VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalliselvitys

LUONNOS
3.5.2022

TIIVISTELMÄ

Yhteiskunnan digitalisoituessa myös tarve digitaalisen turvallisuuden edistämiselle kasvaa. Digitaalisesta turvallisuudesta huolehtiminen edellyttää organisaatiossa riskienhallinnan, jatkuvuudenhallinnan, tietoturvallisuuden, kyberturvallisuuden ja tietosuojan 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 ainakin oman toiminnan, 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 sekä koko julkisen hallinnon kattavaa digitaalisen turvallisuuden yhteistoimintaa, että valtionhallinnon, hyvinvointialueiden ja kuntien yhteistoimintaa, ja myös tutkimustoiminnan sekä 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 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. 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/operatiivisella tasolla, hyvinvointialueilla ja kunnissa. Ohjausta tulee toteuttaa strategia-, normi-, resurssi- ja informaatio-ohjauksena. Digitaalisen turvallisuuden keskeisten vastuiden ja yhteisten toimintamallien tulee olla velvoittavia. Digitaalisen turvallisuuden palvelujen määrittely ja kehittäminen tulee toteuttaa yhdessä. 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. Selvityksen viimeisessä luvussa on kuvattu tavoitetilakuvauksen perusteella valittuja merkittävimpiä kehittämistoimenpiteitä vastuutahoineen.

Sisällys

1 JOHDANTO

1.1 Raportin lähtökohdat

Valtioneuvosto teki 8.4.2020 periaatepäätöksen julkisen hallinnon digitaalisesta turvallisuudesta (VM 2020:33). 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, sekä tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla (Titukri) toimenpiteet sekä EU:n direktiiviehdotus (COM(2020) 823 final) kyberturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella ja verkko- ja tietoturvadirektiivin (EU) 2016/1148 kumoamisesta, eli niin sanottu NIS2[2]. Koordinaatioryhmän jäsenet ovat liitteessä 1.

NIS2-direktiiviehdotuksen mukaan jäsenvaltioiden tulisi määrittää yksi tai useampi valvova viranomainen, joka olisi vastuussa laajamittaisten kyberturvallisuushäiriöiden ja -kriisien operatiivisesta johtamisesta. Jäsenvaltioiden tulisi varmistaa, että valvovilla viranomaisilla on näihin tehtäviin riittävät resurssit. Jokaisen jäsenvaltion tulisi lisäksi tunnistaa valmiudet, resurssit ja prosessit, jotka voidaan käynnistää ja ottaa käyttöön ehdotuksen mukaisissa tilanteissa. NIS2-direktiiviehdotuksen kansallisen toteutuksen yhteydessä on arvioitu tarvittavan julkishallintoa koskevan lainsäädännön tarkastelua.

[1] Esiselvitys Digitaalisen turvallisuuden kunta-valtio yhteistoimintamalli, valtiovarainministeriö 11.6.2021
[2] COM(2020) 823 final NIS2 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823

1.2 Työn toteutus ja rajaukset

Työ toteutettiin haastattelemalla julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamallin koordinaatioryhmän jäseniä ja heidän nimeämiään henkilöitä. Haastattelijoina toimi valtiovarainministeriön Haukka-projektiryhmän jäseniä. Haastatteluissa kartoitettiin digitaalisen turvallisuuden valtio-hyvinvointialue-kunta-yhteistoiminnan nyky- ja tavoitetilaa sekä merkittäviä haasteita yhteistoiminnan toteutumiseksi. 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 sekä koko julkisen hallinnon kattavaa digitaalisen turvallisuuden yhteistoimintaa, että valtionhallinnon yhteistoimintaa, hyvinvointialueiden yhteistoimintaa ja kuntien yhteistoimintaa, ja myös tutkimustoiminnan sekä yksityissektorin kanssa toteutettavaa digitaalisen turvallisuuden yhteistoimintaa.

Valtioneuvoston periaatepäätöksen Kyberturvallisuuden kehittämisohjelma 10.6.2021 yhtenä tehtävänä on jatkokehittää poikkihallinnollisesti viranomaisten varautumista kyberhäiriötilanteisiin. Periaatepäätöksen toteuttaminen on aloitettu käynnistämällä selvitystyö, jossa arvioidaan viranomaisten toimintaedellytyksiä kansallisen 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). Sen on tarkoitus tuottaa ensimmäisiä säädösluonnoksia vuoden 2022 aikana. Kyber-PTR-valmistelussa huomioidaan myös Haukka-toimeenpanosuunnitelman tavoite kehittää kansallista kybertilannekuvaa ja selkiyttää operatiivisen johtamisen vastuita ja järjestelyitä. KEHO- ja Titukri-selvitysten johdosta operatiivisen johtamisen vastuut ja järjestelyt on rajattu tämän selvitystyön ja Haukka-ohjelman ulkopuolelle.

Selvitystyön aikana valmisteltiin myös 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 pääsääntöisesti julkisesti saatavilla oleviin kirjallisiin lähteisiin. Vertailussa käsiteltiin organisaatioita, joilla on sektorikohtaisia vastuita laajempia digitaaliseen turvallisuuteen liittyviä toiminnallisen tason tehtäviä.

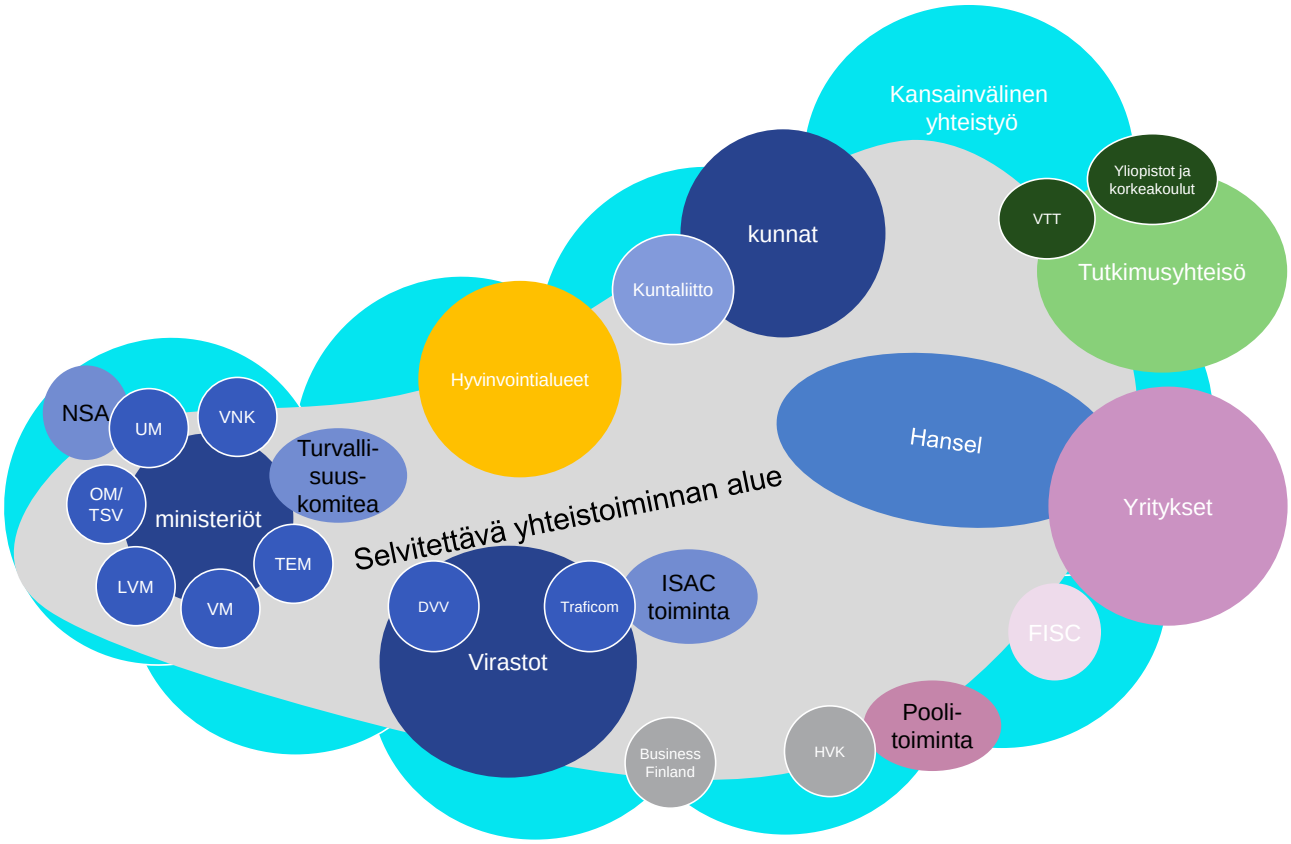
[3] Digitaalisen turvallisuuden yhteistoiminta- ja hallintamallien kansainvälinen vertailu, valtiovarainministeriö 25.4.2022

Selvityksen viimeisenä tehtävänä koordinaatioryhmässä valmisteltiin merkittävimmät kehittämistoimenpiteet. Selvitysraportti on asetettu julkisesti lausuttavaksi lausuntopalveluun 4.5.–3.6.2022 väliseksi ajaksi. Koordinaatioryhmän tarkoituksena on viimeistellä selvitys lausuntopalautteiden perusteella.

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.

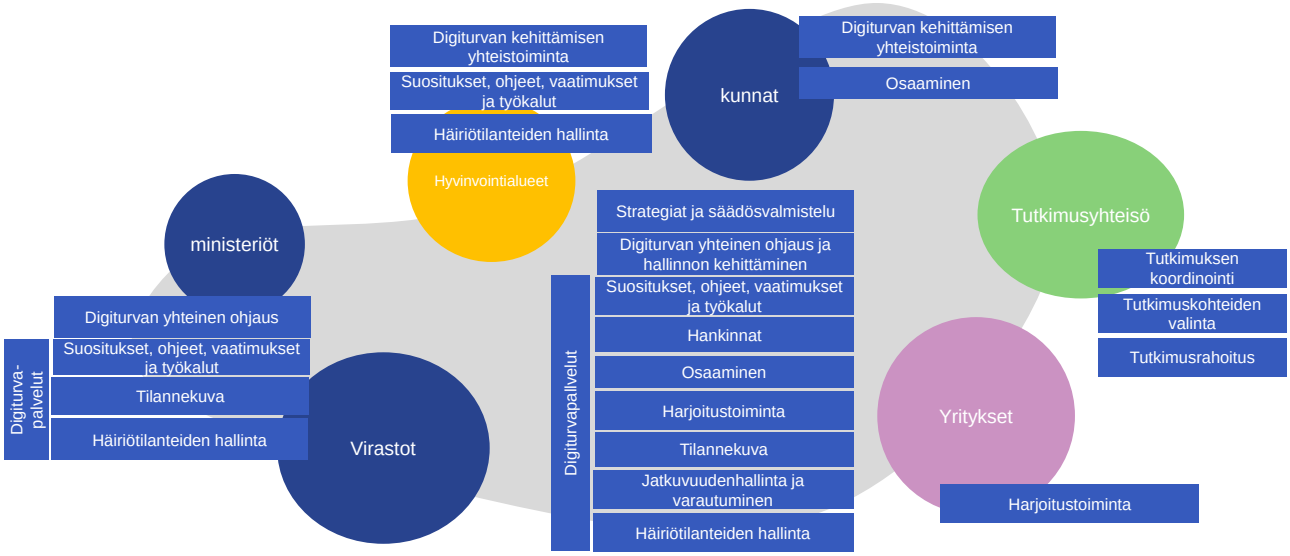


Kuva 1: Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminnan kokonaisuus.

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.



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

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 nykyisin Digi- ja väestötietoviraston ylläpitämä VAHti-verkosto. Se on julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja keskeisten palveluiden tuottamisesta vastaavien organisaatioiden laajapohjainen yhteistyö-, valmistelu- ja koordinaatioelin[4]. Digi- ja väestötietovirasto myös kehittää ja tarjoaa erilaisia julkisen hallinnon digitaalisen turvallisuuden kehittämistä tukevia palveluja ja tuotteita valtiovarainministeriön ohjaamien kehittämisohjelmien alla (esim. Haukka-ohjelma). Liikenne- ja viestintävirasto ja virastoon sijoitettu Kyberturvallisuuskeskus vastaavat valtiohallinnon turvallisuusluokitellun tiedonkäsittelyyn tarkoitettujen tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista ja hyväksynnästä. Kyberturvallisuuskeskus 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. Kyberturvallisuuskeskus tarjoaa myös tietoturvaneuvontaa valtionhallinnolle sekä huoltovarmuuskriittisille toimijoille sekä tuottaa ohjeita ja oppaita yleisesti käytettäväksi organisaatioissa. Digi- ja väestötietoviraston tavoin Kyberturvallisuuskeskus kehittää ja tarjoaa erilaisia julkisen hallinnon digitaalisen turvallisuuden kehittämistä tukevia palveluja ja tuotteita valtiovarainministeriön ohjaamien kehittämisohjelmien alla (esim. Haukka-ohjelma). Kyberturvallisuuskeskus kehittää ja tarjoaa erilaisia palveluja ja tuotteita myös huoltovarmuuskriittisille toimijoille Huoltovarmuuskeskuksen kehittämisohjelmien alla ja rahoittamana. Monet näistä

[4] https://dvv.fi/vahti

huoltovarmuuskriittisille toimijoille tarjotuista ja kehitetyistä palveluista ja tuotteista ovat julkisesti saatavilla ja siten myös muiden kuin huoltovarmuuskriittisten toimijoiden hyödynnettävissä. Suomen Erillisverkot Oy, tieto- ja viestintätekniikkakeskus (Valtori), Kuntien Tiera Oy, Istekki Oy jne. tarjoavat keskitetysti ICT-palveluja, mukaan lukien ICT-laitteita, valtiohallinnon toimijoille, kunnille ja sairaanhoitopiireille sekä jatkossa hyvinvointialueille.

