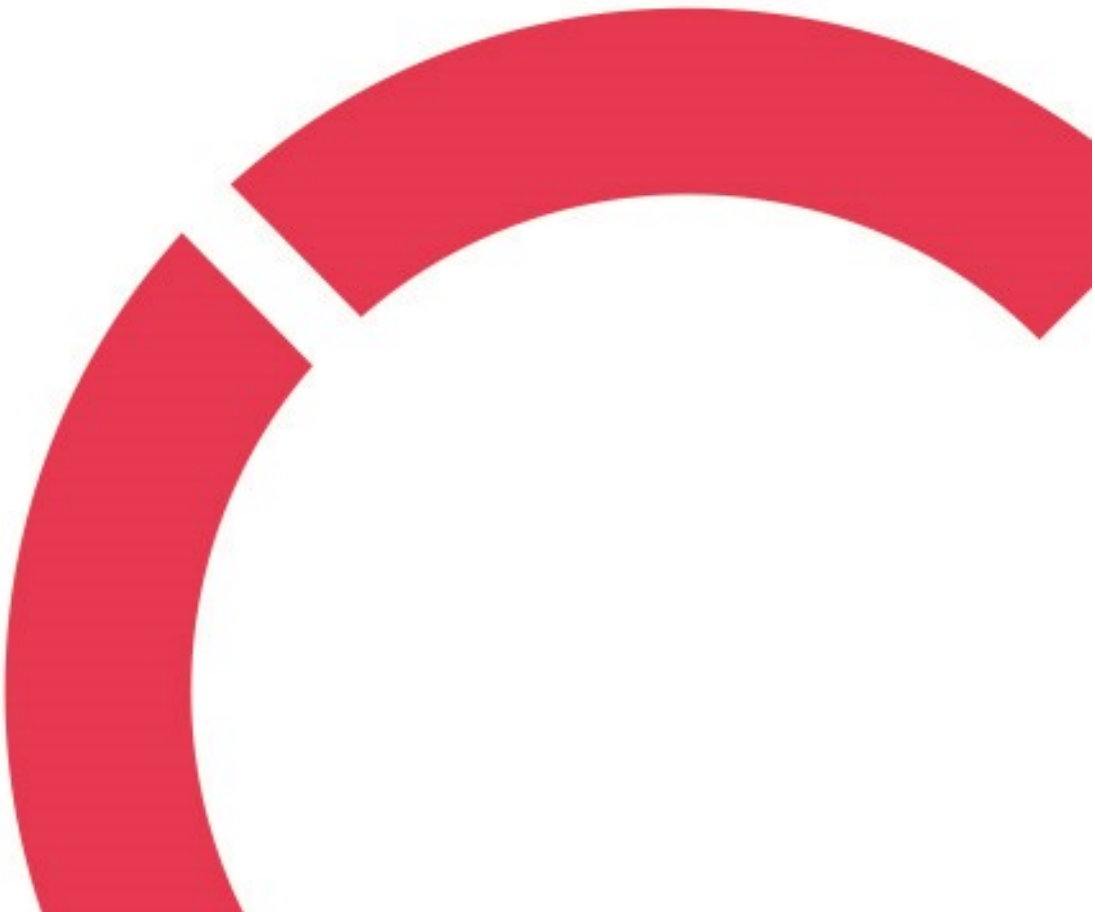
Sari Ontronen

JULKISEN HALLINNON ORGANISAATIOIDEN TIETOVERKKOJEN KEHITTÄMINEN TURVALLISUUDEN JA VARAUTUMISEN NÄKÖKULMASTA

Opinnäytetyö
CENTRIA-AMMATTIKORKEAKOULU
Digitalisaation johtamisen koulutus
Kesäkuu 2025



TIIVISTELMÄ OPINNÄYTETYÖSTÄ

Centria-ammattikorkeakoulu	**Aika** Kesäkuu 2025	**Tekijä/tekijät** Sari Ontronen
Koulutus Digitalisaation johtaminen		☐ AMK ☒ YAMK
Työn nimi JULKISEN HALLINNON ORGANISAATIOIDEN VERKKOJEN KEHITTÄMINEN TURVALLISUUDEN JA VARAUTUMISEN NÄKÖKULMASTA.		
Työn ohjaaja Tero Niemi		**Sivumäärä** 75 + 3
Työelämäohjaaja Jukka Kangasvieri		

Opinnäytetyö toteutettiin julkisen hallinnon organisaatioiden verkkojen suunnittelun ohjeistukseksi painottaen julkisen hallinnon organisaatioiden verkkojen kehittämistä turvallisuuden ja varautumisen näkökulmasta.

Tavoitteena oli tuottaa ohjeistus, joka palvelee julkisen hallinnon eri organisaatioiden (hyvinvointialueiden toimijoiden ja kuntien) verkkoratkaisujen kehittämistyötä huomioiden muuttuneen toimintaympäristön tietoturvallisuuden ja varautumisen asettamat vaatimukset.

Opinnäytetyössä luotiin katsaus eri julkisen hallinnon organisaatioiden tuottamiin verkkoratkaisuihin muissa maissa ja Suomessa, ja tulevaisuuden näkymiin eri verkkoratkaisuissa.
Opinnäytetyössä avattiin verkkoratkaisujen taustalla olevia julkisen hallinnon toimintaa ohjaavia lakeja/normeja ja sieltä nousevia vaateita ja mahdollisia muita organisaatioiden toimintaan liittyviä lisävaateita. Erityistä huomiota kiinnitettiin turvallisuuteen ja verkkojen tekniseen tuottamiseen liittyviin vaateisiin.

Työmenetelminä käytettiin olemassa olevan sähköiseen materiaaliin tutustumista, lisätiedon hakemista eri tietolähteistä ja verkkojen rakentamiseen osallistuneiden henkilöiden haastatteluja.
Opinnäytetyön lopputuotoksena syntyi ohjeistus, missä kerrotaan, mitä vaaditaan ja mitä organisaation kannattaa tehdä suunnitellessaan verkkoratkaisuja ja verkkojen ylläpitoa.

Asiasanat
JULKRI, KATAKRI, kiinteät verkot, kyberturvallisuus, NIS2, pelastuslaki, salaus, tiedonhallinta, turvallisuus, varautuminen, verkko, verkkoratkaisu.

ABSTRACT

Centria University of Applied Sciences	**Date** June 2025	**Author** Sari Ontronen
Degree programme Master of Engineering, Digitalization Management		
Name of thesis DEVELOPING NETWORKS IN PUBLIC ADMINISTRATION ORGANIZATIONS FROM A SECURITY AND PREPAREDNESS PERSPECTIVE		
Centria supervisor Tero Niemi		**Pages** 75 + 3
Instructor representing commissioning institution or company Jukka Kangasvieri		

The thesis was carried out as a guideline for the network design of public administration organizations, emphasizing the development of public administration organizations' networks from a safety and preparedness perspective.
The goal was to produce guidelines that will serve the development of network solutions of various public administration organizations (well-being services county operators, municipalities), considering the requirements set by information security and preparedness in the changed operating environments.
The thesis created an overview of the network solutions produced by various public administration organizations in other countries and in Finland, and the future prospects for different network solutions.
The thesis explored the laws/norms governing public administration operations underlying network solutions, the requirements arising from them, and possible other additional requirements related to the operations of organizations. Special attention was paid to requirements related to security and the technical production of networks.
The working methods used included reviewing existing electronic material, searching for additional information from various sources, and interviews with people who participated in building the networks.
The final product of the thesis was guidelines that explain what is required and what an organization should do when planning network solutions and maintaining networks.

Key words
Cybersecurity, encryption, fixed networks, information management, JULKRI, KATAKRI, network, network solution, NIS2, preparedness, rescue law, security.

