



VALTIOVARAINMINISTERIÖ

# **Esiselvitys julkisen hallinnon digitaalisen toimintaympäristön tietovarannosta**

**15.11.2022**

## Sisällys

1 Johdanto .....	3
1.1 Tausta.....	3
1.2 Tavoitteet .....	4
1.3 Toteutustapa .....	5
1.4 Määritelmiä .....	5
2 Nykytila.....	6
2.1 Yhteisiä palveluja tuottavien palveluntarjoajien, Kuntaliiton ja virastojen näkemyksiä.....	6
2.1.1 Esiselvityksessä haastatellut toimijat .....	6
2.1.2 Palveluntarjoajien, virastojen ja Kuntaliiton näkemyksiä ja ehdotuksia .....	6
2.2 Kuntien näkemyksiä.....	8
2.2.1 Haastatellut kunnat.....	9
2.2.2 Kuntien näkemyksiä ja ehdotuksia .....	9
2.3 Yhteenveto haastatteluista.....	9
3 Suosituksia jatkotoimiksi .....	11
3.1 Tietovarannon suunnittelu, toteutus ja hallinta .....	12
3.2 Esimerkkejä tietoelementeistä.....	13
3.2.1 Yhteystiedot .....	13
3.2.2 Tekniset kuvailutiedot.....	13
4 Haastattelut.....	15

# 1 JOHDANTO

## 1.1 Tausta

Valtioneuvosto teki 8.4.2020 periaatepäätöksen Julkisen hallinnon digitaalisesta turvallisuudesta (VM 2020:23). Periaatepäätöksen mukaan digitaalisen turvallisuuden viitekehykseen sisältyy riskienhallintaan, tietoturvallisuuteen, tietosuojaan, kyberturvallisuuteen sekä toiminnan jatkuvuuden hallintaan ja varautumiseen liittyviä asioita. Periaatepäätöksessä on kuvattu julkisen hallinnon digitaalisen turvallisuuden kehittämisaalueet ja niiden kehittämisen periaatteet sekä keskeiset hallinnon toimintaa ja prosesseja tukevat digitaalisen turvallisuuden palvelut. Periaatepäätöksen linjauksia toteuttaa Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020-2023 (Haukka) (VM 2020:33).

Laki julkisen hallinnon tiedonhallinnasta (906/2019, tiedonhallintalaki) säättää julkisuusperiaatteen ja hyvän hallinnon vaatimusten toteuttamisesta viranomaisten tiedonhallinnassa. Laki sisältää koko julkista hallintoa koskevat säännökset tiedonhallinnan järjestämisestä ja kuvaamisesta, tietovarantojen yhteentoimivuudesta, tietojärjestelmien yhteentoimivuuden toteuttamisesta, teknisten rajapintojen ja katseluyhteyksien sekä tietoturvallisuuden toteuttamisesta. Tiedonhallintalaki säättää valtiovarainministeriön tehtäväksi huolehtia julkisen hallinnon tiedonhallintakartan ylläpidosta. Tiedonhallintakartalla esitetään voimassa olevasta sääntelystä muodostettu kuva julkisen hallinnon tietovarannoista ja tietojenluovutuksista sekä tiedoista vastaavista ja niitä hyödyntävistä toimijoista.

Tiedonhallintayksikön velvollisuutena on ylläpitää tiedonhallintamallia, joka on kuvaus tiedonhallintayksikössä toimivien viranomaisten tehtävien hoidossa toteutettavasta tiedonhallinnasta. Tiedonhallintamalli muodostaa osan siitä informaatiopohjasta, jolla tiedonhallintayksikkö suunnittelee toimintaansa kohdistuvia muutoksia ja kuvaa toimintaansa. Käytännössä kaikkien tietovarantojen tuottamiseksi käytetään ja kehitetään tietojärjestelmiä, tietoverkkoja, ohjelmistoja ja näiden välisiä kytkentöjä. Nämä muodostavat digitaalisen omaisuuden kokonaisuuden, jonka riittävän tarkka kuvaaminen mahdollistaa tiedonhallintayksikön tuottavan toiminnan ja auttaa selviämään häiriötilanteista mahdollisimman tehokkaasti.

Yhtenä Haukka-hankkeen tehtävänä on kunnille tarkoitetut digitaalisen turvallisuuden palvelut. Palvelujen suunnittelussa ja kehittämisessä on yhtenä hankaluutena ollut se, että digitaalisesta toimintaympäristöstä ei ole riittävästi keskitettyä tai muuten tasalaatuista tietoa saatavilla. Tällaisia tietoja ovat esimerkiksi tiedonhallintayksikön digitaaliseen turvallisuuteen ja tiedonhallintaan liittyvät yhteystiedot ja ympäristöä itseään kuvaavat tiedot esimerkiksi verkko-osoiteavaruuksista, palvelujen käyttämistä ohjelmistoversioista ja ohjelmistojen tai niiden osien välisistä yhteyksistä ja riippuvuuksista. Näistä tiedoista osa saattaa olla kuvattuna tiedonhallintamallissa, mutta tietoja voi puuttua tai niiden tarkkuus ei ole riittävä. Tässä selvityksessä näistä tiedonhallintayksikön digitaalista omaisuutta koskevista tiedoista käytetään termiä digitaalisen toimintaympäristön tietovaranto. Selvityksessä on kuvattu myös ehdotus tietovarannon tietosisällöksi.