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 myös huomioida niiden 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 digitaalisen 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.[5] Ryhmä jatkaa julkisen hallinnon uudistamisen poliittiselle johtoryhmälle asetettujen tehtävien edistämistä.

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

	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 on vastuussa siitä, että tilanne on hallinnassa. Vakavassa kyberhäiriötilanteessa liikenne- ja viestintäministeriö koordinoi kyberturvallisuusjohtajan rinnalla tarpeen mukaan niitä ministeriöitä, joita asia koskee. Valtioneuvoston asettaman ministerityöryhmän yhteyteen perustettiin myös digitalisaation ja datatalouden vastuualuetta koskeva yhteistyöryhmä eli Digitoimisto. Digitoimisto on pysyvä yhteistyöryhmä ja sen 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 myös julkisen hallinnon digitaalisen turvallisuuden kehittäminen liittyy digitoimiston tehtäviin. 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.

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

	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	Julkisen hallinnon digitaalisen turvallisuuden kehittämistä koordinoidaan valtiovarainministeriön kaudelle 2020-2024 asettamassa digitaalisen turvallisuuden strategisessa johtoryhmässä sekä Digi- ja väestötietoviraston kaudelle 2020-2024 asettamassa Vahti-johtoryhmässä. Digitaalisen turvallisuuden strategisen johtoryhmän puheenjohtajana on valtiovarainministeriön alivaltiosihteeri ja jäseninä on ministeriöiden ylintä- ja keskijohtoa, Digi- ja väestötietoviraston pääjohtaja, 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 ja keskeisistä sidosryhmistä. Vahti-asiantuntijaverkostoihin osallistuu lisäksi satoja henkilöitä julkisesta hallinnosta 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. Tiedonhallintalautakun-

	nan 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. 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, yhteisillä koulutuksilla, tietoturvatyöpajoilla ja auditoinneilla sekä yhteiseen käyttöön sovitetuilla työkaluilla. Sosiaali- ja terveysministeriön tehtäviin kuuluu hallinnonalan virastojen ja laitosten ohjauksen lisäksi myös 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 sekä kuntien ja kuntayhtymien omistamat yhtiöt ja Huoltovarmuuskeskus tekivät yhteistyötä Kyberterveys-hankkeessa, jossa käsiteltiin erityisesti huolto- ja toimintavarmuutta erilaisissa häiriötilanteissa, sekä tehtiin yhteisiä uhka-arvioita ja turvallisuushankintoja sekä järjestettiin koulutusta. Julkisen hallinnon digitaalisen turvallisuuden kehittämisen yhteistoimintaa toteutuu myös kyberturvallisuuden kehittämisohjelman (KEHO), Titukrin, Digitaalinen turvallisuus 2030 (DT2030) ja Haukan toimeenpanon työryhmissä. Työryhmien haasteena on jäsenten sitoutuminen poikkihallinnolliseen työhön sekä jatkuva uudelleenorganisoituminen ryhmiä perustettaessa.
Suositukset, ohjeet, vaatimukset ja työkalut	Digitaaliseen turvallisuuteen liittyvät suositukset, ohjeet ja vaatimukset muodostavat laajan kokonaisuuden. Tiedonhallintalautakunnan jaostot laativat ja ylläpitävät tiedonhallintalaissa säädettyjen vaatimusten toteuttamista koskevia suosituksia, jotka on julkaistu valtiovarainministeriön julkaisusarjassa. Ministeriöt ja virastot antavat toimialakohtaisia digitaalisen turvallisuuden määräyksiä ja ohjeita. Vahti-asiantuntijaverkostossa tuotetaan digitaalisen turvallisuuden hyvät käytänteet -tukimateriaaleja. Aikaisemmin Vahti tuotti Vahti-ohjeita, joita voi edelleen hyödyntää soveltaen ottaen huomioon muuttunut lainsäädäntö.

	Osa suosituksista, ohjeista ja vaatimuksista 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. Digitaaliseen turvallisuuteen liittyvissä suosituksissa, ohjeissa ja vaatimuksissa on myös tunnistettu ristiriitaisuuksia ja päällekkäisyyksiä. Esimerkiksi hyvinvointialueet ja kunnat vastaanottavat usealta ministeriöltä ja virastolta ohjeistusta, joissa sivutaan digitaalisen turvallisuuden osa-alueita. 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. Kyberturvallisuuskeskuksen tarjoama ja kaikkien hyödynnettävissä oleva kyberturvallisuuden arviointi- ja kehittämistyökalu, Kybermittari, on yksi tällainen työkalu. 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	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 turvallisuuden osaamista tai hankinta-osaamista. Suuret ostovolyymit mahdollistavat lähtökohtaisesti myös hyvät hinta- ja sopimusehdot. Hansel toimii yhteishankintayksikkönä ja sen 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. Ratkaisujen toimittajien näkökulmasta pistemäinen ja ennakoimaton vaatimusmäärittely luo sekä kannattavuushaasteita että kasvavia kustannuksia hankintayksikölle. Yhteishankintoja on mahdollista tehdä myös yhteistyössä eri viranomaisten kesken. Hansel on hiljattain julkaissut tiedonhallinnan ja digitaalisen turvallisuuden asiantuntijapalveluiden sekä tietoturvallisuuden arviointilaitosten arviointipalvelujen dynaamiset hankintajärjestelyt. Hanselin dynaamiset hankintajärjestelyt kattavat laaja-alaisesti digitaalisen turvallisuuden näkökulmasta 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. 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. Kyberturvallisuuskeskuksessa 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. Kyberturvallisuuskeskuksessa on käynnissä kyberturvallisuusuhkien kartoituspalvelun ympäristön kehittäminen ja tuotantokäyttöönotto. Kartoituspalvelun kehittämisessä tavoitteena on kehittää tuotantojärjestelmä ja palvelu, joka mahdollistaa automatisoidun ja jatkuvan tilannekuvan tuottamisen Kyberturvallisuuskeskukselle kuntien sekä kuntayhtymien julkiseen internetiin näkyvistä haavoittuvuuksista ja mahdollisista konfiguraatiovirheistä. Hankkeen pääkokonaisuuksina ovat uhkatiedon keräämisen automatisointi, uhkatiedon sisällyttä-

	minen Kyberturvallisuuskeskuksen muuhun tilannetietoon, tilannekuvan muodostaminen, asiakkuudenhallinta ja kokonaisuuteen liittyvät toimintaprosessit. Palvelun hyödyntäminen kunnissa vaatii kuntaa ylläpitämään ja päivittämään omiin tietojärjestelmäympäristöihin liittyviä tietoja niin, että ne ovat helposti saatavilla esimerkiksi kartoitusten tekemiseksi. Kartoituksesta saatavien tuloksien 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 virastoihin sekä henkilöstön ja johdon osaaminen vaihtelevat. Digitaaliseen turvallisuuteen liittyvää koulutusta on rakennettu eri kohderyhmille: kansalaiset, julkisen hallinnon henkilöstö, digitaalisen turvallisuuden asiantuntijat ja johto. Koulutusta ja koulutukseen sopivaa materiaalia tuotetaan eri virastoissa, joskin osittain hajanaisesti, kenties osittain epätarkoituksenmukaisesti olemassa olevien resurssien tehokkuuden näkökulmasta. Digi- ja väestötietoviraston 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 koulutusmateriaalien toteutuksessa esimerkiksi eOppivassa julkaistujen materiaalien osalta. Toisaalta virastojen järjestämät asiantuntijatilaisuudet ja seminaarit ovat luonnollinen tapa kasvattaa osaamista ja luoda yhteistoimintaan tarvittavia verkostoja. Yhteistyö ja tiedonvaihto erilaisissa verkostoissa on keskeisessä roolissa osaamisen kehittämisessä ja tietoisuuden lisäämisessä. Lisäksi kyberturvallisuusstrategian kehittämisohjelman toimeenpanossa on menossa kyberturvallisuuden koulutus- ja opetustarjonnan nykytilan ja tarpeiden

[7] Digiturvabarometri 10/2021
[8] Organisaation digiturvakysely (8/2021)
[9] https://digiturvallinenelama.fi

	selvitys. Kehittämisohjelmaan liittyen EU:n elpymisvälineen rahoituksella kehitetään kansalaisille kyberturvallisuuden koulutuspakettia, joka tulee saataville kaikilla EU:n virallisilla kielillä. Korkeakoulujen aloituspaikkoja on vuodelle 2022 päätetty luoda 2300, 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. Suomen saama hankeraha EU:n elpymisvälineestä on kolmivuotinen ja arvoltaan viisi miljoonaa euroa.
Digitaalisen turvallisuuden harjoitustoiminta	Julkisen hallinnon harjoitustoiminnassa tunnistettiin eri yhteistoiminnan tasoja. Kansallisen tason harjoitustoimintaa koordinoi Traficomin Kyberturvallisuuskeskus yhdessä DVV:n sekä Huoltovarmuuskeskuksen, 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 EUn elvytyspakettia. Lisäksi alueellista harjoitustoimintaa koordinoi ja suunnittelee aluehallintoviranomainen yhdessä alueen kuntien kanssa. Näissä harjoituksissa painopiste on digitaalisen turvallisuuden edistämiseen sijaan lähinnä huoltovarmuuskysymyksissä. Kyberturvallisuuskeskus tukee huoltovarmuuskriittisten organisaatioiden kyberharjoittelua viranomaispalveluna. Huoltovarmuuskriittisille organisaatiolle tarjottu harjoitusmateriaali on kaikkien organisaatioiden saatavilla ja hyödynnettävissä niiden omien harjoitusten järjestämiseksi. Se sisältää harjoitusohjeen harjoitusten järjestäjille 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. Tähän liittyen laajamittaisten kyberhäiriötilanteiden ohjaus- ja johtamismallin määrittelyä ja toteuttamista on edistetty muun muassa valtiotoimijoiden KYHA- kyberturvallisuusharjoitusten suunnittelun ja toteuttamisen avulla.
Tilannekuva	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 Kyberturvallisuuskeskuksen erilaisista kansallisista ja kansainvälisistä julkisista ja ei-julkisista lähteistä sekä yhteisöjen ja muiden viranomaisten eri lähteistä keräämästä ja tuottamasta tiedosta ja materiaalista. Kyberturvallisuuskeskuksen digitaalisen turvallisuuden tilannekuvan lisäksi DVV julkaisee säännöllisesti kyselyihin perustuvaa digitaalisen turvallisuuden hallinnollista tilannekuvaa. Se sisältää tietoja digitaalisen turvallisuuden tason kehityksestä, henkilö- ja taloudellisista resursseista, koulutuksesta, osaamisesta sekä kehittämiskohteista. Vastaavasti huoltovarmuusorganisaation poolit keräävät ja tuottavat huoltovarmuuden tilannekuvaa, joka sisältää myös digitaalisen turvallisuuden ulottuvuuksia. Huoltovarmuuskeskus ja huoltovarmuusorganisaatio tuottavat lisäksi tilannekuvaa kyberturvallisuuden nykytilasta huoltovarmuuskriittisiltä sektoreilta. Määritetyille osa-alueille kohdentuvaa tilannekuvatietoa jaetaan myös Kyberturvallisuuskeskuksen ylläpitämissä tiedonvaihto- ja yhteistyöryhmissä (ISAC, Information Sharing and Analysis Centre), joita on perustettu eri toimialoilla toimivien toimijoiden välisen ennen kaikkea luottamuksellisen tiedonvaihdon lisäämiseksi. Julkisen hallinnon kannalta keskeisiä ISAC-tiedonvaihtoryhmiä ovat muun muassa Valtiohallinnon ISAC, SOTE-ISAC ja Vesihuollon ISAC.