KÄSITTEIDEN MÄÄRITTELY

Julkinen sektori

Julkinen sektori sisältää valtion sektorin, kunnat, kuntayhtymät ja hyvinvointialueet

CANARIE

Kanadan kansallisten tutkimus- ja koulutusorganisaatioiden runkoverkko

CAA

Crypto Approval Authority, CAA, salaustuotteiden hyväksyntäviranomainen

EU

European Union, EU, Euroopan Unioni

EU-CyCLONe

EU-CyCLONe, Euroopan kyberkriisien yhteysorganisaatioiden verkosto

FN4G-ohjelma

Future Networks 4 Generation, FN4G, Tulevaisuuden verkostot hallinnolle -ohjelma

GC

Government of Canada, Kanadan hallitus

GCSN

GC Science Network, GCSN, Kanadan hallituksen runkoverkko

Julkri

Julkisen hallinnon tietoturvallisuuden arviointikriteeristö

Kyberturvallisuus

Toimia, joita tarvitaan verkko- ja tietojärjestelmien, tällaisten järjestelmien käyttäjien ja muiden asian-osaisten henkilöiden suojaamiseksi kyberuhilta.

AI

Artificial Intelligence, AI, tekoäly

LAN

Local Area Network, lähiverkko

LIAS -palvelu

Paikallinen Internet -yhteyspalvelu

PPDR

Public Protection and Disaster Relief, PPDR, Yleisen turvallisuuden viranomaiset ja järjestöt

PSN

Public Service Network, PSN, Englannin hallituksen julkisten palvelujen verkko

RSA

Rivest-Shamir-Adleman, RSA, RSA -salaus

SLA

Service Level Agreement, SLA, SLA -palvelutaso sopimus palvelun tarjoajan ja asiakkaan välillä

VAHTi-ohje

Digitaalisen turvallisuuden tietopankki

WLAN

Wireless Local Area Network WLAN, langaton lähiverkko

WAN

Wide Area Network, WAN, suuralueverkko

TIIVISTELMÄ
ABSTRACT
KÄSITTEIDEN MÄÄRITTELY
SISÄLLYS

KUVIOT

TAULUKOT

1 JOHDANTO

Julkisen hallinnon organisaatioiden tietoverkkojen kehittämiseen ei ole olemassa kansallista yleistä oheistusta, joka opastaisi tietoverkkojen suunnitelmalliseen tietoturvallisuuden ja varautumisen huomioon ottavaan suunniteluun ja toteutukseen. Tietoverkkojen suunnittelua on tehty kansallisella tasolla suurimmaksi osaksi paikallisesti ja verkot on toteutettu paikallisten toimijoiden toimesta. Tietoverkkojen suunnittelussa ja toteutuksessa käytetyt tekniikat vaihtelevat toimijoittain, kuten myös varautumisen tason ja tietoturvallisuuden huomioiminen.

Opinnäytetyössäni pyrin antamaan näkymän kansallisten ja kansainvälisten julkisten hallintojen organisaatioiden tietoverkkojen historiaan, nykytilanteeseen ja tulevaisuuden näkymiin. Opinnäytetyön kansainvälisten ja kansallisten julkisen hallinnon tietoverkkojen kuvauksissa on huomioitavaa lähdemateriaalien saatavuus, joka aiheutuu kansallisten ja kansainvälisten tietoverkkomateriaalien julkaisemisen rajoituksista. Suurin osa tietoverkkoja kuvaavista materiaaleista esitetään yleisellä tasolla, koska yksityiskohtaisempi tietoverkkoihin liittyvä materiaali on suurimmalta osin salassa pidettävää.

Hahmotan työssäni myös julkisen sektorin erilaisten tietoverkkoratkaisujen taustalta löytyvää lainsäädäntöä, asetuksia ja ohjeita, mitkä ohjaavat tietoverkkojen suunnittelua asettamalla suunnittelulle, toteutukselle ja ylläpidolle reunaehdot ja vaateet. Myös organisaatioiden toimintaan saattaa liittyä edellä mainitun lisäksi omia organisaatio kohtaisia lisävaateita. Valtion hallinnon turvallisuusverkkoa käyttävien organisaatioiden osalta lainsäädäntö, asetukset ja ohjeet määräävät suoraan, miten tietoverkot tulee suunnitella, toteuttaa ja ylläpitää.

Verkon suunnittelu osiossa esittelen yleisemmät tekniikat ja suositukset tietoverkon suunnitteluun, toteutukseen ja ylläpitoon huomioiden julkisen organisaation toimialan erityispiirteet. Pyrkimyksenä on tuottaa ohjeistus, joka ohjaa tietoverkkojen suunnittelua, toteuttamista ja verkkojen ylläpitoa. Opinnäytetyössä huomioidaan julkisen sektorin organisaatioiden rooli erilaisten palvelujen tuottajana. Opinnäytetyössä korostetaan erityisesti tietoturvallisuuden ja varautumisen näkökulmaa tietoverkon suunnittelussa turvallisuustilanteen muutoksen aiheuttamien uhkien minimoimiseksi ja torjumiseksi. Tietoverkkojen suunnittelu rajataan kiinteisiin verkkoihin rajaten ulkopuolelle mobiiliverkot. Myöskään yksityisen sektorin tietoverkkojen suunnittelua en tässä opinnäytetyössä käsittele.

Tietoverkkojen suunnittelun tulevaisuuden trendit, haasteet ja uhat osiossa käsittelen tietoverkkojen tulevaisuuden näkymiä ja suunnitteluun liittyviä haasteita muutamin esimerkein, kuten kansalliselle turvallisuudelle aiheutuvat uhat ja niiltä suojautuminen, jotka liittyvät kansallisiin tietoverkkoihin. Työmenetelminä käytän olemassa olevaan sähköiseen lähdemateriaaliin tutustumista, lisätiedon hakemista eri verkkolähteistä ja verkkojen rakentamiseen osallistuneiden henkilöiden haastatteluja mahdollisuuksien mukaan.

Opinnäytetyön lopputuotoksena syntyy ohjeistus, missä kerrotaan, miten tietoverkot suunnitellaan, toteutetaan ja ylläpidetään huomioiden erityisesti asiakkaiden tarpeet liittyen tietoverkkojen nopeuteen, tehokkuuteen, saatavuuteen ja turvallisuuteen, sekä kansainvälisten ja kansallisten lakien ja säädösten asettamat vaateet, että myös tietoturvallisuuden ja varautumisen näkökulmat.

2 KANSAINVÄLISIÄ JULKISEN SEKTORIN VERKKORATKAISUJA

Tässä luvussa käydään yleisellä tasolla läpi esimerkkejä muiden maiden julkisten sektorien tietoverkkojen ratkaisuista, ja parhaita käytäntöjä (best practices) tietoverkkojen käyttöön liittyen. Kansainvälisiksi esimerkkimaiksi on valittu Tanska, Kanada, Saksa ja Englanti.

2.1 Tanskan valtion julkisen hallinnon verkkoratkaisuja

Tanskan valtion Digitaalisen hallinnon (Agency for Digital Goverment 2017) White book yhteisestä julkisen sektorin digitaalisesta arkkitehtuurista on valittu tähän opinnäytetyöhön esimerkkinä kuvaamaan Tanskan valtion julkisen sektorin digitalisaatiota ja tietoverkkojen kehitystyötä yleisellä tasolla kuvattuna.

Valkoisessa kirjassa esitetään julkisen sektorin visio, perusperiaatteet ja säännöt, jotka ovat johtaneet erialisiin käytännön tuotteisiin ja oppaisiin. Esimerkkinä digitaalisista palveluista voidaan mainita kansallinen portaali Borgetdk ja digitaalisista järjestelmistä sairausvakuutuskorttisovellus. (Agency for Digital Government 2017.)