Digitaalisen toimintaympäristön tietovarantoa tarvitaan paitsi kunnissa, myös muualla julkisessa hallinnossa oman toiminnan ja muiden organisaation kanssa tehtävän yhteistyön mahdollistamiseksi.

Tietovarantoa voisi hyödyntää muun muassa häiriöiden ja haavoittuvuuksien hallinnassa tai ohjelmistoarkkitehtuurin kehittämisessä. Kun laajasti käytetyistä ohjelmistoista (esimerkiksi sähköpostipalvelimet, verkkosivustopalvelimet, etäyhteys- eli VPN-palvelimet) löytyy vakavia tietoturvapuutteita, Liikenne- ja viestintäviraston Kyberturvallisuuskeskus skannaa Suomen verkkoalueita löytääkseen näitä haavoittuvia järjestelmiä. Näin Kyberturvallisuuskeskus voi varoittaa järjestelmien omistajia, jos tunnistaa omistajan. Mikäli digitaalisen toimintaympäristön tiedot olisivat laadukkaasti ja luotettavasti saatavilla keskitetysti, voisi Kyberturvallisuuskeskus yksinkertaisella haulla selvittää missä haavoittuvia järjestelmiä on käytössä ja kuinka näihin toimijoihin saadaan yhteys. Tällä tavalla nopeutunut haavoittuvuuksienhallinta olisi eduksi paitsi tiedonhallintayksiköille, myös koko yhteiskunnalle.

Vastaavasti häiriötilanteissa on tarpeen tietää luotettavasti mitkä tietojärjestelmät ovat riippuvia toisten tietojärjestelmien toiminnasta ja kuinka eri tietojärjestelmien vastuutahoihin saadaan yhteys. Näitä tietoja pitää tällä hetkellä kukin toimija yllä itse, mutta keskitetty ja ajantasainen tietovaranto tehostaisi häiriönhallintaa ja mahdollisesti lyhentäisi häiriöiden kestoja.

Tietovarantoa rakennettaessa tulisi ottaa huomioon, että osa tiedoista on salassa pidettävää tai turvallisuusluokiteltua. Siten tietovarannon digitaalinen turvallisuus on suunniteltava ja toteutettava huolellisesti. Jokainen tiedonhallintayksikkö on tiedonhallintalain nojalla vastuussa omista tiedoistaan ja digitaalisen ympäristönsä dokumentoinnista ja kuvaamisesta. Organisaatioiden rajat ylittävä tiedonhallinta ei ole tällä hetkellä kaikilta osin järjestettyä. Varsinkin pienemmillä organisaatioilla, joita ovat esimerkiksi iso osa kunnista, ei ole resursseja järjestää koko tiedonhallintaansa itse ja näin niiden digitaalisen toimintaympäristön kuvailutiedot hajaantuvat useammalle alihankkijalle ja muulle toimijalle. Digitaalisen toimintaympäristön tietojen hallinta keskitetyssä tietovarannossa voisi olla tehokkain tapa sekä toiminnan että kustannusten kannalta. Tietovarannossa säilytettävien tietojen hallinnan tulisi ottaa huomioon tiedonhallintayksiköiden tarpeet, kuten vähäiset henkilöresurssit ja laajasti käytetyt alihankintaverkostot. Mahdollisen keskitetyn tietovarannon suunnittelussa, toteutuksessa ja hallinnassa tulisi kiinnittää erityistä huomiota tiedon suojaamiseen mm. kasautumisvaikutukseen liittyvien riskien hallitsemiseksi.

Monella yhteiskunnan alueella on käytössä perustietojärjestelmiä: esimerkiksi väestötietojärjestelmässä on tietoa Suomessa asuvista ihmisistä, kiinteistötietojärjestelmässä kiinteistöistä ja yritystietojärjestelmästä yrityksistä. Digitalisaatio etenee ja tietotekniikan merkitys lisääntyy kaiken aikaa. Digitaalisesta toimintaympäristöstä ei keskitettyä tietovarantoa ole, vaan tiedot ovat hajallaan ja kukin toimija koostaa omaan toimintaansa tarvittavaa tietoa useimmiten erillisenä henkilötöyönä. Tämä aiheuttaa päällekkäistä työtä. Digitaalista toimintaympäristöä koskevat tiedot muuttuvat nopeasti ja hajallaan olevia tietoja ei ole mahdollista ylläpitää. Tietojen keräämistä, käsittelyä, ylläpitoa ja analysointia ei ole automatisoitu, mikä aiheuttaa ylimääräisiä kustannuksia. Tämän selvityksen jatkotöissä onkin yhtenä merkittävänä tehtävänä minimoida henkilötöy ja maksimoida tiedon hallinnan automatisointi.