[10] https://dvv.fi/documents/16079645/17634906/6-2020+TAISTO19+raportti.pdf
[11] https://www.tutkihallintoa.fi/valtionhallinnon-abc/

	Kunta-alan toimijoille ollaan myös perustamassa omaa tiedonvaihto ja -yhteistyöryhmää vuosille 2022-2025. Tilannekuvatietoa on myös saatavilla Kyberturvallisuuskeskuksen tilannekuvatuotteiden kautta. Suurelta osin tilannekuvatuotteet ovat 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. Tilannekuvan kokoamiseen liittyvä 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. Myös kehitysohjelmien tilannetietojen ajantasaisuudessa on puutteita. Tilannekuvan hyödyntämisessä on suuria eroja organisaatioittain. Osassa organisaatioita on selkeät toimintamallit eri lähteistä kerätyn digitaalisen turvallisuuden tilannekuvan jalostamiseksi osaksi ylimmän johdon kokonaistilannekuvaa organisaation toiminnasta ja hyödyntämiseksi organisaation päätöksenteossa. Toisissa organisaatioissa digitaalisen turvallisuuden tilannekuva jää sen sijaan vain asiantuntijatason henkilöstön hyödynnettäväksi. Suomessa varautuminen ja yhteiskunnan kriittisten toimintojen varmistaminen on laajasti yksityisten toimijoiden varassa myös digitaalisten palvelujen osalta. Euroopan unionin tasolla on meneillään sääntelyhankkeita, joilla on suoraa vaikutusta sekä tilannekuvan muodostamiseen että toiminnan jatkuvuuden hallintaan mm. varautumisen ja häiriöilmoitusvelvoitteiden osalta. Toiminnan jatkokehittämisen osalta nämä seikat tulee huomioida aiempaa selkeämmin.
Digitaalisen turvallisuuteen	Jokainen viranomainen vastaa omiin lakisääteisiin tehtäviin ja toimialavastuisiin kuuluvien yhteiskunnan elintärkeiden toimintojen kannalta tärkeiden tietojen, tietojärjestelmien, ICT-infrastruktuurin ja palveluntoimittamisen ketjujen

liittyvä toiminnan jatkuvuudenhallinta ja varautuminen	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. Tiedonhallintalakiin on valmisteilla päivitys, jonka luonnos on seuraava: ”Tiedonhallintayksikön on selvitettävä sen tietoaineistojen käsittelyn, tietojärjestelmien hyödyntämisen sekä 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 toiminta jatkuvat mahdollisimman häiriöttömästi normaaliolojen häiriötilanteissa sekä valmiuslaissa (1552/2011) tarkoitetuissa poikkeusoloissa. Viranomaisen on suunniteltava, miten se tiedottaa muille viranomaisille tietojärjestelmänsä häiriöstä, jos häiriö vaikuttaa muiden viranomaisten toimintaan. Viranomaisen digitaalisten palvelujen ja muiden sähköisten tiedonsiirtomenetelmien käyttökatkoista tiedottamisesta yleisölle säädetään digitaalisten palvelujen tarjoamisesta annetun lain (306/2019) 4 §:n 2 momentissa. Viranomaisten yleisestä varautumisvelvollisuudesta poikkeusoloihin sekä valtion tietohallinnon, tiedonkäsittelyn, sähköisten palveluiden, tietoliikenteen ja tietoturvallisuuden järjestämisestä poikkeusoloissa säädetään valmiuslaissa.” Suomessa varautuminen ja yhteiskunnan kriittisten toimintojen varmistaminen on laajasti yksityisten toimijoiden varassa myös digitaalisten palvelujen osalta. Euroopan unionin tasolla on meneillään sääntelyhankkeita, joilla on suora vaikutus sekä tilannekuvan muodostamiseen että toiminnan jatkuvuuden hallintaan mm. varautumisen ja häiriöilmoitusvelvoitteiden osalta. Toiminnan jatkokehittämisen osalta nämä seikat tulee huomioida aiempaa selkeämmin. Häiriötilanteisiin on varauduttu ennakolta. Esimerkiksi vaalien järjestämiseen on liittynyt korotettu valmius informaatiovaikuttamisen sekä digitaalisen turvallisuuden häiriöiden torjumiseksi. Vaalien aikana seurataan mahdollista informaatiovaikuttamista, sekä digitaalisen turvallisuuden mahdollisia häiriöitä tehostetusti.
Häiriötilanteiden hallinta	Häiriötilanteiden hallintaan liittyvät ennalta ehkäisevät ja korjaavat toimenpiteet ovat toimijoiden vastuulla. Kyberturvallisuuskeskus tukee organisaatioita ohjeistuksen ja neuvonnan avulla. Yhteistyö Kyberturvallisuuskeskuksen

	kanssa koetaan hyödylliseksi ja tarpeelliseksi. Vakavan kyberloukkauksen kohteeksi joutuneella organisaatiolla pitää kuitenkin olla riittävä osaaminen, jotta se voi hyödyntää Kyberturvallisuuskeskuksen tarjoamia palveluja. Useissa tapauksissa vakavan kyberloukkauksen selvittämiseen otetaan mukaan tieturvallisuuden konsultointipalveluja tarjoava yritys ja myös näiden palvelujen hankkiminen ja hyödyntäminen vaatii organisaatiolta riittävää osaamista ja tarpeen mukaan riittäviä ennakollisia palvelusopimusjärjestelyitä. Lisäksi häiriötilanteessa toimijan tulee pystyä itse tekemään korjaavia toimenpiteitä, mikä edellyttää riittävää digitaalisen turvallisuuden osaamista ja resursseja. Operatiivista ”kyberpalokuntaa” ei ole, eikä yleisesti valmiiksi kilpailutettuja häiriönhallinnan palveluja ole saatavilla. Valtioneuvoston kanslian johtama ministeriöiden valmiuspäälliköiden verkosto sekä 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 jatkossakaan ottaa vastuuta yhteiskunnan kriittisten tietojärjestelmien ja infrastruktuurin toimivuudesta, vaan niiden tulee olla viranomaisten vastuulla. KyberVPK:n roolin tulisi pysyä kaikissa tilanteissa viranomaistoimintaa täydentävänä.

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. 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	Valtioneuvosto 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 ovat olleet toiminnassa vasta noin puoli vuotta, joten toiminnan tuloksia ei ole ollut mahdollisuutta arvioida haastatteluissa, joita tämän raportin valmistelua varten on tehty, tai koordinaatioryhmässä. 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 johdosta tehtäviä koskevat säädökset ovat jatkuvasti osin vanhentuneita tai epätarkkoja. Tämä tulisi ottaa huomioon säädösvalmistelussa ja pyrkiä joustavuuteen sekä tilanteen mukaisen toiminnan mahdollistamiseen. Vastuiden tulee kuitenkin olla aina selkeitä. Toimijat ovat keskenään sopineet digitaalisen turvallisuuden tarkemmasta tehtäväjaosta myös muistioin ja sopimuksin. Esimerkiksi yhteistyöstä ja työnjaosta Digi- ja väestötietoviraston ja Kyberturvallisuuskeskuksen sekä Kyberturvallisuuskeskuksen ja Huoltovarmuuskeskuksen välillä on sovittu sopimuksin. Ministeriöiden ja virastojen tietoturvapäälliköiden välinen verkosto toimii puutteellisesti. Toiminnan parantamiseksi Vahti on pystyttämässä uutta verkostoa. Digitaalisen turvallisuuden osa-alueilla yhteinen ohjaus toteutuu seuraavasti:

	Tietosuoja: Tietosuojavaltuutetun toimisto antaa tietosuojan toteuttamista koskevia ohjeita. Riskienhallinta: Valtiovarainministeriön controller-toiminto antaa yleisiä ohjeita riskienhallinnan toteuttamisesta valtionhallinnossa. Digitaalisen turvallisuuden strategisessa johtoryhmässä on edustus keskeisistä ministeriöistä. Digi- ja väestötietovirasto tuottaa strategisten digiturvariskien analyysejä, joita on käytetty digiturvan kehittämisen ohjauksessa. Tieto- ja kyberturvallisuus: Tiedonhallintalaki asettaa vaatimukset tiedonhallintayksiköiden tietoturvallisuudelle. Muualla lainsäädännössä on sektorikohtaisia vaatimuksia (esimerkiksi asiakastietolaki). 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.
Suositukset, ohjeet ja vaatimukset	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 yleisellä tasolla poikkeusoloja koskevia 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 tuotetaan keskitetysti Valtorista. 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 osalta ei ole toimivaa digitaalisen turvallisuuden kehittämiseen soveltuvaa toimintamallia. 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. Valtorin tuottamien keskitettyjen palvelujen tietoturvallisuuden arviointi on yksi näkökulma valtiohallinnon digitaalisen turvallisuuden yhteistoimintaan. 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 palvelujen käyttäjät.

	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 toteutumisen arviointikriteeristönä. Palveluiden vaatimusten tulisi rakentua riskiperustaisesti. Jatkuvuudenhallinta: Yhteisten digitaalisen turvallisuuden palvelujen jatkuvuudenhallinta on palveluntuottajan 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 kyberturvallisuuskeskus jakaa tilannetietoa valtionhallinnon tiedonvaihto- ja yhteistyöryhmässä ISAC (Information Sharing and Analysis Centre). 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: Traficom tuottaa kyberturvallisuuden tilannekuvatuotteita erilaisista lähteistä ja jakaa niitä. Traficom neuvoo toimijoita häiriötilanteiden hallinnassa. Jatkuvuudenhallinta: Valtionhallinnon toimijoilla on vastuu oman toiminnan jatkuvuutensa toteuttamisesta ja häiriötilanteiden hallinnasta. Laajavaikutteisten kyberhäiriöiden hallintaryhmässä (VIRT) voidaan sopia tehtävistä ja käytännön toimenpiteistä häiriön hallitsemiseksi.

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.

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 julkiselle hallinnolle vastaamaan tarpeeseen julkisen hallinnon yhteisistä periaatteista ja suosituksista ohjelmointirajapintakehitykselle ja digitalisaation edistämiselle.

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 tietoa esimerkiksi tilannekuvasta. Kyberturvallisuuskeskus onkin tunnistettu hyvinvointialueilla keskeiseksi tahoksi tietoturvallisuuden kehittämisessä. Lisäksi Huoltovarmuuskeskus koordinoi Alue 2030 -ohjelmaa, jossa aluehallintovirastot ja ELY-keskukset ovat mukana suunnittelemassa ja toteuttamassa kehittämistoimenpiteitä toimintaa uhkaavien riskien pienentämiseksi.
Suositukset, ohjeet ja vaatimukset	Hyvinvointialueiden vastuulle siirtyvien erilaisten potilastietojärjestelmien tietoturvavaatimusten selvittäminen on haastavaa, vaikka kriteeristöjä on olemassa. Yhtenäisen digitaalisen turvallisuuden tason saavuttaminen edellyttää sekä hyvinvointialueiden välistä yhteistyötä että kuntien huomiointia digitaalisen turvallisuuden kaikkien osa-alueitten osalta. Huomiota on kiinnitettävä tiedonantovel-

	voitteisiin sekä tiedonsaantioikeuksiin. Kunnille kuuluvat jatkossakin ennalta ehkäisevä hyvinvointi ja tämän edellyttämät riippuvuudet hyvinvointialueen tehtävistä ja palveluista.
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.

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 yhteistoimintaa 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 kaikkien panosta, 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 ohjaaminen kunnissa ei ole toiminnan kehittämisen tasolla suunnitelmallista eikä systemaattista. Usein digitaaliseen turvallisuuteen liittyvät linjaukset ja tekniset toiminnallisuudet tehdään irrallaan laajemmasta kokonaisuudesta. Digitaalisen turvallisuuden kokonaisuus ei ole osa organisaation toiminnan ja toimintaympäristön systemaattista kehittämistä.

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 lisää yhteistoimintaan liittyvää tehottomuutta. Taulukkoon 4 on koottu yhteistoimintaan liittyviä havaintoja digitaalisen turvallisuuden yhteistoiminta-alueittain.

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 (KunTVV) sekä Turvallinen ja kriisinkestävä kunta -verkosto. Kuntaliiton tavoitteena on huolehtia kuntien toimintaedellytyksistä tarjoamalla ja järjestämällä kunnille asiaan liittyviä tilaisuuksia ja näkyvyyden julkisen hallinnon digitaalisen turvallisuuden kehittämiseen kuntakentän osalta. Tähän sisältyvät Kuntaliiton eri yksiköitten asiantuntija- ja tietopalveluitten käytettävyys ja kannanotot. Kuntaliitto toimii yhteistyössä Kyberturvallisuuskeskuksen kanssa väylänä, joka tarjoaa yhteys- ja tiedottamiskanavan Kyberturvallisuuskeskuksen ja kuntakentän tietoturvavastaavien välille. Kaupunkien välinen yhteistyö tiedonhallinnan kehittämisessä on säännöllistä. Vaihtelevaa yhteistyötä tehdään yliopistojen ja sairaanhoitopiirien kanssa. Kuntien ja yksityisen sektorin välinen yhteistoiminta on vähäistä. Yhteistoiminta rajoittuu pitkälti yhteisiin projekteihin, joissa keskitytään yksittäisen järjestelmä-/palvelukokonaisuuden kehittämiseen. Tampereen kaupunki koordinoi yhteistyötä alueen kuntien kesken. Yhteisillä palvelukokonaisuuksilla on omat hallintamallinsa sekä koordinaatioryhmät 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 käytännön tasolla 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 sekä vastaanottaa, käsitellä ja hyödyntää tilannekuvatietoa, tarjolla olevia palveluja ja työkaluja turvallisuusuhkilta suojautuakseen ja turvallisuuta kehittääkseen. Vastavuoroisesti ulkoistamisella voidaan tuottaa kustannushyötyjä ja eritysosaamista, esimerkiksi tietojärjestelmien tietoturva-arviointia, jota varten kuntaan ei välttämättä ole kannattavaa hankkia omaa osaamista. Tärkeintä olisi varmistaa riittävä oma osaaminen.

