kahtena vuotena yhteensä. Hyvinvointialueiden näkökulmasta eOppivaan tulisi rakentaa riittävän kokonaisuuden muodostamat sopivat koulutuspaketit hyvinvointialueiden luottamushenkilöiden, johtavien viranhaltijoiden, riskienhallinnasta vastaavien, tietosuojasta vastaavien, tietoturvasta vastaavien, terveydenhuollon, pelastustoimen ja sosiaalitoimen ammattialaisille. eOppivan integrointi organisaation omaan HR-järjestelmään ja identiteettien hallintaan (esimerkiksi Azure AD, ADFS) olisi tärkeää koulutusten seurannan kannalta ja ylimääräisten tunnusten välttämiseksi. • Henkilöstön osaamisen kehittämiselle on asetettu seurattavat tavoitteet. • Teknistä tietoturvallisuutta on kehitetty käyttäjien päätelaitteisiin ja palveluihin tulevien vaarallisten yhteydenottojen tehokkaammaksi tunnistamiseksi ja estämiseksi. • Korkeakoulujen opetusta on edistetty kyberturvallisuusuusstrategian toimeenpanon osana julkaistun selvityksen[35] linjausten mukaisesti.
Digitaalisen turvallisuuden harjoittelu	Julkisessa hallinnossa on digitaalisen turvallisuuden harjoitustoimintaa kehitettävä ja koordinoitava, jotta julkisen hallinnon digitaalisen turvallisuuden strategisia tavoitteita edistetään parhaalla mahdollisella tavalla. DVV:n tekemässä selvityksessä ”Julkishallinnon digitaalisen turvallisuuden kansallisen harjoitustoiminnan tavoitetilakuvaus”[36] tunnistettiin erilaisia pitkän ja lyhyen aikavälin kehittämistoimenpiteitä. Toimenpiteitä tarvitaan niin lainsäädännön ja rahoituksen kuin ohjauksenkin osa-alueilla. Harjoitustoiminnan koordinaatio tukee yhteisiä tavoitteita ja organisaatioiden palautumista häiriötilanteesta.

35 Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimus – hankkeen loppuraportti, Jyväskylän Yliopisto, 2022.

36 Julkisen hallinnon digitaalisen turvallisuuden kansallisen harjoitustoiminnan tavoitteet ja toimenpiteet (dvv.fi)

Yhteistoiminta-alue/palvelu	Kehitysehdotus
Tilannekuva	Tavoitteena on laajaan, ennakoivaan tietopohjaan ja monipuolisiin mittareihin valtionhallinnosta, hyvinvointialueilta ja kunnista sekä modulaariseen raportointikyvykkyyteen perustuva tilannekuva, joka tukee yhteisen tilannetietoisuuden ja tilanneymmärryksen muodostumista ja päätöksentekoa. • Julkisessa hallinnossa tarvitaan ennakoiva, yhteinen ja jaettu digitaalisen turvallisuuden tilanneymmärrys. Titukri-periaatepäätöksen 10.6.2021 yhtenä toimenpiteenä on valtiovarainministeriön johdolla toteuttava selvitys viranomaisten salassa pidettävän ja turvaluokitellun tiedon käsittely-ympäristöjen luomisen teknologisten ratkaisujen tarpeista. Selvityksen kohteena ovat muun muassa viranomaisten yhdenmukainen salattu sähköpostiviestintä, turvalliset neuvotteluyhteydet ja -palvelut sekä turvallinen tiedonsiirtopalvelu. Selvitys tehdään vuosina 2022–2023 ja selvityksen pohjalta haetaan ja toteutetaan nykyaikaiset ratkaisut vuosina 2023–2024. Selvityksessä arvioidaan lisäksi tiedonvaihdon yhteentoimivuutta kolmansien tahojen kanssa. Nämä ratkaisut ovat välttämättömiä digitaalisen turvallisuuden yhteistoiminnalle ja tilannekuvan jakamiselle. Ratkaisujen suunnittelussa ja toteutuksessa on tärkeää painottaa puolustusjärjestelmän kannalta kriittisten toimintojen ja toimijoiden välisen tiedonvaihdon toteutumista. Lisäksi koko valtionhallintoa koskee kasvava kansainvälisen tiedon käsittelytarve ja siihen liittyviä kysymyksiä tulee ratkaista yhdessä koko valtionhallinnossa. Erityisesti NATOn tuottama tilannekuva ja sen hyödyntäminen on otettava huomioon. Tiedonvaihdon edistämiseksi valtionhallinnossa tuleekin käynnistää laaja-alainen yhteistyö. Se vaatii toteutuakseen tietomalleja, rajapintoja ja yhteisesti sovittuja sekä määriteltyjä käytäntöjä ja prosesseja. • Titukri: Tiedon jakamisen – erityisesti salassa pidettävän ja luokitellun tiedon – mahdollistaminen, tehostaminen ja lisääminen eri viranomaisten välillä. • Tiedonvaihdon ISAC-ryhmien mahdollinen laajentaminen ja korkeakoulu-ISAC-ryhmän perustaminen.
Häiriötilanteiden hallinta	Häiriötilanteiden hallintaan liittyvät valmiudet vaihtelevat eri toimijoiden välillä. Yhteistä toimijoille on rajallinen häiriötilanteiden hallintakyky sekä puutteet osaamisessa, joita on kehitettävä. Toimijoiden välistä yhteistoimintaa on tehostettava siten, että kyvykkäimmät toimijat tukevat osaamisen kasvattamista kaikissa toimijoissa. • Häiriötilanteiden hallintaan liittyvä tuki ja konkreettinen häiriötilanteen aikaisen toiminnan ohjaus edesauttavat organisaatioiden palautumista häiriötilanteesta. Kunnat, hyvinvointialueet ja muut julkisen sektorin toimijat tarvitsevat häiriötilanteissa nopeasti saatavilla olevia resursseja häiriön vaikutusten minimointiin ja tilanteen selvittämiseen. Yhteisen varalla olevan osaamispoolin hankintaa tulisi selvittää. Osaamispoolissa olisi valmiiksi kilpailutettuja palveluntarjoajia ja osaajia, joiden joukosta löytyisi nopeasti apu häiriötilanteissa. • Nopea häiriötilanteen hallinta edellyttää toimijoiden välillä yhtenäisiä prosesseja sekä selkeitä rooleja ja tehtäväkuvauksia.

4.2 Julkisen hallinnon ja tutkimus- ja kehittämistoiminnan välinen yhteistoiminta

Digitaalisen turvallisuuden tutkimukseen liittyvän yhteistoiminnan tulisi perustua todellisiin tarpeisiin ja synergiaetuihin osapuolten välillä. Tutkimusyhteistoiminnan onnistumiseen vaikuttavia tekijöitä ovat vuorovaikutuksen syvyys digitaalisen turvallisuuden osa-alueilla, pitkäaikainen yhteistyö yksittäisten hankkeiden ja projektien sijaan, yhteistyön lisääminen eri organisaatiotasoilla sekä motivointi avoimeen tiedon jakamiseen. Yhteistyömallin muuttaminen pitkäkestoiseksi projekti- tai hankekohtaisen mallin sijaan olisi korkeakoulujen kannalta hyödyllistä.

Tutkimusyhteistoiminnan osapuolten tulee olla toisiaan tukevia ja täydentäviä, jotta yhteistyö voi synnyttää lisäarvoa ja uudenlaisia ratkaisuja. Toisaalta yhteistyön edellytyksenä on toisten ymmärtämisen lisäksi se, että osapuolet ovat jossain määrin saman tasoisia. Vastaaminen yhtäläisen tason haasteeseen edellyttää toisilleen sopivien osapuolten tunnistamista, kohdistamista ja yhteen tuomista.

Konkreettisten toiminnallisten haasteiden ratkaisemisen lisäksi tulisi pyrkiä luomaan myönteisiä asenteita, motivaatiota ja ennakkoluulottomuutta tutkimusyhteistoimintaa kohtaan. Vuorovaikutus rakentaa sekä luottamusta että yhteisymmärrystä, mikä vähentää hallinnollisten toimenpiteiden ja byrokratian tarvetta. Taulukkoon 8 on koottu digitaalisen turvallisuuden tutkimustoiminnan yhteistoiminnan tavoitetilaan liittyviä odotuksia.

Digitaalisen turvallisuuden sisäiset verkostot ovat erittäin tarpeellinen kehityssuunta myös yksittäisen kaupungin tai kunnan sisällä sekä vertaiskuntien kesken. Kuntaliiton mahdollistamaa kuntien tietoturvan verkostoitumistyötä on kannatettavaa jatkaa ja kehittää tämän julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalliselvityksen hengessä.

