VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Muistio

10.6.2025

VN/34688/2024
VN/34688/2024-VM-26

Kriittisen infrastruktuurin tietojen avoin jakaminen arvioidaan uudelleen huomioiden kansallinen turvallisuus. Väliraportti 10.6.2025.

Sisällys

Postiosoite
Postadress
Postal Address
Valtiovarainministeriö

PL 28
00023 Valtioneuvosto

Käyntiosoite
Besöksadress
Office

Snellmaninkatu 1 A
Helsinki

Puhelin
Telefon
Telephone

0295 16001
+358 295 16001

Faksi
Fax
Fax

s-posti, internet
e-post, internet
e-mail, internet

kirjaamo.vm@gov.fi

1 Johdanto

Euroopan turvallisuus on muuttunut perustavanlaatuisesti Venäjän hyökkäyssodan ja laaja-alaisen vaikuttamisen myötä. Suomi toimii nyt vaikeasti ennakoitavassa toimintaympäristössä, jossa kriittinen infrastruktuuri on hybridivaikuttamisen keskiössä.[1] Perinteisten uhkien ja geopoliittisten epävarmuuksien rinnalla tiedon yhteentoimivuutta ja hyödyntämistä haastaa kasvava kompleksisuus: edelleen lisääntyvä keskinäisriippuvuus johtaa siihen, että yhä pienemmillä ja yhä vaikeammin ennakoitavilla häiriöillä on yhä suuremmat ja ennalta-arvaamattomat vaikutukset kriittiseen infrastruktuuriimme.

Avoimesti ja julkisesti saatavilla olevan tiedon jakaminen ja kansallisen turvallisuuden suojaaminen eivät sulje toisiaan pois. Avoimuus edistää demokratiaa, hallinnon läpinäkyvyyttä ja tehokkuutta, lisää turvallisuutta sekä tukee tutkimusta, innovaatiota ja kansalaisten osallistumista. Myös elinkeinoelämä hyötyy avoimista tietovarannoista. Esimerkiksi paikkatieto on keskeinen osa datataloutta tuoden merkittävää lisäarvoa palveluille sekä väestön arkeen.[2]

Samalla digitalisaatio on lisännyt vihamielisten toimijoiden mahdollisuuksia hyödyntää avoimesti ja julkisesti saatavilla olevaa tietoa kriittisestä infrastruktuurista. Tällainen tieto voi tukea toimintaa, joka vakavasti uhkaa kansallista turvallisuutta. Suuri osa kriittisestä infrastruktuurista on yksityisessä omistuksessa. Avoin tieto voi paljastaa yritysten varautumistasoa tai puutteita, mikä voi vaikuttaa niiden kilpailukykyyn tai altistaa ne kohdennetuille hyökkäyksille.[3] Tekoäly ja automaatio tehostavat tiedon keruuta ja analysointia entisestään. Avoimesti ja julkisesti saatavilla oleva tieto voi olla myös alttiina manipuloinnille, mikä voi horjuttaa yhteiskunnan vakautta. Kohdistettu tai laajamittainen tiedonkeruu voi viime kädessä pyrkiä heikentämään demokratiaa. Autoritaariset valtiot hyödyntävät avoimesti saatavilla olevaa tietoa, mutta eivät itse jaa vastaavaa tietoa.[4]

Avoin ja julkisesti saatavilla oleva tieto ei itsessään muodosta välitöntä tai vakavaa uhkaa kansalliselle turvallisuudelle. Sitä voidaan kuitenkin hyödyntää kansallista turvallisuutta uhkaavan toiminnan valmistelussa ja toteuttamisessa.[5]

Digitalisaation ja datan avoimuuden lisääntyessä myös infrastruktuurin omistussuhteet, tietojen hallinta ja kansainväliset riippuvuudet nousevat keskeisiksi turvallisuuskysymyksiksi. Lainsäädäntö, joka vaikuttaa esimerkiksi tiedon avoimuuteen, julkisuuteen tai teknologiseen infrastruktuuriin, voi siten joko vahvistaa tai heikentää kansallista turvallisuutta. Vaikutusten arviointi vaatii poikkihallinnollista yhteistyötä ja turvallisuusviranomaisten asiantuntemusta – erityisesti silloin, kun kyse on säädöksistä, jotka vaikuttavat

[1] Valtioneuvoston puolustusselonteko 2024 ja valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko 2024.
[2] Paikantamisen perustan ja peruspaikkatietojen strategia 2025–2035.
[3] Valtioneuvoston päätös huoltovarmuuden tavoitteista 2024.

[4] Kansallisen turvallisuuden katsaus 2025, Suojelupoliisi.
[5] Paikkatiedon kansallinen riskiarvio 2024.

suoraan tai välillisesti kriittisiin toimintoihin. Turvallisuusvaikutukset voivat perustua paitsi luokiteltuun tietoon, myös julkiseen ja avoimeen aineistoon, jonka merkitys voi muuttua kontekstin tai yhdistelyn kautta.

Parhaillaan on käynnissä useita hankkeita, joissa tarkastellaan kriittistä infrastruktuuria ja tiedon avoimuutta. Erityisesti avoimen tiedon tarkastelu etenee kuntatasolla ja rakennetun ympäristön osalta. Useat suuret kunnat ovat jo ryhtyneet tarkastelemaan alueidenkäyttöön ja rakentamiseen liittyviä tietoja kokonaisuutena. Osaa näistä tiedoista on rajattu avoimen saatavuuden ulkopuolelle, erityisesti rakennetun ympäristön paikkatietoaineistojen osalta. Rajauksilla pyritään estämään tietojen käyttö esimerkiksi kriittisen infrastruktuurin haavoittuvuuksien kartoittamiseen. Riskiperusteisen arvioinnin tehtävä on auttaa löytämään tasapaino tiedon suojaamisen ja avoimuuden välillä. Kyse on jatkuvasta toiminnasta, joka vaatii aikaa sekä resursseja. Viranomaiset voivat tälläkin hetkellä toimia nopeasti hallussaan olevan avoimesti ja julkisesti saatavilla olevan tiedon jakamisen estämiseksi, mikäli katsovat sen tarpeelliseksi Samaa tietoa – usein eri näkökulmista ja eri tarkoituksiin – jakavat useat eri tahot, mukaan lukien elinkeinoelämän toimijat. Kaikkien viranomaisten, myös kuntien, vastuulla on suojata hallussaan oleva kriittiseen infrastruktuuriin liittyvä tieto. Kattava arviointi edellyttää kuitenkin yhteistyötä eri toimijoiden välillä. Viime kädessä avoimuuden suojaamisesta ja tiedon jakamisen arvioinnissa on kyse niistä arvoista, joille yhteiskuntamme rakentuu sekä väestön turvallisuuden ja hyvinvoinnin varmistamisesta.

Paikkatiedon kansallisessa riskiarviossa tunnistettiin, että avoimuuden taustalla ovat perustuslaista johtuva julkisuusperiaate, hallinnon yleislainsäädäntö (julkisuuslaki ja tiedonhallintalaki) sekä mahdollinen sektorikohtainen erityislainsäädäntö. Tiedon avaamista on lisäksi edistetty aktiivisesti myös kansallisilla ohjelmilla ja periaatepäätöksillä. Merkittäviä velvoitteita tiedon avaamiseksi tulee myös Århusin sopimuksesta ja EU-lainsäädännöstä. Monien paikkatietoaineistojen avoimen jakamisen velvoite tulee direktiiveistä (mm. ympäristötietodirektiivi, INSPIRE-direktiivi ja avoimen datan direktiivi sekä useat ympäristödirektiivien raportointivaatimukset), jotka on pantu täytäntöön kansallisella lainsäädännöllä. Sääntely ei kuitenkaan velvoita jakamaan avoimesti kansallisesti salassa pidettävää tietoa. EU-sääntelyyn sisältyy kansallista liikkumavaraa, jonka nojalla velvoitteita voidaan rajata kansallisessa sääntelyssä esimerkiksi kansallisen turvallisuuden perusteella. Edellä mainittu lainsäädäntö on keskiössä myös tämän hankkeen jatkotyössä ja kysymyksenasettelussa.

2 Työn tausta ja tavoitteet

Pääministeri Orpon hallitusohjelman kohdan 8.5 ”Kyberturvallisuus, informaatioturvallisuus ja hybridiuhkien torjuminen” kirjauksen mukaan kriittisen infrastruktuurin tietojen avoin jakaminen arvioidaan uudelleen huomioiden kansallinen turvallisuus.[6] Valtiovarainministeriö asetti päätöksellään (VN/34688/2024) hankkeen toimikaudelle 19.2.2025 – 31.3.2026. Hankkeessa on kyse kriittisten toimijoiden avoimen tiedon riskiarviointien koordinoivasta yhteistyöstä ja kansallisen tilannekuvan muodostamisesta. Hankkeen työ pohjautuu lisäksi 30.8.2023 asetetun paikkatiedon kansallisen riskiarvion työryhmän (VN/15876/2023) tuloksiin. Paikkatiedon kansallinen riskiarvio valmistui 31.5.2024.

Työn ensimmäisen vaiheen tavoitteet

Työryhmä sai asettamispäätöksessään työlleen kaksi välitavoitetta:

[6] Vahva ja välittävä Suomi. Petteri Orpon hallitusohjelma 20.6.2023. Hallitusohjelmassa kriittisen infrastruktuurin turvallisuus nähdään osana laajempaa kokonaisturvallisuutta. Painopiste on ennakoivassa varautumisessa, lainsäädännön ajantasaistamisessa, viranomaisyhteistyön tehostamisessa, sekä yksityisen sektorin roolin tunnistamisessa ja tukemisessa

Välitavoite 1:

Valmistella valtiovarainministeriön ohjauksen tarpeisiin kiireellinen toimeksianto ja ohjeistus muille kuin CER-direktiivin[7] mukaisille kriittisen infrastruktuurin toimijoille siitä, että avoimen tiedon riskiarvioinnit tulee aloittaa. Osana tätä ohjeistusta hyödynnetään Kuntaliiton ohjetta (”Turvallisuusnäkökulma ja kuntien rakennetun ympäristön paikkatietoaineistot”) sekä Paikkatiedon kansallista riskiarviota (VN/15876/2023). Dokumentit jaetaan tarkoituksenmukaisella sekä tietoturvallisella tavalla keskeisten toimijoiden käyttöön.

Välitavoite 2:

Muodostaa keskeisistä kansallisen turvallisuuden kannalta merkittävistä kriittisen infrastruktuurin avoimen tiedon riskeistä tilannekuvaraportti. Tilannekuvaraportti yhdistyy tarkempaan työryhmän toimintasuunnitelmaan ja luo pohjaa sille, mihin asioihin riskiarvioinneissa tulee keskittyä. Tilannekuvaraportin käsittelyn pohjalta työryhmä jatkaa laajemman avoimen tiedon riskien tarkastelun toiseen vaiheeseen.

Työryhmän tuli 10.6.2025 mennessä luovuttaa väliraporttinsa valtiovarainministeriölle.

Tämä väliraportti vastaa työryhmälle asetettuihin välittömiin tavoitteisiin kahdella tavalla. Ensinnäkin se kokoaa yhteen ne toimenpiteet, joita on toteutettu kuntien avoimen ja julkisesti saatavilla olevan tiedon riskiarviointien nykytilan kartoittamiseksi ja arviointikäytäntöjen kehittämiseksi. Toiseksi raportti kuvaa työryhmän alustavan selvitystyön pohjalta keskeisiä ja poikkileikkaavia riskejä, jotka liittyvät kriittiseen infrastruktuuriin liittyvän tiedon avoimeen jakamiseen kansallisen turvallisuuden näkökulmasta. Vaikka raportti ei vielä tarjoa kattavia ratkaisuja kaikkiin tunnistettuihin haasteisiin, muodostaa se perustan jatkotyölle, jossa analyysiä voidaan syventää, ohjeistuksia kehittää ja tarvittaessa tarkentaa myös sääntelyä.

2.1 Käsitteet

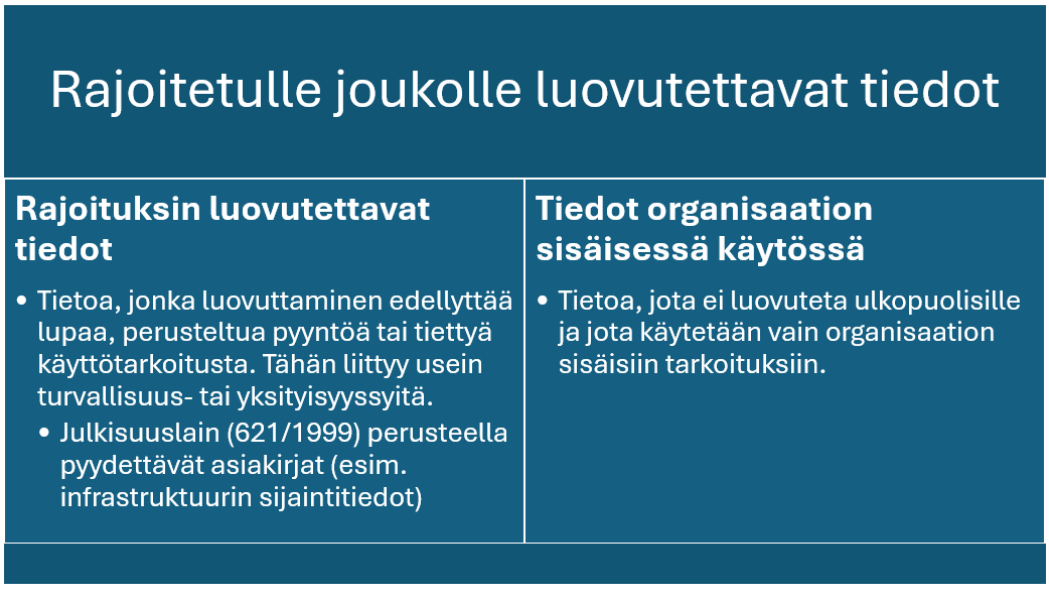
Hankkeen ja väliraportin työssä käytetään seuraavia käsitteitä ja niiden rajauksia. Määritelmiä on avattu tarkemmin liitteessä 1.

[7] Kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2557

Kuva 1: Työssä käytettävien käsitteiden määrittely

Työssä tarkastellaan tiedon avoimuutta ja tunnistetaan avointa sekä julkista tietoa, joka ei ole avoimesti saatavilla mutta on viranomaisten toiminnan julkisuudesta annetun lain (621/1999) mukaisesti julkista. Tästä syystä raportissa käytetään käsitettä avoin ja julkisesti saatavilla oleva tieto.

Kuva 2: Avoimen ja julkisesti saatavilla olevan tiedon kategoriat



Kuva 3: Rajoitetulle joukolle luovutettavat tiedot

3 VÄLITAVOITE 1: Kuntien riskiarvioinnit

Välitavoite 1 liittyi kiireellisen ohjeistuksen laatimiseen valtiovarainministeriön ohjauksen tueksi. Tavoitteena oli valmistella ohjeistus muille kuin CER-direktiivin mukaisille kriittisen infrastruktuurin toimijoille siitä, että avoimen tiedon riskiarvioinnit tulee käynnistää. Työryhmä päätti toteuttaa tavoitteen käytännössä keskittymällä kevätkaudella 2025 kuntien kanssa tehtävään yhteistyöhön, koska kunnat nähtiin merkittävinä kriittisen infrastruktuurin tiedon hallinnoijina ja jakajina.