	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 myös kustannustehokkaampaa ylläpitää esimerkiksi yksittäisten tietojärjestelmien kuin lukuisten tietojärjestelmien turvallisuutta. Mitä enemmän kunnissa käytetään yhteisiä tai samoja tietojärjestelmiä sitä enemmän on mahdollisuus hyödyntää yhteisiä resursseja ja osaamista tietojärjestelmien turvallisuuden ylläpitämiseksi ja kehittämiseksi.

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.[12] 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 esimerkiksi kunnissa voidaan hyödyntää. Myös yksityisen sektorin tekemät selvitykset ja nykytila-analyysit nähdään kuntia hyödyttävinä tuotoksina, joiden pohjalta voidaan määrittää kuntien toimintaan sopivia kehitystoimenpiteitä.

Digitaalisen turvallisuuden yhteistyöryhmissä tutkimuksen rooli on vähäinen. Tutkimusta ja sen tavoitteita ja tutkimustulosten ei nykyisin hyödynnetä riittävästi digitaalisen turvallisuuden kehittämiseksi. Digi- ja väestötietovirasto kerää tietoa digitaalisen turvallisuuden tilasta. Aineiston hyödyntämistä tutkimustyössä arvioidaan parhaillaan.

Taulukko 5: Julkisen hallinnon ja tutkimustoiminnan yhteistoimintaan nykytilassa liittyviä havaintoja.

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

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 viestintävirastoon (Kyberturvallisuuskeskus) 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 heille tarjota tutkimuskohteita tai tutkimukseen tarvittavaa tietoa. Toisaalta kunnat ja kaupungit kokevat, että heille 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	Ulkopuolinen, kilpailutettu rahoitus on merkittävin tutkimusrahoituksen lähde yliopistoissa ja valtion tutkimuslaitoksissa. Yli puolet tutkimuksesta perustuu ulkopuoliseen kilpailutettuun 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. 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

Koordinaatioryhmän jäsenet ovat kuvanneet vapaamuotoisesti taulukkoon 6 on kunkin toimijan tehtävät digitaalisen turvallisuuden yhteistoiminnassa 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 myös yhden luukun yhteyspiste yhteydenotoille, jotka liittyvät data-, digi- ja tietopolitiikan toimialaan
Sisäministeriö	• kyberrikostorjunnan ministeriöohjausvastuu • kansallisen turvallisuuden kyberuhkien torjunnan ja kybertiedustelun ministeriöohjausvastuu

	• valtionhallinnon hybridiuhkaverkoston koordinaatio
Ulkoministeriö	• kansallinen turvallisuusviranomainen (NSA) • kyber- ja hybridilähettilästoiminta kv-verkostoissa
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
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
Sosiaali- ja terveysministeriö	• sektorilainsäädännön mukaiset vastuut • ei erityisiä digitaalisen turvallisuuden poikkihallinnolliseen yhteistoimintaan liittyviä vastuita
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 • yhteistoiminnan järjestäminen hankintoihin liittyen
Kuntayhtymät ja kuntien omistamat yritykset	• osaamisverkoston ylläpito • yhteistoiminta palvelujen kehittämiseksi
Yliopistot	• digitaalisen turvallisuuden opetus- ja tutkimustoiminnan yhteistoiminta julkisen hallinnon toimijoiden kanssa
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[13], 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[14]. 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[15]),
- verkko- ja tietoturvadirektiivi (Directive on Security of Network and Information Systems, NIS (EU) 2016/1148[16],
- NIS-direktiivin uudistettu ehdotus (COM(2020) 823 final) kyberturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella ja verkko- ja tietoturvadirektiivin (EU) 2016/1148 kumoamisesta, eli niin sanottu NIS 2[17],
- akkreditointi- ja markkina-valvonta-asetus (New Legislative Framework, NLF) [18],
- kyberturvallisuusasetus[19],
- Euroopan kyberturvallisuuden kompetenssikeskusta ja kyberturvallisuusverkostoa koskeva asetus (Regulation of European Cybersecurity Competence Centre and the Network of National Coordination Centres)[20], sekä
- 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 tietoturvalouk-kauksista. NIS2-direktiiviehdiotus on parhaillaan trilogineuvotteluissa. NIS 2 -direktiiviehdotuksella säädettäisiin tiukempia tietoturvavaatimuksia, laajennettaisiin lainsäädännön soveltamisalaa uusille toimialoille ja toimintoihin, mukaan lukien julkinen sektori ja annettaisiin uusia valvontamenetelmiä

[13] 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
[14] Digitaalisen turvallisuuden yhteistoiminta- ja hallintamallien kansainvälinen vertailu, valtiovarainministeriö 25.4.2022
[15] (EU) 2016/679 GDPR https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
[16] (EU) 2016/1148 NIS https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG
[17] COM(2020) 823 final NIS2 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0823
[18] (EC) No 765/2008 NLF https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008R0765
[19] (EU) 2019/881 https://eur-lex.europa.eu/eli/reg/2019/881/oj
[20] (EU) 2021/887 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R0887

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 kyberresilienssiasetus (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 kyberturvallisuusertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 (kyberturvallisuusasetus), (jatkossa 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 vaatimuksia, standardeja ja menettelyjä, joiden avulla pyritään rakentamaan luottamusta, lisäämään kyberturvallisuusmarkkinoiden kasvua sekä helpottamaan EU:n laajuista kauppaa. Parhaillaan ollaan esimerkiksi valmistelemassa 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 annettiin lisäksi ENISAlle entistä vahvemman mandaatin tukea jäsenmaita, EU:n toimielimiä ja muita sidosryhmiä kyberhyökkäysten torjumisessa ja sen määräaikainen rooli muutettiin pysyväksi samalla, kun sen tehtäväkenttää laajennettiin EU:n verkko- ja tietoturvavirastosta (European Network and Information Security Agency) EU:n kyberturvallisuusvirastoksi.[21, 22]

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 kyberturvallisuustutkimuksen, -tuotekehityksen ja -innovoinnin alueilla. Kyberturvallisuuskeskus 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.[23]

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:[24]

[21] https://www.consilium.europa.eu/fi/policies/cybersecurity/
[22] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
[23] Laki sähköisen viestinnän palveluista (2014/917) §304
[24] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

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

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 digitaalisen turvallisuuteen liittyviä tehtäviä ja ohjausta ei ole erotettu muista kyberturvallisuuteen liittyvistä tehtävistä ja ohjauksesta samalla tavoin kuin Suomessa. Toisaalta Suomessa Liikenne- ja viestintäviraston Kyberturvallisuuskeskus vastaa monista sellaisista kyberturvallisuuden tehtävistä, jotka eivät kuulu esimerkiksi Ruotsin tai Iso-Britannian Kyberturvallisuuskeskuksen 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 myös 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[25]) 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.

[25] 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 tutkimus-yhteisöä 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[26]. 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.[27] 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 Россиим, ”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, NATO:ssa, ETYJ:ssä, Euroopan neuvostossa, ja Pohjoismaiden neuvostossa. Myös useat alueelliset järjestöt käsittelevät kyberturvallisuuskysymyksiä. Suomessa ulkoministeriö, liikenne- ja viestintäministeriö, sisäministeriö ja puolustusministeriö osallistuvat aktiivisesti kybertoimintaympäristöä koskevaan globaaliin, alueelliseen ja kahdenväliseen keskusteluun ja vaikuttavat kansainvälisellä kyberagendalla olevien kysymysten edistämiseen Suomen etujen mukaisesti.

Suomen kansainvälistä asemaa digitaalisen turvallisuuden alueella seurataan useiden kansainvälisten indeksien perusteella. Niitä ovat 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

[26] https://www.regeringen.se/4af5d9/globalassets/regeringen/dokument/forsvarsdepartementet/regeringsbeslut/uppdrag-om-fordjupad-samverkan-inom-cybersakerhetsomradet-genom-ett-nationellt-cybersakerhetscenter.pdf
[27] https://www.cfcs.se/om-centret/

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[28].

[28] 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 sektorin toimintaa. Digitaaliset ratkaisut ja niissä kerättävä tieto muodostavat perusteen myös digitaalisen turvallisuuden yhteistoiminnalle. Yhteistoiminnan avulla voidaan siirtyä rakentamaan yhteisiä digitaalisen turvallisuuden palvelukokonaisuuksia sekä rajapintoja tiedon jakamiseen ja jalostamiseen. Yhteisten palvelujen keskeisiä etuja ovatkin osaamisen keskittäminen, yhtenäiset prosessit, järjestelmien yhteensopivuus ja päällekkäisen työn vähentäminen esimerkiksi kilpailutuksissa.[29]

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 ovat toimivia ympäristön jatkuvassa muutostilassa. Valtionhallinnon, hyvinvointialueiden ja kuntien digitaalisen turvallisuuden yhteistoiminta edellyttää sekä säänneltyjä että epämuodollisia rakenteita ja entistä tiiviimpää yhteistyötä, sekä yhteistyön koordinointia rajallisten resurssien tehokkaaksi hyödyntämiseksi.

Ministeriöiden tulee määrittää julkisen hallinnon digitaalisen turvallisuuden ohjaukseen tarvittavat säädökset ja panna ne toimeen. Tulee keskittyä toiminnallisten rakenteiden uudistamiseen siten, että yhteistoimintaa organisoidaan todellisten tarpeiden ja osaamisen mukaisesti. Keskitettyjä poikkihallinnollisia julkisen hallinnon digitaalisen turvallisuuden tehtäviä hoitavia keskeisiä virastoja 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 tulee tarkastella hallinnollisten digitaalisen turvallisuuden tehtävien näkökulmasta. Nykyisiä rakenteita tulisi vahvistaa keskittämällä keskeisten toimijoiden toimintaa nykyistä enemmän digitaaliseen turvallisuuteen ja huomioimalla aikaisempaa paremmin myös kansainvälinen toiminta ja tietojenvaihto. Tarvitaan myös tietoturvavastaavan tai digitaalisen turvallisuuden

[29] 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

vastaavan virka jokaiseen organisaatioon. Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminnan tavoitetilaan liittyviä odotuksia on kuvattu tarkemmin taulukossa 7.

EU:n verkko- ja tietoturvadirektiivi eli NIS-direktiivi tulee huomioida julkisen hallinnon digitaalisen turvallisuuden ohjaukseen tarvittavien säädösten määrittämisessä ja toimeenpanossa. Siinä säädetään yhteiskunnan kriittisen infrastruktuurin tarjoajien ja toimijoiden tietoturvavelvollisuuksista sekä havaitsemistaan tietoturvauhkista ja -loukkauksista ilmoittamisesta eli häiriöistä ilmoittamisesta. NIS-direktiiviä ja direktiivin mukaisesti toteutettua kansallista lainsäädäntöä sekä niissä asetettuja velvoitteita sovelletaan erikseen direktiivissä määritellyillä toimialoilla[30]. 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-direktiivin ja siten pääasiassa myös kansallisen lainsäädännössä asetetut tietoturvavelvoitteet ovat hyvin ylätasoisia ilman konkreettisia (minimitason) vaatimuksia tietoturvan toteuttamiselle tai häiriöistä ilmoittamiselle, mikä jättää kansalliselle lainsäätäjälle, valvovalle viranomaiselle ja velvoitteiden kohteena olevalle paljon tulkinnan varaa velvoitteista[31]. Tämä on huomioitu komission NIS2-direktiiviehdotuksessa. Ehdotuksessa ehdotetaan lisäksi 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. Uusina lainsäädännön soveltamisaloina olisivat muun muassa julkishallinnon sektori, sekä jätevesi- ja jätehuolto.

Julkisen hallinnon digitaalisen turvallisuuden säädösten tulee olla lähtökohtaisesti yhteneviä muille kriittisille toimialoille säädettyjen säädösten kanssa. Siten niiden kohteena oleva julkisen hallinnon toimija ei joudu tarpeettomasti soveltamaan erilaisia ja ristiriitaisia vaatimuksia toiminnassaan. Esimerkiksi kunta tai jatkossa hyvinvointialue toimii sekä yleisenä julkisen hallinnon toimijana että NIS-direktiivin alaisena sosiaali- ja terveyspalvelujen tarjoajana, jolloin sekä julkisen hallinnon toimijoille yleisesti että sosiaali- ja terveyspalelujen tarjoajille erityisesti asetettujen vaatimusten tulisi olla ristiriidattomia.