Taulukko 8. Tavoitetilaan liittyviä odotuksia tutkimustoiminnassa

Yhteistoiminta-alue/ teema	Kehitysehdotus
Yhteistoiminnan rakenne	Kyberturvallisuuskeskus on aloittamassa tehtäväänsä edistää kansallisesti eri sektorit ylittävää kyberturvallisuuden tutkimus- ja kehittämistoimintaa ja osallistumista EU-laajuisiin tutkimus- ja kehittämishankkeisiin. Digitaalisen turvallisuuden tutkimusta tekevän ytimen muodostavat korkeakoulut eli yliopistot ja ammattikorkeakoulut sekä VTT. Jatkossa erityisesti yrityksien mahdollisuuksia liittyä konsortioihin ja tutkimusryhmiin tulisi tukea, jotta tutkimustulokset päätyisivät aiempaa tehokkaammin innovaatio-, tuotekehitys- tai muutoin soveltavan tutkimuksen prosesseihin. Erityistä huomiota tulisi kiinnittää siihen, että huomattava osa EU:n rahoitusohjelmista tavoittelee nimenomaan sovellettavien ratkaisujen kehittämistä ja markkinoille saattamista. Ministeriöiden, virastojen, hyvinvointialueiden ja kuntien vahvempaa panostusta digitaalisen turvallisuuden tutkimuksen yhteistoimintaan tarvitaan tuomaan näkökulmia yhteiskunnan kannalta merkittävistä tutkimuskohteista. Digitaalisen turvallisuuden tutkimuksen yhteistyö tulisi koota paremmin näiden kaiken toimijoiden ympärille. • KTK koordinoi kansallista digitaalisen turvallisuuden tutkimuksen yhteistoimintaa ja kokoaa yhteen tutkimusta ja kehittämistä tekevät tai sitä tukevat organisaatiot sekä tutkimustuloksia hyödyntävät tahot. • Yhteistoiminnan rakenteen vaatimuksena on kevyt organisoitumismalli, jotta hallinnollinen byrokratia ei lisäänny. Tapaamisissa keskitytään tutkimustarpeisiin.
Tutkimus- ja kehittämiskohteiden määrittely	Julkisen sektorin digitaaliseen turvallisuuteen liittyviä tutkimustarpeita ei ole systemaattisesti kartoitettu. Tutkimuskohteiden määrittely edellyttää sekä jatkuvaa keskustelua toimijoiden välillä että tutkimuskohteiden tunnistamista. Tutkimuslaitosten ja tutkimusta pyytäneen tahon välillä on oltava luottamussuhde. Tutkimuskohteen tunnistaminen edellyttää molemminpuolista ymmärrystä, jotta tutkimus on mahdollista käynnistää viipymättä. • Mekanismi tutkimuskohteen nopeaan määrittelyyn ja tutkimussuunnitelman laadintaan. • Tutkielma- ja tutkimusaihepankki, josta tutkielmaa ja tutkimusta tekevät opiskelijat ja tutkijat voisivat etsiä sopivia aiheita.
Tutkimustulosten hyödyntäminen	Digitaalisen turvallisuuden tutkimusta tehdään usealla eri tasolla. Tutkimuksella vahvistetaan yhteiskunnan digitaalisen turvallisuuden osaamista. Tutkimusyhteistyö voi tuoda ajantasaista uutta tietoa yhteiskunnan eri toimijoiden päätöksenteon tueksi. Tutkimustulosten hyödyntäminen edellyttää, että organisaatiot kykenevät soveltamaan tuloksia tavoitteidensa mukaisiin kehitystoimenpiteisiin ja niiden vaikuttavuuden mittaamiseen. • Tutkimuksen tulee olla sekä strategista että operatiivista, jotta tutkimuksen avulla voidaan vastata digitaalisen turvallisuuden kehitystarpeisiin. (Ilmiöiden ja trendien analyysit riskien arviointia varten sekä esimerkiksi toimintamallien määrittäminen päivittäisen toiminnan kehittämiseksi) • Tutkimustulosten ympärillä tulee käydä aktiivista keskustelua tutkimustiedon levittämiseksi laajasti yhteiskunnan eri alueilla. • Tutkimuksen tulee tukea ja vahvistaa uuden tiedon soveltamista ja hyödyntämistä erityisesti soveltavassa tutkimuksessa ja innovaatiotoiminnassa. Suomessa tarvitaan huomattavasti enemmän kaupallisia ratkaisuja kehittävien toimijoiden ja tutkimusorganisaatioiden välistä kyberturvallisuuden yhteistyötä.

4.3 Julkisen hallinnon digitaalisen turvallisuuden palvelualueet tavoitetilassa

Julkisen hallinnon digitaalisen turvallisuuden palvelualueet, vastuuorganisaatiot ja kunkin palvelualueen yhteistoiminta- ja hallintamalli tavoitetilassa on kuvattu kuvassa 4 ja taulukossa 9. Tavoitetilatarkastelussa ei ole selvitetty tavoitetilan saavuttamiseksi mahdollisesti tarvittavia säädösmuutostarpeita. Tavoitetilaan liittyviä odotuksia on kuvattu yhteistoimintamallissa. Hallintamallin toteuttaminen edellyttää kuitenkin vielä odotusten tarkentamista käyttäjäorganisaatioitten tason toimijoille ja konkreettisten toimenpiteiden kuvaamista. Digitaalisen turvallisuuden eri osa-alueitten edellyttämät toimenpiteet ovat koko organisaation toiminnassa osittain usein näkymättömiä, mutta kuitenkin välttämättömiä. Ne edellyttävät investointeja, työvoimapanostusta sekä ammatillista tukea ja näistä resursseista on nykyään pulaa. Organisaation kehittämisessä tarvittavat resurssit on voitava perustella. Nykyisin organisaation vastuuhenkilöt tekevätkin usein näitä tehtäviä oman työnsä ohessa.

Kuva 4. Julkisen hallinnon digitaalisen turvallisuuden palvelualueet tavoitetilassa.

Taulukko 9. Julkisen hallinnon digitaalisen turvallisuuden palvelualueiden tavoitetilan kuvaukset

Digitaalisen turvallisuuden yhteinen ohjaus, kehittämisen yhteistoiminta, valvonta ja viestintä

Palvelualueen kuvaus	Palvelualue kattaa digitaalisen turvallisuuden yhteisen ohjauksen, digitaaliseen turvallisuuteen ja kyberturvallisuuteen liittyvien valtioneuvoston periaatepäätösten ja strategioiden sekä niihin liittyvien kehitysohjelmien ja toimeenpanon valmistelun ja toteutuksen koordinoinnin, valvonnan ja kehittämisestä viestimisen. Lisäksi palvelualue sisältää hyvinvointialueiden välisen yhteistoiminnan ja kuntien alueellisesti muodostetun yhteistoiminnan ohjauksen ja kehittämisen. • Strategia-, normi-, resurssi- ja informaatio-ohjauksen valmistelu ja toteuttaminen. • Linjausten mukaisten toimenpiteiden tunnistaminen sekä niiden rahoituksen ja toimeenpanon suunnittelu, toteuttaminen ja seuranta. • Julkisen hallinnon digitaalisen turvallisuuden resurssisuunnitelman ja -seurannan ylläpitäminen. • Ohjauksen ja toimenpiteiden vaikuttavuuden arviointi. • Kansainvälisen yhteistoiminnan sekä yritysten ja yhteisöjen yhteistoiminnan kautta saatavien tietojen jakaminen ja välittäminen koordinoidusti kansalliseen ohjauksen ja kehittämisen yhteistoimintaan. • Kehittämistoimenpiteiden ja niiden tulosten valvonta ja viestintä.	Vastuutaho: Kyberturvallisuusjohtaja Turvallisuuskomitea Digitalisaation, datatalouden ja julkisen hallinnon kehittämisen ministerityöryhmä, Digitoimisto VM, LVM, TEM, UM, STM HVK, TSV
Yhteistoiminnan rakenne	Palvelualueeseen liittyvän yhteistoiminnan tavoitteena on yhteinen näkemys digitaalisen turvallisuuden strategioista, periaatepäätöksistä, normeista ja kehityshankkeista sekä niiden sisällöistä; rahoituksen sekä toimeenpanosuunnitelmien valmistelu ja toteuttaminen sekä toimeenpanon seuranta, valvonta ja viestiminen. Yhteistoiminta koostuu seuraavista elementeistä: • Erilaisten toimijoiden ekosysteemi, johon kuuluvat julkinen hallinto, korkeakoulut ja tutkimuslaitokset sekä erikokoiset yritykset. Näkemysten ja tarpeiden esiin tuomiseksi, strategioiden, normien, linjausten ja toimenpiteiden määrittelemiseksi sekä toteutuksen valmistelemiseksi ja seurannaksi. • Strategiat, periaatepäätökset ja normit valmistellaan yhteistyöryhmässä ja tarkistetaan säännöllisesti. • Kehittämisohjelmat, jotka valmistellaan yhteistyöryhmässä ja tarkistetaan vuosittain, valvotaan ja viestitään systemaattisesti. • Edistetään hyvinvointialueiden välistä digitaalisen turvallisuuden yhteistoimintaa kansallisin toimenpitein. • Hyödynnetään kuntien alueellisen digitaalisen turvallisuuden yhteistoiminnan parhaita käytänteitä ja mahdollistetaan niiden leviämistä. • Tarjotaan kunnille keskitetysti yhteisiä digiturvapalveluja Haukka-ohjelmassa ylläpidettävän kuntien digiturvapalvelujen tiekartan mukaisesti. • Selvitetään ja toteutetaan yhteisten digitaalisen turvallisuuden palvelujen tarjoaminen korkeakouluille.	Yhteistoimintaan osallistuvat: Tiedonhallintayksikön johto ja digitaalisesta turvallisuudesta vastaavat henkilöt
Mittarit	Strategioiden ja normien sekä kehittämisohjelmien vaikuttavuus	