Välitavoite 1 toteutettiin lähettämällä kunnille valtiovarainministeriön ohjauskirje sekä kysely avoimesti ja julkisesti saatavilla olevan tiedon jakamisen riskeistä. Lisäksi hankkeen työryhmä toteutti viiden kunnan pilotin vesihuollon avoimen ja julkisesti saatavilla olevan tiedon riskiarvioinnista.

3.1 Kunnat sekä avoimen ja julkisesti saatavilla olevan tiedon riskit

Kunnat ovat yhteiskunnan turvallisuuden perusta. Yleisen varautumisen kautta ne tukevat kriittisten toimintojen jatkuvuutta ja yhteiskunnan resilienssiä. Jokainen kansallisesti merkittävä toimija – olipa kyseessä viranomainen, infrastruktuuri tai yritys – sijaitsee aina jonkin kunnan alueella, mikä korostaa kuntien keskeistä roolia turvallisuuden kokonaisuudessa. Kunnat tai kuntien omistamat yhtiöt hallinnoivat merkittävää osaa fyysisestä infrastruktuurista, kuten silloista, tunneleista, vesihuollosta, energiaverkoista ja liikenneväylistä. Infrastruktuuria omistaa kuitenkin myös valtio. Kuntien hallinnoimat kohteet voivat olla strategisesti yhtä merkittäviä kuin valtion omistamat rakenteet, mutta niiden suojaaminen ja tiedonhallinta on usein hajautettua. Kuntien tuottama ja ylläpitämä tieto kuten kartat, rakentamislupatiedot ja tekniset suunnitelmat voivat olla avoimesti ja julkisesti saatavilla, ja siten altistaa kriittisiä kohteita tiedustelulle tai hyökkäyksille. Paikallisesti tuotettu avoin ja julkisesti saatavilla oleva tieto voi täydentää valtiollista tiedustelua, jonka kokonaiskuva muodostuu useista lähteistä. Avoimesti ja julkisesti saatavilla oleva kuntien tuottama tieto voi helpottaa vihamielisten toimijoiden mahdollisuuksia tunnistaa ja profiloida kohteita tai työntekijöitä. Tämä voi johtaa vahingollisiin tai häiritseviin tekoihin, joilla on laajempia alueellisia vaikutuksia, kuten esimerkiksi vedenjakelun keskeytyminen.

3.2 Valtiovarainministeriön ohjauskirje kunnille

Valtiovarainministeriö lähetti 2.4.2025 ohjauskirjeen 292:lle Manner-Suomen kunnalle. Kirjeessä avattiin kriittisen infrastruktuurin avoimen tiedon hankkeen taustaa ja tehtäviä sekä sen välittömiä tavoitteita. Valtiovarainministeriö kehotti kirjeessään kuntia jatkamaan tai tarvittaessa aloittamaan avoimesti saatavilla olevan tiedon jakamiseen liittyvät riskiarvioinnit sekä osallistumaan kuntien tilannekuvaa kartoittavaan kyselyyn. Kuntia ohjeistettiin tarkastelemaan eri kanavissa julkisesti jakamaansa infrastruktuuritietoa ja arvioimaan sen jakamista uudelleen nykyinen turvallisuustilanne huomioiden. Esimerkkeinä tuotiin esiin eri julkaisukanavat, tietomuodot sekä julkisuuden tarpeet ja niihin liittyvät riskit. Lisäksi riskiarvioinnissa kehotettiin käsittelemään tietopyyntöjen merkitystä avoimen ja julkisen tiedon jakamisen näkökulmasta.

Riskiarvioiden tekemisessä suositeltiin hyödynnettäväksi Kuntaliiton kautta jaettavaa ohjetta Turvallisuusnäkökulma ja kuntien rakennetun ympäristön paikkatietoaineistot sekä Paikkatiedon kansallista riskiarviota (VN/15876/2023) ja Kansallista riskiarviota (2023). Lisäksi kirjeessä kerrottiin, että kaikki Manner-Suomen kunnat tulisivat saamaan kriittisen infrastruktuurin avoimen tiedon jakamisen tilaa kartoittavan kyselyn Kuntaliitolta huhtikuun 2025 aikana.

3.3 Kuntakyselyn tulokset

Kuntaliiton toimesta lähetettiin 14.4.2025 kysely 292 kuntaan Manner-Suomessa. Kysely pyrki kartoittamaan haasteita ja ongelmakohtia riskiarvioinneissa sekä tietoa toimenpiteistä, joita kunnissa on riskiarviointien pohjalta tehty ja mitä kunnan ominaispiirteet huomioiden tulisi ottaa huomioon. Kuntia ei yksilöity vastausten käsittelyssä eikä kuntien antamia tietoja julkisteta siten, että ne olisivat yhdistettävissä tiettyyn kuntaan. Vastausprosentti oli noin 24 %. Vaikka vastaajajoukko ei edusta koko kuntakenttää tasaisesti, saadut vastaukset ovat sisäisesti johdonmukaisia ja luotettavia. Tulokset eivät kuitenkaan anna kattavaa kuvaa kaikkien kuntien tilanteesta. Niitä voidaan silti hyödyntää ohjaavana aineistona, joka tukee hankkeen jatkosuunnittelua ja jatkotoimenpiteiden kohdentamista.

Kyselyyn vastasi 70 kuntaa määräaikaan mennessä. Näistä kyselyyn vastanneista kunnista:

- 87 % kunnista on käytössä prosessi salassa pidettävän tiedon käsittelyyn, esimerkiksi kunnallisen päätöksenteon yhteydessä.
- 83 % on tehnyt toimenpiteitä, joilla pyritään hallitsemaan kriittisiin kohteisiin liittyvien avoimesti saatavilla olevien tietojen aiheuttamia riskejä.
- 77 % kunnista on arvioinut kriittiseen infrastruktuuriin liittyvän avoimen ja julkisesti saatavilla olevan tiedon riskejä.
- 73 % on poistanut infrastruktuuriin liittyviä paikkatietoja avoimista palveluista.

Eniten kriittisiä kohteita kunnat tunnistivat seuraavilta toimialoilta:

- Vesihuolto
- Digitaalinen infrastruktuuri
- Energia

Kuntien tunnistamat keskeisimmät häiriötilanteet ja riskit:

- Vesihuollon häiriöt: 93 %
- Tieto- ja viestintäverkkojen häiriöt: 85 %
- Sähkönsaannin suurhäiriöt: 82 %
- Energiahuollon häiriöt: 78 %
- Informaatiovaikuttaminen: 71 %

Tietopyyntöjen osalta:

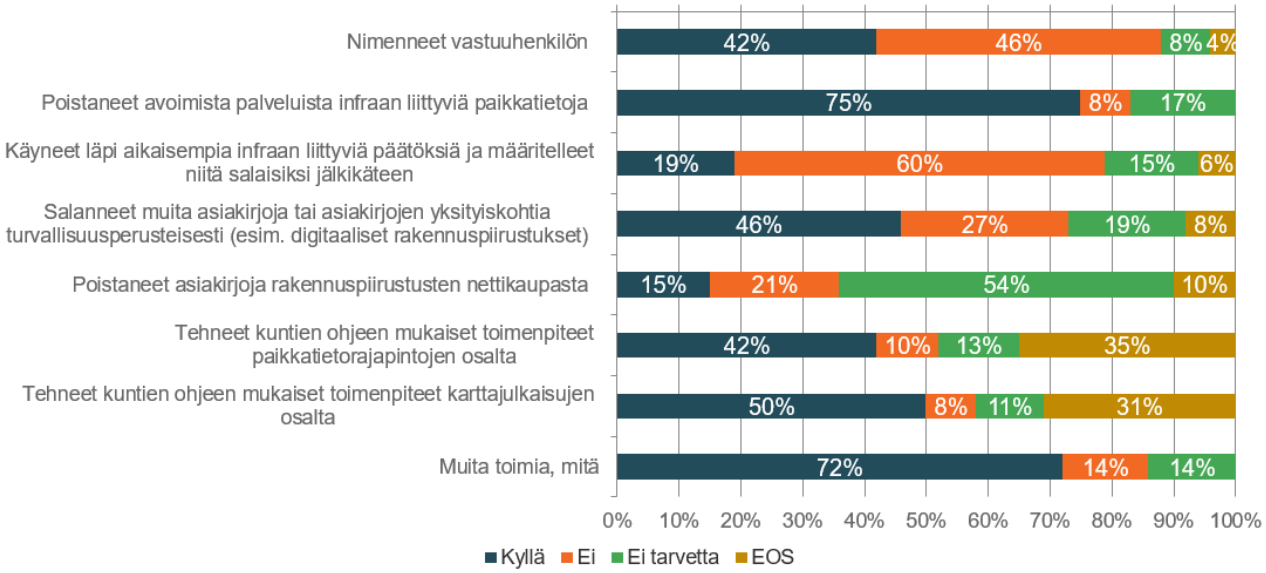
- 59 % vastanneista kunnista on ohjeistanut tietopyyntöjen käsittelyn dokumentoidusti.
- 44 % vastanneista kunnista tilastoi tietopyyntöjä.

Avoin palaute ja ajatuksia jatkotyöhön liittyen kriittisen infrastruktuurin avoimen tiedon hallintaan ja lainsäädäntötarpeisiin

- Julkisuuslain salassapitoperusteet eivät suojaa riittävästi kriittistä infrastruktuuria. Kuntien näkökulmasta salassapitoperusteiden käyttö on liian tulkinnanvaraista ja edellyttää konkreettista uhkaa.
- Tarve selkeille ohjeille ja kansallisille kriteereille siitä, mitä tietoa saa jakaa ja mitä ei – myös tekoälyn ja uusien teknologioiden näkökulmasta.
- Kuntaliitolta ja valtiolta toivotaan aktiivista ohjausta avoimen ja julkisesti saatavilla olevan tiedon jakamisen arviointiin.
- Tarve rajoittaa perusteettomia pyyntöjä ja kehittää prosesseja niiden käsittelyyn. Kunnat kaipaavat tukea, työkaluja ja rahoitusta kriittisen tiedon hallintaan.

- Nykyinen järjestelmä ei mahdollista kaikkien kuntien pääsyä turvallisuusselvitysmenettelyn piiriin, vaikka ne hallinnoisivat tai omistaisivat merkittävää kriittistä infrastruktuuria.

Mitä toimia kunnassanne on tehty turvallisen tiedonhallinnan varmistamiseksi?



Kuva 3: Kuntakyselyn tuloksia toimista, joita kunnissa on tehty turvallisen tiedonhallinnan varmistamiseksi.

3.4 Vesihuollon riskiarvioinnin pilotointi

Osana hankkeelle asetettuja välittömiä toimenpiteitä työryhmä käynnisti viiden kunnan pilotin, jossa arvioitiin vesihuollon avoimen tiedon jakamiseen liittyviä riskejä. Pilotti toteutettiin ajalla 29.4.–23.5.2025, ja sen tavoitteena oli tunnistaa mahdollisia riskejä sekä kerätä havaintoja ja kehitysehdotuksia toiminnan parantamiseksi.

Viiden kunnan edustajat ja kuntien alueella vesihuollosta vastaavat toimijat saivat hankkeelta tehtävänannon, jonka pohjalta käytiin keskustelua pilotin alustavista tuloksista. Myöhemmin osallistujat vielä täydensivät vastauksiaan. Tässä väliraportissa on kuvattu pilotin keskeiset havainnot. Pilotin toimeksiannossa kysyttiin seuraavia asioita:

Avoimen tiedon riskiarvioinnin nykytila

- Miten avoimen tiedon riskiarviointia on tähän mennessä tehty kunnassanne?
- Onko vesihuollon avoimen tiedon jakamisen riskejä arvioitu erikseen?
- Jos ei, onko näitä kysymyksiä käsitelty osana muuta työtä (esimerkiksi tietoturva, varautuminen, tiedonhallinta)?

Havaintoja vesihuollon avoimen tiedon riskiarvioinnista

Jos erillistä arviointia ei ole aiemmin tehty, toivomme, että sitä pilotoidaan hyödyntäen olemassa olevia arviointimenetelmiä. Vastauksissa voi käsitellä seuraavia:

- Mitä avointa tietoa on tunnistettu (yleisellä tasolla, ei yksityiskohtia)?
- Mitkä ovat suurimmat riskit kriittisen infrastruktuurin näkökulmasta?

- Mitä haasteita riskiarvioinnissa on ilmennyt (esimerkiksi päällekkäisyydet avoimen tiedon ja alueellisen riskiarvion välillä)?
- Millainen yhteistyö on ollut muiden toimijoiden (esimerkiksi rakennusvalvonta) kanssa? Mitä havaintoja ja kehittämistarpeita on noussut esiin?
- Millainen tukimateriaali on ollut käytössä? Mitä puutteita tai kehitysehdotuksia siihen liittyy?

Muut kehittämisehdotukset ja toiveet hankkeen suhteen

- Onko muita huomioita, joita haluatte tuoda esiin liittyen avoimen tiedon hallintaan, riskiarviointiin tai hankkeen jatkoon?

Riskiarvioinnin nykytila

Pilottikaupungit ovat hyödyntäneet paikkatiedon riskien arviointiin laadittua ohjeistusta vaihtelevasti. Vesihuoltoa tarkastellaan osana kriittisen infrastruktuurin paikkatietokokonaisuutta, ja avoimen tiedon jakamiseen liittyvät riskit ovat monin paikoin tiedostettuja. Arviointia tehdään tapauskohtaisesti eri tilanteissa ja työtehtävissä, ja se voi kattaa esimerkiksi tietoturvaan, tietosuojaan ja luottamuksellisen tiedon käsittelyyn liittyviä näkökulmia.

Tunnistettu avoin tieto

Avoimesti saatavilla olevia tietoja ovat esimerkiksi vesihuollon toiminta-alueet, päätökset, lupapäätökset, lausunnot, raportit ja yritysten verkkosivut. Tietopyynnöt ovat ajoittain haasteellisia. Myös selvitysraportit, suunnitelmat ja tutkimusjulkaisut voivat sisältää suojaamattomia kriittisiä paikkatietoja. Julkiset karttapalvelut ja paikkatietorajapinnat on karsittu ja karkeutettu ohjeistuksen mukaisesti. Ongelmia aiheuttavat myös kaavoituksen ja infran suunnittelun päätösten liitteet sekä kilpailutusten taustamateriaalit.

Suurimmat riskit

Organisaatioilla ei aina ole tarkkaa tietoa siitä, mitä vesihuoltoon liittyvää tietoa viranomaiset jakavat. Tämä voi johtaa salassa pidettävän tiedon päätymiseen vääriin käsiin ja mahdollistaa vahingontekojen suunnittelun. Esimerkiksi erään suuren kaupungin karttapalveluun kohdistuu viikoittain noin 100 000 kyselyä ja avoimiin rajapintoihin noin 200 000. Venäjän aloittaman hyökkäyssodan jälkeen kyselymäärät ovat kasvaneet jopa kymmenkertaisiksi, mikä viittaa mahdollisiin palvelunestohyökkäyksiin tai hybridivaikuttamiseen. Yhdistämällä avointa tietoa voidaan muodostaa kokonaiskuva kriittisistä toiminnoista.