2.2 Kanadan julkisen hallinnon verkkoratkaisu

Kanadan hallitus käynnisti vuonna 2011 laajamittaisen tietoverkkoinfrastruktuurin uudistuksen, jonka tavoitteena oli keskittää, standardoida ja modernisoida julkishallinnon IT-ympäristöä. Uudistuksessa on korvattu vanhentunut ja hajautettu verkkorakenne nykyaikaisella, turvallisella ja tehokkaalla ratkaisulla, joka tukee muun muassa pilvipalveluita, tekoälyä ja etätyötä. (SSC 2022.)

2.2.1 Hallituksen tietotekniikkainfrastruktuurin uudistaminen

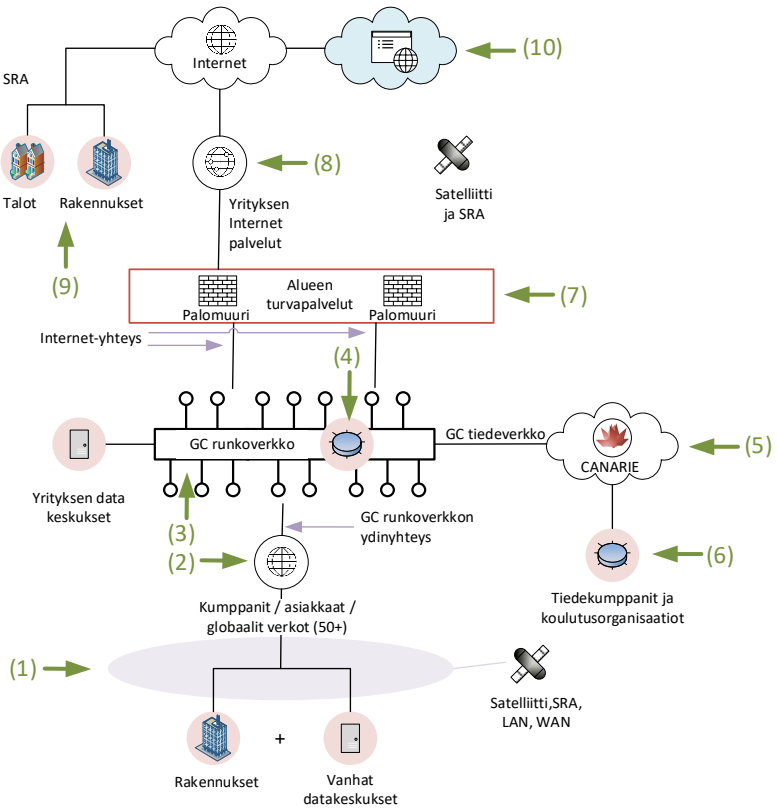
Shared Services Canada (SSC) sai vuonna 2011 Kanadan hallitukselta toimeksiannon uudistaa ja lujittaa Kanadan hallituksen (Goverment of Canada, GC) tietotekniikkainfrastruktuuria. Lähtötilanteena oli

monimutkainen ja vanheneva verkkoinfrastruktuuri periytyneenä useilta eri organisaatioilta. Ongelmana olivat vanhan verkon ylläpidon kalleus ja vanhentunut tekniikka, mikä ei tukenut nykyaikaisia palveluja kuten pilvipalveluita, puhe- ja dataliikennettä. (SSC 2022.)

SSC on lujittanut, vakauttanut ja modernisoinut verkon hallituksen IT-infrastruktuuria standardoidulla tekniikalla ja sopimuksilla. SCC on myös yksinkertaistanut hallinnollisia vaatimuksia liittyen verkkojen luotettavuuden ja vakauden lisäämiseen. Verkon uudistamisen tuloksena vuosina 2022–2023 kriittisten tapausten määrä väheni edellisvuoden 113 tapauksesta 105 tapaukseen. (SSC 2022.)

2.2.2 Hallituksen tietoverkon aikaisempi konfiguraatio

Kuvio 1 kuvaa Kanadan hallituksen (GC) tietoverkkojen aikaisempaa konfiguraatiota. Kaaviokuvassa on suluissa olevalla numerolla, esimerkiksi (1) viitattu alla olevan tekstin vastaavaan numeroituun kohtaan (1).



KUVIO 1. Kanadan hallituksen tietoverkon aikaisempi konfiguraatio (SSC 2022, mukaillen)

Kuviossa 1 kuvataan Kanadan hallituksen ja sen organisaatioiden tietoverkkojen vanhaa rakennetta. Kaaviokuvassa on suluissa olevilla numeroilla esimerkiksi (1) viitattu alla olevan tekstin vastaavasti numeroituihin kohtiin (1).

Rakennukset ja vanhat datakeskukset (1) muodostavat yhteyden kumppani- ja asiakasverkkoihin, sekä globaaleihin yli 50 verkkoon (2):

- satelliittien,
- suojatun etäkäytön (SRA),
- lähiverkkojen (LAN) tai
- suuralueverkkojen (WAN) kautta (SSC 2022).

Nämä verkot sekä yritysten datakeskukset muodostavat yhteyden GC:n runkoverkkoon (3), jossa on myös GC tiedeverkko (4). GC tiedeverkko muodostaa yhteyden CANARIE -palveluun (5), joka on Kanadan tiedepilvi, käytyään läpi suojapalomuurit. Myös tiedekumppani- ja koulutusorganisaatiot (6) muodostavat yhteyden CANRIE:en.

GC runkoverkko muodostaa yhteyden Internetiin verkkosuojauspalomuurien (7) kautta yrityksen Internet -palveluun (8). Myös talot ja rakennukset (9) muodostavat yhteyden Internetiin SRA:n ja mahdollisten satelliittien kautta.
Internetin kautta muodostuu yhteys myös luokittelemattomiin pilvipalveluntarjoajiin (10). (SSC 2022.)