Myös yleisiä julkisen hallinnon digitaalisen turvallisuuden säädöksiä on tarpeen selkeyttää. Nykytilan kuvauksen perusteella julkisen hallinnon digitaalista turvallisuutta koskevia säädöksiä, määräyksiä,

[30] 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.

[31] 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".

ohjeita ja suosituksia annetaan eri tahoilta ja näitä pidetään osittain jopa keskenään ristiriitaisina. Julkisen hallinnon digitaalisen turvallisuuden kokonaisvaltainen kehittyminen edellyttää yhtenäistä ohjeistusta, joka olisi saatavissa yhdestä paikasta. Vaikka erilaista ohjeistusta tuotettaisiin jatkossakin eri lähteistä, tulisi näiden sisältämien vaatimusten, määräysten, ohjeiden ja suositusten olla keskenään ristiriidattomia. Määräysten, ohjeiden tai suositusten soveltaminen voi olla vaikeaa toimijalle, jolla ei ole riittävästi osaamista tai resursseja. Siksi näiden lisäksi olisi tuotettava ja ylläpidettävä soveltamisohjeita, jotta käyttöönotto sujuisi mahdollisimman ketterästi. Soveltamisohjeiden pitäisi kuitenkin jättää riittävästi liikkumavaraa erilaisille toteutuksille. Yhteisten määräysten, suositusten ja ohjeiden sekä mahdollisten soveltamisohjeiden keskittämistä riittävän laajapohjaiselle toimijalle tulisi harkita.

Norminomaiseksi tulkittavia suosituksia tai ohjeita tulee välttää ja suositusten ja ohjeiden 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 Kyberturvallisuuskeskuksen kehittämää Kybermittaria.

Hyviä käytäntöjä säännösten vaatimusten toteuttamiseksi sekä toiminnan kehittämiseen liittyviä toimintamalleja tulee jakaa yhteistoiminnan kautta viestinnän ja vuorovaikutuksen eri keinoin. Valtiohallinnon tulee korostaa, että suosituksia ei tule valvonnassa tulkita normatiivisina. Lisäksi valtiohallinnon tulee siirtyä 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 myös tärkeää, että annetut suositukset ja ohjeet sekä yhteiset työkalut pidetään ajan tasalla.

Taulukko 7: Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminnan tavoitetilaan liittyviä odotuksia.

Yhteistoiminta-alue/palvelu	**Kehitysehdotus**
Digitaalisen turvallisuuden ohjaus	Digitaalista turvallisuutta tulee ohjata ja seurata aiempaa vahvemmin sekä koko julkisessa hallinnossa, että sen eri alueilla: ministeriöt, valtionhallinnon toiminnallinen/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 tulee 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 tulee jatkaa (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 tulee selkeyttää ja viestintää niistä lisätä.

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 yhteishankintayksikköä Hanselin avulla on mahdollista toteuttaa enemmän yhteisiä kilpailutuksia, jotka eivät vaadi toimijakohtaisia minikilpailutuksia, sekä huomioida huoltovarmuusvaatimuksia ja niiden toteutumista entistä paremmin.

Esimerkiksi Suomessa hyvinvointialueilla tulisi tulevaisuudessa olla käytössä enintään 2-3 toistensa kanssa yhteentoimivaa asiakas- ja potilastietojärjestelmää, 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, ja järjestelmät voivat olla hyvinvointialueittain toisistaan eriytettyjä, vaikka niissä olisikin samat ja yhdessä kehitetyt ohjelmistot, jotta koko Suomessa ei toimita yhden järjestelmän varassa. Yhtäkin järjestelmää voidaan käyttää, mutta tällöin tulee huolehtia riittävästä palvelinympäristöjen maantieteellisestä eriyttämisestä ja häiriötilanteissa käyttöönotettavista 1-2 varajärjestelmästä, eli kopiosta tuotantojärjestelmästä.

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.

➔ Vuodesta 2023 alkaen tarvitaan Haukka-ohjelmaa seuraava julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma toimeenpanosuunnitelmineen. Sen tulee sisältää tärkeimmät tavoitteet kehitystoimenpiteineen ja aikatauluineen. Toimeenpano-ohjelman tavoitteiden asettaminen ja tavoitteista johdettujen kehitystoimenpiteiden tulee pohjautua mitattuun ja analysoituun tietoon di-

gitaalisen 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 tulee seurata aktiivisesti. Kehitystoimenpiteiden vaikutuksia 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. 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. 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 tulee dokumentoida.

➔ Hyvinvointialueiden digitaalisen turvallisuuden yhteistoimintamalli tulee valmistella ja ottaa käyttöön. Hyvinvointialueille tulee tarjota tukea, johon sisältyy

	mm. suosituksia, ohjeita ja vaatimuslistoja digitaaliseen turvallisuuteen liittyvien vastuiden kuvaamiseen infrastruktuureihin liittyvien digitaalisen turvallisuuden vaatimusten määrittämiseen. Tuen antamiseen tarvitaan vastuutaho, joka ymmärtää operatiivista toimintaa ja kykenee toimimaan strategisen ja operatiivisen toiminnan välimaastossa nämä yhdistävänä tekijänä. Vastuutaho vastaa siitä, että annettava tuki on ajan tasalla. ➔ Vastuutaho vastaisi lisäksi annettavien suositusten, ohjeiden, vaatimuslistojen ja työkalujen ylläpidosta ja päivittämisestä. Vastuutaho voisi myös 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.
Suositukset, ohjeet, vaatimukset ja työkalut	Digitaalisen turvallisuuden riskienhallintamallit, suositukset, ohjeet, vaatimukset ja hyväksyntäkriteerit käytettävien palveluiden turvallisuudesta tulee olla 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 digitaalista turvallisuutta koskeva lainsäädäntö, ohjeet, suositukset, työkalut tulee saattaa saataville yhdestä paikasta ja niistä tulee viestiä yhtenä kokonaisuutena. ➔ Tarvitaan vastuutaho, joka vastaa siitä, että ohjeet, suositukset ja työkalut ovat ajan tasalla. Virastoilla on velvoite arvioida riskejä, mutta riskiarviointia ei toteuteta systemaattisesti, eikä yhteistä mallia riskien arvioimiseksi ja hallinnoimiseksi, yhteistä näkymää arvioituihin riskeihin tai toimintamallia riskitiedon jakamiseksi ja laaja-alaiseksi hyödyntämiseksi ole. Reagoiva toimintatapa tulee muuttaa ennakoivaksi, jossa hyödynnetään tehtyjä riskianalyyseja sekä selvityksiä johtopäätösten tekemiseksi ja suojaustoimenpiteiden toteuttamiseksi yhdessä ja yhtenäisesti. Yhteistyön koordinointia varten tulee nimetä erikseen henkilöt ja varata riittävät resurssit. Tiedonhallintamallin avulla varmistetaan tietojärjestelmien ja tietovarantojen yhteentoimivuus. Digitaalisen turvallisuuden osalta julkisen hallinnon toimijat tarvitsevat vahvaa tiedolla johtamista ja sitä tukevia tietokantoja tai -varantoja. Valtiotoimijoilta odotetaan konkreettisia ohjeita, tarkastuslistoja ja materiaalipankkia, jotka ovat saatavissa yhdestä paikasta tai yhdeltä viranomaiselta.

	Tietopankeista löytyy sopimusmalleja ja valmiita vaatimusluetteloita (esim. listaus järjestelmän ei-toiminnallisista vaatimuksista, valmisohjelman tarkastuslista tai toimenpidelista häiriötilanteissa) 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 digitaaliseen turvallisuuteen liittyvän roolia jokaisessa virastossa. ➔ Tunnistettuja työkalutarpeita ovat: Tiedonluokittelu, siihen liittyvät ohjeet ja mallit ohjeistuksen keskitetyltä sivustolta saatavissa. ➔ Vastuullinen virasto, joka ylläpitää hankintoihin ja sopimuksiin, sekä tietoturvallisuuden arviointiin liittyvää tietopankkia ja jakaa tietoa eri toimijoille.
Digitaalisen turvallisuuden hankinnat ja hankkeet	Digitaalisen turvallisuuden yhteisiä hankintoja ja hankkeita tulee edistää niihin kannustavalla hallinto- ja rahoitusmallilla. Siten ohjataan valtionhallintoa, hyvinvointialueita ja kuntia toimimaan yhdessä digitaalisen turvallisuuden kokonaisvaltaiseksi kehittämiseksi. Keinona voi olla rahasto, josta jaettaan rahoitusta hyvinvointialueiden ja kuntien digitaalisen turvallisuuden kehittämishankkeisiin. Rahoituksen ehtona voi esimerkiksi olla se, että vähintään x kuntaa ja/tai x hyvinvointialuetta osallistuu hankkeeseen ja että 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. Esimerkkinä yhteisesti kehitettävä palvelusta voi olla organisaation digitaalisen turvallisuuden kypsyystason mittari. Sen avulla kypsyystasoja voitaisiin mitata yhtenevästi, ja mittauksen pohjalta voitaisiin määrittää yhteisiä tavoitteita sekä kehityskohteita ja -alueita. Tämä mahdollistaisi ja loisi puitteet muun muassa yhteisen tilannekuvan jakamiselle julkisen hallinnon digitaalisen turvallisuuden tasosta, digitaalisen turvallisuuden osaamisen jakamisen, yhteisten hankintojen ja turvallisuusvaatimusten valmistelun sekä yhteisten, keskeisimpiin kehityskohteisiin ja -alueisiin kohdistuvien harjoitusten valmistelun ja pitämisen. Tämä mahdollistaisi myös uusien kehityshankeaihioiden esille tuomisen ja toteuttamisen osana koko julkisen hallinnon digitaalisen turvallisuuden kehittämistä seuraavan hallituskauden aikana.

	➔ Rahoitusmalli, joka kohdentaa rahoituksen yhteishankkeisiin ja -hankintoihin yksittäisten kehitystoimenpiteiden sijaan ja ohjaa yhteistyöhön.
Digitaalisen turvallisuuden palvelut	Digitaalisen turvallisuuden palvelujen kehittäminen ja ylläpito on samankaltaista eri toimijoiden välillä. Niiden määrittely ja kehittäminen tulisi toteuttaa yhdessä. Tämän mahdollistamiseksi nykytilan jäsennyksessä käytettyä, kuvassa 2 hahmotettua palvelualuekokonaisuutta on tavoitetilakuvauksessa selkiytettävä palveluiden sisällön, vastuuorganisaatioiden sekä palvelukohtaisten yhteistoiminta- ja hallintamallien osalta. ➔ Digitaalisen turvallisuuden palveluiksi tavoitetilassa on tunnistettu suositukset ja ohjeet, vaatimukset ja työkalut; hankinnat; tutkimuksen koordinointi; osaaminen; harjoitustoiminta; tilannekuva; toiminnan jatkuvuuden hallinta ja varautuminen; sekä häiriötilanteiden hallinta. ➔ Tavoitetilassa palveluissa tulee huomioida nykyistä enemmän ennakointi. Kyky tunnistaa digitaalisen turvallisuuden toimintaan vaikuttavia ilmiöitä ja trendejä, sekä lukea signaaleja digitaalisen turvallisuuden uhista. Siten mahdollistetaan muun muassa ennakoivampi koulutus ja oppiminen sekä ennakoivampi häiriöhallinta. Palveluita on kuvattu tarkemmin kappaleessa 4.3.
Digitaalisen turvallisuuden osaaminen	Henkilöstön, digiturva-asiantuntijoiden ja johdon osaamisen kehittämistä tulee jatkaa aktiivisesti tarjoten jokaiselle kohderyhmälle parhaiten heille sopivia menetelmiä. Vuosittaiselle osaamisen kehittämiselle tulee asettaa minimitavoitteet, joita organisaatioiden tulee seurata. Tämän ohella tule panostaa teknisen tason tietoturvallisuuden kehittämiseen, jotta voidaan esimerkiksi paremmin estää henkilöille toimitettavia haittaohjelmia tai muita kalasteluviestejä sisältävät yhteydenotot eri digipalveluissa. Jokainen tällainen estetty viesti pienentää riskiä, että organisaatio joutuisi henkilötietojen tietoturvaloukkauksen tai tietomurron kohteeksi. ➔ Henkilöstön osaamisen kehittämiselle on asetettu seurattavat tavoitteet. ➔ Teknistä tietoturvallisuutta on kehitetty käyttäjien päätelaitteisiin ja palveluihin tulevien vaarallisten yhteydenottojen tehokkaammaksi tunnistamiseksi ja estämiseksi.
Digitaalisen turvallisuuden	Digitaalisen turvallisuuden harjoitustoimintaa tulee kehittää ja koordinoida julkisessa hallinnossa, jotta julkisen hallinnon digitaalisen turvallisuuden strategisia tavoitteita edistetään parhaalla mahdollisella tavalla. Digi- ja väestötietoviraston tekemässä selvi-