Haasteet riskiarvioinnissa

Kunnat pyrkivät rajoittamaan kriittisen datan jakelua, mutta valtion virastot ja yhtiöt voivat julkaista tietoa omassa toiminnassaan. Myös yksityiset toimijat, kuten Google, OpenStreetMap ja konsultit jakavat tietoa hallitsemattomasti. Pilottiin osallistuneiden kuntien mukaan tarvitaan valtionhallinnon yhtenäistä ohjeistusta ja mahdollisesti lakimuutoksia. Tiedon jakamisen ja suojaamisen välinen jännite on tunnistettu ja huomioitu päivittäistoiminnassa.

Tukimateriaali ja kehitysehdotukset

Pilottiin osallistuneiden kuntien näkökulmasta riskiarvioinnin yhtenäistäminen viranomaisten kesken olisi hyödyllistä. Yhteistyö esimerkiksi rakennusvalvonnan kanssa toisi lisäarvoa. Kuntaliiton ohjeistus toimii, mutta se on vain rajatussa käytössä eikä jaettavissa muille viranomaisille. Yhtenäinen ja perusteltu ohjemateriaali, joka olisi jaettavissa laajasti, helpottaisi kriittisten kohteiden tietojen hallintaa. Tarvitaan myös valtakunnallista koulutusta ja yhteinen arviointimatriisi. Tietopyyntöjen käsittely perustuu julkisuuslakiin, jonka avoimuusperiaate ei kaikilta osin huomioi kuntien tarpeita suojata kriittiseen infrastruktuuriin liittyviä tietoja. Tämä voi johtaa tilanteisiin, joissa tietopyynnöt vaarantavat turvallisuuskriittisen tiedon suojaamisen. Valtionhallinnolla ei ole vastaavaa konkreettista ohjeistusta, ja myös konsulttitoimijat tarvitsisivat velvoittavaa ohjeistusta. Vesihuollossa on jo olemassa tietoa rajaava toimintakulttuuri, mutta sen tueksi tarvitaan selkeitä linjauksia ja ohjeita.

4 VÄLITAVOITE 2: Tilannekuva avoimen ja julkisesti saatavilla olevan tiedon riskeistä

4.1 Tilannekuvan muodostaminen

Toista välitavoitettaan varten työryhmä kartoitti kriittisen infrastruktuurin avoimesti ja julkisesti saatavilla olevan tiedon riskejä ja tarkasteli niitä kansallisen turvallisuuden näkökulmasta. Työryhmän tilannekuvan näkökulma on siten uhkien ja riskien kautta hahmottuva ilmiötaso, joka ei pyri kaiken kattavaan tai yksityiskohtaiseen riskiarviointiin. Arvioitaessa kansallisen turvallisuuden kannalta merkittävän kriittisen infrastruktuurin avoimen ja julkisesti saatavilla olevan tiedon riskejä, **työryhmä lähti liikkeelle siitä avoimesti ja julkisesti saatavilla olevasta tiedosta, joka liittyy kriittisen infrastruktuuriin ja jatkoi aiheen tarkastelua kansallisen turvallisuuden näkökulmasta.**

Seuraava vaihe oli pohtia sitä, **miten tällainen edellä kuvattu avoin ja julkisesti saatavilla oleva tieto voisi edesauttaa sellaisen kansallista turvallisuutta vakavasti uhkaavan toiminnan toteutumista**, joka kohdistuu kriittiseen infrastruktuuriin. Kansallisen riskiarvion uhkamallit ovat yksi esimerkki siitä, miten tällainen toiminta voi ilmentyä ja millaisia muotoja se voisi ottaa. **Lopuksi tilannekuvatyössä keskityttiin tunnistamaan niitä poikkileikkaavia riskejä**, jotka kytkeytyvät erityisesti kansallisen turvallisuuden kannalta olennaisen kriittisen infrastruktuurin avoimesti ja julkisesti saatavilla olevan tiedon vihamieliseen hyödyntämiseen keskeisiä kansallisia suojattavia etujamme vastaan.

Kuva 4: Esitys siitä, mihin hankkeen tilannekuvatyössä keskityttiin. Tarkastelun lähtökohtana oli avoimesti saatavilla oleva tieto, ja sen perusteella arvioitiin, miten tällainen tieto voisi mahdollistaa kansallista turvallisuutta vakavasti uhkaavaa toimintaa, joka kohdistuu kriittiseen infrastruktuuriin tai hyödyntää sitä.

Työryhmä lähestyi aihepiiriä sekä kohde- että uhkalähtöisesti. *Kohdelähtöistä* näkökulmaa rajasi hankkeen työmääritelmä kriittisestä infrastruktuurista sekä edelleen CER-direktiivin toimeenpanolain myötä tapahtuva sektori- ja vaikuttavuustarkastelu. *Uhkien kautta tapahtuvaa tarkastelua* taas edusti näkökulma, missä avoimen tiedon jakaminen otettiin lähtökohdaksi sille pohdinnalle, miten avoimesti ja julkisesti saatavilla oleva tieto voisi osaltaan mahdollistaa kansallista turvallisuutta vakavasti uhkaavaa toimintaa, joka kohdistuu tai hyödyntää kriittisen infrastruktuurin kohteita.

Työryhmän alustavan selvitystyön pohjalta kansallisen turvallisuuden kannalta merkittäviä kriittinen infrastruktuurin avoimesti ja julkisesti saatavilla olevan tiedon jakamiseen liittyviä keskeisiä sekä poikkileikkaavia riskejä ovat:

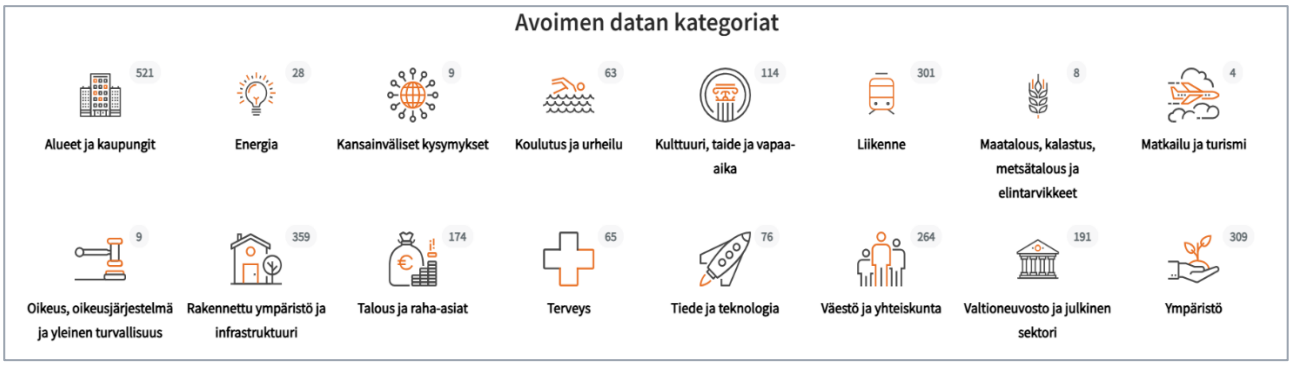
- Kriittiseen henkilöstöön liittyvä avoin ja julkisesti saatavilla oleva tieto
- Ei-digitaalinen avoin ja julkisesti saatavilla oleva tieto
- Yhdisteltävyys
- Kasautuminen
- Tiedon kriittisyyden muutos ajassa (riskien kehittymisen osalta)
- Tekoälyn hyödyntäminen
- Tiedon keruun volyymi ja joukkoistus
- Tiedon kerääminen maastosta
- Tiedon tarkoitushakuinen kerääminen ja yhdistely

4.2 Keskeisiä avointen ja julkisesti saatavilla olevien tietovarantojen riskejä

4.2.1 Kategorioittain jaoteltuja riskiesimerkkejä

Hankkeen työryhmän 26.3.2025 pidetyssä tilannekuvatyöpajassa tunnistettiin avoimesti ja julkisesti saatavilla olevia tietovarantoja sekä näihin liittyviä riskejä, jotka voivat vaikuttaa kansalliseen turvallisuuteen. Tämänkaltaiset avoimesti ja julkisesti saatavilla olevat tietovarannot voivat yhdessä tai kontekstuaalisesti yhdistettyinä auttaa vihamielisiä toimijoita esimerkiksi kartoittamaan kriittisiä kohteita (energiaverkot, logistiikkareitit), suunnittelemaan häiriötoimia (kyber- tai fyysiset hyökkäykset) tai arvioimaan yhteiskunnan resilienssiä.

Työpajan työskentelyssä nousseita esimerkkejä verrattiin avoimen datan tietoluokkiin. Avoin data on jaettu avoindata.fi -sivustolla esitetyn mukaisesti seuraaviin tietoluokkiin:



Kuva 5: Avoindata.fi -palvelun ylimmän tason tietoluokat

Tietoluokkia on hyödynnetty tässä väliraportissa tietovarantojen luokittelun selkeyttämiseksi. Työpajan esimerkit on koostettu näiden kategorioiden alle. Kaikki esimerkit eivät ole välttämättä saatavilla avoindata.fi -sivustolta.

Valtioneuvosto ja julkinen sektori

- Tietokategoria: Julkisen hallinnon organisaatiorakenteet ja toimipisteet.
- Riski: Tietoa viranomaisten sijainneista, mikä voi paljastaa keskeisiä hallinnon solmukohtia, ja julkisen hallinnon organisaatiorakenteita.

Liikenne

- Tietokategoria: Tieverkko-, rataverkko- ja satamatiedot.
- Riski: Tietoa siitä, miten kriittiset kuljetukset liikkuvat. Esimerkiksi polttoaine- ja elintarvike-kuljetusreitit, raideyhteydet satamiin.

Ympäristö

- Tietokategoria: sää- ja meriolosuhteisiin liittyvät havainnot ja ennusteet, maanjäristysdata, tulvariskialueet, mittausinfrastruktuurin tekniset tiedot ja sijaintitiedot.
- Riski: Sään tai luonnonilmiöiden vaikutusten analysointi kriittiseen infrastruktuuriin. Vaikuttamisen ajoittaminen saadun tiedon pohjalta. Esimerkiksi myrskyt sähköverkkoa vastaan, tulvavauhkat vedenpuhdistamoille.

Energia

- Tietokategoria: Julkaisut sähkön siirtoverkoista ja uusiutuvan energian tuotantopaikoista
- Riski: Sähköverkon rakenteet, muuntamoiden sijainnit ja siirtokapasiteetit voivat paljastaa haavoittuvuuksia energiahuollossa.

Terveys

- Tietokategoria: Avoimet tilastot terveydenhuollon kapasiteetista ja alueellisista palveluista
- Riski: Tietoa sairaaloiden sijainneista ja kuormituksesta voi käyttää arvioitaessa hätävalmiutta tai pandemiatilanteiden hallintaa.

Rakennettu ympäristö ja infrastruktuuri

- Tietokategoria: Maastotietokanta, rakennusten sijainti ja käyttötarkoitukset, OpenStreetMap-sovellus aineistoineen, alueidenkäytön suunnittelun prosesseihin liittyvät kuulemiset, joita käydään avoimessa verkossa ja sen yhteydessä jaettavat infrakohdetiedot.
- Riski: Karttapohjainen tieto kriittisten rakennusten sijainnista voi helpottaa vihamielistä kartoitusta.

Talous ja raha-asiat

- Tietokategoria: Yritysrekisteritiedot, suurimmat työnantajat ja tuotantolaitokset, yritysten jakamat avoimet tiedot toiminnastaan, sijaintikohteistaan ja yhteistyökumppaneistaan nettisivuillaan, julkisten hankintojen kautta avoimesti saatavilla olevat tiedot voivat liittyä myös kansallisen turvallisuuden kannalta merkitykselliseen kriittiseen infrastruktuuriin.
- Riski: Tiedot suurista työllistäjistä ja tuotantoketjuista voivat osoittaa taloudellisesti kriittisiä kohteita tai alihankintaketjuja.

Tiede ja teknologia

- Tietokategoria: Korkeakoulujen tutkimusinfrastruktuurit, laboratorioiden sijainnit, satelliittiyritykset, joilta voi ostaa tietoa, pistepilviaineistot, joita kerätään erilaisten keilausten yhteydessä.
- Riski: Tiedot kriittisten tutkimuslaitosten sijainnista voivat olla kiinnostavia uhkatoimijoille.

Oikeus, oikeusjärjestelmä ja yleinen turvallisuus

- Tietokategoria: Poliisilaitosten ja oikeuslaitosten sijaintitiedot, oikeustapauksien tilastot
- Riski: Tietoa oikeusjärjestelmän rakenteesta ja fyysisistä toimipisteistä, jotka voivat vaikuttaa yhteiskunnan toimintakykyyn kriisitilanteessa.

Kulttuuri, taide ja vapaa-aika

- Tietokategoria: Tapahtumatiedot, väestötilastot tietyiltä alueilta, museot ja muut julkiset kokoontumispaikat, pelillistämisen kautta tapahtuva tiedon kerääminen.
- Riski: Suurten kokoontumisten ennustettavuus voi liittyä väestönsuojeluun ja joukkoturvallisuuteen esimerkiksi uhkatilanteissa.

4.2.2 Kriittiseen henkilöstöön liittyvä avoin ja julkisesti saatavilla oleva tieto

Kriittiseen henkilöstöön liittyvä avoimesti ja julkisesti saatavilla oleva tieto voi avata sellaisia haavoittuvaisuuksia, jotka osaltaan kytkeytyvät kansallisen turvallisuuden kannalta kriittisiin kohteisiin, toimintoihin tai virtoihin.

Keskeisiä keinoja tiedustella ja vaikuttaa kriittiseen henkilöstöön ovat muun muassa:

- Henkilöprofilointi: Julkisesti saatavilla oleva tieto (esimerkiksi LinkedIn, uutiset, haastattelut) mahdollistaa kriittisten henkilöiden tunnistamisen ja analysoinnin.
- Sosiaalinen manipulointi (social engineering): Avoimesti ja julkisesti saatavilla olevan tiedon avulla voidaan kohdentaa huijauksia, kuten tietojenkalastelua tai valehenkilöllisyyksiä.
- Verkostojen kartoitus: Organisaatioiden sisäisten ja ulkoisten suhteiden kartoittaminen voi, helpottaa vihamielisen vaikuttamisen suunnittelua.
- Toimintojen häirintä: Henkilöstön kautta voidaan vaikuttaa kriittisiin toimintoihin, kuten infrastruktuuriin, tietojärjestelmiin tai päätöksentekoon.

Kriittinen henkilöstö voi joutua kohdennettujen kyberhyökkäysten (esimerkiksi spear phishing) tai erilaisten sisäpiiririskien (esimerkiksi rekrytointi, kiristys, vaikuttaminen) kohteeksi. Onnistuessaan tällainen vaikuttaminen voi johtaa kriittisen henkilöstön toimintakyvyn heikentymiseen, jos esimerkiksi henkilöstöä häiritään, manipuloidaan tai kriittistä tietoa vuodetaan ulos organisaatiosta. Henkilöstön suojaamiseen erittäin kriittisissä tehtävissä voi kuulua nimettömyyden ja yksityisyyden turvaaminen työantajan puolelta.