Yhteiset määräykset, ohjeet, vaatimukset, suositukset ja työkalut

Palvelualueen kuvaus	Digitaalisen turvallisuuden yhteisten riskienhallintamallien, määräysten, ohjeiden, suositusten, vaatimusten ja käytettävien palveluiden turvallisuuden hyväksyntäkriteerien on oltava yhteneviä ja pohjautua yleisesti hyväksyttyihin ja käytettyihin periaatteisiin, kuten yleisiin kansainvälisiin standardeihin. Julkista hallintoa koskevien yhteisten digitaalisen turvallisuuden määräysten, ohjeiden, vaatimusten ja suositusten hyväksymiskriteereineen tulee olla saatavissa järjestettynä yhdestä paikasta. Lisäksi näihin on tarjottava riittävä tuki ja koulutus. Ohjeiston tulee sisältää julkishallinnolle yhteiset teknisten ominaisuuksien asennussuositukset, joilla esimerkiksi EU/ETA-alueen ulkopuolisen pilvipalvelutoimittajan Euroopasta tarjoamat digiratkaisut ovat julkishallinnon henkilötietojen, julkisuuslain sekä julkishallinnon tietojenkäsittelyä koskevien erillislakien vaatimusten mukaiset. Valtionhallinto tarjoaa yhteisiä työkaluja organisaatioiden tueksi ja digitaalisen turvallisuuden ylläpitämiseksi, mittaamiseksi ja kehittämiseksi julkisen hallinnon organisaatioissa. Palvelussa tuotetaan ja ylläpidetään yhteisiä kontrollitavoitteita, vaatimuksia ja ohjeistusta, jotka linjaavat, miten digitaalisen turvallisuuden tavoitteet saavutetaan. Palvelu koostuu seuraavista osista: • Digitaaliseen turvallisuuteen liittyvien yhteisten määräysten, ohjeiden, vaatimusten, suositusten ja työkalujen keskitetty hallinta. • Yhteisten määräysten, ohjeiden, vaatimusten ja suositusten sekä työkalujen tarpeiden ennakoiva tunnistaminen ja hallinta. • Osallistuminen mahdollisuuksien mukaan standardien, viitekehysten ja suositusten kansainväliseen valmisteluun ja kansainvälisen ohjeistuksen huomioimiseen kansallisessa valmistelussa.	Vastuutaho: Tiedonhallinta-lautakunta: suositukset DVV: yleisohjeet; vaatimusten, ohjeiden ja suositusten saatavuus järjestettynä yhdestä paikasta
Yhteistoiminnan rakenne	Palvelualueeseen liittyvän yhteistoiminnan tavoitteena on julkisen hallinnon digitaalisen turvallisuuden tarpeita ja tavoitteita tukevien yhteisten määräysten, ohjeiden, vaatimusten, suositusten ja työkalujen ennakoiva tunnistaminen ja keskitetty hallinta. Yhteistoiminta koostuu seuraavista elementeistä: • Vastuutaho tunnistaa ja ylläpitää yhteisten ohjeistusten eli määräysten, ohjeiden, vaatimusten, suositusten ja työkalujen kehittämistarpeita sekä osallistaa yhteistoimintaan osallistuvia niiden valmisteluun. • Vastuutaho ottaa huomioon asiakassegmentoinnin yhteisen ohjeistuksen valmistelussa ja niistä viestimisessä. • Vastuutaho järjestää seminaareja yhteisestä ohjeistuksesta ja työkaluista. • Vastuutaho ylläpitää portaalia yhteisen digitaalisen turvallisuuden ohjeistuksen jakamiseksi. • Yhteistoimintaan osallistuvat kehittävät yhteistä ohjeistusta, vievät niitä käytäntöön omissa organisaatioissaan ja keräävät palautetta niiden kehittämiseksi.	Yhteistoimintaan osallistuvat: Tiedonhallintayksikön digitaalisesta turvallisuudesta vastaavat henkilöt KTK TSV DVV
Mittarit	• Yhteisen ohjeistuksen vaikuttavuuden arviointi ja vaikuttavuus. • Seminaarien osallistujien määrä ja palaute.	

Yhteiset hankinnat, hankkeet ja digipalvelut

Palvelualueen kuvaus	Palvelualue kattaa julkisen hallinnon digitaalisen turvallisuuden palvelujen yhteishankintajärjestelyt ja -hankkeet. • Kilpailutetaan yhteishankintana digitaalisen turvallisuuden palveluja, joita voidaan ottaa käyttöön välittömästi tai jotka voidaan hankkia minikilpailutuksen kautta. Välittömästi käyttöön otettava palvelu on esimerkiksi tuki häiriötilanteissa. Minikilpailutuksen kautta hankittaviksi soveltuvia palveluja ovat erilaiset jatkuvaa toimintaa tukevat palvelut, kuten asiantuntijatuki hankkeissa tai tietoturvallisuuden arviointipalvelut. • Kilpailutuksissa huomioidaan kansainvälisten asiantuntijoiden ja osaamisen saaminen käyttöön • Pyritään kehittämään yhteisiä sopimusmalleja eri kilpailutuksissa ja palveluissa hyödynnettäväksi. • Esimerkki tavoitetilasta: Kunnille on hankittu Euroopassa toimivan kansainvälisen pilvipalvelutoimittajan ratkaisuja sellaisilla hankintaehdoilla ja teknisillä ominaisuuksilla, että ne täyttävät kaikki säädetyt vaatimukset, mukaan lukien viranomaisten toiminnan julkisuudesta annettu laki (621/1999), tietosuojasäännökset sekä kuntia koskevat erityissäännökset. Yhteisesti hankittaville palveluille on asetettava yhteisesti digitaalisen turvallisuuden vaatimukset julkisen hallinnon tietoturvallisuuden arviointikriteeristön (Julkri) avulla. Vaatimustenmukaisuus on arvioitava ennen palvelun käyttöönottoa ja säännöllisesti palvelun käytön aikana. Vaatimustenmukaisuutta on valvottava teknisin toimenpitein. • Velvoitetaan vaatimustenmukaisuus arvioitavaksi julkisen hallinnon digitaalisen turvallisuuden arviointikriteeristön (Julkri) avulla. Arviointien tuloksista viestitään esimerkiksi yhteisen seurantapohjan avulla, joka on julkisen hallinnon tai digipalvelun/tietojärjestelmän käyttäjien nähtävillä ja kommentoitavissa. • Velvoitetaan digiturvallisuuden perusasioiden arviointi julkisen hallinnon tietojärjestelmäkehityshankkeissa. • Velvoitetaan julkisten palveluiden digiturvaratkaisujen valvonta systemaattisesti automaattisin toimenpitein. Tämän mahdollistamiseksi velvoitetaan digitoimintaympäristön tietojen ylläpito ja tietojenvaihto.[37]	Vastuutaho: VM (velvoittaminen) Hansel
Yhteistoiminnan rakenne	Palvelualueeseen liittyvän yhteistoiminnan tavoitteena on digitaaliseen turvallisuuteen liittyvien yhteisten hankintojen ja hankkeiden nopea toteutus. Yhteistoiminta koostuu seuraavista elementeistä: • Vastuutaho käy keskustelua toimittajien ja julkisen hallinnon asiakkaiden kanssa. • Valmiiksi kilpailutetut sopimuskokonaisuudet, puitejärjestelyt ja dynaaminen hankintajärjestelmä. • Puitejärjestelyn valmistelua varten koottu yhteistyöryhmä tarvittavien määrittelyjen, sopimusehtojen ja vertailuperusteiden tekemiseksi. • Yhteistoimintaan osallistuvat hyödyntävät hankintoja tehdessään ensisijaisesti yhteishankintajärjestelyjä ja osallistuvat hankintatarpeiden määrittelyyn.	Yhteistoimintaan osallistuvat: Tiedonhallintayksikön digitaalisesta turvallisuudesta vastaavat henkilöt
Mittarit	• Puitejärjestelyjen kautta hankittujen palvelujen arvo euroina. • Puitejärjestelyjen asiakaspalaute.	

37 Esiselvitys digitaalisen toimintaympäristön tietovarannosta, valtiovarainministeriö 11/2022

Tutkimuksen koordinointi

Palvelualueen kuvaus	Palvelualueella tunnistetaan digitaalisen turvallisuuden eri osa-alueilla tutkimus-, kehitys- ja innovaatiokohteita riski- ja uhka-analyysien sekä vaatimustarpeiden perusteella. • Digitaalisen turvallisuuden kenttää ja digitaalista turvallisuutta arvioidaan kansainvälisessä vuorovaikutuksessa. Ennakoidaan tutkimuskohteita huomioiden kansainväliset tutkimushankkeet ja -julkaisut. • Kootaan yhteen digitaalisen turvallisuuden kansallista tutkimusta, kehitystyötä ja innovointia. • Ylläpidetään ja arvioidaan julkiselle hallinnolle tarpeellisten tutkimus-, kehitys ja innovaatiokohteiden kokonaiskuvaa. • Tunnistetaan rahoituslähteitä ja vaikutetaan yhdessä rahoituksen järjestymiseksi. • Edistetään, kannustetaan ja tuetaan kansallisia toimijoita osallistumaan rajat ylittäviin ja EU:n rahoittamiin hankkeisiin.	Vastuutaho: Kyberturvallisuusjohtaja, KTK, tutkimusyhteisö
Yhteistoiminnan rakenne	Palvelualueeseen liittyvän yhteistoiminnan tavoitteena on digitaalisen turvallisuuden tutkimus-, kehitys- ja innovaatiokohteiden ennakoiva tunnistaminen, arviointi ja hallinta, verkostoituminen sekä yhteistoiminnan lisääminen. Yhteistoiminta koostuu seuraavista elementeistä: • Erilaisten toimijoiden ekosysteemi, johon kuuluu esimerkiksi erikokoisia yrityksiä, korkeakouluja ja tutkimusorganisaatioita sekä rahoittajia ja julkisen hallinnon toimijoita osaamisen ja verkostojen yhteen tuomiseksi. • Vuosittain järjestettävä kansallinen työpaja digitaalisen turvallisuuden tutkimuskohteiden ennakoivaksi tunnistamiseksi.	Yhteistoimintaan osallistuvat: Digitaalisen turvallisuuden tutkimusta tekevien tutkimuslaitosten henkilöstö Digitaalisen turvallisuuden yhteistoiminnasta vastaavat tahot Digitaalisen turvallisuuden palveluja tarjoava elinkeinoelämä
Mittarit	• Tutkimushankkeiden lukumäärä suhteessa tunnistettuihin tutkimuskohteisiin • Hankerahoituksen määrä	