## **1.2 Tavoitteet**

Tämän esiselvityksen tavoitteena on selvittää eri toimijoita haastatteleamalla mitä tietoja digitaalisesta toimintaympäristöstä pitäisi kerätä, kuinka tietoja kerättäisiin sekä mikä toimija niitä keräisi ja mihin

tarkoitukseen. Esiselvityksen tavoitteena on ollut erityisesti kuntien digitaalisen toimintaympäristön kehittäminen. Valtiovarainministeriön tehtävien mukaisesti samalla on pohdittu myös koko julkisen hallinnon toimintaympäristön kehittämistä.

Tämän esiselvityksen haastattelukysymyksiä olivat:

- Onko tarvetta digitaalisen ympäristön kuvaamisen tietovarannolle?
- Mitä tietoja pitäisi kerätä?
- Ketkä tuottaisivat ja käyttäisivät tietoja?
- Pitäisikö olla keskitetty vai hajautettu järjestelmä, johon tietoja kerättäisiin?
- Mikä taho vastaisi tiedon hallinnasta?
- Millä toimenpiteillä päästäisiin kohti tavoitetilaa?

### **1.3 Toteutustapa**

Tämä esiselvitys on koottu eri toimijoiden haastatteluista ja avoimista tietolähteistä. Kaikki haastatteluun kutsutut kunnat eivät päässeet osallistumaan, mutta haastateltavat ovat eri puolilta maata ja hyvin erikokoisia. Haastatellut kunnat olivat Enontekiö, Mäntsälä ja Turku. Julkiselle hallinnolle yhteisiä palveluita tuottavista tai järjestävistä toimijoista haastateltiin Liikenne- ja viestintävirasto Traficom, Digi- ja väestötietovirasto (DVV) sekä Valtion tieto- ja viestintätekniikkakeskus Valtori. Kunta- ja sote-sektorin toimijoista haastateltiin Suomen Kuntaliitto, DigiFinland ja Pohjois-Suomen kuntien ja kuntaomisteisten yhtiöiden omistama LapIT Oy.

Haastatteluihin oli varattu aikaa 30-45 minuuttia. Haastattelijoina toimi valtiovarainministeriön virkamies ja Haukka-hankkeeseen kilpailutettuja konsultteja.

### **1.4 Määritelmiä**

Tietoteknisessä palvelutuotannossa laajasti käytetyn ITIL-viitekehyksen (Information Technology Infrastructure Library) käsite konfiguraatietietokanta (CMDB, Configuration Management Database) sisältää konfiguraatio- eli kuvailutietueita (CI, Configuration Item). Näitä voivat olla tiedot tietoteknisistä laitteista, niiden osista, ohjelmistoista ja muista ominaisuuksista sekä yhteyksistä muihin tietueisiin. Haastatteluissa pyrittiin välttämään käsitettä konfiguraatietietokanta, jottei liian helposti rajauduttaisi pelkkään tekniseen kuvailutietoon. Tässä selvityksessä ja haastatteluissa on käytetty termiä digitaalisen toimintaympäristön tietovaranto.

Tietovaranto on tiedonhallintalain (906/2019) mukaan viranomaisen tehtävien hoidossa tai muussa toiminnassa käytettäviä tietoaineistoja sisältävä kokonaisuus, jota käsitellään tietojärjestelmien avulla tai manuaalisesti. Mahdollisesti kehitettävän ja toteutettavan digitaalisen toimintaympäristön tietovarannon tavoitteena olisi kuvata digitaalista omaisuutta ja sen hallintaan käytettäviä tietoja ja yhteyksiä.

## 2 NYKYTILA

### 2.1 Yhteisiä palveluja tuottavien palveluntarjoajien, Kuntaliiton ja virastojen näkemyksiä

#### 2.1.1 Esiselvityksessä haastatellut toimijat

Julkiselle hallinnolle yhteisiä palveluita tuottavista toimijoista tässä esiselvityksessä haastateltiin Valtion tieto- ja viestintätekniikkakeskus Valtori, Liikenne- ja viestintävirasto Traficom, Digi- ja väestötietovirasto (DVV), DigiFinland ja LapIT Oy. Lisäksi haastateltiin Kuntaliitto.

Valtori tuottaa valtionhallinnon toimialariippumattomat ICT-palvelut sekä korkean varautumisen ja turvallisuuden vaatimukset täyttäviä tieto- ja viestintätekniisiä palveluita ja integraatiopalveluita.