4.2.3 Ei-digitaalinen avoin ja julkisesti saatavilla oleva tieto

Ei-digitaalinen, mutta avoin ja julkisesti saatavilla oleva tieto kriittisestä infrastruktuurista voi aiheuttaa merkittäviä riskejä kansalliselle turvallisuudelle useilla tavoilla – erityisesti silloin, kun se yhdistyy digitaaliseen tiedusteluun tai fyysisiin uhkiin. Painetut kartat, rakennuspiirustukset tai tekniset dokumentit voivat sisältää tietoa kriittisten kohteiden sijainnista, rakenteista tai huoltoyhteyksistä (esimerkiksi vesijohtoverkosto, sähkölinjat, tunnelit). Tällainen tieto voi päätyä vääriin käsiin esimerkiksi kirjastoista, rakennustyömailta tai arkistoista. Vanhemmat, mutta edelleen relevantit tiedot voivat olla saatavilla kirjastoissa, yliopistoissa tai viranomaisarkistoissa. Tiedon yhdisteltävyys voi tässäkin yhteydessä paljastaa haavoittuvuuksia, joita ei yksittäisinä lähteinä tunnistettaisi.

Paperimuotoiset aineistot jäävät helposti arvioinnin ulkopuolelle. Koska viranomaisten tiedonhallinta ja riskiarviointi keskittyvät usein sähköisiin järjestelmiin ja digitaalisesti jaettaviin tietoihin, eivät paperimuotoiset aineistot tule aina luonnostaan osaksi arviointia. Tämä voi johtaa siihen, että niiden sisältämät kriittiset tiedot jäävät suojaamatta tai niiden jakamisen vaikutuksia ei arvioida systemaattisesti. Paperimuotoisuus itsessään voi lisätä riskiä tietyissä tilanteissa. Esimerkiksi, jos paperiaineistoja säilytetään ilman asianmukaista valvontaa tai ne ovat helposti kopioitavissa ja levitettävissä, ne voivat muodostaa tietoturva- tai turvallisuusriskin – erityisesti silloin, kun ne sisältävät kriittiseen infrastruktuuriin liittyvää tietoa. Tämä riski ei kuitenkaan liity pelkästään siihen, että aineisto on paperilla, vaan siihen, mitä tietoa se sisältää ja miten sitä käsitellään.

4.2.4 Yhdisteltävyys

Yksittäinen tieto ei välttämättä ole vaarallinen, mutta yhdisteltäessä useista avoimesti ja julkisesti saatavilla lähteistä olevia tietoja, voi olla mahdollista selvittää kriittisiä haavoittuvuuksia. Yhdisteltävyys kasvattaa avoimesti saatavilla olevan tiedon käyttöarvoa. Eri tietovarantoja yhdistelemällä voidaan tunnistaa vaikuttavuuspolkuja ja riippuvuuksia. Tiedon yhdisteltävyys lisää riskiä, että vihamielinen toimija saa kokonaiskuvan järjestelmästä. Paikkatietojen yhdistämisessä voidaan hyödyntää rinnakkain eri sijaintia tai ominaisuutta kuvaavia tietoja, kuten yksilöiviä tunnuksia, koordinaatteja tai osoitetietoja.

4.2.5 Kasautuminen

Tiedon kasautumisella tarkoitetaan tiettyjen teemojen ajallisen ja maantieteellisen kattavuuden kasvamista. Kasauma voi muodostua lyhyellä aikajänteellä harvoista tietolähteistä tai pitkällä aikavälillä useista tietolähteistä. Kasauman muodostumista voidaan rajoittaa pitämällä aineistot teknisesti erillään toisistaan, siten ettei niitä ole helposti saatavilla kerralla tai luovuttamalla aineistoa tapauskohtaisesti vain rajatulta alueelta ja ajalta. Erillään pito voidaan toteuttaa yhdessä tai useammassa organisaatiossa hajauttamalla tieto eri tietovarantoihin, joissa on eri teknologiat ja käyttäjähallintamenettelyt. Tietoja voidaan luovuttaa rajatusti pala kerrallaan, jolloin tiedon pyytäjälle ei kerry tietoa niin nopeasti, että kasauma muodostuisi helposti.

Avoimesti ja julkisesti saatavilla oleva tieto voi kasautua ajan myötä siten, että sen kokonaismerkitys muuttuu. Yksittäiset datapisteet voivat muodostaa ajan kuluessa strategisesti arvokkaan kokonaisuuden, jota voidaan hyödyntää haitallisesti. Pitkän aikavälin paikkatietojen julkaisu voi paljastaa kriittisen infrastruktuurin kehityssuunnan ja laajennukset.

Tieto voi kasaantua myös pelillistämisen keinoin, jolloin esimerkiksi saman teeman tai rakenteiden kerääminen pelin avulla – joskus nopeastikin – yhteen paikkaan ja avoimesti katsottavaksi ja hyödynnettäväksi, voi kasata tietoa kriittisestä infrastruktuurista siitäkin huolimatta, että pelin alkuperäinen tarkoitus on ollut vaaraton.

Yksittäiset julkiset tiedot eivät muodosta salassa pidettävää kokonaisuutta, vaikka niitä olisi suuri määrä. Tämä tarkoittaa, että esimerkiksi verkkotietojen suojaaminen ei voi perustua pelkästään siihen, että tietoa on paljon – vaan edellyttää, että tiedot luokitellaan erikseen salassa pidettäviksi julkisuuslain mukaisesti. Ilman tätä luokittelua tietojen suojaaminen ei ole oikeudellisesti perusteltua, vaikka niiden yhdistäminen voisi käytännössä aiheuttaa turvallisuusriskejä.

4.2.6 Tiedon kriittisyyden muutos ajassa

Tiedon arvo muuttuu ajassa eikä tiedon turvallisuusluonne ole pysyvää. Aikamuuttuja voi heikentää yksittäisen aikapisteen tiedon luotettavuutta tai mahdollistaa tiedon kertymisen

historiatiedoksi, jolloin ilmiöiden kehittymistä voidaan analysoida pidemmillä aikajänteillä. Toinen vaikutus ajalla on, että aiemmin harmittomaksi arvioitu tieto voi ajan kuluessa muuttua riskiksi toimintaympäristön tai teknologian kehittyessä. Kerran avattu ja luovutettu tieto on hyödynnettävissä myöhemmin, eikä mahdollisesti ajan kanssa kehittyvää riskiä voida enää poistaa kokonaan.

Turvallisuustilanteen muutos voi myös muuttaa salassapitovelvoitteiden tulkintaa. Tiedon formaatit tai tarkkuudet muuttuvat, jolloin hyödyntämisessä ilmenee myös uusia riskejä. Uudenlaisia ristiriitatilanteita voi ilmetä tulevaisuudessa, mikäli huomataan joidenkin kriittisen infrastruktuurin avoimesti ja julkisesti saatavien tietojen avoimuuden olevan edellytys vaikkapa tiettyjen palveluiden digitaaliselle kehittymiselle ja tehostamiselle. Näin esimerkiksi rakennuslupatiedot, jotka eivät aiemmin olleet arkaluonteisia, voivat muuttua kriittisiksi uuden infrastruktuurihankkeen myötä. Lisäksi kerran julkistetun ja yhä avoimesti saatavilla olevan avoimen ja julkisesti saatavilla olevan tiedon säilyminen voi muodostaa merkittäviä riskejä kansallisen turvallisuuden näkökulmasta, erityisesti digitaalisessa ympäristössä, jossa tieto ei unohdu.

Tiedon tarkkuuden ja rakenteen muutos lisää riskejä. Aiemmin staattisessa muodossa julkaistut tiedot (esimerkiksi karttakuvat tai PDF-muotoiset suunnitelmat) voivat muuttua turvallisuusnäkökulmasta merkittäviksi, kun ne muunnetaan rakenteiseen, koneluettavaan muotoon, kuten esimerkiksi 3D-kaupunkimalleiksi. Nämä mahdollistavat yksityiskohtaisen analyysin kriittisistä rakenteista ja voivat paljastaa haavoittuvuuksia, joita ei aiemmin ollut mahdollista havaita.

4.2.7 Tekoälyn hyödyntäminen

Nykyaikaisilla tekoälytyökaluilla (suuret kielimallit, LLM) voidaan yhdistellä suuria tietomääriä, jolloin eri ilmiöitä voidaan analysoida tehokkaasti ja luovasti. Tekoälyllä nopeutetaan tekstipohjaisen ja kuvallisen paikkatiedon luokittelua, yhdistämistä ja ristiin analysointia. Näin tekoäly voi esimerkiksi analysoida avoimesti ja julkisesti saatavilla olevia paikkatietoja ja tunnistaa sitä kautta kriittisiä solmukohtia infrastruktuuriverkossa. Tämä voi paljastaa haavoittuvuuksia, joita ihmisanalyysi ei havaitsisi, ja nopeuttaa vihamielisen toiminnan suunnittelua.

Tekoäly tuottaa nykyisin myös virhetulkintoja, mutta laajemmassa kuvassa oikeaan suuntaan meneviä päätelmiä. Tekoälyä voidaan hyödyntää myös miehittämättömien maa-, vesi- ja ilmalaitteiden autonomisessa käytössä. Tekoälyn viime vuosien nopea kaupallinen kehitys on esimerkki uuden teknologian tuomasta riskistä, jota ei aiemmin ole osattu ennakoida tiedon avaamiseen liittyvässä päätöksenteossa. Internet on luonteeltaan avoin, ja sieltä saatava valtava tietomäärä on ollut keskeinen työkalu nykyaikaisten suurten kielimallien koulutuksessa.

Yksi merkittävä riski liittyy siihen, että käyttäjä voi tietämättään syöttää salaiseksi luokiteltua tietoa avoimessa internetissä toimiville generatiivisille tekoälypalveluille. Näitä palveluita kehittävät yritykset keräävät laajasti verkossa julkaistua sisältöä tekoälytuotteidensa kouluttamiseen. Tämän vuoksi myös sellainen tieto, joka on julkaistu vain hetkellisesti tai sittemmin poistettu, on voinut päätyä tekoälysovellusten käyttöön. Tekoälyä voidaan hyödyntää esimerkiksi tietopyyntöjen tekemiseen julkiseen tietoon, sillä lainsäädäntö ei edellytä pyytäjän tunnistautumista. Näin ollen tekoälyllä on periaatteessa pääsy kaikkeen julkiseen tietoon, vaikka sitä ei olisi julkaistu avoimena datana internetissä.

Tekoälyn avulla voidaan myös automatisoida tietopyyntöjä. Tulevaisuudessa on mahdollista, että tekoälyn (robottien) avulla laaditaan kohdennettuja tietopyyntöjä toistuvasti, mikä haastaa julkisen ja avoimen datan välistä eroa ja työllistää organisaatioita, jotka joutuvat käsittelemään tietopyyntöjä.

4.2.8 Tiedon keruun volyymi ja joukkoistus

Teknologian kehitys on mahdollistanut tiedonkeruun volyymin kasvun hyvin suureksi. Joukkoistettu tiedonkeruu voi tuottaa yksityiskohtaista ja ajantasaista tietoa, jota viranomaiset eivät hallitse ja jonka viranomainen saattaisi jättää julkaisematta. Esimerkiksi harrastajaverkostot voivat kerätä ja julkaista tietoa kriittisistä kohteista valokuvaamalla laitoksia drooneilla. Tämä voi johtaa siihen, että kriittistä tietoa päätyy julkisuuteen ilman turvallisuusnäkökulmien riskiperusteista arviointia. Tämä vaikeuttaa tiedon avoimuuden arviointia ja hallintaa.

Nykyinen satelliittikuvien laaja saatavuus avoimista karttapalveluista muodostaa haasteen kohteiden suojaamiselle. Tämä kehitys korostaa tarvetta panostaa rakenteelliseen suojaamiseen, valvontaratkaisuihin ja nopeaan reagointikykyyn. Näillä keinoilla voidaan hallita riskejä, joita syntyy, kun yksityiskohtainen paikkatieto on yhä helpommin saatavilla ja yhdistettävissä muihin tietolähteisiin.

Ilmakuvaus- ja laserkeilaushankkeiden lupamenettelyt eivät tällä hetkellä koske kaikkia toimijoita samalla tavalla. Julkiset toimijat, kuten kunnat ja viranomaiset, tarvitsevat Puolustusvoimien luvan laajamittaiseen ilmakuvaukseen tai laserkeilaukseen, erityisesti jos toiminta kohdistuu alueisiin, joilla voi olla maanpuolustuksellista merkitystä.[8] Sen sijaan yksityiset tiedonkerääjät eivät aina kuulu saman lupamenettelyn piiriin, mikä voi johtaa epätasapainoon tiedonkeruun valvonnassa ja turvallisuudessa. Tämä herättää kysymyksen siitä, pitäisikö lupakäytännöt yhdenmukaistaa, jotta kaikki toimijat – julkiset ja yksityiset – toimisivat samojen pelisääntöjen mukaan, erityisesti kansallisen turvallisuuden näkökulmasta.

4.2.9 Tiedon kerääminen maastosta

Tarkkaa sijaintitietoa voidaan kerätä tiedustelutarkoituksessa maastokäynneillä, ja GNSS-järjestelmien (esimerkiksi GPS, Glonass, Galileo) avulla tuotettua dataa voidaan käyttää aiemmin kerättyjen karttatietojen varmentamiseen tai yhdistämiseen. Näin voidaan muodostaa tarkkoja koordinaattitietoa esimerkiksi kriittisten kohteiden maalittamista varten. Historiallisesti on osoitettu, että laajoja ja tarkkoja kartta-aineistoja on pystytty tuottamaan jo ennen nykyisiä satelliittipaikannusjärjestelmiä – esimerkiksi kylmän sodan aikaisessa tiedustelutoiminnassa.[9]

4.2.10 Tiedon tarkoitushakuinen kerääminen ja yhdistely

Toimintaa, missä avoimesti ja julkisesti saatavilla olevaa tietoa kerätään, yhdistellään ja tallennetaan järjestelmällisesti tarkoituksena valmistella tai mahdollistaa kansallista turvallisuutta vakavasti uhkaavaa toimintaa, voidaan kutsua oikeudettomaksi tiedonhankinnaksi. Vaikka tieto olisi julkista tai avointa, sen tarkoitushakuinen kerääminen ja yhdistely voi rikkoa hybridivaikuttamisen torjuntaan liittyviä normeja, täyttää rikoksen valmistelun tai törkeän tietojärjestelmän häirinnän

tunnusmerkistön, jos tiedonkeruu liittyy hyökkäyksen suunnitteluun tai johtaa turvallisuusluokitellun tiedon paljastumiseen epäsuorasti yhdistelyn kautta.

4.3 Haasteita ja huomioitavia seikkoja avoimen ja julkisen tiedon riskien arvioinnissa

Avoimen tiedon julkaisun tarpeellisuuden ja väärinkäytettävyyden tulkinta

Joidenkin aineistojen osalta tiedon julkaisun tarpeellisuutta voi olla vaikea mitata tai muutoin määrittää. Sama pätee aineistojen väärinkäytettävyyteen. Tästä syystä kaksi toimijaa voi päätyä erilaisiin

[8] https://puolustusvoimat.fi/ilmakuvauslupa
[9] https://www.wired.com/2015/07/secret-cold-war-maps/

tulkintoihin ja yksi toimija voi päätyä avaamaan saman tiedon, jonka toinen toimija pyrkisi suojaamaan. Avaamispäätös voi johtua myös ajatuksesta, että tietoa ei kannata yrittää suojata, kun se on muutenkin löydettävissä. Tämä ei kuitenkaan ole kestävä peruste tiedon julkistamiselle. Se, että tieto on aiemmin ollut saatavilla tai on jossain muodossa löydettävissä, ei poista viranomaisen vastuuta arvioida sen ajankohtaista turvallisuus- tai salassapitotarvetta. Tietojen avoimuutta tulee arvioida aina kulloisenkin kontekstin, käyttötarkoituksen ja riskien perusteella. Aiempi jakaminen ei automaattisesti tarkoita, että tiedon julkistaminen olisi edelleen perusteltua – erityisesti, jos olosuhteet, teknologiset mahdollisuudet tai turvallisuusympäristö ovat muuttuneet.