Osaaminen

Palvelualueen kuvaus	Palvelualue vastaa digitaalisen turvallisuuden osaamisen ja yhteiskunnan turvallisuuskulttuurin kehittämisestä ja vaalimisesta. Kulttuurin perusta on tietoisuus turvallisuusriskeistä sekä ymmärrys ja osaaminen tarvittavista toimenpiteistä. Digitaaliseen turvallisuuteen liittyvän julkisen hallinnon yleiseen tarpeeseen sopivan osaamisen kehittämiseen liittyvää tarjontaa lisätään eri kohderyhmille suunnatuilla oppimiskokonaisuuksilla, kuten esimerkiksi verkkotapahtumilla, ohjatuilla harjoituksilla sekä itseopiskelun verkkokursseilla. Palvelualue koostuu seuraavista osista: • Digitaalisen turvallisuuden kansallisen tutkimustiedon kokoaminen yhteen, koulutusohjelmien suunnittelu ja laatiminen sekä ylemmän asteen koulutuksen tarjoaminen koordinoidusti. • Ennakoiva digitaalisen turvallisuuden koulutusten tuottaminen julkisen hallinnon työntekijöille ja ylläpidon suunnittelu ja koordinointi. • Digitaalisen turvallisuuden kansallisen tason viestintä eri tasoilla (kansalainen, työntekijä, johtaja tai hallituksen jäsen ja ICT-asiantuntija). • Merkittävien digitaalisen turvallisuuden EU- ja kansainvälisten seminaarien ja tapahtuminen markkinointi hallinnon asiantuntijoille. • Vertailu ja oppiminen verrokkivaltioissa tapahtuvasta osaamisen kehittämisestä (esimerkiksi Alankomaat, Iso-Britannia, Ruotsi).	Vastuutaho: Yliopistot, ammattikorkeakoulut, VTT, DVV
Yhteistoiminnan rakenne	Palvelualueeseen liittyvän yhteistoiminnan tavoitteena on digitaalisen turvallisuuden osaamisen kehittäminen vastaamaan strategisia tavoitteita. Yhteistoiminta koostuu seuraavista elementeistä: • Erilaisten toimijoiden ekosysteemi, joka kokoaa yhteen erikokoisia yrityksiä, tutkimusorganisaatioita ja julkisen sektorin toimijoita koulutustuotteiden toteuttamiseksi. • Vastuutahon tuki osaamisen kehittämiseksi yhteiseen portaaliin, jonne on koottu keskeinen ja ajantasainen hallinnon henkilöstön osaamisen kehittämiseen liittyvä aineisto. • Vastuutahon tekemä vuosittainen kysely osaamisen kehittämistarpeista. • Yhteistoimintaan osallistuvat osallistavat organisaatioiden henkilöstöä kehittämään osaamistaan ja osallistumaan koulutuksiin, tuovat esille koulutus- ja kehitystarpeita sekä osallistuvat ja osallistavat organisaatioitaan digitaalisen turvallisuuden seminaareihin ja tapahtumiin.	Yhteistoimintaan osallistuvat: Tiedonhallintayksikön digitaalisesta turvallisuudesta vastaavat henkilöt KTK
Mittarit	• Yhteisten opetusta tarjoavien ylemmän asteen koulutusohjelmien määrä. • Yhteisiin ylemmän asteen koulutusohjelmiin osallistuvien ja koulutusohjelmista valmistuvien määrät. • Koulutuksiin ja tietoiskuihin osallistuneiden määrä. • Koulutusten ja tietoiskujen vaikuttavuuden arviointi. • Koulutusten ja osallistuvien organisaatioiden kattavuus.	

Harjoitustoiminta

Palvelualueen kuvaus	Ylläpidetään ja kehitetään ohjeistusta digitaalisen turvallisuuden harjoitusohjelmien ja harjoitusten suunnittelua ja toteutusta varten. Julkisen hallinnon käyttöön tuotetaan virtuaalisia harjoitusympäristöjä. Valtakunnallisten harjoitusten aikataulu julkaistaan vuosittain. Palvelualue kattaa valittujen häiriö- tai poikkeustilanteiden kansallisesti ja/tai toimialakohtaisesti yhteisesti toteutettujen harjoitusten ja harjoitustoimintapalveluiden suunnittelun. Harjoitustoiminnalla varmistetaan kyky reagoida häiriöihin ja varmistetaan toimenpiteiden kattavuus vahinkojen rajaamiseksi. Palvelu koostuu seuraavista osista: • Harjoitusten järjestämiseen liittyvien ohjeiden ja skenaarioiden laadinta ja ylläpito. • Kansainvälisten ja kansallisten harjoitusten koordinointi. • Harjoitustoiminnan kokonaiskuvan ja vaikuttavuuden viestintä.	Vastuutaho: LVM, DVV, KTK, HVK, VTT, yksityiset palveluntarjoajat
Yhteistoiminnan rakenne	Palvelualueeseen liittyvän yhteistoiminnan tavoitteena on edistää julkisen hallinnon yhteisiä harjoitustoiminnan hyviä käytäntöjä, kuten harjoitustoimintamalleja, työkaluja ja ohjeita ja aikatauluja (esimerkiksi vuosikello) sekä kehittää ja toteuttaa yhteisesti järjestettyjä harjoituksia soveltuvin osin. Yhteistoiminta koostuu seuraavista elementeistä: • Vastuutaho tukee harjoitustoimintaa yhteisen ohjeistuksen, mallien, palveluiden ja valmiiden harjoitusten avulla. • Harjoitustoimintakoordinaattori tukee yhteisen harjoitustoiminnan palveluiden suunnittelua, toteutusta, seurantaa ja viestintää. • Toteutetaan valtiohallinnon, hyvinvointialueiden, kuntien, korkeakoulujen sekä muiden toimijoiden yhteiset harjoitustoimintaryhmät. • Muodostetaan alueellisia ekosysteemejä viranomaisten, aluehallinnon, kuntien sekä yhteisöjen toimintavalmiuden kehittämiseksi. • Järjestetään yhteisten harjoitusten ja harjoitustoimintapalveluiden kehittämisen ja koordinaation foorumeita 2–4 kertaa vuodessa. Niihin kutsutaan yhteisten harjoitustoimintapalveluiden kehittämisestä ja koordinaatiosta vastaavat toimijat sekä tarvittaessa myös harjoitustoimintapalveluiden käyttäjiä ja tuottajia.	Yhteistoimintaan osallistuvat: Tiedonhallintayksikön varautumisesta vastaavat henkilöt
Mittarit	• Harjoitusten vaikuttavuus ja saatavuus eri julkisen hallinnon toimijoille. • Harjoituskohtaiset palautekyselyt. • Yhteisharjoitusten kattavuus: osallistuvat toimijat ja henkilöt sekä taloudellisuus verrattuna kunkin toimijan erikseen järjestämiin harjoituksiin.	

Tilannekuva

Palvelualueen kuvaus	Tuotetaan julkiselle hallinnolle keskitetysti digitaalisen turvallisuuden tilannekuvatuotteita. Tavoitteena on tuottaa yhteisiä ja jaettuja digitaalisen turvallisuuden ja informaatioturvallisuuden tilannekuvaratkaisuja, jotka pohjautuvat laajaan dataan, monipuolisiin mittareihin koko julkisesta hallinnosta sekä modulaariseen raportointiin, joka tukee yhteisen tilannetietoisuuden ja tilanneymmärryksen muodostumista ja päätöksentekoa. Ratkaisuja voidaan täydentää tai rikastaa sisäisillä tilannekuvatiedoilla. Kukin organisaatio huolehtii itse sisäisten tilannekuvatietojensa hallinnasta. Tilannekuvatietoja tarvitaan kattavasti julkisesta hallinnosta sekä yhteisöistä. Palvelualue tuottaa, ylläpitää ja kehittää julkisen hallinnon käyttöön digitaalisen turvallisuuden tilannekuvatietoja ja -tuotteita, jotka perustuvat asiantuntijoiden analyyseihin. Hyödynnetään muun muassa ennakointia, organisaatioiden kypsyysarviointeja, tietojärjestelmien vaatimustenmukaisuusarviointeja sekä automaattista teknistä valvontaa. Palvelualue koostuu seuraavista osista: • Tietojen kerääminen ja koostaminen analysointia ja tilannekuvatuotteiden muodostamista varten. • Tilannekuvatietojen jakelu ja julkaisu tarjotaan osittain itsepalveluna ”on-demand”-ratkaisuna ja erikseen määritellyille ryhmille organisaatiokohtaisia tilannekuvatietojen koosteita varten. Tunnistettuja eri käyttötapauksiin liittyviä tilannekuvapalvelun sisältökokonaisuuksia: • Velvoitetaan julkisen hallinnon digitaalisen turvallisuuden toimintaympäristön kansallinen ennakointi ja seuranta ja siihen liittyvä riskienhallinnan, vaatimustenmukaisuusarviointien ja teknisen valvonnan tietojenvaihto. – Ulkoisen uhkatiedon kerääminen ja analysointi. – Toimintaympäristön turvallisuutta kuvaava analyysi ja tilannekuvan ylläpito. – Riskienhallintaan, vaatimustenmukaisuusarviointeihin tai tekniseen valvontaan perustuva tilannekuvan ylläpito. – Digitaalisen turvallisuuden kypsyysarviointeihin perustuva tilannekuva. – Digitaalisen turvallisuuden resurssien tilannekuva. • Hallinnollisen digitaalisen turvallisuuden tilanteen jatkuva ylläpito DVV:n kokonaiskuvapalvelussa. • Tilannekuvatiedon vaihtaminen kansainvälisten toimijoiden kanssa.	Vastuutaho: KTK VM, ennakointi DVV, hallinnollinen tilannekuva

Yhteistoiminnan rakenne	Palvelualueeseen liittyvän yhteistoiminnan tavoitteena on tilannekuvaan tarvittavan tiedon kerääminen ja tilannekuvan jakaminen. Yhteistoiminta koostuu seuraavista elementeistä: • Vastuutaho ylläpitää kuvausta tilannekuvatuotteistaan; myös valtakunnallisia, alueellisia ja toimialakohtaisia tilannekuvatuotteita. • Vastuutaho ylläpitää kanavaa tietojen keräämiseen ja jakamiseen toimijoiden välillä. • Tiedon toimittaminen vastuutaholle. • Vastuutahon kokoamat tilannekuvatuotteet. • Työpajoja ja seminaareja tilannekuvatuotteiden perusteella. • Yhteistyötoimintaan osallistuvat määrittelevät oman organisaationsa tilannekuvan jakamisen sisäiset säännöt ja osallistuvat tilannekuvatiedon ja parhaiden käytänteiden jakamiseen yhteistoimintaan osallistuvien kesken.	Yhteistoimintaan osallistuvat: Tiedonhallintayksikön digitaalisesta turvallisuudesta vastaavat henkilöt Tiedonvaihtoryhmät (ISAC) Yhteisöt
Mittarit	Käyttäjäorganisaatioiden antama palaute tilannekuvatuotteiden laadusta.	