2.2.3 Hallituksen tietoverkon nykyinen konfiguraation verkkolaitteet ja yhteyspalvelut

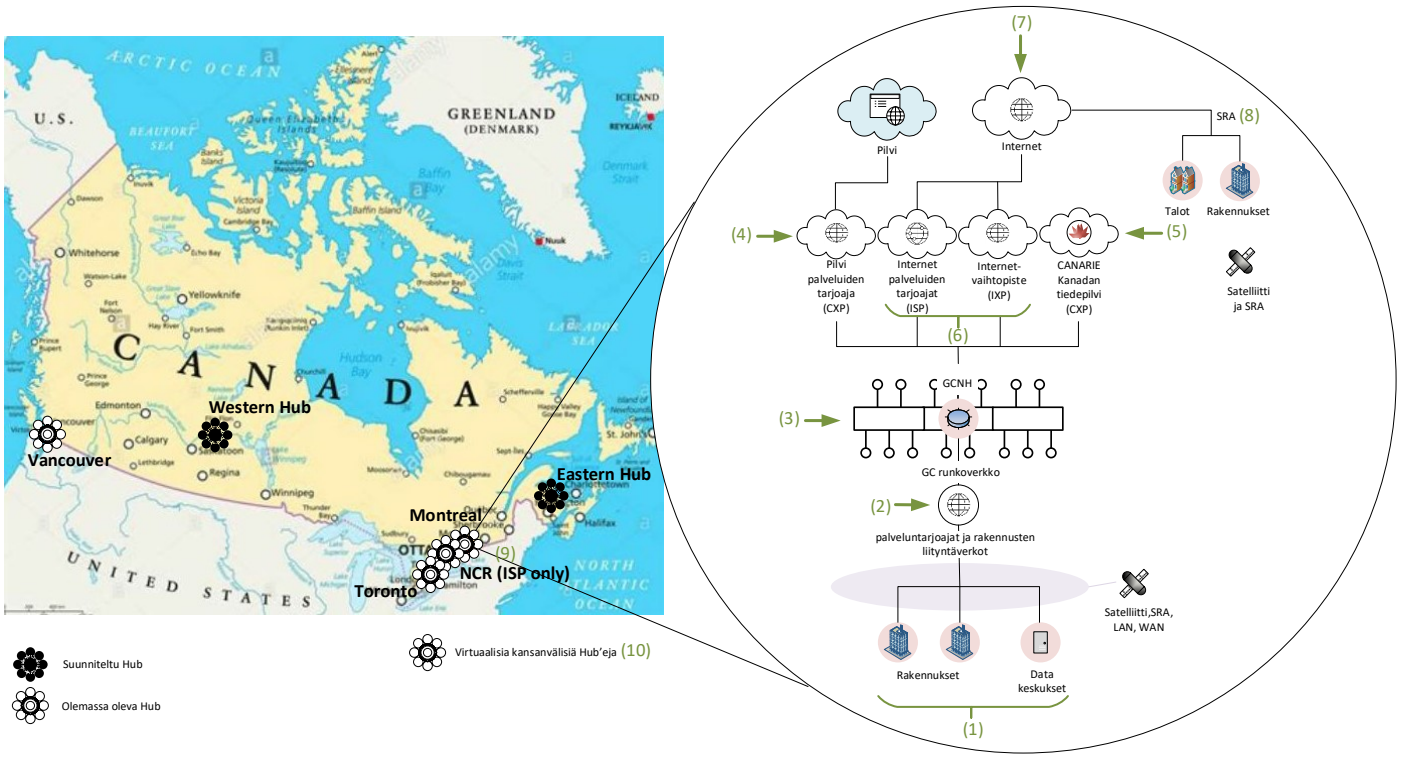
SSC ylläpitää Kanadan hallituksen sisäisiä verkkoja ja laajaverkkoja, runkoverkkoa, GCSN -verkkoa, Internet- ja pilviyhteyksiä, sekä tuottaa verkkoihin liittyviä palveluja. Taulukossa 1 on lueteltu SCC:n tuottamat palvelut, verkkotyypit, käyttäjäryhmät ja käyttöpaikat.

TAULUKKO 1. SSC:n Kanadan hallitukselle tuottamat ja ylläpitämät verkkolaitteet ja yhteyspalvelut (SSC 2022)

Verkko	Palvelut	Verkkotyyppi	Käyttäjät	Käyttöpaikka
Sisäiset verkot	Yhteyspalvelut	LAN, WLAN	GC:n käyttäjät	Hallintorakennukset, muut työpaikat
Laajaverkot	Yhteyspalvelut datakeskuksiin, pilveen, LIAS -palveluun, satelliitteihin, matkapuhelimiin	WAN	GC:n käyttäjät	Hallintorakennukset
Suojattu etäkäyttö	Yhteyspalvelut etäkäyttöön	Turvallinen yhteys	GC:n käyttäjät	Toimipisteen ulkopuolella
GC Backbone	GC WAN -yhteyspalvelut (palvelun ydin)	WAN	GC:n käyttäjät	Rakennuksien sisäiset ja osastojen verkot, GC:n palvelinkeskukset, Internet
Yrityksen Internet -yhteys	Nopeat yhteydet GC -runkoverkon ja Internetin välillä	Internet	GC:n käyttäjät	GC:n runkoverkkoja Internetin välillä
GCSN (GC Science Network)	Kanadan kansalliset tutkimus- ja koulutusorganisaatiot	CANARIE (runkoverkko)	Liittovaltion tiedeosastot ja -virastojen käyttäjät	Liittovaltion tiedeosastot ja -virastot
Pilviyhteys	Yhteyspalvelut pilvipalveluun	Internet	GC Backbone käyttäjät	GC Backbone ja pilvipalvelun tarjoajien välillä

2.2.4 Hallituksen nykyinen Hub-malli

Government of Canada Networks Hub Model (GCNH) eli Hub -malli hyödyntää ohjelmiston määrittämää verkkoinfrastruktuuria ja tekoälyä (AI) liikenteen sujuvuuden ja ylläpidon automatisoimiseksi parantaen yhteyksien hallittavuutta ja suorituskykyä mahdollistaen Kanadan hallituksen pilvipalvelustrategian. Päivitetty verkko käyttää uusimpia turvatoimenpiteitä, jotka antavat paremman henkilötietosuojan, yhdistävät saumattomasti pilvi- ja yritysdatakeskuksiin ja mahdollistavat nopeat ja riittävän laajat yhteydet käyttäjille työtehtävien suorittamiseen. SSC tekee yhteistyötä liittovaltion kumppaneidensa ja asiakkaidensa modernisoidakseen yhteyksiä yhdistämällä ja standardisoimalla heille saatavilla olevia vaihtoehtoja. Nämä toimenpiteet tekevät Kanadan hallituksesta reagoivamman kanadalaisten palveluihin. (SSC 2022.)



KUVIO 2. Kanadan hallituksen tietoverkon Hub -malli (SSC 2022)

Kuviossa 2 kuvataan Kanadan nykyisen hallituksen tietoverkon Hub -mallia. Kaaviokuvassa on suluissa olevalla numerolla, esimerkiksi (1) viitattu alla olevan tekstin vastaavaan numeroituun kohtaan (1).

Hub -mallin kaaviokuvan karttaan on symboleilla merkitty Kanadan kuuden verkkokeskuksen sijainnit eri puolilla maata:

- Nykyiset verkkokeskukset:
  Vancouver, Toronto, National Capital Region (NRC), Montreal
- Suunnitellut verkkokeskukset:
  Länsikeskus (Western Hub sijaitsee preerialla), Itäinen keskus (Eastern Hub sijaitsee Maritimes'issa) (SSC 2022).

NRC-verkkokeskuksessa on vain Internet-yhteys. Edellä mainittujen verkkokeskusten lisäksi suunnitteilla on myös laajennuksia, esimerkiksi NRC-verkkokeskus (9) ja virtuaalisia kansainvälisiä keskuksia (10) tukemaan Kanadan hallituksen työtä ympäri maailmaa.

Rakennukset ja datakeskukset (1) yhdistyvät palveluntarjoajien ja rakennusten liityntäverkkoihin (2) satelliitin, SRA:n, LAN:n ja WAN:n kautta.
Palveluntarjoajat ja rakennusliityntäverkot muodostavat yhteyden GC -runkoverkkoon (3), jossa sijaitsee Kanadan hallituksen verkkokeskus. (SSC 2022.)

GC -runkoverkosta eteenpäin keskitin yhdistää

- Pilvipalveluiden tarjoajan (CXP) (4), joka muodostaa yhteyden pilveen
- CANARIE:n (5), joka on Kanadan tiedepalvelupilvi
- Internet -palveluntarjoajat (ISP, IXP) (6), jotka muodostavat yhteyden Internettiin (7) (SSC 2022).

Talot ja rakennukset muodostavat yhteyden Internettiin suojatun etäkäytön SRA:n kautta (8). Kaikki edellä mainitut yhteydet ovat mahdollisia myös SRA:n ja satelliittien kautta (SSC 2022).

GC Networks Hub (GCNH) -lähestymistapa hyödyntää ohjelmiston määrittämää verkkoinfrastruktuuria ja tekoälyä (AI) liikenteen sujuvuuden ja ylläpidon automatisoimiseksi mahdollistaen verkkoyhteyden hallittavuuden ja suorituskyvyn paranemisen. Jokainen GCNH tarjoaa myös ulkoisen verkkoyhteyden GC-runkoverkon ja pilvi-, Internet- ja Canarie-keskusten välillä. (SSC 2022.)