Traficomin tehtäviin kuuluu mm. toimia viestinnän rekisteriviranomaisena (FI-verkkotunnukset). Sen yhteydessä toimii Kyberturvallisuuskeskus, jolla on merkittävä rooli julkisen hallinnon ja muiden toimijoiden tietoturvallisuuden häiriötilanteiden selvitystyössä. Kyberturvallisuuskeskus tuottaa myös teknisen kyberturvallisuuden tilannekuvaa.

DVV edistää yhteiskunnan digitalisaatiota ja tuottaa hallinnollisen turvallisuuden tilannekuvaa. DVV:n palveluvalikoimassa on tällä hetkellä useita yhteiskunnalle tärkeitä tietovarantoja, kuten esimerkiksi väestötietojärjestelmä, palvelutietovaranto, hankesalkku ja varmennepalvelu.

DigiFinlandin tehtävänä on kehittää sosiaali- ja terveydenhuollon, pelastustoimen ja muiden toimialojen tuottavuutta ja vaikuttavuutta parantavia kansallisia digitaalisia ratkaisuja osana julkisen hallinnon kokonaisuutta. Lisäksi sen tehtävänä on tukea viranomaisten kansallisten sähköisen asioinnin tukipalvelujen hyödyntämistä sekä edistää julkisen hallinnon ICT:n integraatiota ja yhteentoimivuutta.

LapIT Oy tukee Lapin maakunnassa kuntien, kuntayhtiöiden ja kuntien liikelaitosten asiakkaita sekä maakuntahallinnon, erikoissairaanhoidon, kuntien perusterveydenhuollon ja sosiaalitoimen organisaatioita.

Kuntaliitto toimii kuntasektorin edunvalvojana, kehittäjäkumppanina sekä asiantuntija- ja tietopalvelujen tarjoajana. Sen jäseniä ovat Suomen kunnat ja kaupungit. Toiminnassa ovat mukana myös maakuntien liitot, sairaanhoitopiirit, kuntayhtymät ja kuntataustaiset osakeyhtiöt. Kuntaliitto palvelee kuntia ja sopimuskumppaneita kunta-alan asiantuntemuksella läpi toimialojen ja kuntatoimijoita koskevien yhteisten teemojen.

#### 2.1.2 Palveluntarjoajien, virastojen ja Kuntaliiton näkemyksiä ja ehdotuksia

Tässä kappaleessa on koottu yhteen palveluntarjoajien, virastojen ja Kuntaliiton keskeisimmät näkemykset ja suositukset.

## Esiselvityksen taustasta ja tarpeesta

Selvityskokonaisuutta pidettiin haastavana, mutta samalla mielenkiintoisena ja tarpeellisena. Aihetta on pohdittu ja ratkaisuja haettu jo pitkään, siinä kuitenkin täysin onnistumatta. Osa haastateltavista toivoi, että selvittävää asiaa olisi määritelty ennalta tarkemmin ja olisi keskitytty enemmän tietovarannon hoitamiseen, ehkä jopa tekniseen toteuttamiseen, kuin konseptiin. Yhteisten palveluiden näkökulmasta kuntakenttää pidettiin yhtenä kokonaisuutena, eikä tarkkaa tietoa yksittäisten kuntien digitaalisesta ympäristöstä koettu tarpeelliseksi tuntea.

Haastateltavat pitivät erittäin tärkeänä selvittää mihin tarkoitukseen tietoja kerätään. Olisi keskeistä tunnistaa ketkä tarvitsevat tietoja, ketkä voivat tuottaa tietoja ja minkä asian hoitamiseen tietoja tarvitaan. Mahdollisen tietovarannon kehittämisen tulisi tapahtua pienin askelin aloittamalla kaikkein välttämättömimmistä tiedosta ja laajentamalla tietomallia myöhemmin. Tietoa yhdistelemällä ja rikastamalla tietovarannosta voisi olla saatavana tietoa, jota ei muualla vielä ole.

Digitaalisen toimintaympäristön kuvailutietojen hallinta on tällä hetkellä pirstaleista ja toimijoita on useita. Näiden toimijoiden saaminen tuottamaan yhteismitallista tietoa tiettyyn paikkaan on vaikeaa. Eri toimijoiden vastuut ja roolit tulisi tämän vuoksi määritellä, mahdollisesti lainsäädännöllä.

Haastateltavat kokivat tarpeelliseksi tehostaa kuntakentän digitaaliseen toimintaan liittyvää tiedonvaihtoa ja koordinoitua, jossa ratkaisuna voisi olla valtionhallinnon järjestämä koordinaatio- tai yhteistyöryhmä. Myös jo nyt toiminnassa olevia ryhmiä, kuten Vahti-toimintaa ja Kuntaliiton eri ryhmiä voisi hyödyntää enemmän.