Toiminnan jatkuvuuden hallinta ja varautuminen

Palvelualueen kuvaus	Palvelualue kattaa toiminnan varautumisen koordinointiin sekä tietojärjestelmien arviointiin ja valvontaan liittyvät kokonaisuudet. Palvelualue koostuu seuraavista osista: • Valmius-, jatkuvuus- ja toipumissuunnitelmien mallipohjien ja ohjeiden ylläpito. • Tuki suunnitelmien laadintaan kansainvälisten standardien ja hyvien käytäntöjen mukaisesti. • Raportointi varautumisen kattavuudesta. • Alueellisen varautumisen kehittämisen alueellinen ekosysteemi.	Vastuutaho: DVV, KTK, HVK, Aluehallintovirasto(t)
Yhteistoiminnan rakenne	Palvelualueeseen liittyvän yhteistoiminnan tavoitteena on julkisen hallinnon yhteinen varautumisen malli. Yhteistoiminta koostuu seuraavista elementeistä: • Vastuutahon tuki varautumiselle yhteisen ohjeistuksen ja mallien avulla. • Valtakunnallinen yhteistoiminta. • Aluehallintotason yhteistoiminta. • Alueellinen ekosysteemi viranomaisten, aluehallinnon, hyvinvointialueiden, kuntien sekä yhteisöjen digitaalisen turvallisuuden varautumisen suunnitteluun ja testaamiseen. Yhteistoimintaan osallistuvat hyödyntävät yhteisiä ohjeistuksia ja malleja oman organisaationsa ja keskeisten yhteistyötahojensa yhteisen varautumisen kehittämisessä ja toteuttamisessa.	Yhteistoimintaan osallistuvat: Tiedonhallintayksikön varautumisesta vastaavat henkilöt
Mittarit	• Varautumisaikatavoitteet • Yhteistoiminnan kattavuus	

Häiriötilanteiden hallinta

Palvelualueen kuvaus	Vahvistetaan käytäntöjä ja toimintatapoja, joiden avulla organisaatiot saavat käyttöönsä nopeasti resursseja häiriön vaikutusten minimointiin sekä tilanteen selvittämiseen. Laajennetaan tietoturvallisuuden kartoituspalvelu kattamaan koko julkinen hallinto julkisen hallinnon organisaatioiden ulkoverkon tietoturvahaavoittuvuuksien havaitsemiseksi. Laajennetaan palvelu kattamaan digitaalisen turvallisuuden häiriönhallintamallin kehittämisen ja ylläpitämisen sekä laajavaikutteisten digitaaliseen turvallisuuteen kohdistuvien häiriötilanteiden selvittämisen tuen. Palvelu koostuu seuraavista osista: • Tietoturvahaavoittuvuuksien havainnointi ja havaintojen raportointi kartoituspalvelun kohdeorganisaatiolle • Häiriönhallintamallin kehittäminen ja ylläpito • Kansallisen tason häiriöhallinnan aktivointi laajavaikutteisessa häiriötilanteessa ja tuki häiriötilanteen selvittämiseksi. • Mahdollisen kansainvälisen avun antamisen ja vastaanottamisen koordinointi KTK:ssa.	Vastuutaho: KTK, yksityisen sektorin asiantuntijayritykset
Yhteistoiminnan rakenne	Palvelualueen yhteistoiminnan tavoitteena on yhtenäinen toimintatapa häiriötilanteiden hallintaan jaettujen resurssien hyödyntämiseksi. Yhteistoiminta koostuu seuraavista elementeistä: • Vastuutaho kilpailuttaa Hanselin puitejärjestelyjen perusteella sopimukset tarvittavan asiantuntijatuen hankkimiseksi markkinoilta välittömästi julkisen hallinnon käyttöön laajavaikutteisissa häiriötilanteissa. • Työpajoja ja seminaareja häiriöhallintamallin kehittämiseksi. • Vastuutaho ylläpitää yhteisesti sovittua häiriötilanteiden hallintamallia. • Vuotuinen alueellinen harjoitus resurssien jakamisesta; harjoituksen järjestysvastuu vaihtuu. Yhteistoimintaan osallistuvat dokumentoivat tarvittavat tiedot ja varmistavat tietoturvallisuuden riittävän resursoinnin käyttääkseen kartoituspalvelua. Yhteistoimintaan osallistuvat dokumentoivat oman organisaationsa digitaalisen turvallisuuden häiriönhallintaprosessit ja varmistavat riittävän resursoinnin vastaanottaakseen nopeaa häiriön hallinnan asiantuntijatukea. Yhteistoimintaan osallistuvat toimijat dokumentoivat oman ICT-ympäristönsä ja ylläpitävät dokumentaation ajan tasalla. Toimijat raportoivat ICT-ympäristönsä määritetyin osin keskitettyyn digitaalisen toimintaympäristön tietovarantoon.	Yhteistoimintaan osallistuvat: Tiedonhallintayksikön häiriötilanteiden hallinnasta vastaavat henkilöt
Mittarit	• Kartoituspalvelua käyttäneiden organisaatioiden määrä. • Kartoituksissa tehtyjen havaintojen kehitys. • Markkinoilta kilpailutetun sopimuksen perusteella hankittujen asiantuntijoiden vuosittainen toteutunut tarve, saatavuus ja käyttö häiriötilanteissa.	

4.4 Digitaalisen turvallisuuden yhteistoiminta- ja hallintamallin toimijat tavoitetilassa

Ministeriöiden tulee määrittää julkisen hallinnon digitaalisen turvallisuuden ohjaukseen tarvittavat säädökset ja toteuttaa ne. Toimeenpanossa tulee keskittyä toiminnallisten rakenteiden uudistamiseen siten, että yhteistoimintaa organisoidaan todellisten tarpeiden ja osaamisen mukaisesti. Keskitettyjä poikkihallinnollisia julkisen hallinnon digitaalisen turvallisuuden tehtäviä hoitavia keskeisiä virastoja ja toimijoita ovat Digi- ja väestötietovirasto (DVV), Liikenne- ja viestintävirasto (Traficom) ja Suomen Erillisverkot Oy sekä valtiotoimijoiden näkökulmasta Valtion tieto- ja viestintätekniikkakeskus (Valtori). Keskeisten toimijoiden roolia ja tehtäviä on tarkasteltava hallinnollisten digitaalisen turvallisuuden tehtävien näkökulmasta. Nykyisiä rakenteita tulisi vahvistaa keskittämällä keskeisten toimijoiden toimintaa nykyistä enemmän digitaaliseen turvallisuuteen ja huomioimalla aikaisempaa paremmin kansainvälinen toiminta ja tietojenvaihto.

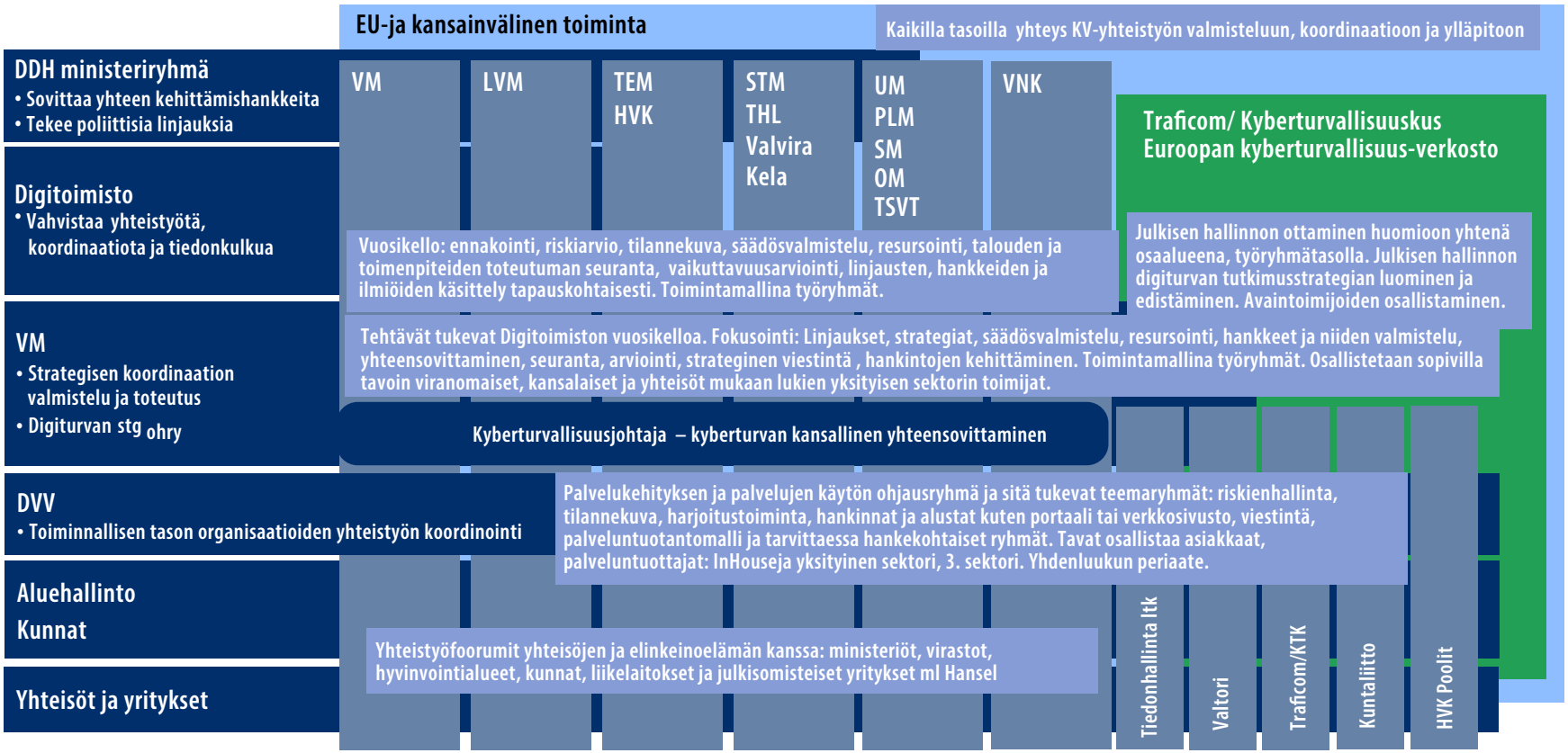
Kuvassa 5 on visualisoitu julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamallia tavoitetilassa. Tavoitetilan saavuttaminen edellyttää digitaalisen turvallisuuden keskeisen toimijoiden tehtävien arviointia ja tarkentamista säädösvalmistelun avulla sekä yhteistoiminnan keskeisten ryhmien ja prosessien tarkempaa kuvausta ja toteuttamista.