Kaikki avoin ja julkisesti saatavilla oleva tieto ei ole yksiselitteisesti hyödyllistä tai haitallista. Tiedon julkaiseminen vaatii tasapainottelua hyötyjen ja väärinkäytön mahdollisuuksien välillä – virheellinen tulkinta voi johtaa joko tarpeettomaan rajoittamiseen tai vaaralliseen avoimuuteen. Esimerkiksi lentoesteiden sijaintitiedot ovat turvallisuuden kannalta välttämättömiä, mutta voivat myös paljastaa kriittisiä rakenteita.

Avoimen tiedon jakamatta jättäminen

Tiedon salaaminen voi itsessään aiheuttaa riskejä, jos se estää turvallisen toiminnan tai vahinkojen ehkäisyn. Tiedon rajoittaminen voi olla yhtä haitallista kuin sen liiallinen avoimuus. Vaikka osa kriittisen infrastruktuurin tiedoista voi muodostaa turvallisuusriskin, niiden liiallinen rajoittaminen voi aiheuttaa haittaa palveluiden kehittämiselle, kuten liikenteen, rakentamisen tai pelastustoimen digitaalisille ratkaisuille. Tutkimus ja innovaatio, jotka perustuvat avoimeen dataan voi hidastua. Esimerkiksi sähkö- tai tietoliikennekaapeleiden sijaintia koskevien tietojen puuttuminen voi johtaa maalla henkilö- tai omaisuusvahinkoihin kaivuutöiden yhteydessä, tai merellä kriittisten kansainvälisten yhteyksien katkeamiseen. Merikaapelit voivat aiheuttaa myös turvallisuusriskin esimerkiksi troolikalastusta harjoittaville aluksille, mistä syystä niiden sijaintitietojen pitäisi olla ainakin jollain tasolla tiedossa julkisissa merikartoissa

Samalla on tärkeää muistaa, että avoimuus on demokraattisen yhteiskunnan perusta. Kansalaisten oikeus seurata päätöksentekoa ja viranomaistoimintaa edellyttää mahdollisimman laajaa tiedonsaantia. Siksi tiedon julkisuutta ja salassapitoa on punnittava huolellisesti – ei vain teknisin perustein, vaan myös yhteiskunnallisen luottamuksen ja turvallisuuden näkökulmasta. Tiedonhallinnan tavoitteena tulisi olla tasapaino: suojata aidosti kriittinen tieto, mutta samalla turvata avoimuus ja läpinäkyvyys siellä, missä se on perusteltua ja turvallista.

Avoimen ja julkisesti saatavilla olevan tiedon suojaaminen

Avoimen tiedon rajaaminen ja kohteiden suojaaminen on keskeinen osa kansallisen turvallisuuden varmistamista. Suojaamistoimet voivat kuitenkin paradoksaalisesti paljastaa suojattavat kohteet, altistaen ne maalittamiselle tai häirinnälle – esimerkiksi droonitiedustelun avulla. Karttapalveluista poistettavat kriittiset kohteet, kuten infrastruktuuri tai kaapelireitit, kytkeytyvät tietoaineistojen vastuukysymyksiin sekä tiedonhallinnan toimenpiteisiin. Liiallinen suojaaminen voi myös vaikeuttaa viranomaisten toimintaa tai herättää tarpeetonta huomiota. Yksittäisten kohteiden suojaamisen sijaan tulisi painottaa laajempaa toimintaympäristöanalyysiä, jossa huomioidaan myös viranomaisten vasteen testaamiseen liittyvät riskit ja vaikutukset.

5 Jatkotyössä huomioitavia seikkoja

5.1 Työn kannalta ajankohtaisia hankkeita

Parhaillaan on käynnissä useita hankkeita, joilla on vaikutusta tämän hankkeen toteutukseen. Nämä hankkeet voivat vaikuttaa suoraan kriittiseen infrastruktuuriin, sen tietopohjaan ja tiedonhallintaan.

Lisäksi näiden hankkeiden kautta on mahdollista tunnistaa käytännön kehityssuuntia, mahdollisia riskejä sekä yhteensovittamisen tarpeita, jotka voivat vaikuttaa tiedon avoimuuteen, turvallisuuteen ja viranomaisten toimintaympäristöön. Seuranta tukee myös kokonaiskuvan muodostamista ja varmistaa, että työryhmän suositukset ovat ajantasaisia ja yhteensopivia muiden käynnissä olevien prosessien kanssa.

Erityisesti kansallisen turvallisuuden strategian eteneminen sekä EU:n CER-direktiivin kansallinen täytäntöönpano vaikuttavat suoraan hankkeen tehtävien toteutukseen. Lisäksi seurataan muita samanaikaisia hankkeita, joilla voi olla merkitystä työn etenemisen ja yhteensovittamisen kannalta.

Valtioneuvoston turvallisuusjohtamisen toimintamallin kehittämishanke toimeenpanee pääministeri Orpon hallitusohjelman keskeiset turvallisuusjohtamista koskevat kirjaukset. Hankkeen alatyöryhmissä on uudistettu Suomen kyberturvallisuusstrategia (2024–2035) ja parhaillaan valmistellaan ensimmäistä kansallisen turvallisuuden strategiaa.

EU:n CER-direktiivi (Critical Entities Resilience Directive, EU 2022/2557) tuli voimaan tammikuussa 2023. Sen toimeenpanoa varten on laadittu hallituksen esitys eduskunnalle laiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ja eräiksi muiksi laeiksi. Hallituksen esityksen käsittely eduskunnassa on päättynyt. Eduskunta on antanut vastauksen (EV 47/2025 vp ─ HE 205/2024 vp). Tavoitteena on saada lait vahvistettavaksi ja voimaan mahdollisimman pian. NIS2-direktiivin tavoitteena on varmistaa kyberturvallisuuden yhteinen vähimmäistaso koko EU:ssa. Direktiivin mukaiset velvoitteet tulivat voimaan 8.4.2025, ja hallituksen esitys sen täytäntöönpanosta hyväksyttiin 8.5.2025. Uusi kyberturvallisuuslaki (124/2025) on tullut voimaan 8.4.2025.

Julkisuuslain ajantasaistamisen tavoitteena on valmistella hallituksen esitys, joka tasapainottaa viranomaistoiminnan avoimuuden ja salassapidon tarpeet.[10] Uudistuksessa arvioidaan kattavasti julkisuuslain ajantasaistamistarpeet. Alueellisen varautumisen yhteistyön ja tilannekuvatoiminnan kehittämishanke tarkastelee, miten alueellista varautumista, koordinaatiota ja tilannekuvatoimintaa voidaan uudistaa tukemaan tehokkaasti häiriötilanteiden ja poikkeusolojen hallintaa.[11]

Naton vastejärjestelmän kansallinen soveltamisohje on parhaillaan työn alla. Järjestelmä sisältää useita toimenpiteitä, joilla pyritään rajoittamaan tiedon saatavuutta turvallisuustilanteen niin vaatiessa.

5.2 Tasapaino tiedon avoimuuden ja kansallisen turvallisuuden näkökohtien välillä

Datan sujuvan jakamisen merkitys on todettu Suomen digitaalisessa kompassissa[12]. **Datatalouden, alustatalouden ja sujuvien digitaalisten palveluiden kehitys perustuu digitaalisen tiedon, eli datan, sujuvalle jakamiselle eri toimijoiden välillä.** Hyödyt syntyvät yhdistämällä ja analysoimalla dataa uusin tavoin esimerkiksi digitaalisten palveluiden pohjaksi tai uusien prosessien, tuotteiden ja liiketoimintamallien kehittämiseksi. Ketterä ja reiluin ehdoin tapahtuva dataan pääsy kaikenkokoisille yrityksille sekä rohkeus avata dataa ja kehittää uudenlaisia liiketoimintamalleja luovat uutta datatalouden kasvuliiketoimintaa. Myös yksi Orpon hallituskauden tavoitteista on luoda kilpailukykyä datataloudesta ja

[10] Julkisuuslain ajantasaistaminen OM083:00/2020. Katso myös Julkisuuslain salassapitoperusteiden uudistustarpeiden kartoitus, lausuntopyyntö VN/27452/2020-OM-548

[11] Alueellisen varautumisen yhteistyön ja tilannekuvatoiminnan kehittämishanke SM029:00/2024

[12] Suomen digitaalinen kompassi VN 2022/65; http://urn.fi/URN:ISBN:978-952-383-906-9

digitalisaatiosta ja parantaa siten yritysten valmiuksia hyödyntää dataa liiketoiminnan sekä tuotteiden ja palveluiden kehittämiseen.

Kriittiseen infrastruktuuriin liittyvien tietojen avoin ja julkinen saatavuus on välttämätöntä monille yhteiskunnan keskeisille toiminnoille kuten esimerkiksi yksityisen sektorin tarjoamille palveluille, logistiikalle, suunnittelulle ja liikenteen automaation kehitykselle. Pääsy tietoihin mahdollistaa palvelujen tehokkaan toiminnan ja kehittymisen. Toisaalta samat tiedot voivat muodostaa merkittävän turvallisuusriskin, jos niitä voidaan hyödyntää esimerkiksi kohdennetuissa hyökkäyksissä tai tiedustelussa. Siksi on tärkeää tunnistaa tarkasti, mitä tietoa eri toimijat tarvitsevat, ja arvioida jatkuvasti avoimen datan hyötyjä ja haittoja.

Valtioneuvoston päätöksessä huoltovarmuuden tavoitteista 564/2024 on todettu, että digitaalisissa tietovarannoissa keskeistä on turvata tiedon hyödynnettävyys ja tieto-omaisuuksien saatavuus, eheys ja suojaus siten, että niihin voidaan luottaa myös normaaliolojen vakavissa häiriötilanteissa ja poikkeusoloissa. Kriittisten tietojen turvallisen siirtämisen ja säilyttämisen jatkuvuudenhallinnasta on huolehdittava ja lisäksi on **varmistettava, ettei avoimissa tietokannoissa ole vapaasti saatavilla huoltovarmuuskriittisiin aloihin ja kohteisiin liittyviä tietoja, jotka voisivat vaarantaa kansallista turvallisuutta, maanpuolustusta tai sotilaallista huoltovarmuutta**.

Paikkatiedon kansallisen riskiarvion mukaan tietyillä avoimilla tai julkisesti saatavilla olevilla paikkatiedoilla tai palveluilla voi olla mahdollisesti merkittävä välillinen vaikutus kansallisen tason uhkien toteutumiseen tai seurauksiin. **Paikkatietojen avoimella saatavuudella voi olla vaikutusta suomalaiseen yhteiskuntaan kohdistuvan uhan suunnitteluun.** Avoimia ja julkisia paikkatietoja voidaan mahdollisesti käyttää tavalla, joka lisää riskiä uhkien toteutumiseksi. Paikkatieto, kuten myös muu avoin tieto, tuo kuitenkin myös merkittävää lisäarvoa erilaisille palveluille ja kansalaisten jokapäiväiselle toiminnalle datatalouden puitteissa.

Avointa tietoa tarvitaan esimerkiksi tekoälyn kouluttamiseen. Avoin viranomaistieto on viranomaisvastuun takia laadukasta ja mahdollistaa tekoälyn kouluttamisen ilman merkittävää vinoumariskiä. Tekoälyn suorituskyky on suoraan riippuvainen siitä, kuinka laadukasta ja kattavaa dataa sen kouluttamisen tai käytön aikana on hyödynnetty, joten on syytä huolehtia käytettävissä olevan datan avoimuudesta. Näin osaltaan mahdollistetaan uusien käyttötapauksien ja innovaatioiden kehittäminen vauhdittamaan Suomen tuottavuutta ja kilpailukykyä. Esimerkiksi tekstiaineistojen käyttämisen rajoittavuus ja suomenkielisen koulutus- ja hienosäätödatan heikko saatavuus osoittautuivat haasteiksi liikenne- ja viestintäministeriön hankkeessa[13], jossa kokeiltiin suomalaisiin kielimalleihin perustuvan luovan tekoälyn hyödyntämistä lainvalmistelun tukena. Palveludemossa ei voitu hyödyntää koko Suomen lainsäädäntöä Finlex-palvelun käyttöehtojen sisältämien rajoitusten vuoksi. Edellytys suomalaisten kielimallien tehokkaalle kehitykselle on eri tehtäviin sopivan laadukkaan datan kerääminen, luominen ja avoin jakaminen.

Osa avoimista paikkatiedoista on välttämätöntä sen ehkäisemiseksi, että yhteiskunnan toiminnan kannalta keskeisille fyysisille rakenteille, järjestelmille ja liikennevälineille ei aiheutuisi tahatonta haittaa tai vahinkoa. Infrastruktuurien sijaintitietojen, kuten esimerkiksi merikaapelien, lentoesteiden ja droonikielto- ja rajoitusalueiden, julkistaminen on sen vuoksi arvioitu välttämättömäksi. Tietojen julkistamatta jättäminen voisi vaarantaa jopa ihmishenkiä.

Ympäristötietojen julkisuuteen ja avoimuuteen liittyy paljon EU- ja kansallista lainsäädäntöä. Paikkatiedon avoimuuden taustalla ovat perustuslaista johtuva velvoite, että julkisen vallan on pyrittävä mahdollisuus vaikuttaa elinympäristöään koskevaan päätöksentekoon (PL 20 §), hallinnon yleislainsäädäntö (julkisuuslaki ja tiedonhallintalaki) sekä mahdollinen sektorikohtainen erityislainsäädäntö. Tiedon avaamista on lisäksi edistetty aktiivisesti myös kansallisilla ohjelmilla ja periaatepäätöksillä. Merkittäviä

[13] Luovan tekoälyn palveludemo liikenne- ja viestintäministeriön lainvalmistelutyön tueksi: Loppuraportti http://urn.fi/URN:ISBN:978-952-243-743-3

velvoitteita tiedon avaamiseksi tulee Århusin sopimuksesta ja EU-lainsäädännöstä. Monien paikkatietoaineistojen avoimen jakamisen velvoite tulee direktiiveistä (mm. ympäristötieto-direktiivi, INSPIRE-direktiivi ja avoimen datan direktiivi sekä useat ympäristödirektiivien raportointivaatimukset), jotka on pantu täytäntöön kansallisella lainsäädännöllä.