## Häiriön- ja riskienhallinnasta sekä tietovarannon riskeistä

Viestintä ja yhteystiedot nähtiin keskeiseksi osaksi häiriöiden, uhkien ja riskien hallintaa. Kuntakentän kirjavuus ja erityisesti pienten kuntien väistämätön henkilösidonaisuus koettiin haastavaksi. Yksi palveluntarjoaja ehdotti, että tiedonvaihtokanavaksi tulisi perustaa kuntakohtainen sähköpostiosoite, esimerkiksi muotoa tietoturva@kunta.fi. Kuntaliitto on kerännyt kuntien tietoturvallisuuteen liittyvän yhteystietorekisterin ja tiedonvaihtofoorumin. Kaikilla haastateltavilla ei näiden olemassaolosta kuitenkaan ollut tietoa. Moni kunta on myös vastustanut ylimääräisen sähköpostiosoitteen luomista, koska siitä voi seurata ylimääräistä haittapostiliikennettä.

Digitaalisen ympäristön kuvailutietojen sisällön turvallisuudesta tulee huolehtia. Keskitetty tietovaranto muodostaisi merkittävän hyökkäyskohteen ja keinon kartoittaa muita hyökkäyskohteita, joten tietovarannon toteuttamisen tietoturvallisuutta ja muuta arkkitehtuuria, kuten esimerkiksi hajautetun ja keskitetyn tuotantomallin välisiä etuja ja haittoja, tulee arvioida tarkkaan. Osa tietosisällöstä saattaisi olla salassa pidettävää tai turvallisuusluokiteltua mistä seuraisi vaatimuksia tietovarannon toteutukselle, palvelun tuottajalle ja myös käyttäjille. Pelkkä tietojen arkaluonteisuus ei luonnollisesti tarkoita sitä, että tietoja ei pidä kerätä, sillä arkaluonteisimmat tiedot ovat luultavasti julkisen hallinnon toiminnalle kriittisimpiä ja siten niiden saatavuudesta ja eheydestä kaikissa olosuhteissa tulee huolehtia luottamuksellisuuden lisäksi.

Eri järjestelmät ja palvelut ovat tulossa entistä enemmän riippuvaisiksi toisistaan ja häiriö yhdessä palvelussa saattaa heijastua muihin palveluihin. Siten niiden välisten riippuvuuksien ymmärtäminen

on tärkeää ja ne pitäisi kuvata. Toisaalta järjestelmien käyttämien ohjelmistokomponenttien kuvaaminen helpottaisi haavoittuvuushallintaa. Myös MISP-uhkatietoaalustan IOC-tietojen (Indication of Compromise) kohdentamisessa riippuvuuksien ja muiden kuvailutietojen tunteminen on oleellista.

Haastatteluissa esitettiin väite, että digitaalisen toimintaympäristön tietovarannon puute aiheuttaa jo nyt riskejä, joita haastateltavat pitivät merkittävänä.

### Teknologia

Tässä esiselvityksessä ei ole suunniteltu tietovarannon teknistä toteutusta eikä tehty teknologiavalintoja. Olisi tärkeä tunnistaa mitä tietoja olisi välttämätöntä kerätä jo ensi vaiheessa ja mitä voitaisiin ottaa mukaan myöhemmin. Olisi tärkeä ottaa huomioon olemassa olevat ratkaisut ja kartoittaa niiden hyödyntämismahdollisuudet. Tiedon kerääminen ja hallinta tulisi automatisoida mahdollisimman pitkälle, jotta tiedot pysyisivät ajan tasalla. Yhteisten palvelujen tuottajilla on jo käytössä kuvailutietokantoja ja erityisesti näiden välillä tietoja voitaisiin välittää integraatorajapintojen kautta. Tästä huolimatta tietojen päivittämisen tulisi olla mahdollista myös manuaalisesti.

Keskitetyn ja usean toimijan käyttämän tietovarannon tietomallia tulee hallita, jotta tietovaranto palvelisi koko käyttäjäkuntaa. Käyttövaltuuksien hallinta tulisi suunnitella jo alkuvaiheessa, koska tiedoista riippuen niiden käyttäjäkunta voisi olla hyvinkin laaja julkisesta hallinnosta ja palveluntarjoajista jopa kansalaisiin asti.

Erityisesti yhteisten palvelujen kuvaamisessa korostuu riippuvuuksien kuvaaminen. Riippuvuustieto on tarpeellista esimerkiksi kriittisten kohteiden tunnistamisessa sekä häiriön- ja haavoittuvuushallinnassa.

### Resurssit ja omistajuus

Useimmilla kunnilla on hyvin vähän tietohallinnosta ja tietoturvallisuudesta vastaavia henkilöitä ja pieni tietohallintobudjetti. Siksi uusia tehtäviä, kuten tietovarantojen ylläpitoa, saattaa olla vaikea toteuttaa. Lisäarvoa pitäisi pystyä tuottamaan joko täysin ilman lisätyötä tai ainakin hyötyjen tulisi olla selvästi työpanosta suuremmat.