Kuvassa 5 on hahmotettu tarvittavia muutoksia, jotka ovat:

- EU- ja kansainvälinen toiminta: Kaikilla toiminnan tasoilla yhteys kansainvälisen yhteistyön valmisteluun, koordinaatioon ja ylläpitoon.
- Digitoimisto: Vuosikello: ennakointi, riskiarvio, tilannekuva, säädösvalmistelu, resursointi, talouden ja toimenpiteiden toteutuman seuranta, vaikuttavuusarviointi, linjausten, hankkeiden ja ilmiöiden käsittely tapauskohtaisesti. Toimintamallina työryhmät.

- Valtiovarainministeriö:
  - Digiturvan strategisen koordinaation valmistelu ja seuranta, digitaalisen turvallisuuden strateginen johtoryhmä, digiturvan säädösten valmistelufoorumi.
    - Tehtävät tukevat Digitoimiston vuosikelloa.
    - Fokusointi: Linjaukset, strategiat, säädösvalmistelu, resursointi, hankkeet ja niiden valmistelu, yhteensovittaminen, seuranta, arviointi, strateginen viestintä, hankintojen kehittäminen.
    - Toimintamallina työryhmät. Osallistetaan sopivilla tavoilla viranomaiset, kansalaiset ja yhteisöt mukaan lukien yksityisen sektorin toimijat.

Kuva 5. Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalli tavoitetilassa



- Digi- ja väestötietovirasto: Toiminnallisen tason organisaatioiden yhteistyön koordinointi.
  - Palvelukehityksen ja palvelujen käytön ohjausryhmä ja sitä tukevat teemaryhmät: riskienhallinta, tilannekuva, harjoitustoiminta, hankinnat ja alustat, kuten portaali tai verkkosivusto, viestintä, palveluntuotantomalli ja tarvittaessa hankekohtaiset ryhmät.
  - Tavat osallistaa asiakkaat, palveluntuottajat: ns. "in-house" ja yksityinen sektori, kolmas sektori. Yhden luukun periaate.

- Traficom/KTK: Julkisen hallinnon huomioiminen yhtenä osa-alueena työryhmissä. Julkisen hallinnon digiturvan tutkimusstrategian luominen ja edistäminen. Avaintoimijoiden osallistaminen.
- Yhteistyöfoorumit yhteisöjen ja elinkeinoelämän kanssa: ministeriöt, virastot, hyvinvointialueet, kunnat, liikelaitokset ja julkisomisteiset yritykset mukaan lukien Hansel sekä yritykset ja kansalaisjärjestöt.

Jokaiseen organisaatioon tarvitaan tietoturvavastaavan tai digitaalisen turvallisuuden vastaavan rooli. Huomiota tulee kiinnittää siihen, miten digitaalisen turvallisuuden kokonaisuutta toteutetaan parhaiten jatkuvana toimintana, joka mahdollistaa ennakoivan ja suunnitelmallisen toimintamallin.

5 Yhteenveto

Selvityksessä on tunnistettu runsaasti tarpeita ja ehdotuksia julkisen hallinnon digitaalisen turvallisuuden yhteistoiminnan ja sen hallintamallin kehittämiseksi. Keskeiset esille nostetut ehdotukset ja kehittämistarpeet on kuvattu tässä luvussa. Niihin liittyvät digitaalisen turvallisuuden yhteistoiminnan tarkemmat kuvaukset ovat kappaleissa 4.3 ja 4.4. Keskeisiä ehdotuksia ja kehittämistarpeita on valmisteltu yhdessä Suomen digikompassin valmistelun kanssa. Niiden jatkovalmistelussa ja toteuttamisessa on huomioitava kansainväliset velvoitteet mukaan lukien muuttuva EU-sääntely.

5.1 Keskeisiä esille nostettuja ehdotuksia ja kehittämistarpeita

Yhteistoiminnan ohjaus

Digitaalisen turvallisuuden yhteistoiminta edellyttää vahvaa ohjausta sekä koko julkisessa hallinnossa että hallinnon eri alueilla: ministeriöissä, valtionhallinnon toiminnallisella ja operatiivisella tasolla, hyvinvointialueilla ja kunnissa. Ohjausta tulee toteuttaa strategia-, normi-, resurssi- ja informaatio-ohjauksena. Ohjaukseen liittyvien tavoitteiden ja kehitystoimenpiteiden tulee pohjautua jaettuun ja analysoituun tilannetietoon todellisesta tilanteesta. Arviointien tulee perustua todennettuihin mittareihin. Digitaalisen turvallisuuden keskeisten vastuiden ja yhteisten toimintamallien tulee olla velvoittavia.

1. Yhteinen ohjaus, kehittämisen yhteistoiminta, valvonta ja viestintä: Arvioidaan ja tarkennetaan julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamallin tavoitetilan keskitettyjä tehtäviä ja toimijoita sekä yhteistoiminnan keskeisten ryhmien ja prosessien kuvauksia ja toimintaa. Huomioidaan EU-sääntely mukaan lukien NIS2- ja CER-direktiivien kansallinen soveltaminen.

   Vastuu: Digitoimisto, VM, LVM, TEM, DVV, Traficom, kyberturvallisuusjohtaja
   Aikataulu: 2022–2024
   Valmistelu ja rahoitus: Arvioitavaksi digitoimistossa. Rahoitus tarkennetaan suunnittelun edetessä.

2. Yhteinen ohjaus, kehittämisen yhteistoiminta, valvonta ja viestintä: Ylläpidetään keskitetysti julkisen hallinnon digitaalisen turvallisuuden yhteisen kehittämisen resurssitilannekuvaa.

   Vastuu: VM, kyberturvallisuusjohtaja, Valtiokonttori
   Aikataulu: 2024–2027
   Valmistelu ja rahoitus: Arvioitavaksi digitoimistossa. Rahoitus tarkennetaan suunnittelun edetessä.

3. Yhteinen ohjaus, kehittämisen yhteistoiminta, valvonta ja viestintä: Muodostetaan yhteinen näkemys julkisen hallinnon digitaalisen turvallisuuden kehitysohjelmasta Digiturva2027 ja sen rahoituksesta vuosille 2023–2027.

   Vastuu: VM, LVM, TEM, DVV, Traficom
   Aikataulu: 2022–2023
   Valmistelu ja rahoitus: Toteutetaan linjatyönä. Käsitellään digitoimistossa. Ei vaadi lisärahoitusta.

4. Tilannekuva: Velvoitetaan toteuttamaan julkisen hallinnon digitaalisen turvallisuuden toimintaympäristön kansallinen ennakointi ja seuranta sekä siihen liittyvä riskienhallinnan, vaatimustenmukaisuusarvioitien ja teknisen valvonnan tietojenvaihto.

   Hyödynnetään laajaa tietopohjaa ja monipuolisia mittaristoja mukaan lukien soveltuvin osin digiturvan kypsyysarviointien, riskienhallinnan, vaatimustenmukaisuusarvioiden ja teknisen valvonnan julkiset, salassa pidettävät ja turvallisuusluokitellut tiedot. Toteutetaan modulaarista raportointikykyä. Ennakointi- ja seurantatietoja käytetään yhteisen näkemyksen muodostamiseksi digitaalisen turvallisuuden ja informaatioturvallisuuden kehittämisestä ja yhteisessä toimeenpanossa.

   Vastuu: VM, DVV, julkisen hallinnon organisaatiot, VTT ja yksityiset toimijat tiedontuottajina
   Aikataulu: 2023–2025
   Valmistelu ja rahoitus: Arvioitavaksi digitoimistossa. Rahoitus tarkennetaan suunnittelun edetessä.

5. Tilannekuva: Kehitetään tiedolla johtamisen edellytyksiä julkisten digipalveluiden turvallisuuden hallinnassa. Velvoitetaan kuvaamaan ja toteuttamaan digitoimintaympäristön tietojen ylläpito ja tietojenvaihto.