Vesihuollon aineistoissa rajanveto ympäristötiedon ja turvallisuuskriittisen tiedon välillä on usein haastavaa. Perinteisesti monet vesihuoltoon liittyvät tiedot on mielletty ensisijaisesti ympäristötiedoksi, joka kuuluu avoimen tiedon piiriin. Kuitenkin muuttunut turvallisuusympäristö ja teknologian kehitys ovat tuoneet esiin sen, että osa näistä tiedoista voi muodostaa kriittisen infrastruktuurin suojaamisen kannalta merkittävän riskin. Tämä edellyttää tarkempaa arviointia siitä, **milloin tieto palvelee yleistä ympäristötiedon avoimuutta ja milloin sen jakaminen voi vaarantaa vesihuollon toimintavarmuutta tai turvallisuutta**. Tiedon luokittelussa tarvitaan siis aiempaa systemaattisempaa lähestymistapaa, jossa otetaan huomioon sekä lainsäädännön vaatimukset että muuttuvat uhkakuvat.

Paikkatietoinfrastruktuurista (421/2009) annetulla lailla on pantu täytäntöön kansallisesti INSPIRE-direktiivin mukainen sääntely. Mainitun lain 3 §:n mukaisesti lain säännöksiä sovelletaan viranomaisten hallussa oleviin julkisiin paikkatietoaineistoihin, jotka kuuluvat johonkin luetelluista INSPIRE-direktiivin liitteissä I, II ja III määritellyistä tietoryhmistä, sekä niiden sisältämiin tietoihin liittyviin paikkatietopalveluihin. Lain 4 §:n mukaan soveltamisalaan kuuluvaa **paikkatietoa hallinnoivan viranomaisen on laadittava ja pidettävä ajan tasalla paikkatietoaineistoja ja -palveluja kuvaavat tiedot, jotka mahdollistavat kyseisten aineistojen ja palvelujen löytämisen, luetteloinnin ja käytön (metatieto).**

Metatiedon ylläpitovaatimusta sovelletaan myös salassa pidettäviä tietoja sisältäviin paikkatietoaineistoihin, jollei näitä ole säädetty salassa pidettäviksi Suomen kansainvälisten suhteiden, yleisen turvallisuuden tai maanpuolustuksen etujen suojaamiseksi. Lain 6 §:n mukaan soveltamisalaan kuuluvaa paikkatietoa hallinnoivan viranomaisen on laadittava ja pidettävä ajan tasalla paikkatietoaineistosta yhteiskäyttöön soveltuva versio (yhteiskäyttöinen paikkatietoaineisto) sekä huolehdittava siihen liittyvien paikkatietopalvelujen yhteiskäyttöisyydestä. Lain 7 §:n mukaan paikkatietoa hallinnoivan viranomaisen on huolehdittava siitä, että yhteiskäyttöinen paikkatietoaineisto on saatavilla tietoverkossa aineiston katselua ja lataamista varten. Yhteiskäyttöisen paikkatietoaineiston ei tarvitse sisältää täsmälleen kaikkia teemoja kuin alkuperäisissä asiakirjoissa, mikä mahdollistaa tiettyjen herkkien sisältöjen karsimista jaettavasta aineistosta. Avoimen datan direktiivillä annettu asetus arvokkaista tietoaineistoista täydentää tiedon jakeluvaatimuksia osaan INSPIRE-aineistoista. Esimerkiksi kuntien ja maakuntien liittojen on pyynnöstä jaettava voimassa oleva kaavatieto rajapintapalvelun ja massalatauspalvelun kautta. Jakeluvelvoite koskee myös historiatietoa, mikäli se on muunnettu sähköiseen muotoon.

Avoimen datan jakaminen kriittisestä infrastruktuurista voi olla perusteltua, mutta tietojen jakamisen ohessa tulee pohtia tiedon rajaamista huolellisesti. Riskiperusteinen lähestymistapa mahdollistaa sekä turvallisuuden että yhteiskunnallisen hyödyn yhteensovittamisen. Ristikkäisistä tarpeista ja mahdollisuuksista johtuen jo Paikkatiedon kansallisessa riskiarviossa on todettu, että paikkatiedon avoimuutta on arvioitava tapauskohtaisesti, sekä huomioiden yhtäältä tiedon avoimuuden ja toisaalta tiedon rajoittamisen mahdolliset vaikutukset. Turvallisuusympäristön muutos, yhdistettynä teknologiseen kehitykseen ja erityisesti tekoälyn nopeasti kehittyviin ratkaisuihin merkitsee kuitenkin sellaista toimintaympäristön muutosta, jossa totuttuja käytäntöjä on tarpeen tarkastella uudelleen, minkä ei automattisesti välttämättä tarkoita sitä, että tiedon saatavuutta olisi rajoitettava. Paikkatietoa hallinnoivien toimijoiden on kuitenkin syytä huomioida yhteiskunnallinen muutos ja tarkistaa omat toimintatapansa suhteessa ajantasaiseen kansalliseen riskiarvioon.[14] Samankaltaista arviointia tulee edellyttämään myös muu avoin tieto kuin paikkatieto, jotta tasapaino avoimuuden ja kansallisen turvallisuuden välillä voidaan varmistaa.

[14] Paikkatiedon kansallinen riskiarvio (VN/15876/2023)

Lainsäädännön vaikutusten arvioinnissa on olennaista tunnistaa säädösehdotuksen vaikutukset tietoverkkoihin tai muun kriittisen infrastruktuurin tai tiedon suojaamiseen taikka huoltovarmuuteen. Lakien vaikutusarvioinnilla vahvistetaan päätöksenteon tietopohjaa tunnistamalla ja arvioimalla esityksen olennaiset vaikutukset ja arvioimalla niitä. Vaikutusarviointi tuottaa lisäksi tietoa esityksen vaikutusten suhteesta yhteiskunnallisten tavoitteiden kokonaisuuteen ja tukee sääntelyn kehittämistä. Lainvalmistelun vaikutusarviointiohje kattaa taloudellisten ja ympäristövaikutusten lisäksi muut ihmisiin kohdistuvat ja yhteiskunnalliset vaikutukset. Näihin sisältyvät vaikutuslajeina ja kohderyhminä on turvallisuus, joka huomioi kansallisen turvallisuuden näkökulman sekä tietoyhteiskunta ja tietosuoja.[15]

5.3 Tiedon avoimuuden tarkastelua jatketaan kunnissa

Tiedon avoimuuden tarkastelussa on jo tehty paljon, ja työ jatkuu erityisesti kuntatasolla sekä rakennetun ympäristön osalta. Avoimesti ja julkisesti saatavilla olevien paikkatietojen riskien arviointia varten neljä suurta kaupunkia ovat laatineet yhteistyössä ohjeen ”Turvallisuusnäkökulma ja kuntien rakennetun ympäristön paikkatietoaineistot”. Ohje on kuntien saatavilla pyynnöstä Kuntaliitosta.

Suurimmat kunnat ovat alkaneet tarkastella alueidenkäytön ja rakennustiedon kokonaisuuksia ja rajanneet osan avoimesti ja julkisesti saatavilla olevista tiedoista. Rajaukset koskevat erityisesti rakennetun ympäristön paikkatietoaineistojen avoimuutta. Tavoitteena on estää tietojen käyttö esimerkiksi kriittisen infrastruktuurin haavoittuvuuksien kartoittamiseen. Rajauksia on mahdollista tehdä vain tiettyihin teemoihin tai yksittäisiin asiakirjoihin liittyen. Tiedon rajaamista on lain mukaan tulkittava suppeasti ja tapaus kerrallaan. Esimerkiksi kaikkien kaavatietojen poistaminen yleisestä verkosta ei ole lain mukaan mahdollista. Rajauspäätöksiä tehdessä on noudatettava voimassa olevaa lainsäädäntöä, joka velvoittaa kyseisten tietojen jakamiseen (kts. luku 5.2).

Rakennetun ympäristön paikkatietojen turvallista hallintaa on valmisteltu valtioneuvostossa osana laajempaa tietohallinnan ja sääntelyn uudistusta, jota koordinoi ympäristöministeriö. Ympäristöministeriön Ryhti-hanke on luonut perustan valtakunnalliselle rakennetun ympäristön tietojärjestelmälle. Sen tavoitteena on yhdenmukaistaa kaava- ja rakentamistietoa, parantaa tiedon laatua ja varmistaa sen yhteentoimivuus. Samalla kehitetään sen tiedonhallintaa ja tietoturvaa. Yhtenäistämällä kuntien ja muiden viranomaisten rakennetun ympäristön tiedonhallintaa voidaan lisätä tietoturvaa samalla kun varmistetaan yhteiskunnalle tärkeän avoimen tiedon käytettävyys.

Kunnan infrapalvelujen digitalisointi ja koulutusmateriaali kunnan kriittisen infran hallinnointiin (INDIKO) – hankeen tavoitteena oli parantaa kuntien kriittisen infrastruktuurin – erityisesti vesihuollon ja liikenneverkon – tietojen hallintaa, hyödyntämistä ja turvallisuutta. Hanke toteutettiin yhdeksässä kunnassa. Kunnat ottivat käyttöön uusia tietojärjestelmiä ja paransivat olemassa olevia. Arkkitehtuuriselvityksiä ja paikkatietoratkaisuja laadittiin kriittisen infran hallintaan. Käyttöön otettiin palveluja, jotka mahdollistavat kohdennetun viestinnän kuntalaisille kriisitilanteissa. Yhteistyössä Maanmittauslaitoksen kanssa laadittiin uhkamalli, joka sisältää suosituksia kuntien johdolle ja operatiivisille toimijoille kriittisen infran suojaamiseksi. Jokaisessa kunnassa toteutettiin konkreettisia toimenpiteitä, kuten verkostojen kartoituksia, tietojen digitointia ja järjestelmien käyttöönottoa. Yhteentoimivuus ja ajantasainen tieto tehostavat toimintaa ja vähentävät vahinkoja, mikä tuo säästöjä. Jatkotoimina todettiin, että kuntien tulee jatkaa kehittämistä ja ottaa uhkamallin suositukset käyttöön. Lisäksi tarvitaan kansallista koordinaatiota ja ohjeistusta hallitun tiedonjakelun varmistamiseksi. Yhteistyötä valtionhallinnon ja yksityisen sektorin kanssa tulee tiivistää.

Huoltovarmuuskeskus tukee kuntia kriittisten kohteiden suojaamisessa ja jatkuvuudenhallinnan kehittämisessä. Tähän liittyen Huoltovarmuuskeskus lähetti 7.10.2024 kuntien rakennusvalvontaviranomaisille kirjeen, jonka aiheena oli rakennuslupatietojen julkisuus ja mahdollinen vihamielinen tiedonhankinta. Kirjeen taustalla oli Huoltovarmuuskeskuksen havainnot yrityksistä hankkia kriittisiin kohteisiin liittyviä

[15] Lainvalmistelun vaikutusarviointiohje, http://urn.fi/URN:ISBN:978-952-383-922-9

rakennuslupatietoja kuntien rakennusvalvonnan kautta. Tämän vuoksi kirjeessä esitettiin, että kuntien tulisi tunnistaa alueellaan sijaitsevat yhteiskunnan kannalta kriittiset kohteet. Näihin liittyvät rakennusvalvonnan asiakirjat tulisi arvioida ja tarvittaessa luokitella salassa pidettäviksi julkisuuslain (621/1999) perusteella. Salassapitoperusteita voivat olla esimerkiksi turvallisuusjärjestelyt, varautuminen poikkeusoloihin, maanpuolustus tai liikesalaisuudet. Salassa pidettäviä asiakirjoja ei saa julkaista verkossa tai pitää esillä viranomaisen toimipisteessä tai sähköisissä palveluissa.

Valtiovarainministeriön käynnistämä Kansallinen julkisten hankintojen tietovaranto-hanke tähtää kansallisen tietovarannon luomiseen, joka kokoaa julkisen sektorin hankinta- ja ostotiedot koko hankinnan elinkaaren ajalta. Tavoitteena on tehostaa hankintoja, parantaa päätöksenteon tietopohjaa ja vähentää kustannuksia. Hanke perustuu pääministeri Orpon hallitusohjelmaan ja on osa Hankinta-Suomi-ohjelmaa. Tietovaranto mahdollistaa esimerkiksi kuntien ostotietojen tarkastelun, kilpailutilanteen seuraamisen ja hankintojen laadun kehittämisen. Se parantaa myös taloustietojen vertailukelpoisuutta. Valtiovarainministeriö vastaa strategisesta ohjauksesta ja lainsäädäntömuutoksista, Valtiokonttori järjestelmän toteutuksesta.

Alueidenkäytön suunnittelulla on tunnistettu merkittävä rooli kriittisen infrastruktuurin suojaamisessa sekä tulevaisuuden huoltovarmuuteen vaikuttamisessa. Huoltovarmuuskeskus on käynnistämässä hanketta, jonka tavoitteena on saada kokonaisymmärrys alueidenkäytön suunnittelusta sekä siitä, miten ja millä tavoin huoltovarmuusnäkökulmat olisivat tarpeen ja mahdollista huomioida kaavoituksessa. Lisäksi tavoitteena on ymmärtää kaavoitukseen liittyvien paikkatietojen ja niiden julkisuuden huoltovarmuusvaikutuksia, huomioiden sekä julkisuus- että luovuttamisnäkökulma. Hankkeessa huomioidaan koko alueidenkäytön suunnittelujärjestelmä (valtakunnalliset alueidenkäyttötavoitteet, maakunta-, yleis- ja asemakaavoitus) ja erilaiset poikkeamislupamenettelyt, kuten rakentamislain 57 §:n mukainen menettely. Hankkeen fokus on poikkeusoloissa ja niihin rinnastettavissa olevissa vakaviin häiriötilanteisiin varautumisessa (ennakollinen toiminta), niihin vastaamisessa (reagointi / vaste) ja niistä toipumiseen tai palautumiseen. Erityisenä painopisteenä on sotilaallinen voimankäyttö.[16]

Projektin tuotoksena syntyy erilaisia kirjallisia kuvauksia huoltovarmuuden ja alueidenkäytön suhteesta sekä tukimateriaalia kaavoittajille. Työ sisältää tietotarpeiden määrittelyä, tietojen hankintaa, analysointia ja kuvaamista.

Hankkeessa on tarkoitus kuvata:

1. mikä on kaavoituksen rooli kriittisen infrastruktuurin suojaamisessa sekä tulevaisuuden huoltovarmuuden vaikuttamisessa;
2. miten huoltovarmuusnäkökulmat on huomioitu kaavoituksessa (sisältäen ohjaavat säädökset);
3. tunnistaa huoltovarmuuden kannalta tarkoituksenmukaisia säädösmuutostarpeita;
4. määrittää eri kaavatasojen (maakunta-, yleis- ja asemakaava) ja suunnittelemattomuuden sekä erilaisten poikkeamislupien suhde huoltovarmuuteen;
5. kuvata, millaisilla suunnitteluratkaisuilla voidaan turvata huoltovarmuutta ja millaisia huoltovarmuusnäkökulmia kaavoituksessa tulee huomioida;
6. kuvata, millaisilla tavoilla kaavoitus voi rajoittaa huoltovarmuutta ja mitä huoltovarmuuden kannalta olennaista kaavoituksessa tulee välttää;

[16] Hankkeen säädöstarkastelut tehdään suhteessa voimassa olevaan alueidenkäyttölakiin siten, että huomioidaan käynnissä oleva lakivalmistelu ja nykyisen alueidenkäyttölain suunnittelujärjestelmän perusta, keskeiset periaatteet ja tarkoitus, lähtien maankäyttö- ja rakennuslain säätämisestä eli sekä nykyinen että vireillä oleva alueidenkäyttölaki huomioidaan. Lisäksi tulee huomioida ja kuvata, miten valtakunnalliset alueidenkäyttötavoitteet (VAT) voisivat tukea huoltovarmuuden tavoitteita. Työssä tulee esittää myös arvio, tarvitaanko VAT:ien sisältöön täydennyksiä tai tarkennuksia huoltovarmuuden näkökulmasta.