2.3 Saksan julkisen hallinnon aikaisempia ja tulevia verkkoratkaisuja

Liittovaltion verkot syntyivat useista osavaltioiden edeltäneistä verkoista, jotka eri virastot perustivat ja hallinnoivat:

- Berliini-Bonnin tietoverkko (IVBB) ja
- liittovaltion hallinnon tietoverkko / liittovaltion hallintoverkosto (IVBV/BVN). (BDBOS 2025a.)

Näiden erilaisten verkostojen yhtenäistämiseksi ja lujittamiseksi on perustettu projektiryhmä. Liittovaltion sisäministeriö on määritellyt vaatimukset viranomaisverkolle yhdessä käyttäjäviranomaisten ja Liittovaltion tietoturvaviraston kanssa. (BDBOS 2025a.)

Liittovaltion verkot muodostavat hallituksen ja Saksan hallinnon digitaalisen viestintäverkoston, johon on kytkettynä noin 200 liittovaltion viranomaista ja yli 300 000 työntekijää käyttää verkkoa. Liittovaltion verkoilla on verkko rajapintoja eri valtioiden ja kuntien verkkoihin. Saksan liittovaltion verkkoinfrastruktuurille ja verkkojen kautta tarjottaville toiminnoille on ominaista erikoisuutena erittäin korkea käytettävyys. Keskimääräinen verkon käytettävyys on 99,95 %, mikä vastaa alle 1 minuutin verkon käyttämättömyyttä vuorokaudessa. Verkkoinfrastruktuuri täyttää korkeimmat turvallisuusstandardit, mikä mahdollistaa myös arkaluonteisen tiedon siirron ilman ongelmia. (BDBOS 2025a.)

Pitkän aikavälin tavoite on kehittää laajentamalla (julkihallinnon tietoverkko, IVÖV) yhteinen verkosto koko Saksan julkishallinnolle. (BDBOS b.) Edellä mainittu radioverkko perustuu TETRA -standardiin. Federal Agency for Public Safety Digital radio, BDBOS vastaa verkko-operaattorina Saksan liittovaltion verkkojen toimivuudesta edistäen verkkojen konsolidointia ja muutosta. BDBOS on liittovaltion virasto ja kuuluu liittovaltion sisä- ja yhteistyöministeriöön. (BDBOS 2025a.)

Yleisen turvallisuuden viranomaiset ja järjestöt (Public Protection and Disaster Relief, PPDR), joita ovat poliisi, palokunta ja pelastuslaitokset ja niin edelleen, käyttävät Bublic Safety Digital radiota sekä päivittäisissä toimissa että monimutkaisissa toimita tilanteissa, kriisitilanteissa ja katastrofeissa. (BDBOS 2025c.)

2.3.1 Digitaalisten yhteyksien kehittäminen Saksassa

Saksan valtion liittohallituksen tekemässä koalitiosopimuksessa vuonna 2021 digitaalinen infrastruktuuri asetettiin yhdeksi prioriteetiksi, ja tavoitteena oli FTTH- ja 5G -verkkojen valtakunnallinen tarjonta vuoteen 2025 mennessä. Perusperiaatteita ovat avoin saatavuus oikeudenmukaisin ehdoin ja verkon neutraalius.
Saksan liittovaltion digitaalistrategialla ja Saksan gigabittistrategialla vuodelta 2022 pyritään valokuituteknologian ja uusimpien matkaviestintäteknologioiden valtakunnalliseen tarjontaan kaikilla alueilla vuoteen 2030 mennessä. (EU 2025.)

Liittovaltion digitaali- ja liikenneministeriö (Bindesministerium fu Digitales und Verkehr, BMDV) vastaa digitaalisten yhteyksien kehittämisestä ja liittohallituksen digitaalisten yhteyksien strategian täytäntöönpanosta.
Saksaan kansallinen laajakaistaa käsittelevä virasto (BCO) on liittovaltion gigabittivirasto, joka on liittovaltion digitaali- ja liikenneministeriön (Gigabitburo des Bundes) osaamiskeskus.
Liittovaltion talous- ja ilmastoministeriö (Bundesministerium fur Wirtschaft und Klimaschutz) edistää digitaalisen infrastruktuurin ja liikenneinfrastruktuurin keskeisiä aloja. (EU 2025.)

2.4 Englannin julkisen hallinnon verkkoratkaisuja

Julkisten palvelujen verkko (Public Services Network, PSN) on vanha Englannin hallituksen korkean suorituskyvyn verkko, joka auttaa julkisen sektorin organisaatioita työskentelemään yhdessä, vähentämään päällekkäisyyksiä ja jakamaa resursseja (GOV.UKa. 2015a).

PSN -verkko käynnistettiin virallisesti vuonna 2005 osana Transformational Government Strategy -strategiaa alkuperäisellä nimellään Public Sector Network. Ennen PSN -verkon virallista käynnistämistä eräät paikallishallinnon osat olivat jo onnistuneet toteuttamaan konseptin. Hampshire Public Services Network (HPSN) oli ensimmäinen PSN -verkko, joka otettiin käyttöön vuonna 1999.
(GOV.UKa. 2015.)

Verkostojen alkuperäinen konsepti perustui paikallishallinnossa jo tehtyyn työhön ja rikosoikeudellisen alan etujärjestön (COI) tunnustamiseen Office for Criminal Justice Reform (OCJR) työskentelyn

aikana vuosina 2005 – 2007 tietojen jakamisen mahdollistamiseksi liiketoimintayksiköiden välillä. (GOV.UKa. 2015.)

PSN:n tekniset ja arkkitehtuurin vaatimustenmukaisuuskriteerit perustettiin vuodesta 2007 lähtien, kun GDS työskenteli Socitmin (Informaatioteknologian hallinnan yhdistyksen) paikallishallinnon johtajien kanssa kansallisessa CIO -neuvostossa ja paikallisessa CIO -neuvostossa. PSN -verkko yhdisti verkkoinfrastuktuurin tarjoamisen Englannin julkisella sektorilla toisiinsa yhdistetyksi ”verkkoverkostoksi” tavoitteena tehokkuuden lisäämiseksi ja julkisten kokonaismenojen vähentämiseksi. (GOV.UKa. 2015.) PSN luo mielikuvan yhdestä verkosta, joka kattaa koko Englannin hallituksen ja jota useat palveluntarjoajat tarjoavat. PSN -verkko koostuu Government Conveyance Network (GCN) -verkosta, Direct Network Service Provider (DNSP) - verkosta ja muista PSN -verkoista (GOV.UKa. 2015).

GCN yhdistää PSN -verkot toisiinsa. Sen tarkoituksena on mahdollistaa asiakkaille pääsy minkä tahansa palveluntarjoajan palveluihin missä tahansa verkossa.
PSN on nyt vanha ja julkisen sektorin organisaatiot ovat siirtymässä käyttämään julkisen Internetin palveluita. (GOV.UKa. 2015.)

2.4.1 Hallituksen PSN -tietoverkon aikaisempi konfiguraatio

PSN koostuu ydinverkosta, GCN -palveluntarjoajien tai GCNSP:n tarjoamasta Government Conveyancing Networkista tai GCN:stä (GOV.UKa. 2015).

GCN yhdistää useita operaattoriverkkoja, joita kutsutaan suoriksi verkkopalveluntarjoajiksi eli DNSP:ksi. Tilaajaorganisaatiot tekevät sopimuksen paikallisen osallistuvan DNSP:n yhteydessä, ja muodostavat yhteyden sen kautta GCN:n ja siten eteenpäin muihin yhteen liitettyihin verkkoihin ja palveluihin. GCN -verkko perustuu kokonaan IPv4:n ja MPLS:n, eikä GCNSP:t ole tällä hetkellä valtuutettuja tarjoamaan IPv6:ta, vaikka niillä pitäisi olla etenemissuunta sen toteuttamiseksi tarvittaessa. (GOV.UKa. 2015.)