   Vastuu: VM, DVV, julkisen hallinnon organisaatiot tiedontuottajina
   Aikataulu: 2023–2025
   Valmistelu ja rahoitus: Arvioitavaksi digitoimistossa. Rahoitus tarkennetaan suunnittelun edetessä.

6. Yhteinen ohjaus, kehittämisen yhteistoiminta, valvonta ja viestintä: Digitaalisen turvallisuuden kehitysohjelmien ja niiden tuotosten vaikuttavuutta arvioidaan ja arviointien tuloksista viestitään. Arvioidaan Haukka-ohjelman vaikuttavuus.

   Vastuu: VM
   Aikataulu: 2022–2023
   Valmistelu ja rahoitus: Toteutetaan linjatyönä. Rahoitustarve arvioidaan tapauskohtaisesti. Haukka-ohjelman vaikuttavuuden arviointi: valmistelu ja rahoitus Haukka-ohjelmassa.

7. Yhteinen ohjaus, kehittämisen yhteistoiminta, valvonta ja viestintä: Edistetään kansallisin toimenpitein hyvinvointialueiden välistä digitaalisen turvallisuuden kehittämisen yhteistoimintaa.

   Vastuu: STM, SM, VM, DVV
   Aikataulu: 2022–2027
   Valmistelu ja rahoitus: Arvioitavaksi digitoimistossa. Rahoitus tarkennetaan toimenpidekohtaisesti.

8. Yhteinen ohjaus, kehittämisen yhteistoiminta, valvonta ja viestintä: Uudistetaan digiturvan yhteistoiminnan johtamista ja toimintakulttuuria valtiolla, kunnissa ja hyvinvointialueilla. Velvoitetaan valtiotoimijoita, hyvinvointialueita ja kuntia nimeämään tietoturvavastaavan roolia hoitavat toimijat.

   Vastuu: VM, julkisen hallinnon organisaatiot
   Aikataulu: 2023–2027
   Valmistelu ja rahoitus: Arvioitavaksi digitoimistossa. Rahoitus tarkennetaan suunnittelun edetessä.

Digitaalisen turvallisuuden palvelut

Digitaalisen turvallisuuden palvelujen kehittäminen ja ylläpito ovat samankaltaista eri toimijoiden välillä. Niiden määrittely ja kehittäminen tulee toteuttaa yhdessä. Yhteistoiminta edellyttää toiminnallisten rakenteiden uudistamista siten, että organisoituminen voidaan tehdä todellisten tarpeiden ja osaamisen mukaisesti.

9. Yhteiset määräykset, ohjeet, vaatimukset, suositukset ja työkalut: Velvoitetaan julkisten digipalvelujen yhteiselle digitaalisen turvallisuuden ohjeistukselle ylläpitäjä sekä ajantasaistetaan ja karsitaan ohjeistusta. Julkista hallintoa koskevat yhteiset digitaalisen turvallisuuden säädösluettelot, ohjeet, vaatimukset, suositukset ja työkalut ovat saatavilla yhdestä paikasta tietopankista soveltamiskohteiden mukaisesti tai muutoin järjestettynä. Kullakin yhteisellä ohjeella, tai ohjeistuksen kokonaisuudella tulee olla selkeä vastuutaho, joka huolehtii ohjeistuksesta koko sen elinkaaren ajan.

   Vastuu: VM, DVV
   Aikataulu: 2024–2027
   Valmistelu ja rahoitus: Arvioitavaksi digitoimistossa. Rahoitus tarkennetaan suunnittelun edetessä.

10. Yhteiset määräykset, ohjeet, vaatimukset, suositukset ja työkalut: Ohjeistuksessa kuvataan pilviteknologian turvallisen käytön yleiset, kansalliset vaatimukset. Digitaalisen turvallisuuden näkökulmasta on tärkeä tunnistaa, miten eri organisaatioissa voitaisiin hyödyntää pilvipalveluita turvallisesti ja miten esimerkiksi pilvipalveluita hyödyntämällä voidaan turvata palveluiden saatavuutta.

    Vastuu: Tiedonhallintalautakunta, DVV
    Aikataulu: 2022–2027
    Valmistelu ja rahoitus: Toteutetaan linjatyönä. Ei vaadi lisärahoitusta.

11. Yhteiset hankinnat, hankkeet ja digipalvelut: Yhteistoiminta-alueet yhteensovittavat ja hyvinvointialueet kehittävät yhdessä keskitetysti tarjottuja työkaluja ja palveluita digitaalisen turvallisuuden arviointiin ja kehittämiseen, hyvinvointialueiden kansallisen tilannekuvan, keskitetyn valvonnan ja hyvinvointialueiden välisen yhteistoiminnan toteuttamiseen sekä pilvipalveluiden digitaalisen turvallisuuden varmistamiseen.

    Vastuu: Yhteistoiminta-alueet, hyvinvointialueet, DigiFinland
    Aikataulu: 2022–2027
    Valmistelu ja rahoitus: Yhteistoiminta-alueet ja hyvinvointialueet hankkeistavat. Rahoitus tarkennetaan suunnittelun edetessä.

12. Osaaminen: Hyödynnetään kuntien alueellisen digitaalisen turvallisuuden yhteistoiminnan hyviä käytänteitä ja edistetään niiden leviämistä. Kehitetään kuntien, hyvinvointialueiden ja yhteistoiminta-alueiden alueellista verkostoitumista. Kehitetään yhteistä digitaalisen turvallisuuden varautumista ja harjoittelua.

    Vastuu: Kuntaliitto, hyvinvointialueet, Traficom (KTK)/Kunta-ISAC, DVV
    Aikataulu: 2024–2027
    Valmistelu ja rahoitus: Toteutetaan linjatyönä. Rahoitus sisällytetään talousarvioehdotuksiin.

13. Yhteiset hankkeet, hankinnat ja digipalvelut: Kunnille tarjotaan keskitetysti yhteisiä digiturvapalveluita. Hyödynnetään esimerkiksi Haukka-ohjelmassa laadittua kuntien digiturvapalveluiden tiekarttaa.

    Vastuu: Traficom (KTK), DVV, kuntien ja kuntayhtymien ICT-yhtiöt, Kuntaliitto
    Aikataulu: 2022–2027
    Valmistelu ja rahoitus: Toteutetaan linjatyönä. Rahoitus tarkennetaan palvelukohtaisesti.

14. Häiriötilanteiden hallinta: Varmistetaan asiantuntijatuen riittävyys laajoissa tietoturvaloukkaustilanteissa. Järjestetään julkisen hallinnon toimijoille markkinoilta välittömästi hankittavissa olevaa asiantuntijatukea laajavaikutteisissa häiriötilanteissa. Selvitetään ja toteutetaan mahdolliset säädösmuutokset.

    Vastuu: LVM, Traficom (KTK)
    Aikataulu: 2022–2024
    Valmistelu ja rahoitus: Arvioitavaksi digitoimistossa. Toteutetaan linjatyönä. Rahoitusmalli tarkennetaan suunnittelun edetessä.

15. Häiriötilanteiden hallinta: Laajennetaan tietoturvallisuuden kartoituspalvelu kattamaan koko julkinen hallinto julkisen hallinnon organisaatioiden ulkoverkon tietoturvahaavoittuvuuksien havaitsemiseksi.

    Vastuu: Traficom (KTK), VM, LVM
    Aikataulu: 2023–2024
    Valmistelu ja rahoitus: Vuosina 2022–2023 tehtävä valmistelu ja rahoitus Haukka-ohjelmassa.

Tutkimus ja osaamisen kehittäminen

Toimijoiden välistä keskustelua digitaalisen turvallisuuden tutkimuskohteista tulee kehittää sekä varmistaa tutkimukselle riittävä rahoitus. Tutkimustuloksia tulee jakaa laajasti yhteiskunnassa ylläpitämällä jatkuvaa ja aktiivista keskustelua digitaalisen turvallisuuden tilasta ja kehittämisestä. Digitaalisen turvallisuuden varmistaminen, välttämättömän tiedon jakaminen ja nopea reagointi poikkeamiin edellyttää osaamista ja yhtenäisempiä toimintatapoja toimijoiden välillä.

16. Tutkimuksen, kehityksen ja innovoinnin koordinointi: Tunnistetaan, hallitaan sekä seurataan kansallisia, EU- ja kansainvälisiä tutkimus-, kehitys- ja innovaatiokohteita ja tarvittavaa tutkimusrahoitusta. Luodaan eri toimijoita yhteen tuova kansallinen verkosto.

    Vastuu: Traficom (KTK), Kyberturvallisuusjohtaja, VTT
    Aikataulu: 2023–2025
    Valmistelu ja rahoitus: Toteutetaan linjatyönä. Rahoitusmalli tarkennetaan suunnittelun edetessä.

17. Osaaminen sekä yhteiset hankinnat, hankkeet ja digipalvelut: Parannetaan digiturvaosaamista sekä riskien ja uhkien hallintaa yhteisillä koulutusratkaisuilla, asiantuntijaverkostoilla ja harjoittelemalla. Kehitetään teknistä digiturvaosaamista ja teknisten työkalujen käyttöä. Kehitetään teknisten työkalujen yhteishankintaa.

    Vastuu: DVV, Traficom (KTK), VTT, HAUS, Hansel
    Aikataulu: 2022–2027
    Valmistelu ja rahoitus: Arvioitavaksi digitoimistossa. Rahoitus tarkennetaan suunnittelun edetessä. Vuosina 2022–2023 tehtävä valmistelu ja rahoitus Haukka-ohjelmassa.

18. Harjoitustoiminta: Selvitetään digitaalisen turvallisuuden yhteisen harjoitustoiminnan vaikuttavuus ja poikkeamatilanteissa tarvittavan ohjeistuksen tarpeet.