Tietovarannon hallinnan ja tuotantotavan päätöksessä olisi otettava huomioon tietovirrat alkulähteiltä käyttäjään asti, mitä toimijoita matkan varrella on, kuka tiedon ”omistaa” missäkin vaiheessa ja kuinka tietoa tulee suojata. Näiden tietojen perusteella tulisi päättää olisiko tietovarannon tai tietovarantojen hallinta esimerkiksi yhden tai useamman viraston lakisääteinen tehtävä. Samalla on myös huolehdittava, että tietovarannon hallintapalvelua on oltava mahdollista tuottaa koko julkiselle hallinnolle.

## **2.2 Kuntien näkemyksiä**

Suomessa on yli kolmesataa kuntaa. Suurin osa kunnista on pieniä ja niissä on vain vähän digitaalisen turvallisuuden tehtäviin liittyvää henkilöstöä.



### *2.2.1 Haastatellut kunnat*

Haastatteluihin osallistuivat Enontekiö, Mäntsälä ja Turku, jotka ovat hyvin eri kokoisia ja eri puolilta Suomea. Kuntien digiturvallisuuden tehtäviin osallistuu hyvin erilainen määrä henkilöstöä.

Jo näiden kolmen haastatellun kunnan tietohallinto on järjestetty eri tavoilla: Enontekiöllä on yksi ATK-vastaava. Mäntsälässä on tietohallintoyksikkö, joka on osana hallintopalveluita ja ICT-tuotanto on ulkoistettu useamman kunnan yhteisomistuksessa olevalle Kuuma-ICT:lle. Turun kaupungilla puolestaan on erillinen IT-palveluorganisaatio, joka suunnittelee, hankkii ja toteuttaa kaupungin ICT-palvelut ja organisaatiolla on erilliset tietohallintopäällikön ja tietoturvapäällikön virat.

### *2.2.2 Kuntien näkemyksiä ja ehdotuksia*

Kunnat haluavat kehittää tiedolla johtamista kaikessa hallinnossa ja siten myös tiedonhallinnassa. Tällä hetkellä digitaalisen omaisuuden dokumentaatio ei ole riittävää. Tiedon puutetta pidetään jopa turvallisuusriskinä. Vaillinainen tieto heikentää taloutta, tiedonhallintaan ja digitaaliseen turvallisuuteen liittyvää päätöksentekoa.

Digitaalisen toimintaympäristön tietovaranto parantaisi tilannetta, kunhan sen tietoja pidettäisiin jatkuvasti ajantasaisena mikä puolestaan vaatii resursointia. Monen kunnan resurssit ovat niukat eikä uusi tietovaranto saisi lisätä työtehtäviä liikaa siitä saatavaan hyötyyn nähden. Erikseen mainittiin esimerkkinä valtakunnallinen palvelutietovaranto, jonka työllistävä vaikutus on koettu kohtuuttomana siitä saatavaan hyötyyn verrattuna.

Mahdollisessa tietovarannossa olevan tiedon ja toimintojen kriittisyysluokittelua voitaisiin käyttää hyväksi toiminnan priorisoinnissa niin toiminnan kuin talouden näkökulmasta.

## **2.3 Yhteenveto haastatteluista**

Haastateltavat pitivät digitaalisen toimintaympäristön tietovarantoa tarpeellisena. Ajatus ei ole uusi. Aikaisemmat yritykset vastaavan tietovarannon luomiseksi ovat epäonnistuneet, mahdollisesti siksi, että vastuut ja velvollisuudet ovat olleet epäselviä. Ehkä aikakaan ei ole vielä tuolloin ollut kypsä keskitetylle tiedon keräämiselle, koska tietojärjestelmien toiminnallinen rooli sekä erityisesti tietojärjestelmien välinen keskinäisriippuvuus ei vielä ollut yhtä laajaa. Myös tiedonhallintalain voimaantulo on lisännyt julkisen hallinnon velvollisuuksia kuvata tiedonhallintaansa. Keskitetysti hallinnoitujen tietojen käyttö olisi suunniteltava ja toteutettava huolellisesti, jotta tietojen turvallisuus ja tietosuoja saataisiin säilytettyä tarvittavalla tavalla.

Eri toimijoiden yhteystietojen hallinta on vaikeaa. Esimerkiksi digitaalisesta turvallisuudesta vastaavien henkilöiden tavoitettavuutta vaikeuttaa vaihtelevat tehtävänimikkeet, henkilöiden vaihtuvuus tai että tietoja ei yksinkertaisesti ole julkisesti tai edes rajoitetusti saatavilla. Joitain rekistereitä on olemassa, mutta ne eivät kata koko julkista hallintoa eikä niiden ajantasaisuutta varmisteta automaattisesti.