2.4.2 Future Networks for Government (FN4G) -ohjelma

FN4G -ohjelma perustettiin auttamaan hallinnon organisaatioita siirtymään pois vanhasta PSN -verkosta nykyaikaisiin verkkoratkaisuihin, koska PSN -verkkoa oli yhä vaikeampi suojata. Nykyaikaiset verkkoratkaisut tarjoavat kilpailukykyisempiä kaupallisia ehtoja, suurempaa joustavuutta ja skaalautuvuutta. FN4G -ohjelma oli Cabinet Office -ohjelma, joka päättyi vuonna 2023. (GOV.UKb 2022b.)

Englannin hallituksen Central Digital and Data Office'n tehtävänä oli:

- valvoa ja hallita PSN -yhteensopivuusprosessia
- valvoa keskeisiä PSN -palveluita ja tarjota asiakkaalle tarvittava tuki
- tarjota tukea ja opastusta sekä asiakkaille että palveluntarjoajille PSN- yhteyden muodostamisessa
- tarjota palveluita ja ohjeita, jotka auttavat sekä asiakkaita että palveluntarjoajia saavuttamaan ja ylläpitämään PSN -yhteensopivuutta (GOV.UKb 2022).

FN4G -ohjelma koordinoi ja raportoi organisaatioiden suunnitelmista siirtyä pois PSN:n verkon käytöstä. Ohjelman ennakoiva strategia nykyaikaisen verkkoarkkitehtuurin tunnistamiseksi ja edistämiseksi tarjosi parempaa tietoturvallisuutta ja tuki samanaikaisesti julkisen sektorin organisaatioiden pois siirtymistä PSN:n käytöstä. (GOV.UKb 2022.)

Useimmissa tapauksissa paikallisviranomaiset käyttivät paikan päällä jo olevaa infrastruktuuria erillisen linjan vetämiseen suoraan PSN:ään. Julkisen sektori organisaatiot pystyivät käyttämään PSN yhteensopivia palveluita PSN:n kautta. Myös kaupalliset palveluntarjoajat pystyivät myymään palveluita julkisen sektorin organisaatioille PSN:ssa, mutta niiden oli oltava PSN -yhteensopivia. (GOV.UKb 2022.)

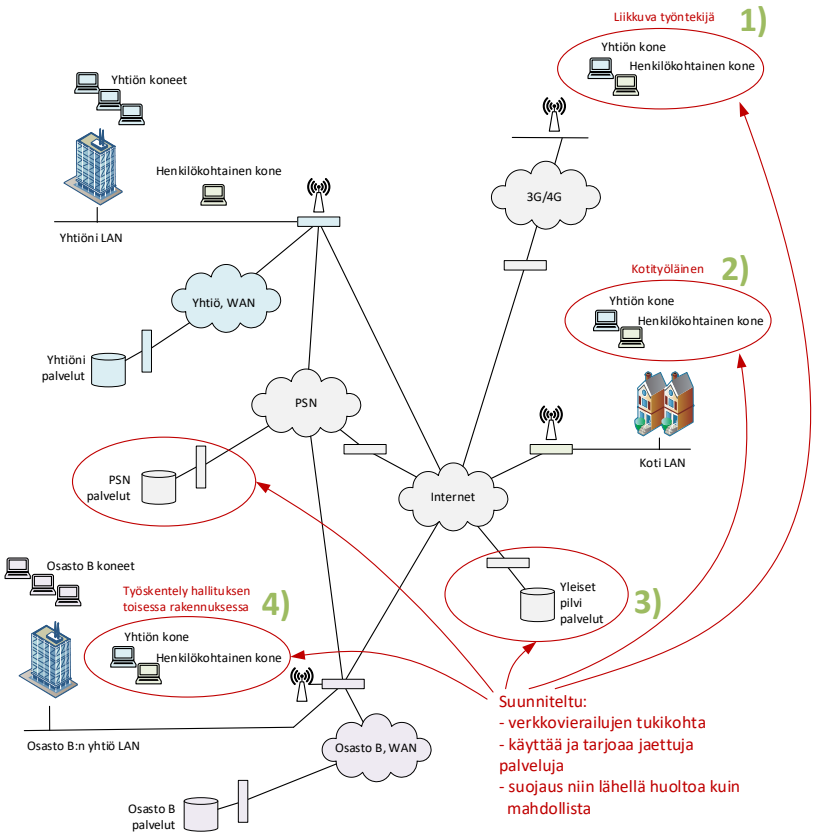
FN4G -ohjelma esitti neljä vaihtoehtoista tapaa muodostaa yhteys PSN -ekosysteemiin. Yhteydenmuodostustavat olivat työpöytäpalvelu, jaettu pääsy PSN:ään (SAP), tunneloitu pääsy PSN:ään (TAP) ja yhdyskäytävän käyttöoikeus PSN:ään (GAP) (GOV.UKb 2022).

Esimerkki: Valtion suojatun intranetin verkkotunnusten muutosGovernment Secure Intranet (GSi) oli Englannin hallituksen laaja alueverkko, jonka päätarkoituksen oli mahdollistaa verkkoon liittyvien or-

ganisaatioiden kommunikointi sähköisesti ja turvallisesti alhaisella suojausmerkintätasolla. Se tunnettiin valtion sähköpostien .gsi.gov.uk -verkkotunnuksista. Siirtyminen pois näistä verkkotunnuksista alkoi vuonna 2019 ja saatettiin päätökseen vuonna 2024. (GOV.UKb. 2025.)

2.4.3 Valtion verkoston suunnittelun periaatteet

Englannin valtion verkot muodostavat alustan, joka mahdollistaa digitaalisten palveluiden toimittamisen valtion verkon loppukäyttäjille eli henkilöille, joka käyttävät palveluja. Loppukäyttäjille verkon tulisi näyttäytyä läpinäkyvänä, joustavana ja on kaikkialla saatavilla. Verkon suunnittelun periaatteina on myös edellä mainittujen lisäksi huomioitu tasapaino nopeuden, laadun, turvallisuuden, hallinnan ja kustannusten välillä. (GOV.UKc. 2015.) Valtion verkkojen muodostama alusta on suunniteltu (KUVIO 3) verkkovierailukäyttöön, yhteisten palvelujen käyttöön ja tarjoamiseen, ja tarjoamaan suojan mahdollisimman lähellä palveluja. (GOV.UKc. 2015.)



KUVIO 3. Verkot, joihin valtion tietoverkon käyttäjät voivat olla yhteydessä (GOV.UKc. 2015, mukaillen)

Kuviossa 3 on kuvattu julkisen hallinnon verkon työntekijän liittymisvaihtoehtoja julkisen hallinnon verkkoon ja PSN -ekosysteemin palveluihin:

1) liikkuvan työntekijänä 3G/4G(/5G) -verkkojen ja Internetin kautta
2) koti työntekijänä lähiverkon (LAN) ja Internetin kautta
3) julkinen pilvipalvelun ja Internetin kautta
4) toisesta hallintorakennuksesta yrityksen osasto B:n lähiverkon (LAN) kautta (GOV.UKc. 2015).