harjoittelu	tyksessä Julkishallinnon digitaalisen turvallisuuden kansallisen harjoitustoiminnan tavoitetilakuvauksessa[32] tunnistettiin erilaisia pitkän ja lyhyen aikavälin kehittämistoimenpiteitä. Toimenpiteitä tarvitaan niin lainsäädännön ja rahoituksen kuin ohjauksenkin osa-alueilla. Harjoitustoiminnan koordinaatio edesauttaa yhteisteisten tavoitteiden tukemista ja organisaatioiden palautumista häiriötilanteesta.
Tilannekuva	Tavoitteena on laajaan dataan, monipuolisiin mittareihin valtionhallinnosta, hyvinvointialueilta ja kunnista sekä modulaariseen raportointikyvykkyyteen perustuva tilannekuva, joka tukee yhteisen tilannetietoisuuden ja tilanneymmärryksen muodostumista ja päätöksentekoa. ➔ Tarvitaan yhteinen ja jaettu digitaalisen turvallisuuden tilanneymmärrys julkisessa hallinnossa. Titukri-periaatepäätöksen 10.6.2021 yhtenä toimenpiteenä on valtiovarainministeriön johdolla toteuttava selvitys viranomaisten tarpeista teknologisille ratkaisuille salassa pidettävän ja turvaluokitellun tiedon käsittely-ympäristöjen luomiseksi. Selvityksen kohteena ovat muun muassa viranomaisten yhdenmukainen salattu sähköpostiviestintä, turvalliset neuvotteluyhteydet ja -palvelut sekä turvallinen tiedonsiirtopalvelu. Selvitys tehdään vuonna 2022 ja selvityksen pohjalta haetaan ja toteutetaan nykyaikaiset ratkaisut vuosina 2023-2024. Selvityksessä arvioidaan myös tiedonvaihdon yhteentoimivuutta kolmansien tahojen kanssa. Nämä ratkaisut ovat välttämättömiä digitaalisen turvallisuuden yhteistoiminnalle ja tilannekuvan jakamiselle. ➔ Titukri: Tiedon jakamisen – erityisesti luokitellun tiedon – mahdollistaminen, tehostaminen ja lisääminen eri viranomaisten välillä.
Häiriötilanteiden halinta	Häiriötilanteiden hallintaan liittyvät valmiudet vaihtelevat eri toimijoiden välillä. Yhteistä toimijoille on rajallinen kyvykkyys häiriötilanteiden hallintaan sekä puutteet osaamisessa. ➔ Häiriötilanteiden hallintaan liittyvä tuki ja konkreettinen ohjaus häiriötilanteen aikaiseen toimintaan edesauttaa organisaatioiden palautumista häiriötilanteesta. Kunnat, hyvinvointialueet ja muut julkisen sektorin toimijat tarvitsevat häiriötilanteissa nopeasti saatavilla olevia resursseja häiriön vaikutusten minimointiin sekä tilanteen selvittämiseen. ➔ Nopea toiminta edellyttää toimijoiden välillä yhtenäisiä prosesseja sekä selkeitä rooleja ja tehtäväkuvauksia häiriötilanteen hallinnan osalta.

[32] Julkisen hallinnon digitaalisen turvallisuuden kansallisen harjoitustoiminnan tavoitteet ja toimenpiteet (dvv.fi).

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.

Tutkimusyhteistoiminnan osapuolten tulee olla toisiaan tukevia ja täydentäviä, jotta yhteistyö voi synnyttää lisäarvoa ja uudenlaisia ratkaisuja. Toisaalta yhteistyön edellytyksenä on toisten ymmärtäminen lisäksi se, että osapuolet ovat jossain määrin samantasoisia. Vastaaminen samantasoisuuden 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 tarvetta hallinnollisille toimenpiteille ja byrokratialle. Taulukkoon 8 on koottu digitaalisen turvallisuuden yhteistoiminnan tavoitetilaan liittyviä odotuksia.

Taulukko 8: Tavoitetilaan 7liittyviä odotuksia tutkimustoiminnassa.

Palvelu / 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 yliopistot, 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 paremmin koota näiden kaiken toimijoiden ympärille. ➔ Kyberturvallisuuskeskus koordinoi kansallista digitaalisen turvallisuuden tutkimuksen yhteistoimintaa ja kokoaa yhteen tutkimusta ja kehittämistä tekevät tai tukevat organisaatiot sekä tutkimustuloksia hyödyntävät tahot.

	➔ Kevyt organisoitumismalli on vaatimus yhteistoiminnan rakenteelle, 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 osaamista digitaalisesta turvallisuudesta. Tutkimusyhteistyö voi tuoda ajantasaista uutta tietoa yhteiskunnan eri toimijoiden päätöksenteon tueksi. Tutkimustulosten hyödyntäminen edellyttää, että organisaatioilla on kyky soveltaa tuloksia tavoitteiden mukaisiin kehitystoimenpiteisiin sekä niiden vaikuttavuuden mittaamiseen. ➔ Tutkimusta tulee tehdä sekä strategisella että operatiivisella tasolla, 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 yhteistyötä myös kyberturvallisuudessa.

4.3 Julkisen hallinnon digitaalisen turvallisuuden palvelut tavoitetilassa

Julkisen hallinnon digitaalisen turvallisuuden palvelut, vastuuorganisaatiot ja kunkin palvelun yhteistoiminta- ja hallintamalli tavoitetilassa on kuvattu taulukossa 9. Tavoitetilatarkastelussa ei ole selvitetty tavoitetilan saavuttamiseksi mahdollisesti tarvittavia säädösmuutostarpeita.

Taulukko 9: Julkisen hallinnon digitaalisen turvallisuuden palvelut tavoitetilassa.

Digitaalisen turvallisuuden yhteinen ohjaus ja kehittämisen yhteistoiminta		
Palvelun kuvaus	Palvelu kattaa digitaalisen turvallisuuden yhteisen ohjauksen, digitaaliseen turvallisuuteen ja kyberturvallisuuteen liittyvien valtioneuvoston periaatepäätösten ja strategioiden sekä niihin liittyvien kehitysohjelmien ja toimeenpanon valmistelun ja toteutuksen koordinoinnin. Lisäksi palvelu 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 kautta saatavien tietojen jakaminen ja välittäminen koordinoidusti kansalliseen ohjauksen ja kehittämisen yhteistoimintaan.	Vastuutaho: Kyberturvallisuusjohtaja Turvallisuuskomitea Digitalisaation, datatalouden ja julkisen hallinnon kehittämisen ministerityöryhmä, Digitoimisto VM, LVM, TEM, UM HVK
Yhteistoiminnan rakenne	Palveluun liittyvän yhteistoiminnan tavoitteena on yhteinen näkemys digitaalisen turvallisuuden strategioista, periaatepäätöksistä, normeista ja kehityshankkeista sekä niiden sisällöistä, ja rahoituksen sekä toimeenpanosuunnitelmien valmistelu ja toteuttaminen, sekä toimeenpanon seuranta. Yhteistoiminta koostuu seuraavista elementeistä: • Erilaisten toimijoiden ekosysteemi: julkinen hallinto, tutkimuslaitokset ja 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	Yhteistoimintaan osallistuvat: Tiedonhallintayksikön johto ja digitaalisesta turvallisuudesta vastaavat henkilöt

	• Kehittämisohjelmat, jotka valmistellaan yhteistyöryhmässä ja tarkistetaan vuosittain • 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.	
Mittarit	• Strategioiden ja normien sekä kehittämisohjelmien vaikuttavuus	
Suositukset, ohjeet, vaatimukset ja työkalut		
Palvelun kuvaus	Digitaalisen turvallisuuden riskienhallintamallit, suositukset, ohjeet, vaatimukset ja hyväksyntäkriteerit käytettävien palveluiden turvallisuudesta tulee olla yhteneviä ja pohjautua yleisesti hyväksyttyihin ja käytettyihin periaatteisiin, kuten yleiset kansainväliset standardit. Julkista hallintoa koskevat yhteiset digitaalisen turvallisuuden vaatimukset, ohjeet ja suositukset hyväksymiskriteereineen tulee olla saatavissa järjestettynä yhdestä paikasta. Valtionhallinto tarjoaa yhteisiä työkaluja organisaatioiden tueksi ja digitaalisen turvallisuuden ylläpitämiseksi, mittaamiseksi ja kehittämiseksi julkisen hallinnon organisaatioissa. Palvelussa tuotetaan ja ylläpidetään kontrollitavoitteita, vaatimuksia ja ohjeistusta, jotka linjaavat, miten digitaalisen turvallisuuden tavoitteet saavutetaan. Palvelu koostuu seuraavista osista: • Digitaaliseen turvallisuuteen liittyvien suositusten, ohjeiden, vaatimusten ja työkalujen keskitetty hallinta • Suositus-, ohje-, vaatimus-, ja työkalutarpeiden ennakoiva tunnistaminen ja hallinta	Vastuutaho: Tiedonhallintalautakunta: suositukset DVV: yleisohjeet; vaatimusten, ohjeiden ja suositusten saatavuus järjestettynä yhdestä paikasta

	• Osallistuminen mahdollisuuksien mukaan standardien, viitekehysten, suositusten kansainväliseen valmisteluun ja kansainvälisen ohjeistuksen huomioimiseen kansallisessa valmistelussa.	
Yhteistoiminnan rakenne	Palveluun liittyvän yhteistoiminnan tavoitteena on julkisen hallinnon digitaalisen turvallisuuden tarpeita ja tavoitteita tukevien suositusten, ohjeiden, vaatimusten ja työkalujen ennakoiva tunnistaminen ja keskitetty hallinta. Yhteistoiminta koostuu seuraavista elementeistä: • Vastuutaho tunnistaa ja ylläpitää suositusten, ohjeiden, vaatimusten ja työkalujen kehittämistarpeita sekä osallistaa yhteistoimintaan osallistuvia niiden valmisteluun. • Vastuutaho järjestää seminaareja suosituksista, ohjeista, vaatimuksista ja työkaluista. • Vastuutaho ylläpitää portaalia digitaalisen turvallisuuden materiaalien jakamiseen. • Yhteistoimintaan osallistuvat kehittävät suosituksia, ohjeita, vaatimuksia ja työkaluja, vievät niitä käytäntöön omissa organisaatioissaan ja keräävät palautetta niiden kehittämiseksi. • Vastuutaho tarjoaa kanavan yhteiseen käyttöön tarkoitettujen digitaalisen turvallisuuden dokumenttien jakamiseen.	Yhteistoimintaan osallistuvat: Tiedonhallintayksikön digitaalisesta turvallisuudesta vastaavat henkilöt Kyberturvallisuuskeskus
Mittarit	• Ohjeiden, suositusten, vaatimuskriteeristöjen ja työkalujen vaikuttavuuden arviointi ja vaikuttavuus • Seminaarien osallistujien määrä ja palaute	
Hankinnat		
Palvelun kuvaus	Palvelu kattaa julkisen hallinnon digitaalisen turvallisuuden palvelujen yhteishankintajärjestelyt. • Kilpailutetaan yhteishankintana sekä välittömästi käyttöön otettavissa olevia että minikilpailutuksen kautta hankittavissa olevia digitaalisen turvallisuuden palveluja. Välittömästi käyttöön otettavia palveluita ovat esimerkiksi tuki häiriötilanteissa. Minikilpailutuksen kautta hankittaviksi soveltuvia	Vastuutaho: Hansel

	palveluja ovat erilaiset jatkuvaa toimintaa tukevat palvelut, kuten asiantuntijatuki hankkeissa tai tietoturvallisuuden arviointipalvelut. • Kilpailutuksissa huomioidaan kansainvälisten asiantuntijoiden ja osaamisen saaminen käyttöön • Esimerkki tavoitetilasta: Kunnille on hankittu Euroopassa toimivan kansainvälisen pilvipalvelutoimittajan ratkaisuja sellaisilla hankintaehdoilla ja teknisillä ominaisuuksilla, että ne täyttävät kaikki säädetyt vaatimukset, mukaan viranomaisten toiminnan julkisuudesta annettu laki (621/1999), tietosuojasäännökset sekä kuntia koskevat erityissäännökset.	
Yhteistoiminnan rakenne	Palveluun liittyvän yhteistoiminnan tavoitteena on digitaaliseen turvallisuuteen liittyvien hankintojen 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 • Yhteistoimintaa osallistuvat hyödyntävät ensi sijaisesti yhteishankintajärjestelyjä hankintoja tehdessään ja osallistuvat hankintatarpeiden määrittelyyn.	Yhteistoimintaan osallistuvat: Tiedonhallintayksikön digitaalisesta turvallisuudesta vastaavat henkilöt
Mittarit	• Puitejärjestelyjen kautta hankittujen palvelujen arvo (euroina)	
Tutkimuksen koordinointi		
Palvelun kuvaus	Palvelu tunnistaa tutkimus,- kehitys- ja innovaatiokohteita riski- ja uhka-analyysien sekä vaatimustarpeiden kautta digitaalisen turvallisuuden eri osa-alueilla. • Arvioidaan kansainvälisessä vuorovaikutuksessa digitaalisen turvallisuuden kenttää ja digitaalista turvallisuutta sekä ennakoidaan tutkimuskohteita	Vastuutaho: Kyberturvallisuusjohtaja, Kyberturvallisuuskeskus,