Keskitetysti hallinnoitu tietovaranto voisi parantaa digitaalisen turvallisuuden toimintoja kuten häiriön- ja haavoittuvuuksienhallintaa, jos yhteystietojen lisäksi sieltä löytyisi tietoja käytetyistä ohjelmistokomponenteista ja niiden versioista sekä mahdollisista muista uhkista. Tietovaranto voisi kuitenkin toimia tietolähteenä paitsi julkiselle hallinnolle itselleen, myös pahantahtoisille toimijoille. Tämä on otettava tietomallin ja pääsynhallinnan suunnittelussa ja toteutuksessa huomioon.

Mikäli digitaalisen ympäristön tietovaranto toteutettaisiin keskitetysti, sen tuottajan tehtävästä pitäisi mahdollisesti säätää lailla. Samoin olisi selvitettävä olisivatko jotkin tiedonhallintayksikkö-, tietojärjestelmä- tai palvelukohtaiset tiedot lakisääteisiä.

### 3 SUOSITUKSIA JATKOTOIMIKSI

Digitaalisen toimintaympäristön tietovaranto parantaisi tiedonhallintayksiköiden ja muiden toimijoiden ymmärrystä tietojärjestelmien välisistä riippuvuuksista, tietojärjestelmien komponenteista ja niiden versiotiedoista, tietoverkoista ja niiden komponenteista. Näitä tietoja tarvitaan mm. omaisuudenhallinnassa, häiriönhallinnassa, haavoittuvuuksienhallinnassa sekä järjestelmien kehittämisessä ja jatkuvassa ylläpitotoiminnassa. Digitaalisen toimintaympäristön tietovarannon avulla olisi mahdollista parantaa julkisen hallinnon tiedonhallinnan laatua ja erityisesti digitaalista turvallisuutta ja turvallisuuteen liittyvää toimintaa.

Digitaalisen toimintaympäristön tietovaranto tulisi säätää jollekin virastolle tehtäväksi, esimerkiksi Digi- ja väestötietovirastolle. DVV:n mahdollisena tehtävänä se täydentäisi muita DVV:n vastuulla olevia perustietovarantoja.

Tässä kappaleessa esitetään joitain jatkotoimia, jotka tulisi ottaa huomioon digitaalisen toimintaympäristön tietovarannon sekä siihen liittyvien tehtävien ja toimintojen käynnistämisessä, kehittämisessä ja hallinnassa. Tietovarantoa tulisi kehittää ja ottaa käyttöön vaiheittain. Karkealla tasolla myöhemmän vaiheen tietovarannon tulisi sisältää tiettyjä perustietoja, sekä tietoja toiminnan, palveluiden ja tietojärjestelmien tasoilla (Kuva 1).

Perustietoja voisivat olla organisaation tai tiedonhallintayksikön yksilöintitiedot, fyysiset sijainnit ja tilat, muut yhteystiedot sekä palvelutaso- ja muut sopimukset. Toiminnan tasolla voitaisiin kuvata asiakkaille tarjottavat palvelut, lakisääteinen toiminta ja muut toiminta. Palveluiden tasolla voitaisiin kuvata asiakasrajapinnan palvelut, (teknisen) palvelurajapinnan palvelut ja taustapalvelut. Tietojärjestelmätasolla voitaisiin kuvata tietojärjestelmät (konesalissa tai pilvessä) sekä niiden integraatiot, organisaation käyttäjien laitteet ja ohjelmistot, tietojärjestelmien komponentit (tietokannat jne.), infrastruktuuripalvelut (nimipalvelu, hakemistopalvelu, käyttövaltuudet, varmuuskopiot jne.) sekä tietoliikenteen tiedot (IP-osoitteet, verkkoavaruudet jne.).

Tietoelementtejä koskevissa alustavissa suosituksissa on esitetty myös viitteellinen arvio niiden salassa pidon tarpeesta. Tämä arvio ei ole kattava tai sitova, vaan lopullinen tietojen luokittelu riippuu kustakin tiedonhallintayksiköstä, sen toiminnan luonteesta ja yksittäisestä tietoelementistä. Merkinällä salassa pidettävä ei tässä yhteydessä oteta kantaa salassa pidon tasoon tai siitä seuraaviin täsmällisiin vaatimuksiin.

### Perustiedot

- Organisaatiotiedot
- Sijainnit ja tilat
- Muut yhteystiedot
- Palvelutaso- ja muut sopimukset

### Toiminnan taso

- Asiakkaille tarjottavat palvelut
- Lakisääteinen toiminta
- Muu toiminta

### Palveluiden taso

- Asiakasrajapinnan palvelut
- Palvelurajapinnan palvelut
- Taustapalvelut

### Järjestelmätaso

- Tietojärjestelmät (konesalissa tai pilvessä) ja integraatiot
- Organisaation käyttäjien laitteet ja ohjelmistot
- Tietojärjestelmien komponentit (tietokannat jne.)
- Infrastruktuuripalvelut (nimipalvelu, hakemistopalvelu, käyttövaltuudet, varmuuskopiot jne.)
- Tietoliikenne (IP-osoitteet, verkkoavaruudet jne.)