Verkon suunnittelussa käytettyjä periaatteita ovat:

1. Ymmärrä käyttäjän tarve:
    - ymmärrä verkon perusvaatimukset
    - kotoa käsin tai muissa työnantajan toimipisteissä
    - mahdollista suunnittelupalveluiden laajempi käyttö (kehitä työkaluja, joihin pääsee ilman ylimääräistä asiakasohjelmistoa myös muista hallintorakennuksista)
    - suunnittelu verkko organisaatioille, jotka jakavat sivustoja myös verkkoon
    - harkitse mobiilidataa (3G, 4G, 5G) vaihtoehtoisen tiedonsiirtomekanismina
    - hanki taidot ja työkalut tukea käyttäjiä (GOV.UKc. 2015).
2. Suunnittele verkkoja verkkovierailukäyttöön (GOV.UKc. 2015).
3. Käytä palveluita tietojesi suojaamiseen (älä luota verkkoon):
    - ymmärrä uhat ja kehitä selkeä strategia verkkojen turvallisuudelle
    - suunnittele palveluiden suojaus mahdollisimman lähelle palvelun rajaa.
    - suojaa laitteesi ja palvelusi pilvitietoturvaperiaatteella ja julkaise verkkojen reitit oletuksena
    - ota salaus käyttöön suorituskyvystä tinkimättä
    - suojaa verkkosi
    - varmista tietoturvasi (GOV.UKc. 2015).
4. Yhteistyön ja joustavuuden suunnittelu:

- käytä avoimia julkaistuja standardeja
- maksimoi kaupallisten palveluiden käyttö
- yhdistä tietoverkkojen käyttö ja siirry IP -pohjaisiin teknologioihin
- julkaise DNS -nimet
- poista tekniset esteet valtioiden väliseltä pääsyltä
- tarjoaa joustavuutta (GOV.UKc. 2015).

2.4.4 Valtion digitaalihallinnon tilannekatsaus -raportti

Englannin valtion digitaalihallinnon tilannekatsaus -raportti esittelee keskeiset havainnot digitaalisen hallinnon tilasta, missä on mahdollista rakentaa menestystä, missä on parannettava, ja yksilöidään viisi perimmäistä syytä kohdattuihin haasteisiin. (GOV.UKd. 2025.)

Englannin julkisella sektorilla on valtavat digitaaliset resurssit. Julkinen sektori käyttää vuosittain yli 26 miljardia puntaa digitaalitekniikkaan työllistäen liki 100 000 digitaali- ja data-alan ammattilaista, ja toimittaa miljoonia verkkotapahtumia eri tyyppisinä digitaalisina palveluina päivittäin. (GOV.UKd. 2025.)

Nämä edellä mainitut resurssit voivat tuottaa erinomaisia tuloksia, jos ne käytetään tehokkaasti. Onnistumiset saavutetaan kuitenkin liian usein järjestelmästä huolimatta eikä sen vuoksi. Luotetaan asiantuntijoiden omistautumiseen, jotka tekemät parhaansa rajallisilla resursseilla, toteuttavat politiikkoja, joita ei ole suunniteltu ensisijaisesti digitaalisiksi, navigoivat prosesseja, joita ei ole suunniteltu digitaaliselle aikakaudelle, ja niin edelleen.
Raportti nostaa esiin viisi perimmäistä syytä digitaalisen hallinnon kohtaamiin haasteisiin:

1. Johtajuus
    - Palvelun digitalisoinnin, luotettavuuden tai riskien vähentämisen priorisoinnista ei juurikaan palkita
2. Rakenne
    - Hajanaisuus on järjestelmän ominaisuus. Julkisen sektorin organisaatiot ovat riippumattomia elimiä, joilla on rajalliset mekanismit tehdä sopimuksia palveluista
3. Mittaus

   - Julkisella sektorilla ei ole yhtenäisiä digitaalisen suorituskyvyn mittareita, yhdistettyjä ja summattuja tietoja palveluiden laadusta ja käyttökokemuksista

4. Lahjakkuus
   - Palkkaus ja urakehitys eivät ole kilpailukykyisiä yksityisen sektorin kanssa.
5. Rahoitus
   - Kulutus on painotettu uusiin ohjelmiin. Olemassa olevien järjestelmien, erityisesti vanhojen omaisuuserien tehokasta toimintaa ja ylläpitoa ei priorisoida riittävästi. (GOV.UKd. 2025.)

Raportin johtopäätös oli, että digitalisaatio on yksi voimakkaimmista julkisen palvelun uudistuksen voimista, jo onnistuessaan se muuttaa elämää ja julkista kokemusta hallinnosta.
Esimerkiksi terveydenhuollon alalla, jossa Cambridge NHS Trust otti käyttöön ”virtuaaliset osastot” potilaiden hoitamiseksi heidän kotonaan, ja säästi yli 1 000 vuodepäivää sairaalakapasiteetista kuukaudessa.
Raportissa esiin nostetut viisi syytä digitaalisen hallinnon haasteisiin eli lähestymistapa johtajuuteen, rakenteeseen, mittaamiseen, lahjakkuuteen ja rahoitukseen ei vielä kuitenkaan anna oikeutta tälle potentiaalille, mikä vaatii muutosta ja uudistusta tapaan toimia digitaalisesti (GOV.UKd. 2025.)

3 KANSALLISIA JULKISEN SEKTORIN VERKKORATKAISUJA

3.1 Julkisen sektorin ICT

Suomessa valtiovarainministeriö ohjaa julkisen sektorin tietohallintoa, rakennekehitystä sekä yhteisiä palveluja ja palvelu tarjontaa. Valtiovarainministeriö ohjaa myös tietoturvallisuuden yleisiä kriteerejä, valmistelee tieto- ja hallintopolitiikkaa sekä kehittää digitaalista hallintoa.
Kukin ministeriö ohjaa tietohallinnon ja siihen liittyvien hankkeiden kehittämistä omalla hallintoalallaan. (VM 2025a.)

Julkisen sektorin ICT-osasto luo edellytyksiä julkisen sektorin digitalisoitumiselle ja on vahvana esimerkkinä. Tämä tehdään digitalisoimalla julkisen sektorin palveluita, edistämällä hallinnon välistä yhteen toimivuutta ja mahdollistamalla viranomaisten toiminnan turvallisuus. (VM 2025a.)

3.1.1 Julkisen hallinnon turvallisuusverkkotoiminta (TUVE)

Julkisen hallinnon turvallisuusverkkotoiminnalla (TUVE -toiminta) turvataan valtion ylimmän johdon ja yhteiskunnan turvallisuuden kannalta tärkeiden viranomaisten yhteistyötä ja viestintää kaikissa tilanteissa. Julkisen hallinnon turvallisuusverkkotoiminnasta on säädetty lailla (FINLEX 2015a.). Tuve -verkko on valtion omistuksessa tai hallinnassa oleva viranomaisverkko, johon kuuluu viestintäverkko, siihen liittyvät laitetilat ja laitteet sekä yhteiset tieto- ja viestintätekniset palvelut. Palveluita tuotetaan, valvotaan ja hallitaan kellon ympäri. Verkolla mahdollistetaan jokapäiväinen työskentely sekä operatiivisessa toiminnassa että hallinnollisissa tehtävissä. Tuve -verkon palvelut ovat käytettävissä koko valtakunnan alueella ja myös kansainvälisissä tehtävissä. (VM. 2025b.)

Tuve-palveluja tuotetaan Tuve-laissa määritetyille käyttäjäryhmille valtioneuvostossa, Poliisin eri organisaatioissa, Rajavartiolaitoksessa, Hätäkeskuslaitoksessa, Maahan-muuttovirastossa, Puolustusvoimissa, Tullissa, pelastustoimessa, ensihoidossa sekä eräissä näitä viranomaisia tukevissa organisaatioissa. Edellä mainituille palveluilla on noin 35 000 käyttäjää. (VM. 2025b.)

Valtion tieto- ja viestintätekniikkakeskus Valtori tuottaa turvallisuusverkon tieto- ja viestintäteknisiä palveluja ja integraatiopalveluja. Suomen Erillisverkot Oy, joka on valtion kokonaan omistama, tuottaa

turvallisuusverkon verkko- ja infrastruktuuripalveluja. Erillisverkot tuottaa myös Tuve-lain tarkoittamat viranomaisradioverkon sekä viranomaisten aikakriittisen laajakaistaisen matkaviestinnän tieto- ja viestintätekniset palvelut eli niin sanotut Virve -palvelut.