	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.	tutkimusyhteisö
Yhteistoiminnan rakenne	Palveluun liittyvän yhteistoiminnan tavoitteena on digitaalisen turvallisuuden tutkimus,- kehitys ja innovaatiokohteiden ennakoiva tunnistaminen, arviointi ja hallinta, verkostoituminen sekä yhteistoiminnan lisääminen. Yhteistoiminta koostuu seuraavista elementeistä: • Ekosysteemi erilaisten toimijoiden, kuten erikokoisten yritysten, tutkimusorganisaatioiden, rahoittajien ja julkisen hallinnon toimijoiden osaamisen ja verkostojen yhteen tuomiseksi • Vuosittainen kansallinen työpaja digitaalisen turvallisuuden tutkimuskohteiden ennakoivaksi tunnistamiseksi.	Yhteistoimintaan osallistuvat: Digitaalisen turvallisuuden tutkimusta tekevien tutkimuslaitosten johto Digitaalisen turvallisuuden yhteistoiminnasta vastaavat tahot Digitaalisen turvallisuuden palveluja tarjoava elinkeinoelämä
Mittarit	• Tutkimushankkeiden lukumäärä suhteessa tunnistettuihin tutkimuskohteisiin • Hankerahoituksen määrä	
Osaaminen		
Palvelun kuvaus	Palvelu vastaa digitaalisen turvallisuuden osaamisen ja yhteiskunnan turvallisuuskulttuurin kehittämisestä ja	Vastuutaho:

	vaalimisesta. Kulttuurin perusta on tietoisuus turvallisuusriskeistä sekä ymmärrys ja osaaminen tarvittavista toimenpiteistä. Palvelu koostuu seuraavista osista: • Digitaalisen turvallisuuden kansallisen tutkimustiedon yhteenkokoaminen, koulutusohjelmien suunnittelu ja laatiminen sekä ylemmän asteen koulutuksen tarjoaminen koordinoidusti • Ennakoiva digitaalisen turvallisuuden koulutusten tuottamisen julkisen hallinnon työntekijöille ja ylläpidon suunnittelu ja koordinointi • Digitaalisen turvallisuuden kansallisen tason viestintä eri tasoilla (kansalainen, työntekijä, johtaja/hallituksen jäsen ja ICT-asiantuntija) • Merkittävien digitaalisen turvallisuuden EU- ja kansainvälisten seminaarien ja tapahtuminen markkinointi hallinnossa asiantuntijoille • Vertailu ja oppiminen verrokkivaltioissa tapahtuvasta osaamisen kehittämisestä (esimerkiksi Alankomaat, UK, Ruotsi).	Yliopistot, ammattikorkeakoulut, DVV
Yhteistoiminnan rakenne	Palveluun liittyvän yhteistoiminnan tavoitteena on digitaalisen turvallisuuden osaamisen kehittäminen vastaamaan strategisia tavoitteita. Yhteistoiminta koostuu seuraavista elementeistä: • Ekosysteemi erilaisten toimijoiden, kuten erikokoisten yritysten, tutkimusorganisaatioiden ja julkisen sektorin toimijoiden kokoaminen yhteen 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 ja osallistavat organisaatioiden henkilöstöä kehittämää osaamistaan ja osallistumaan koulutuksiin, tuovat esille koulutus- ja kehitystarpeita sekä osallistuvat ja osallistavat	Yhteistoimintaan osallistuvat: Tiedonhallintayksikön digitaalisesta turvallisuudesta vastaavat henkilöt Kyberturvallisuuskeskus

	organisaatioitaan digitaalisen turvallisuuden seminaareihin ja tapahtumiin.	
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 • Osallistuvien organisaatioiden kattavuus.	
Harjoitustoiminta		
Palvelun kuvaus	Ylläpidetään ohjeistusta digitaalisen turvallisuuden harjoitusohjelmien ja harjoitusten suunnittelua ja toteutusta varten. Julkisen hallinnon käyttöön tuotetaan virtuaalisia harjoitusympäristöjä. Valtakunnallisten harjoitusten aikataulu julkaistaan vuosittain. Palvelu kattaa laajavaikutteisia häiriö- tai poikkeustilanteita koskevan harjoitustoiminnan suunnittelun. Harjoitustoiminnalla varmistetaan kyky reagoida häiriöihin sekä varmistaa 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, Kyberturvallisuuskeskus, HVK, yksityiset palveluntarjoajat
Yhteistoiminnan rakenne	Palveluun liittyvän yhteistoiminnan tavoitteena on julkisen hallinnon yhteinen harjoitustoiminnan malli, aikataulu ja harjoitukset. Yhteistoiminta koostuu seuraavista elementeistä: • Vastuutaho tukee harjoitustoimintaa yhteisten suositusten, ohjeiden, mallien, palveluiden ja valmiiden harjoitusten avulla	Yhteistoimintaan osallistuvat: Tiedonhallintayksikön varautumisesta vastaavat henkilöt

	• Harjoitustoimintakoordinaattori tukee harjoitustoiminnan suunnittelua, toteutusta, seurantaa ja viestintää • Toteutetaan valtiohallinnon, hyvinvointialueiden, kuntien ja muiden toimijoiden yhteiset harjoitustoimintaryhmät • Muodostetaan alueellisia ekosysteemejä viranomaisten, aluehallinnon, kuntien sekä yhteisöjen toimintavalmiuden kehittämiseen • Toteutetaan yhteisiä harjoituksia suunnitteleva foorumi 2-4 kertaa vuodessa.	
Mittarit	• Harjoitusten vaikuttavuus. • Harjoituskohtaiset palautekyselyt. • Yhteisharjoitusten kattavuus.	
Tilannekuva		
Palvelun kuvaus	Tuotetaan julkiselle hallinnolle keskitetysti digitaalisen turvallisuuden tilannekuvatuotteita. Tavoitteena on yhteinen ja jaettu digitaalisen turvallisuuden tilannekuvaratkaisu, joka pohjautuu laajaan dataan, monipuolisiin mittareihin koko julkisesta hallinnosta sekä modulaariseen raportointikyvykkyyteen, joka tukee yhteisen tilannetietoisuuden ja tilanneymmärryksen muodostumista ja päätöksentekoa. Ratkaisua voidaan täydentää tai rikastaa myös sisäisillä tilannekuvatiedoilla. Kukin organisaatio huolehtii itse sisäisten tilannekuvatietojensa hallinnasta. Tilannekuvatietoja tarvitaan kattavasti julkisesta hallinnosta sekä yhteisöistä. Palvelu tuottaa, ylläpitää ja kehittää julkisen hallinnon käyttöön digitaalisen turvallisuuden tilannekuvatietoja ja -tuotteita, jotka perustuvat asiantuntijoiden analyyseihin sekä valvomotietoihin. Palvelu koostuu seuraavista osista: • Tietojen kerääminen ja koostaminen analysointia ja tilannekuvan muodostamista sekä raportointia varten	Vastuutaho: Kyberturvallisuuskeskus VM, ennuste DVV, hallinnollinen tilannekuva

	• Tilannekuvatiedon jakelu ja julkaisu tarjotaan osittain itsepalveluna ”on-demand” -ratkaisuna ja erikseen määritellyille ryhmille, myös organisaatiokohtaisia tilannekuvatietojen koosteita varten. • Ulkoisen uhkatiedon kerääminen ja analysointi • Toimintaympäristön turvallisuutta kuvaava analyysi ja tilannekuvan ylläpito • Riskienhallintaan, vaatimustenmukaisuusarvioihin ja valvontaan perustuva julkisen hallinnon digiturvallisuuden ennusteen laadinta vuosittain • Hallinnollisen digiturvan tilannekuvan ylläpito kokonaiskuvapalvelussa. Hallinnollisen digiturvan tilanne kuvaa sitä, miten hyvin organisaatio on tunnistanut, kuvannut ja ottanut käyttöön digitaaliseen turvallisuuteen liittyvät menettelytavat, prosessit ja ohjeet. Organisaatiot raportoivat (itsearvioidusta) hallinnollisen digiturvan tilanteesta DVV:n kokonaiskuvapalvelussa. Se on verkkopalvelu, joka mahdollistaa oman tilanteen kehittymisen seurannan sekä vertailun muiden organisaatioiden tilanteeseen. Palvelu tuottaa myös raportteja ja seurantatietoa digitaalisen turvallisuuden kehittymisestä koko julkisen hallinnon tasolla. • Tilannekuvatiedon vaihtaminen kansainvälisten toimijoiden kanssa	
Yhteistoiminnan rakenne	Palveluun 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/seminaareja tilannekuvatuotteiden perusteella.	Yhteistoimintaan osallistuvat: Tiedonhallintayksikön digitaalisesta turvallisuudesta vastaavat henkilöt Tiedonvaihtoryhmät (ISAC) Yhteisöt

	• Yhteistyötoimintaan osallistuvat määrittelevät oman organisaation sisäiset säännöt tilannekuvan jakamisesta organisaatiossa ja osallistuvat osaltaan tilannekuvatiedon ja parhaiden käytänteiden jakamiseen yhteistoimintaa osallistuvien kesken.	
Mittarit	• Käyttäjäorganisaatioiden antama palaute tilannekuvatuotteiden laadusta	
Jatkuvuudenhallinta ja varautuminen		
Palvelun kuvaus	Palvelu kattaa toiminnan varautumisen koordinointiin liittyvät kokonaisuudet. Palvelu koostuu seuraavista osista: • Valmius-, jatkuvuus-, ja toipumissuunnitelmien mallipohjien ja ohjeiden ylläpito • Tuki suunnitelmien laadintaan kansainvälisten standardien ja hyvien käytäntöjen mukaisesti • Raportointi varautumisen kattavuudesta • Alueellinen ekosysteemi alueellisen varautumisen kehittämiseen.	Vastuutaho: DVV, Kyberturvallisuuskeskus, HVK, Aluehallintovirasto(t)
Yhteistoiminnan rakenne	Palveluun liittyvän yhteistoiminnan tavoitteena on julkisen hallinnon yhteinen varautumisen malli. Yhteistoiminta koostuu seuraavista elementeistä: • Vastuutahon tuki varautumiselle yhteisten suositusten, ohjeiden ja mallien avulla • Valtakunnallinen yhteistoiminta • Aluehallintotason yhteistoiminta • Alueellinen ekosysteemi viranomaisten, aluehallinnon, hyvinvointialueiden, kuntien sekä yhteisöjen varautumisen suunnitteluun ja testaamiseen. Yhteistoimintaan osallistuvat hyödyntävät yhteisiä varautumissuosituksia, -ohjeita ja -malleja oman organisaation ja keskeisten yhteistyötahojen yhteisen varautumisen kehittämisessä ja toteuttamisessa.	Yhteistoimintaan osallistuvat: Tiedonhallintayksikön varautumisesta vastaavat henkilöt
Mittarit	• Varautumisaikatavoitteet • Yhteistoiminnan kattavuus	

Häiriötilanteiden hallinta		
Palvelun 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. Palvelu kattaa digitaalisen turvallisuuden häiriöhallintaprosessin sekä tapahtumien havainnoinnin ja analysoinnin. Palvelu koostuu seuraavista osista: • Digitaaliseen turvallisuuteen liittyvän valvonnan ja turvallisuushäiriöiden hallinta • Tuki häiriöiden tutkintaan • Kansallisen tason häiriöhallinnan aktivointi laajavaikutteisessa häiriötilanteessa • Mahdollisen kansainvälisen avun antamisen ja vastaanottamisen koordinointi Kyberturvallisuuskeskuksessa.	Vastuutaho: Kyberturvallisuuskeskus, yksityisen sektorin asiantuntijayritykset
Yhteistoiminnan rakenne	Palveluun liittyvän yhteistoiminnan tavoitteena on yhtenäinen toimintatapa häiriötilanteiden hallintaan jaettujen resurssien hyödyntämiseksi Yhteistoiminta koostuu seuraavista elementeistä: • Vastuutaho kilpailuttaa Hanselin puitejärjestelyjen perusteella sopimukset tarvittavan asiantuntijatuen hankkimiseksi markkinoilta laajavaikutteisissa häiriötilanteissa välittömästi julkisen hallinnon käyttöön • Työpajoja/seminaareja häiriöhallintamallin kehittämiseksi • Vastuutaho ylläpitää yhteisesti sovittua mallia häiriötilanteiden hallintaan • Vuotuinen alueellinen harjoitus resurssien jakamisesta, harjoituksen järjestysvastuu vaihtuu.	Yhteistoimintaan osallistuvat: Tiedonhallintayksikön häiriötilanteiden hallinnasta vastaavat henkilöt

	Yhteistoimintaan osallistuvat dokumentoivat tarvittavat tiedot ja varmistavat riittävän resursoinnin tietoturvallisuuden kartoituspalvelua käyttääkseen. Yhteistoimintaan osallistuvat dokumentoivat oman organisaationsa digitaalisen turvallisuuden häiriönhallintaprosessit ja varmistavat riittävän resursoinnin nopean häiriön hallinnan asiantuntijatuen vastaanottaakseen.	
Mittarit	• Kartoituspalvelua käyttäneiden organisaatioiden määrä • Kartoituksissa tehtyjen havaintojen kehitys • Markkinoilta kilpailutetun sopimuksen perusteella hankittujen asiantuntijoiden vuosittainen toteutunut tarve, saatavuus ja käyttö häiriötilanteissa	

5 KEHITTÄMISTOIMENPITEET

Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamallin kehittämiseksi on tunnistettu seuraavat toimenpiteet. Niihin liittyvät digitaalisen turvallisuuden yhteistoiminnan tarkemmat kuvaukset ovat luvussa 4.3. Julkisen hallinnon digitaalisen turvallisuuden palvelut tavoitetilassa. Kehittämistoimenpiteitä on valmisteltu Suomen digikompassin valmistelun kanssa yhdessä.