    Vastuu: DVV, VTT
    Aikataulu: 2023
    Valmistelu ja rahoitus: Valmistelu ja rahoitus Haukka-ohjelmassa.

5.2 Jatkotoimenpiteet ja seuraavat vaiheet

Digitaalisen turvallisuuden yhteistoiminnan ja hallintamallin kehittämisen keskeisten ehdotusten ja kehittämistarpeiden suunniteltu jatkovalmistelu on kirjattu ehdotusten yhteyteen. Ehdotusten sisällön perusteella niiden jatkovalmistelu on ohjattu linjatyöksi, osaksi Haukka-ohjelmaa tai arvioitaviksi digitoimistossa. Valtiovarainministeriön suunnitelmana on tuoda laajemmat ehdotukset arvioitaviksi ja mahdollisesti tarkemmin valmisteltaviksi digitoimistossa syksyn 2023 ja alkutalven 2024 aikana. Arviointi ja tarkempi valmistelu sisältävät myös rahoituksen suunnittelun.

Kunkin ehdotuksen tarkoituksena on kiinnittää huomiota eri käyttäjäorganisaatioiden valmiuksiin, osaamiseen ja olemassa oleviin resursseihin. Tavoitteiden toteuttaminen ja tunnistettujen vaikutusten aikaansaaminen edellyttävät arjen tehtävien systemaattista ja käytännönläheistä tukea. Tutkimuksen ja osaamisen kehittämisen avulla on tarkoitus löytää keinoja ja toimintamalleja kuntien ja yksityisen sektorin yhteistoiminnan lisäämiseksi digitaalisen turvallisuuden osa-alueilla hyödyntäen hyväksi havaittua käytäntöä, Suomen digitaalisuuden menestystekijää - julkinen sektori kirittää yksityistä ja yksityinen julkista sektoria.

Monet kehittämisehdotukset tarvitsevat lisärahoitusta ja niiden kustannustehokkuuteen sekä kustannus- ja hyötylaskelmiin tulee kiinnittää erityistä huomioita, jotta voidaan varmistua resurssien kohdentumisesta tarkoituksenmukaisimpiin kohteisiin. Lisärahoitusta tarvitsevien ehdotusten aikataulu on viitteellinen. Päätökset lisärahoituksesta on tehtävä vähintään puoli vuotta ennen ehdotuksen toteuttamisen aloitusajankohtaa, jotta esitetty aikataulu olisi mahdollinen. Menokehyksen puitteet tulee huomioida mahdollisten resurssitarpeiden ja niiden kattamisen yhteydessä. Mahdollisia rahoitustarpeita tulee käsitellä julkisen talouden suunnitelman ja valtion talousarvioiden valmistelun yhteydessä sovittaen ne yhteen muiden julkisen talouden menotarpeiden kanssa.

LIITE 1: Koordinaatioryhmän jäsenet

Tuija Kuusisto, VM, puheenjohtaja
Niko Mäkilä, VM, varapuheenjohtaja
Sami Aalto, OKM
Aaro Hallikainen, Helsingin kaupunki
Kimmo Janhunen, OM
Jaakko Jokela, TEM
Jukka-Pekka Juutinen, Traficom
Marko Karjalainen, Business Finland, 1.1.2022 alkaen
Juha Koivisto, Tampereen kaupunki
Kalervo Koskimies, OKM
Tuukka Lahkela, Business Finland, 31.12.2021 saakka
Vesa Laitinen, Hämeenlinnan kaupunki
Martti Lehto, Jyväskylän yliopisto
Jaana Merta, MMM
Harri Mäntylä, PLM
Kari Nykänen, Oulun kaupunki
Tarja Nylander, SM
Ismo Paananen, Agendium oy
Rauli Paananen, LVM
Sauli Pahlman, Traficom, varajäsen
Pekka Pajuoja, Business Finland, 1.1.2022 alkaen
Peter Sund, Kyberala ry (FISC), 1.1.2022 alkaen
Matti Parviainen, UM, varajäsen
Mikko Pitkänen, DVV
Tero Reponen, VTT
Kimmo Rousku, DVV
Seppo Ruotsalainen, Kuopion kaupunki
Juha Röning, Oulun yliopisto
Kari Santalahti, SM
Marko Tanska, Salon kaupunki
Ari Uusikartano, UM
Jukka-Pekka Virtanen, PLM, varajäsen
Teemupekka Virtanen, STM
Jari Ylikoski, Kuntaliitto
Jarkko Yliruka, ESAVI

LIITE 2: Haastattelut

Osallistujat
valtioneuvoston kanslia
ulkoministeriö
oikeusministeriö
sisäministeriö
puolustusministeriö
maa- ja metsätalousministeriö, Ruokavirasto
liikenne- ja viestintäministeriö
sosiaali- ja terveysministeriö
työ- ja elinkeinoministeriö
Digi- ja väestötietovirasto
Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus
aluehallintovirasto
Pohjois-Savon sairaanhoitopiiri
Kuntaliitto
Tietosuojavaltuutetun toimisto
Jyväskylän yliopisto
Oulun yliopisto
VTT
Business Finland
Agendium oy
Helsingin kaupunki
Hämeenlinnan kaupunki
Kuopion kaupunki
Oulun kaupunki
Tampereen kaupunki
KyberVPK

LIITE 3: Yleiset mallit yhteistoiminnan järjestämiseksi

Tunnistetut ja määritellyt yhteistoiminnan rakenteet

Muodolliset ja epämuodolliset yhteistyön muodot

Haastatteluissa nousi esiin useita kommentteja yhteistoiminnan erilaisista muodoista ja niiden sopivuudesta eri tarkoituksiin. Myös useat tutkimukset osoittavat, että parhaita tuloksia yhteistoiminnalla saadaan, kun hyödynnetään erilaisia vaikutustapoja samanaikaisesti. Muodollista yhteistoimintaa ja vuorovaikutusta julkishallinnossa edustavat jo olemassa olevat rakenteet, kuten esimerkiksi yhteishankinnat tai kuntien perustamat yhteiset ICT-palveluyhtiöt. Epämuodollista yhteistyötä puolestaan ovat poolitoiminta sekä ISAC-tiedonvaihtoryhmät.

Digitaalisen turvallisuuden yhteistoiminnan tulee sisältää sekä muodollista että epämuodollista vuorovaikutusta osapuolten välillä. Osapuolten on osallistuttava aktiivisesti eri yhteistoiminnan muotoihin, jotta organisaation omat tavoitteet on mahdollista saavuttaa mahdollisimman tehokkaasti.[38]

Ekosysteemi yhteistoiminnan mallina

Digitaalisen turvallisuuden yhteistoiminnassa ekosysteemeillä voidaan tarkoittaa julkisen ja yksityisen sektorin välistä tiivistä yhteistyötä sekä kehittämistoimenpiteiden koordinointia. Tyypillisesti ekosysteemiajatteluun liitetään

- avoin innovaatiotoiminta sekä sitä tukevat toimintamallit tarvittavien toimijoiden tunnistamiseksi ja yhteen kokoamiseksi
- toimintamalleja yhteistyössä tehtävää kehittämistä varten.

Digitaalisen turvallisuuden kehittämiseen liittyvässä ekosysteemissä valtiotoimijoilla on erilaisia rooleja. Lainsäätäjänä valtiotoimijat voivat korjata toimintaympäristöön liittyviä epäkohtia. Perinteinen ohjausmalli säädös- ja resurssiohjauksineen on selkeä, mutta joustamattomana vaikeuttaa digitaalisen turvallisuuden toimijoiden sopeutumista toimintaympäristön nopeisiin muutoksiin.

Valtiotoimijat voivat uudistaa toimintamalleja ja tuoda esiin tarpeita digitaalisen turvallisuuden kehittämiseksi. Tämä edellyttää osaamista, jota tarvitaan muun muassa digitaalisen turvallisuuden toimijoiden sekä tarpeiden analyysiin, toimintaympäristön riskien,

38 https://www.vaikuttavuussaatio.fi/wp-content/uploads/2021/02/vaikuttavuussaatio_selvitys.pdf

uhkien ja trendien analyysiin sekä ekosysteemien mahdolliseen koordinointiin tai tukemiseen. Ekosysteemeihin osallistuville yhteistyön on oltava vastavuoroista: erilaiset toimijat, kuten erikokoiset yritykset, tutkimusorganisaatiot, rahoittajat ja julkisen sektorin toimijat tuovat ekosysteemiin oman osaamisensa ja verkostonsa. Työ- ja elinkeinoministeriö on julkaissut ekosysteemeihin liittyviä selvityksiä ja raportteja.[39] VTT on julkaissut ekosysteemioppaan.[40]

Digitaalisen turvallisuuden yhteistoiminnan tasot

Digitaalisen turvallisuuden yhteistoimintaan tarvitaan useita eri tarkoituksiin soveltuvia tasoja sekä osallistujatahon eri tasoilla tehtävän yhteistyön tehokasta ohjausta

- velvoittava – vapaaehtoinen
- kansainvälinen – kansallinen – alueellinen
- osaamisekosysteemit – liiketoimintaekosysteemit – innovaatioekosysteemit
- muodollinen – epämuodollinen yhteistoiminta.

Kutakin digitaalisen turvallisuuden palvelua voidaan tarkastella sekä yhteistoiminnan rakenteiden, että yhteistoiminnan eri tasojen kautta.

39 https://tem.fi/documents/1410877/4429776/Ekosysteemit+uuden+elinkeino-+ja+innovaatiopolitiikan+kohteena/f46d3709-fdcf-4a73-83df-e84ae24b4196

40 https://www.vttresearch.com/sites/default/files/pdf/publications/2020/Yhdessa_kestavaa_kasvua_17022021.pdf

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin 0295 160 01
vm.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-201-7 (pdf)

Joulukuu 2022