7. simuloida eri kaavatasojen toimivuutta erikseen määriteltävässä sotilaallisen voimankäytön skenaariossa;
8. kuvata kaavoitukseen liittyvien paikkatietojen ja niiden julkisuuden huoltovarmuusvaikutuksia; sekä
9. kuvata kaavojen laadintaprosessien vuorovaikutteisuuden ja asiakirjajulkisuuden vaatimusten sekä huoltovarmuuden asettamien vaatimusten suhdetta säädösten tasolla ja käytännön toiminnassa.

6 Työryhmän jatkotoimet

Hankkeelle asetetut tavoitteet ja tehtävät

Hankkeen tavoitteena yleisellä tasolla on edistää kansallista turvallisuutta sekä vastuullista tietopolitiikkaa arvioimalla uudelleen kriittisen infrastruktuurin tiedon avoimuus. Valtiovarainministeriö asettaa seuraavaksi kaksi alatyöryhmää, joiden tehtävänä on tukea hankkeen tavoitteiden saavuttamista 19.2.2025 asettamispäätöksessä kuvatulla tavalla. Hankkeen arvioinnin kohteena on kriittisen infrastruktuurin sekä avoimesti saatavilla oleva tieto että tieto, joka ei ole avoimesti saatavilla, mutta on julkisuuslain mukaisesti julkista ja saatavilla viranomaiselta. Valtiovarainministeriö lähetti 20.5.2025 nimeämispyynnöt kahteen alatyöryhmään ja pyrkii asettamaan ryhmät nopealla aikataululla 6.6.2025 määräajan jälkeen siten, että työskentely voi jatkua tehokkaasti elokuussa 2025.

Alatyöryhmä 1: CER-toimijoiden riskiarvioinnin pilotointi

Ensimmäinen alatyöryhmä keskittyy tulevien CER-toimijoiden kriittisen infrastruktuurin avoimen

tiedon riskiarvioiden tukemiseen. Ministeriöt hyödyntävät CER-direktiivin valmisteilla olevan toimeenpanolain[17] kriteeristöä sekä tulevaa kansallisen turvallisuuden strategiaa yhteistyön kannalta keskeisten toimijoiden valinnassa. Valitut toimijat toteuttavat riskiarvioinnin osana omaa toimintaansa.

Alatyöryhmä tukee toimijoiden avoimen tiedon riskiarviointia, tekee sitä tukevia linjauksia sekä tarjoaa yhteistyörakenteen arvioinnissa nousevien kysymysten käsittelyä ja yhteensovittamista varten yhdessä hankkeen aiemmin asetetun työryhmän kanssa. Alatyöryhmän työ tukee hankkeen loppuraportin kansallisen turvallisuuden kannalta merkityksellisen kriittisen infrastruktuurin avoimen tiedon strategista tilannekuvaa. Alatyöryhmän puheenjohtajana toimii hankkeen asettamispäätöksen mukaisesti sisäministeriön työryhmäjäsen. Alatyöryhmään nimetään jäsenet seuraavista organisaatioista: Sisäministeriö (varapuheenjohtaja), liikenne- ja viestintäministeriö, puolustusministeriö, valtioneuvoston kanslia, Huoltovarmuuskeskus ja Elinkeinoelämän keskusliitto

Alatyöryhmä 2: Riskipohjainen malli päätöksenteon tueksi

Toinen alatyöryhmä työstää yhteistyössä kuntien, alueiden sekä muiden sidosryhmien kanssa yleistä, riskipohjaiseen arviointiin perustuvaa mallia tiedon jakamista koskevan päätöksenteon tueksi. Tukimateriaalin tekemisessä hyödynnetään Kuntaliiton kautta kunnille jaettavaa ohjetta Turvallisuusnäkökulma ja kuntien rakennetun ympäristön paikkatietoaineistot sekä Paikkatiedon kansallista riskiarviota (VN/15876/2023) ja Kansallista riskiarviota (2023). Alatyöryhmän tuottamaa tukimateriaalia voidaan hyödyntää myöhemmin elinkeinoelämän, kuntien, kaupunkien sekä hyvinvointialueiden toimesta heidän arvioidessaan kriittisen infrastruktuurinsa avoimen tiedon jakamista turvallisuusnäkökulmasta. Alatyöryhmän työ tukee hankkeen työryhmän tavoitetta tuottaa erilaisten toimijoiden tarpeet huomioiva tukimateriaali tiedon jakamista koskevan päätöksenteon tueksi. Alatyöryhmän puheenjohtajana toimii hankkeen

[17] HE laiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ja eräiksi muiksi laeiksi (205/2024).

työryhmän puheenjohtaja. Alatyöryhmään nimetään jäsenet seuraavista organisaatioista: Valtiovarainministeriö, sisäministeriö, ympäristöministeriö, Kuntaliitto, Tilastokeskus, Huoltovarmuuskeskus, Tampereen kaupunki, Vantaan kaupunki, Maanmittauslaitos, Pirkanmaan hyvinvointialue.

7 LIITE 1: Keskeisten käsitteiden tarkastelu

Tässä väliraportissa ehdotetaan hankkeen käyttöön määritelmiä kolmelle keskeiselle käsitteelle. Määritelmät rajaavat hankkeen työtä perustuen työryhmän toimeksiantoon.

Riski

Kielteisen seikan tai tapahtuman todennäköisyyden ja vaikutusten yhdistelmä. Riski ilmaistaan tavallisesti riskin lähteiden, mahdollisten tapahtumien, niiden seurausten ja niiden todennäköisyyden yhdistelmänä. Riskit voivat kohdistua esimerkiksi ihmisiin, eläimiin, omaisuuteen, tietojärjestelmiin, ympäristöön tai yhteisöllisiin arvoihin. Joissakin yhteyksissä riski voidaan käsittää laajemmaksi käsitteeksi, johon ei aina liity kielteisiä seikkoja. Esimerkiksi Riskienhallinnan standardissa ISO 31000 riski on määritelty epävarmuuden vaikutukseksi tavoitteisiin.[18]

Uhka

Mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku Uhka eroaa vaarasta siten, että uhka on epävarmempi kehityskulku ja vaara puolestaan käytännöllinen ja riskienhallinnallisin toimenpitein käsiteltävä asia.[19]

Kriittinen infrastruktuuri ja yhteiskunnan elintärkeä toiminto

Kriittinen infrastruktuuri: aineelliset tai aineettomat perusrakenteet, palvelut ja niihin liittyvät toiminnot, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi.

Yhteiskunnan elintärkeä toiminto: toiminto, joka välttämätön yhteiskunnan toimivuuden kannalta.

Kriittinen infrastruktuuri määritellään tämän hankkeen tavoitteita varten perusrakenteiksi, palveluiksi sekä niihin liittyviksi toiminnoiksi, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi. Kriittiseen infrastruktuuriin kuuluu sekä fyysisiä laitoksia ja rakenteita että sähköisiä ja digitaalisia toimintoja ja palveluja.

Erilaisia kriittisen infrastruktuurin määritelmiä löytyy mm. kokonaisturvallisuuden sanastosta, valtioneuvoston päätöksestä huoltovarmuuden tavoitteista (568/2024) ja Kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta annettu Euroopan parlamentin ja neuvoston direktiivistä (EU) 2022/2557 eli CER-direktiivistä. Lisäksi yhteiskunnan elintärkeitä toimintoja on määritelty Yhteiskunnan turvallisuusstrategiassa VN 2025:1.

---

[18] Käsitteen tiedot perustuvat Kokonaisturvallisuuden sanastoon (TSK 50, 2017).

[19] Käsitteen tiedot perustuvat Kokonaisturvallisuuden sanastoon (TSK 50, 2017).

Suomessa kriittinen infrastruktuuri on suurimmaksi osaksi yksityisen sektorin omistuksessa ja hallinnassa. Kriittisen infrastruktuurin suojaaminen on ensisijaisesti omistajien ja kohteissa toimivien vastuulla. Viranomaiset tukevat ja koordinoivat sekä huolehtivat erityisesti kansallisen tason suorituskykyjen turvaamisesta. Kriittisen infrastruktuurin turvaaminen on pitkälti huoltovarmuuden varmistamista, ja huoltovarmuusorganisaatioon kuuluvat yritykset muodostavat kriittisen infrastruktuurin perustan.

- CER-direktiivi (11 sektoria) toimii tämän hankkeen puitteissa kriittisen infrastruktuurin käsitteen yleisenä kehikkona ja lähtökohtana (hankkeen lopputuotteet, hankkeen työryhmä sekä molemmat alatyöryhmät). Mikäli työryhmässä päädytään siihen, että jokin tietty sektori, palvelu tai toiminnallisuus tulee lisätä tähän listaan, voidaan se nostaa tähän tarkasteluun mukaan.
- Huoltovarmuuden näkökulmasta kriittistä infrastruktuuria ovat ne rakenteet, järjestelmät ja palvelut, joiden toiminta on välttämätöntä yhteiskunnan elintärkeiden toimintojen turvaamiseksi poikkeusoloissa ja häiriötilanteissa. Kriittisyys määräytyy usein sen mukaan, kuinka keskeinen toimija tai infrastruktuuri on yhteiskunnan toimintakyvyn ja väestön hyvinvoinnin kannalta.

Hankkeen työmääritelmä kriittisestä infrastruktuurista ei ole poissulkeva. Yksittäisten toimijoiden (CER-kriittiset toimijat, kunnat, kaupungit, hyvinvointialueet, elinkeinoelämä) riskiarviointityön myötä voidaan päätyä tilanteeseen, jossa jokainen organisaatio lopulta katsoo kriittisen infran käsitettä omasta näkökulmastaan. Viime kädessä keskeistä on se, miten jonkin kriittisen infrastruktuurin häiriö, vahingoittuminen tai toimintakyvyttömyys vaikuttaa väestön mahdollisuuksiin elää turvallista ja sujuvaa arkea. Tähän sisältyy myös elinkeinoelämän toiminnan jatkuvuus sekä viranomaisten toiminnan edellytysten varmistaminen. Jonkin infrastruktuurin kriittisyyden voidaan siten ajatella kytkeytyvän aina väestön hyvinvointiin ja turvallisuuteen.

Fyysisen infrastruktuurin ja siihen liittyvä digitaalinen omaisuus

- Fyysinen infrastruktuuri viittaa konkreettisiin rakenteisiin ja järjestelmiin, kuten sähköverkkoihin, tunneleihin, vesilaitoksiin tai tietoliikennekeskuksiin.
- Digitaalinen tieto fyysisestä infrastruktuurista tarkoittaa kaikkea siihen liittyvää dataa: sijaintitietoja, teknisiä piirustuksia, huoltohistoriaa, kapasiteettia, valvontajärjestelmiä, omistussuhteita jne.
- Ero on kriittinen, koska uhkatoimijat voivat hyödyntää digitaalista tietoa ilman, että heidän tarvitsee fyysisesti lähestyä kohdetta – tai he voivat käyttää sitä valmistautuakseen fyysiseen hyökkäykseen. Huomioitavaa kuitenkin on, että fyysisen hyökkäyksen toteutuminen vaatii yleensä paikan päälle fyysisesti menemistä, jolloin fyysiset suojauskeinot ovat keskeisessä roolissa. Harvoin pelkän digitaalinen tiedon avulla pystyy esimerkiksi hyökkäämään kohteeseen. Tästä syystä digitaalisen tiedon tunnistamisen lisäksi on tärkeää tunnistaa ne kohteet, joiden fyysistä suojaustasoa tulisi nostaa esimerkiksi aitojen, lukitusten tai valvontakameroiden ja vartioinnin osalta.

CER-direktiivin sektorit (11 kpl) ovat: energia, liikenne, pankkitoiminta, finanssimarkkinoiden infrastruktuurit, terveydenhuolto, juomavesi, jätevesi, digitaalinen infrastruktuuri, julkishallinto, avaruus ja elintarvikkeiden tuotanto, jalostus ja jakelu.

Työryhmän lopputuotteista kansallisen turvallisuuden kannalta merkityksellisen kriittisen infrastruktuurin avoimen tiedon riskiarvio ja kansallisen turvallisuuden kannalta merkityksellisen kriittisen infrastruktuurin

avoimen tiedon strateginen tilannekuva vaativat kuitenkin molemmat rajausta siitä, mistä infrastruktuurista puhumme tämän hankkeen yhteydessä.

Kansallisen turvallisuuden kannalta merkityksellistä kriittistä infrastruktuuria ei ole yksiselitteisesti määritelty tai tunnistettu. Parhaillaan eduskuntakäsittelyssä olevassa laissa yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta[20] on kuitenkin määritelty kriteerit lain mukaan nimettäville CER-kriittisille toimijoille 11 eri sektorilta. Jäsenvaltion on määritettävä kriittiset toimijat viimeistään 17.7.2026 CER-direktiivin liitteessä tarkoitetuilla toimialoilla ja alasektoreilla. Tässä hankkeessa lähdetään siitä, että nämä toimijat hallinnoivat kansallisen turvallisuuden kannalta kriittistä infrastruktuuria.

Ministeriöiden nimeäminen CER-toimijoiden lisäksi Huoltovarmuusorganisaatio määrittelee huoltovarmuuskriittiset toimijat perustuen Valtioneuvoston päätökseen huoltovarmuuden tavoitteista 568/2025. Lisäksi kyberturvallisuuslaki (124/2025) velvoittaa tiettyjä toimijoita tunnistamaan, arvioimaan ja hallitsemaan riskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Myös edellä mainittujen toimijoiden joukosta löytyy kansallisen turvallisuuden kannalta kriittistä infrastruktuuria.

Kansallinen turvallisuus

Työryhmä keskittyy tilannekuvatyössään kartoittamaan *keskeisiä kansallisen turvallisuuden kannalta merkittäviä kriittisen infrastruktuurin avoimen tiedon riskejä*. Kansallisessa turvallisuudessa on kyse koko suomalaisen yhteiskunnan yhteisestä turvallisuudesta, yhteiskunnan ja kansalaisten selviytymisestä sekä Suomen suvereniteetista. Käsitteenä kansallinen turvallisuus on dynaaminen ja määrittyy sekä ajassa että suhteessa Suomen muuttuvaan uhka- ja toimintaympäristöön. Aiemmin kansallisen turvallisuuden sijaan on puhuttu valtion turvallisuudesta.

Kansallista turvallisuutta kuvataan usein siihen kohdistuvien *uhkien* kautta. Nämä ovat uhkia, jotka vaikuttavat koko suomalaiseen yhteiskuntaan kuten esimerkiksi terrorismi, vakoilu ja vieraan valtion vahingollinen toiminta. Myös hybridivaikuttaminen, ja kyberuhat ja kriittisen infrastruktuurin suojaaminen kytkeytyvät kansalliseen turvallisuuteen.

Kansallinen turvallisuus voidaan kuvata myös yhteiskunnan tilana, jossa yhteiskunnan ja demokraattisen valtiojärjestelmän sekä toiminta että toimintaedellytykset ja valtiosuvereniteetti on suojattu vakavilta uhkilta.

Kansallisen turvallisuuden käsitteelle on annettu määritelmä Sisäisen turvallisuuden sanastossa.