Yhteistoiminnan ohjaus

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

1. Ohjauksen ja kehittämisen yhteistoiminta: Ylläpidetään keskitetysti julkisen hallinnon digitaalisen turvallisuuden kehittämisen resurssisuunnitelmaa.

   Vastuu: VM, kyberturvallisuusjohtaja

   Aikataulu: 2023-2024

   Rahoitus: Ei vaadi lisärahoitusta.

2. Ohjauksen ja kehittämisen yhteistoiminta: Muodostetaan yhteinen näkemys julkisen hallinnon digitaalisen turvallisuuden kehitysohjelmasta ja sen rahoituksesta vuosille 2023-2027.

   Vastuu: VM

   Aikataulu: 2022-2023

   Rahoitus: Rahoitetaan Haukka-ohjelmasta.

3. Tilannekuva: Valmistellaan ja ylläpidetään strategiseen riskienhallintaan, arviointeihin ja valvontaan perustuvaa jaettua digitaalisen turvallisuuden ennustetta, joka pohjautuu laajaan dataan, monipuolisiin mittareihin sekä modulaariseen raportointikyvykkyyteen.

   Vastuu: VM, DVV, julkisen hallinnon organisaatiot tiedontuottajina

   Aikataulu: 2022-2025

   Rahoitus: Vaatii lisärahoitusta.

4. Ohjauksen ja kehittämisen yhteistoiminta: Edistetään digitaalisen turvallisuuden yhteisiä hankintoja ja hankkeita niihin kannustavalla hallinto- ja rahoitusmallilla.

Vastuu: VM, Hansel

Aikataulu: 2024-2027

Rahoitus: Vaatii lisärahoitusta, tarkennettava.

5. Ohjauksen ja kehittämisen yhteistoiminta: Digitaalisen turvallisuuden kehitysohjelmien ja niiden tuotosten vaikuttavuutta arvioidaan. Arvioidaan Haukka-ohjelman vaikuttavuus.

   Vastuu: VM

   Aikataulu: 2022-2023

   Rahoitus: Rahoitetaan Haukka-ohjelmasta.

6. Ohjauksen ja kehittämisen yhteistoiminta: Edistetään kansallisin toimenpitein hyvinvointialueiden välistä digitaalisen turvallisuuden kehittämisen yhteistoimintaa.

   Vastuu: STM, SM, DVV/Vahti-verkosto

   Aikataulu: 2023-2027

   Rahoitus: Vaatii lisärahoitusta, tarkennettava muuten kuin DVV:n osalta.

Digitaalisen turvallisuuden palvelut

Digitaalisen turvallisuuden palvelujen kehittäminen ja ylläpito on 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.

7. Suositukset, ohjeet, vaatimukset ja työkalut: Julkista hallintoa koskevat yhteiset digitaalisen turvallisuuden säädösluettelot, ohjeet, suositukset, vaatimukset ja työkalut ovat saatavilla yhdestä paikasta tietopankista soveltamiskohteiden mukaisesti tai muutoin järjestettynä. Selvitetään tietopankin ylläpidon mahdolliset säädösmuutostarpeet.

   Vastuu: DVV

   Aikataulu: 2022-2024

   Rahoitus: Vaatii lisärahoitusta.

8. Kehittämisen yhteistoiminta: Säädöksissä, suosituksissa, ohjeissa, vaatimuksissa ja työkaluissa tuetaan mahdollisuuksien mukaan pilviteknologiaan käyttöä. Tärkeää on tunnistaa käyttötapaukset, joissa pilviteknologialla on saavutettavissa hyötyjä. Nämä hyödyt liittyvät

jaettuihin alusta- ja etäkäyttöratkaisuihin sekä kustannustehokkaasti toteutettuihin tietoturvaratkaisuihin.

Vastuu: VM, Tiedonhallintalautakunta, DVV

Aikataulu: 2022-2027

Rahoitus: Ei vaadi lisärahoitusta.

9. Kehittämisen yhteistoiminta: Hyvinvointialueille tarjotaan keskitetysti yhteisiä digitaalisen turvallisuuden arvioinnin ja kehittämisen, hyvinvointialueiden kansallisen tilannekuvan ja keskitetyn valvonnan, hyvinvointialueiden välisen yhteistoiminnan, ja pilvipalveluiden digitaalisen turvallisuuden tukemisen palveluja.

   Vastuu: DigiFinland, hyvinvointialueet

   Aikataulu: 2023-2027

   Rahoitus: Vaatii lisärahoitusta, tarkennettava.

10. Kehittämisen yhteistoiminta: Hyödynnetään kuntien alueellisen digitaalisen turvallisuuden yhteistoiminnan parhaita käytänteitä ja edistetään niiden leviämistä.

    Vastuu: Kuntaliitto, hyvinvointialueet, Kyberturvallisuuskeskus/Kunta-ISAC

    Aikataulu: 2023-2027

    Rahoitus: Tarkennettava.

11. Kehittämisen yhteistoiminta: Kunnille tarjotaan keskitetysti yhteisiä digiturvapalveluja Haukka-ohjelmassa ylläpidettävän kuntien digiturvapalvelujen tiekartan mukaisesti.

    Vastuu: Kuntaliitto, Kyberturvallisuuskeskus, DVV, kuntien ja kuntayhtymien ICT-yhtiöt

    Aikataulu: 2022-2027

    Rahoitus: Vaatii lisärahoitusta, tarkennettava muuten kuin DVV:n osalta.

12. Jatkuvuudenhallinta ja varautuminen: Muodostetaan alueellisia ekosysteemejä viranomaisten, aluehallinnon, hyvinvointialueiden, kuntien sekä yhteisöjen varautumisen suunnitteluun ja testaamiseen.

    Vastuu: Aluehallintovirasto, hyvinvointialueet

    Aikataulu: 2025-2027

    Rahoitus: Tarkennettava.

13. Hankinnat: Toteutetaan digitaalisen turvallisuuden yhteishankintoja, joiden kautta on mahdollista valita toimittaja kohtuullisessa hankintaan kuluvassa kalenteriajassa ilman erillistä minikilpailutusta tai muita toimenpiteitä.

    Vastuu: Valtori, DigiFinland, kuntien ja kuntayhtymien omistamat ICT-yhtiöt

    Aikataulu: 2023-2026

    Rahoitus: Rahoitusmalli on määritettävä.

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

    Vastuu: Traficom/Kyberturvallisuuskeskus

    Aikataulu: 2023-2024

    Rahoitus: Rahoitusmalli on määritettävä.

Tutkimus ja osaamisen kehittäminen

Toimijoiden välistä keskustelua digitaalisen turvallisuuden tutkimuskohteista tulee kehittää sekä varmista 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.

15. Tutkimuksen, kehityksen ja innovoinnin koordinointi: Tunnistetaan, hallitaan sekä seurataan kansallisia, EU- ja kansainvälisiä tutkimus-, kehitys- ja innovaatiokohteita ja tarvittavaa tutkimusrahoitusta.

    Vastuu: Kyberturvallisuusjohtaja, Traficom/Kyberturvallisuuskeskus

    Aikataulu: 2023-2025

    Rahoitus: Tarkennettava.

16. Osaamisen kehittäminen: Parannetaan digiturvaosaamista yhteisillä koulutusratkaisuilla, asiantuntijaverkostoilla ja harjoittelemalla.

    Vastuu: DVV

    Aikataulu: 2022-2027

    Rahoitus: Vuonna 2022 rahoitetaan Haukka-ohjelmasta, vuodesta 2023 alkaen vaatii lisärahoitusta.

17. Harjoitustoiminta: Selvitetään digitaalisen turvallisuuden harjoitustoiminnan vaikuttavuus.

    Vastuu: DVV

    Aikataulu: 2023

    Rahoitus: Vaatii lisärahoitusta.

Kehittämistoimenpiteiden liittyminen Suomen digikompassiin ja kauden 2023-2027 kehittämistoimenpiteisiin kuvataan lausuntokierroksen palautteen käsittelyn yhteydessä. Samoin kehittämistoimenpiteiden rahoitustarve arvioidaan kokonaisuutena lausuntokierroksen ja sen palautteen käsittelyn aikana. Alustavasti Digi- ja väestötietoviraston rahoitustarve kehittämistoimenpiteiden 3, 6, 7, 11, 16, 17 osalta yhteensä vuosina 2022-2023 on arviolta noin 600 000 euroa, ja vuodesta 2024 alkaen noin 800 000 euroa vuodessa. Vastuutoimijoita pyydetään myös arvioimaan kehittämistoimenpiteiden rahoitustarvetta lausuntokierroksen yhteydessä.

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

Osallistuja(t)
valtioneuvoston kanslia
ulkoministeriö
oikeusministeriö
sisäministeriö
puolustusministeriö
maa- ja metsätalousministeriö, Ruokavirasto
liikenne- ja viestintäministeriö
sosiaali- ja terveysministeriö
työ- ja elinkeinoministeriö
Digi- ja väestötietovirasto
Kyberturvallisuuskeskus, Liikenne- ja viestintävirasto
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

Formaalit ja informaalit 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. Formaali yhteistoimintaa ja vuorovaikutusta julkishallinnossa edustavat jo olemassa olevat rakenteet esimerkiksi yhteishankinnat tai kuntien perustamat yhteiset ICT-palveluyhtiöt. Informaalia yhteistyötä puolestaan ovat poolitoiminta sekä ISAC-tiedonvaihtoryhmät.

Digitaalisen turvallisuuden yhteistoiminnan tulee sisältää sekä formaalia että informaalia vuorovaikutusta osapuolten välillä. Osapuolten tulee aktiivisesti osallistua eri yhteistoiminnan muotoihin, jotta organisaation omat tavoitteet on mahdollista saavuttaa mahdollisimman tehokkaasti.[33]

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,
- sekä 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.

Valtiotoimijoilla on myös mahdollisuus uudistaa toimintamalleja ja tuoda esiin tarpeita digitaalisen turvallisuuden kehittämiseksi. Tämä edellyttää osaamista, jota tarvitaan muun muassa digitaalisen turvallisuuden toimijoiden sekä tarpeiden analyysiin, toimintaympäristön riskien, uhkien ja trendien analyysiin sekä ekosysteemien mahdolliseen koordinointiin tai tukemiseen. Ekosysteemeihin osallistuville yhteistyön on oltava vastavuoroista: erilaiset toimijat kuten erikokoiset yritykset, tutkimusor-

[33] https://www.vaikuttavuussaatio.fi/wp-content/uploads/2021/02/vaikuttavuussaatio_selvitys.pdf

ganisaatiot, rahoittajat ja julkisen sektorin toimijat tuovat ekosysteemiin oman osaamisensa ja verkostonsa. Työ- ja elinkeinoministeriö on julkaissut selvityksiä ja raportteja ekosysteemeihin liittyen.[34] VTT on myös julkaissut ekosysteemi-oppaan.[35]

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
- Formaali – Informaali yhteistoiminta

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

[34]https://tem.fi/documents/1410877/4429776/Ekosysteemit+uuden+elinkeino-+ja+innovaatiopolitiikan+kohteena/f46d3709-fdcf-4a73-83df-e84ae24b4196
[35] https://www.vttresearch.com/sites/default/files/pdf/publications/2020/Yhdessa_kestavaa_kasvua_17022021.pdf