*Kuva 1 Digitaalisen omaisuuden tietovaranto, mahdollinen tavoitetila*

### 3.1 Tietovarannon suunnittelu, toteutus ja hallinta

Suunnitteluvaiheen tehtävinä olisi tietovarannon hallintatoiminnon ja itse tietovarannon suunnittelu ja kehittäminen. Tietovarannolle tulisi määrittää tärkeimmät käyttötapaukset, niihin liittyvät tiedot, käyttäjryhmät sekä niiden vastuut ja tehtävät. Tavoitteena olisi saada aikaan toimintatapa, joka ei muodostuisi toiminnan alkuvaiheessa liian raskaaksi yksittäiselle tiedonhallintayksikölle, vaan mieluummin alkuvaiheen työpanos voisi olla tietovarannosta vastaavalla virastolla tavoitetilaa suurempi. Sekä tietovarannon tietosisältöä, että sen hallinnan toimintamalleja voisi siten kehittää ketterästi ja vaiheittain. Toimintamallien tulisi tähdätä siihen, että tiedonhallintayksiköissä ei tehtäisi päällekkäistä työtä, täysin uuden työn määrä olisi minimaalinen tai tarvittava kokonaistyömäärä jopa vähentäisi.

Alkuvaiheessa toteutettava tietovaranto voisi olla hyvin kevyt ja toteuttaa jonkin rajatun käyttötapausten. Käyttötapaustoteutuksia ja toimijoita voisi lisätä myöhemmin ja siirtyminen järeään tietojärjestelmään olisi mahdollista siinä vaiheessa, kun tietovarannon hallintatoimet ja tietosisältö olisivat selkiytyneet niin, että pääasialliset toimijat ja heidän tehtävänsä olisivat selvillä. Tietojärjestelmän voisi tietovarannosta vastaavan viraston tukena tuottaa palvelukeskus, esimerkiksi Valtori, jolla mahdollisesti olisi jo tarvittava järjestelmä käytössä.

Hallintavaiheen käynnistyminen olisi myös vaiheittaista. Käytännössä hallinta olisi aloitettava samaan aikaan toteutusvaiheen kanssa, jotta kehittäminen olisi joustavaa ja ottaisi kaiken aikaa huomiioon toimintaympäristön muutokset. Tässä vaiheessa olisi mahdollisesti automatisoitavissa osa tehtävistä, kuten joidenkin tiedonhallintayksiköiden tietojen hallinta.

## 3.2 Esimerkkejä tietoelementeistä

### 3.2.1 Yhteystiedot

Kuntaliitto kerää jo nyt kuntatoimijoiden digitaaliseen turvallisuuteen liittyviä yhteystietoja. Nämä tiedot tulee saattaa kaikkien sitä tarvitsevien tietoon ajantasaisina. Tiedot olisi hyvä laajentaa kattamaan koko julkinen hallinto.

Tärkeimpiä tietoelementtejä olisivat:

- Tiedonhallintayksikön yksilöintitiedot (julkinen)
- Digitaalisen turvallisuuden yhteystiedot: sähköpostiosoite, puhelinnumero jne. (julkinen ja mahdollisesti salassa pidettäviä lisätietoja).
- Digitaalisen turvallisuuden yhteyshenkilöt yhteystietoineen (julkinen tai salassa pidettävä). Näitä voisivat olla esimerkiksi tietoturvavastaava, tietosuojavastaava, tietohallintopäällikkö jne.

### 3.2.2 Tekniset kuvailutiedot

Teknisen kuvailutiedon koostaminen on aloitettu muutaman kerran menneinä vuosina, mutta tulokset ovat olleet laihoja eikä siten koko julkisen hallinnon tai kuntasektorin tasolla vielä ole kuvailutietoja olemassa. Suunnitteluvaiheessa onkin tärkeä miettiä, kuinka tiedot saadaan kerättyä niin, että kriittinen massa saadaan aikaan kuormittamatta tiedon luovuttajia liiaksi.

Tärkeimpiä tietoelementtejä olisivat:

- Tiedonhallintayksikön yksilöintitiedot (julkinen)
- Käytössä olevat julkiset IP-osoitealueet (osittain salassa pidettävä)
- Reititystietojen AS-numerot (osittain salassa pidettävä)

- Julkiset tietojärjestelmien yksilöintitiedot, esim. IP-osoite tai URL (julkinen)
- Muiden tietojärjestelmien yksilöintitiedot (salassa pidettävä tai julkinen)
- Tietojärjestelmien komponentit versiotietoineen (salassa pidettävä)

## **4 HAASTATTELUT**

DigiFinland 27.9.2021

DVV 27.8.2021

Enontekiö 28.10.2021

LapIT Oy 13.12.2021

Kuntaliitto 13.9.2021

Mäntsälä 11.11.2021

Traficommin kyberturvallisuuskeskus 23.8.2021

Turku 2.12.2021

Valtori 30.9.2021