[20] HE 205/2024 vp

Termitietueen merkintä	Merkinnän selitys
2	käsitteen numero
kansallinen turvallisuus	suomenkieliset termit; suositettava termi ensimmäisenä ja sen jälkeen sallittavat synonyymit
mieluummin kuin: valtion turvallisuus	ei-suositettava termi; termin käyttöä ei suositeta esimerkiksi kielellisistä syistä
en national security	englanninkieliset vastineet
yhteiskunnan tila, jossa yhteiskunnan ja demokraattisen valtiojärjestelmän toiminta ja toimintaedellytykset sekä valtiosuvereniteetti on suojattu vakavilta *uhkilta*	määritelmä; alkaa pienellä kirjaimella, ei pistettä lopussa; kursivointi viittaa sanastossa määriteltyyn käsitteeseen
Kansalliseen turvallisuuteen kohdistuvia uhkia ovat toiminta ja kehityskulut, jotka uhkaavat vakavasti kansanvaltaista valtio- ja yhteiskuntajärjestystä, *yhteiskunnan elintärkeitä toimintoja*, valtiosuvereniteettia, suuren ihmismäärän henkeä ja terveyttä tai Suomen taloudellisia tai muita tärkeitä etuja. Näitä etuja uhkaavat esimerkiksi sotilaallinen hyökkäys, vieraan valtion harjoittama tiedustelu, *terrorismi* ja vakava valtiollinen *hybridivaikuttaminen*. Kansallinen turvallisuus on yhteydessä sekä ulkoiseen että *sisäiseen turvallisuuteen*. Termiä valtion turvallisuus käytetään eräissä säädöksissä, mutta yleisesti sitä pidetään vanhentuneena.	huomautus; normaali virke, erotettu määritelmästä sisennyksellä; antaa lisätietoa käsitteestä, esimerkkejä, tietoa termien käytöstä yms.

Kansallinen turvallisuus on aikaan ja paikkaan sidottu sekä poliittisen ulottuvuuden sisältävä valtion, yhteiskunnan ja kansalaisten yhteinen tavoite- ja tahtotila, jonka ytimessä on valtion ja yhteiskunnan olemassaolon ja toimintakyvyn turvaaminen sekä kyky tuottaa turvallisuutta valtiolle ja kansalaisille.

Kansallinen turvallisuus suojaa ydinintressejämme uhkilta ja mahdollistaa kansallisten intressien edistämisen, toteutumisen ja niihin pyrkimisen. Siinä missä kansallinen turvallisuus saa muotonsa ajassa ja paikassa, tarkentuvat kansallisen turvallisuuden intressit niin ikään kulloinkin vallitsevassa yhteiskunnallisessa tilassa, ulko- ja turvallisuuspoliittisessa toimintaympäristössä ja poliittisessa tahtotilassa. Kuitenkin valtion ja kansakuntamme olemassaoloon liittyvät kansallisen turvallisuuden ydinintressimme pysyvät varsin muuttumattomina. Kansallisen turvallisuutemme ydinintressit ovat: kansakunnan turvallisuus ja hyvinvointi; valtion jatkuvuus; valtiosuvereniteetti ja alueellinen koskemattomuus; demokraattinen valtiojärjestys ja oikeusvaltio; ja yhteiskunnallinen vakaus.

Kansallista turvallisuutta kuvataan usein siihen kohdistuvien uhkien kautta. Nämä ovat uhkia, jotka vaikuttavat koko suomalaiseen yhteiskuntaan kuten esimerkiksi terrorismi, vakoilu ja vieraan valtion vahingollinen toiminta. Myös hybridivaikuttaminen, ja kyberuhat ja kriittisen infrastruktuurin suojaaminen kytkeytyvät kansalliseen turvallisuuteen.

Kansallisen turvallisuuden kannalta merkityksellinen kriittinen infrastruktuuri

Tulevaisuudessa hallinnonalat tunnistavat CER-kriittiset toimijat. Näiden toimijoiden voidaan katsoa olevan keskeisiä kansallisen turvallisuuden ylläpitämiseksi. Hankkeen näkökulmasta tulevat CER-kriittiset toimijat voidaan käsittää olevan kansallisen turvallisuuden kannalta merkityksellistä kriittistä infrastruktuuria työryhmän toimeksiantoa sekä tarpeita vastaavalla tavalla.

Tulevat CER-kriittiset toimijat (11 sektoria) muodostavat [tämän hankkeen tavoitteita varten] riittävän edustavan otoksen kansallisen turvallisuuden kannalta merkityksellisestä kriittisestä infrastruktuurista. CER-kriittisten toimijoiden tunnistaminen perustuu lakiin yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta (erityisesti 10 § Kriittisen toimijan määrittäminen ja 11 § Merkittävä haitallinen vaikutus).

Hankkeen työmääritelmä ei ole poissulkeva, vaan myös esimerkiksi huoltovarmuuskriittiset yritykset ovat keskeinen osa kansallista turvallisuutta, sillä ne ylläpitävät yhteiskunnan toiminnan kannalta välttämättömiä palveluita ja toimitusketjuja. Näihin kuuluvat muun muassa energia-, logistiikka-, elintarvike-, lääke- ja tietoliikennesektorin toimijat. Yritykset hallinnoivat usein kriittistä infrastruktuuria tai sen osia, ja niiden toiminnan häiriintyminen voi nopeasti heijastua koko yhteiskuntaan. Jatkotyötä ajatellen on myös huomioitava, että CER-kriittisiksi määritettävät toimijat eivät tule edustamaan koko kriittisen infrastruktuurin kokonaisuutta. Suomessa yhteiskunnan elintärkeiden toimintojen turvaaminen kattaa CER-direktiiviä laajemman joukon toimialoja ja toimijoita.

Avoin ja julkisesti saatavilla oleva tieto

Hankkeen asettamispäätöksessa ensimmäinen tavoite on tunnistaa kansallisen turvallisuuden kannalta merkitykselliseen kriittiseen infrastruktuuriin liittyvä avoin tieto.

Tämän hankkeen tavoitteita varten avoimesti ja julkisesti saatavilla olevalla tiedolla tarkoitetaan avoimesti saatavilla olevaa tietoa sekä tietoa, joka ei ole avoimesti saatavilla, mutta on viranomaisten toiminnan julkisuudesta annetun lain (621/1999) mukaisesti julkista.

Tieto voi tässä yhteydessä tarkoittaa informaatiota, joka ilmentää infrastruktuuria esimerkiksi sen ominaisuuksia, käyttötarkoituksia, organisaatioita, ihmisiä, sovelluksia, sijaintia, kustannuksia, merkityksiä ja haavoittuvuuksia sekä keskinäisiä riippuvuuksia ja sidonnaisuuksia.

Avoin data on digitaalisessa muodossa olevaa informaatiota, joka on kaikkien vapaasti käytettävissä mihin tahansa käyttöön, kunhan sen alkuperäinen lähde mainitaan.

Avoin data on nimenomaan avoimen datan käyttöehdoilla saatavilla ja rakenteisessa muodossa ladattavissa seuraavien määritelmien mukaisesti:

- **Avoin** = Datalla on avoimen hyödyntämisen mahdollistava käyttölupa eli lisenssi[21]. Käytännössä Creative Commons BY 4 tai CC0 1.0.
- **Data** = Koneluettavaa tietoa. Esimerkiksi taulukkoja, tekstiä, kuvia, karttoja, videoita, äänitiedostoja yms.[22]

[21] Lisätietoa lisensseistä: Avoimen datan lisenssit | avoindata.fi
[22] https://www.avoindata.fi/fi/tietoa-avoimesta-datasta/mita-on-avoin-data#avoin-data-yhteiskunnassa

Datalla tarkoitetaan digitaalisesti tallennettua, merkeistä ja symboleista koostuvaa koneellisesti luettavissa olevaa informaatiota, joka voi muodostaa esimerkiksi dokumentteja, tietokantoja, kuulemisten transkripteja ja audiotallenteita. Se voidaan ymmärtää raaka-aineena, jota jalostamalla syntyy merkityksellistä informaatiota.

Avoin data voidaan määritellä myös siten, että se on löydettävissä ja saatavilla Internetistä kokonaisena ja maksutta käyttökelpoisessa ja muokattavassa (siis koneluettavassa) muodossa. Avoin data on kaikkien vapaasti katseltavissa, ladattavissa, kopioitavissa, muokattavissa, jaettavissa ja käytettävissä missä tahansa lainmukaisessa toiminnassa ilman taloudellisia, juridisia, teknisiä, sosiaalisia tai käytännöllisiä rajoitteita. Lisäksi avoimen datan käyttöehdot ja lisenssit takaavat datan tuottajalle tämän halutessa oikeuden tulla asianmukaisesti nimetyksi ja käyttäjälle varmuuden datan alkuperästä. Muunlaisia käyttöä rajoittavia ehtoja ei ole.[23]

Avoin tieto voi siten olla esimerkiksi reaaliaikaista tietoa bussien sijainnista tai tilastotietoa suosituimmista nimistä. Julkisuuslain (621/1999) nojalla julkinen tieto ei ole sama asia kuin avoin data, sillä siitä puuttuu monia avoimen datan määrityksen mukaisia elementtejä kuten avoimen datan käyttölupa ja datan saatavuus koneluettavassa muodossa avoimesta internetistä. On kuitenkin tapauksia, joissa nämä voivat olla sama asia eli julkista tietoa voi olla avattu avoimeksi dataksi. Osa tiedosta kuitenkin päätetään riskiarvioon perustuen jättää avaamatta, jolloin tieto on julkista mutta ei avointa. Työssä tulee tarkastella avointa tietoa, joten sen vuoksi käytetään käsitettä ”avoin ja julkinen tieto”. Mikäli raportissa tarkoitetaan vain julkisuuslain mukaista julkista tietoa, jolla ei ole salassapitoperusteita tai vain avointa dataa, käytetään raportissa näitä käsitteitä.

[23] Open Knowledgen ylläpitämä avoimen tiedon määritelmä (englanniksi)

8 LIITE 2: Kunnille lähetetty kysely

Manner-Suomen 292 kunnalle lähetettiin Kuntaliiton toimesta seuraava kysely 14.4.2025. Kyselyn sisältö valmisteltiin hankkeen työryhmän ja Kuntaliiton yhteistyössä.

Kunnille tehtävän kyselyn tarkoituksena on kartoittaa avoimen tiedon jakamisen ja riskiarvioiden tasoa kunnissa. Kuntia ei yksilöidä vastausten käsittelyssä eikä kuntien antamia tietoja julkisteta siten, että ne olisivat yhdistettävissä tiettyyn kuntaan. Kyselyn tuloksia käytetään valtiovarainministeriössä käynnissä olevan ”Kriittisen infrastruktuurin avoin tieto arvioidaan uudelleen huomioiden kansallinen turvallisuus” -hankkeen (VN/34688/2024) jatkotyössä ja eri toimijoille tehtävän tukimateriaalin laadinnan tukena. Korostamme riskiarviointien tärkeyttä jokaisessa kunnassa.

PERUSTIEDOT

Kunta:

Kunnan koko: pieni / keskikokoinen / suuri (onko näille määritelmää? esimerkiksi Kuntaliiton)

Maakunta: (tai jokin muu sijaintitieto)

Rajakunta: kyllä / ei

KYSYMYKSET

Onko kunnassanne nimettyä henkilöä, jonka vastuulla on arvioida avoimesti saatavilla olevan tiedon jakamista? kyllä / ei

Toimiala tai ammattinimike: _____

Onko kunnassanne arvioitu avoimeen tietoon liittyviä riskejä? (kyllä / ei)

Miltä toimialoilta olette tunnistaneet kriittisiä kohteita? (rasti ruutuun + avoin)

- energia
- liikenne
- pankkitoiminta
- finanssimarkkinoiden infrastruktuurit
- terveydenhuolto
- juomavesi
- jätevesi
- digitaalinen infrastruktuuri
- julkishallinto

- avaruus
- elintarvikkeiden tuotanto, jalostus ja jakelu.
- jotain muita, mitä: _____

Oletteko tunnistaneet näiden toimialojen kriittistä kohteista avoimesti saatavilla olevaa (kenen tahansa julkaisemaa) tietoa? (kyllä / ei)

JOS Kyllä, mainitse toimiala (kts. edellisen kysymyksen toimialat): _____

Mitä keskeisiä kriittisen infrastruktuurin avoimen tiedon jakamiseen liittyviä mahdollisia häiriötilanteita ja/tai riskejä olette tunnistaneet? (rasti ruutuun + avoin + linkki kansalliseen riskiarvioon) **(jaottelu kansallisen riskiarvion mukaisesti)**

- Informaatiovaikuttaminen
- Poliittinen, taloudellinen ja sotilaallinen painostus
- Sotilaallisen voiman käyttö
- Laajamittainen maahantulo ja painostaminen maahantulijoita ohjaamalla
- Yhteiskunnan rakenteisiin tai laajoihin ihmisjoukkoihin tehty terroristinen tai muu väkivaltainen isku
- Isojen väkijoukkojen, ryhmien tai yhteisöjen väkivaltainen liikehdintä tai yhteiskunnan järjestystä vaarantava toiminta
- Julkisen talouden häiriö
- Rahoitusjärjestelmän häiriö
- Energiahuollon häiriöt:
    - sähkönsaannin suurhäiriö
    - Polttoaineiden saannin vakavat häiriöt
- Tieto- ja viestintäverkkojen palveluiden häiriöt
- Kuljetusten jatkuvuuden häiriöt
- Terveysturvallisuuden häiriöt
    - mikrobilääkeresistenssi,
    - pandemia tai muu vastaava laajalle levinnyt epidemia,
    - eläintautiepidemiat
- Vesihuollon häiriöt
- Elintarvikehuollon häiriöt ja ruoka- ja ravintoturvan heikkeneminen
- Laajat tai pitkäkestoiset onnettomuustilanteet
    - merellinen monialaonnettomuus,
    - vakava ydinvoimalaitosonnettomuus Suomessa tai Suomen lähialueilla,
    - useampi yhtäaikainen laaja maastopalo,
    - äärimmäisen voimakas avaruusmyrsky
- jotain muita: _____

Onko kunnassanne tehty toimia, joilla kriittisistä kohteista avoimesti saatavilla olevan tiedon aiheuttamaa riskiä/uhkaa kyetään hallitsemaan? (kyllä / ei)

Onko kunnassanne dokumentoidusti ohjeistettu tietopyyntöjen käsittely? (kyllä / ei)

Onko kunnassanne prosessi salassa pidettävän tiedon käsittelylle (esimerkiksi kunnallisessa päätöksenteossa)? (kyllä / ei)

Tilastoidaanko kunnassanne tietopyyntöjen määrää? (kyllä / ei)

AVOIMET KYSYMYKSET

Mitä haasteita olette tunnistaneet avoimen tiedon jakamisessa? (avoin) (merkkimäärän rajoitus)

Minkälaista tukea tarvitsette kriittisen infrastruktuurin avoimesti saatavilla olevan tiedon arvioinnin tueksi? (avoin) (merkkimäärän rajoitus)

Oletteko tunnistaneet tarvetta laatia/täydentää ohjeistusta tietopyyntöjen käsittelyyn? Millaista? (avoin) (merkkimäärän rajoitus)

Avoin palaute/ajatukset jatkotyöhön (avoin) (merkkimäärän rajoitus)