3.1.2 Sosiaali- ja terveystoimen korkean varautumisen tietojärjestelmät ja verkot

Sosiaali- ja terveystoimessa on käytössä useita eri tietojärjestelmiä. Kansallisesti korkean varautumisen viestintä- ja tietojärjestelmillä tarkoitetaan:

- viranomaisverkko Virve'ä
- viranomaisten yhteiskäyttöistä kenttäjärjestelmä Kejo'a
- viranomaisten yhteiskäyttöistä hätäkeskustietojärjestelmä Erica'a (STM 2021).

Näiden järjestelmien lisäksi sosiaali- ja terveystoimella on käytössä hallinnon turvallisuusverkko TUVE. Edellä mainituilla järjestelmillä ja verkoilla turvataan sujuva viranomaisyhteistyö ja tiedonvaihto kaikissa olosuhteissa. Hätäkeskusrajapinnassa toimiville viranomaisille välitetään tehtävät vain näiden järjestelmien kautta. (STM 2021.)

4 SUOMESSA JULKISEN HALLINNON TOIMINTAA OHJAAVAT LAIT, ASETUKSET JA OHJEET

Suomessa lait, asetukset ja ohjeet säätelevät julkisen hallinnon organisaatioiden toimintaa. Näitä ovat muun muassa:

- Laki julkisen hallinnon turvallisuusverkkotoiminnasta 10/2015
- Laki julkisen hallinnon tiedonhallinnasta 906/2029
- Valtioneuvoston asetus julkisen hallinnon turvallisuusverkko-toiminnasta 1109/2015
- Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)
- Tietoturvallisuuden arviointityökalu Katakri
- Euroopan Unionin (EU) kyberturvallisuusdirektiivi NIS2 2022/2555
- Euroopan komission täytäntöönpano asetus 2024/2690
- Liikenne- ja viestintäviraston Traficomin NCSA -toiminnon hyväksymät salausratkaisut.

Opinnäytetyön ulkopuolelle rajataan kansainväliset valtioiden julkisen sektorin toimintaa ohjaavat lait ja ohjeet.

4.1 Laki julkisen hallinnon turvallisuusverkkotoiminnasta 10/2015

Lailla varmistetaan valtion ylimmän johdon, turvallisuus viranomaisten ja muiden toimijoiden yhteistoiminnan keskinäinen viestintä kaikissa olosuhteissa. Olosuhteet jaetaan normaali oloihin, normaali olojen häiriötilanteisiin ja poikkeus oloihin. Yhteistoiminnan keskinäinen viestintä on toimittava häiriöttömästi ja jatkuvasti. Viestinnässä tiedon on oltava eheää, käytettävää ja luottamuksellista (Laki julkisen hallinnon turvallisuusverkkotoiminnasta 10/2015).

Lain sovelluskohteita ovat julkisen hallinnon käyttämä turvallisuusverkko ja sen palvelut, sekä muu turvallisuusverkkotoiminta. Edellä mainitun lisäksi lakia sovelletaan lisäksi laajakaistaiseen matkaviestintään, joka on aikakriittistä, sekä erilaisiin viestintä- ja tietoteknisiin palveluihin (Laki julkisen hallinnon turvallisuusverkkotoiminnasta 10/2015).

Turvallisuusverkkoon ja turvallisuusverkkotoimintaan sovelletaan eri lakeja, esimerkiksi turvallisuusverkkoon sovelletaan sähköisen viestinnän palvelu lain viranomaisverkkoa koskevia säännöksien osuutta. Lisäksi turvallisuusverkkotoimintaan sovelletaan julkisen hallinnon tiedonhallinta lain (906/2019) säännöksiä, ja valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisen lain (1226/2013) säännöksiä. Laajakaistaisen matkaviestinnän viestintä- ja tietoteknisiin palveluihin sovelletaan sähköisen viestinnän palvelu lain viranomaisten viestintäpalvelua koskevien säännöksien osuutta. (Laki julkisen hallinnon turvallisuusverkkotoiminnasta 10/2015).

Turvallisuusverkon käyttövelvoite sisältää viranomaisten yhteistoiminnan ja viestinnän, joka on joko sisäistä, ulkoista tai viranomaisten välistä, ja jossa noudatetaan korkean varautumisen tai turvallisuuden vaatimuksia. Edellä mainittu viranomaisten yhteistoiminta ja viestintä liittyy alla lueteltuihin tehtäviin:

- valtion johtamiseen ja turvallisuuteen
- yleiseen järjestykseen ja turvallisuuteen
- maanpuolustukseen tai rajaturvallisuuteen
- hätäkeskustoimintaan tai pelastus- tai meripelastustoimintaan
- maahanmuuttoon
- ensihoitopalveluun (LIITE 1, LIITE 2.).

Turvallisuusverkon käyttövelvoite käsittää myös turvallisuusverkon laitetilojen, laitteiden ja muun infrastruktuurin, sekä yhteisten palvelujen käytön (Laki julkisen hallinnon turvallisuusverkkotoiminnasta 10/2015).

Turvallisuusverkon palvelujen jatkuvuuden turvaamisessa on tehtäviä, jotka jaetaan eri palvelujen tuottajien kesken. Turvallisuusverkon toimintaan liittyviä palveluja ovat tieto- ja viestintätekniset-, integraatio- ja muut palvelut (Laki julkisen hallinnon turvallisuusverkkotoiminnasta 10/2015).

Palvelukeskus toimii turvallisuusverkon valtion yhteisten tieto- ja viestintäteknisten palvelujen tuottajana. Palvelukeskuksen tehtävä on tuottaa, ylläpitää ja kehittää turvallisuusverkon yhteiset tieto- ja viestintätekniset palvelut sekä vastata tehtäväalueellaan turvallisuusverkkoa koskevien turvallisuus-, valmius-, varautumis- ja jatkuvuusvaatimusten toteutumisesta kaikissa olosuhteissa. Valtioneuvoston

asetus antaa tarkempia säännöksiä palvelujen tuottajan tehtävistä, palveluista ja niiden käytöstä. Asetuksessa on myös säännöksiä menettelytapoihin ja tietojärjestelmiin, joilla tuetaan palvelujen tuottamista (FINLEX 2015b.).
Suomen valtion Suomen Erillisverkot Oy -niminen osakeyhtiö tai sen tytäryhtiö toimivat viranomaisradioverkon, viranomaisten laajakaistaisen matkaviestinnän tieto- ja viestintäteknisten sekä turvallisuusverkon verkko- ja infrastruktuuripalvelujen tuottajana. Suomen Erillisverkot Oy:n ja sen tytäryhtiön tehtävänä on tuottaa, ylläpitää ja kehittää viranomaisradioverkon sekä viranomaisten laajakaistaisen matkaviestinnän yhteisiä tieto- ja viestintäteknisiä palveluja. Yritys vastaa tieto- ja viestintäteknisiä palveluja koskevien turvallisuus-, valmius-, varautumis- ja jatkuvuusvaatimusten toteutumisesta kaikissa olosuhteissa (Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta 1109/2015).

Turvallisuusverkon integraatiopalvelujen tuottajan tehtävänä on yhdistää turvallisuusverkon palvelut käyttäjien muihin tieto- ja viestintäteknisiin palveluihin, sekä vastata näiden palvelujen välittämisestä ja tarjoamisesta käyttäjille. Edellä mainittu palvelun tuottaja vastaa myös tehtäväalueellaan turvallisuusverkkoa koskevien turvallisuus-, valmius-, varautumis- ja jatkuvuusvaatimusten toteutumisesta kaikissa olosuhteissa (Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta 1109/2015).

Valtiovarainministeriö vastaa turvallisuusverkkotoiminnan strategiasta, yleishallinnosta, taloudesta, tieto- ja viestintäteknisestä varautumisesta, sekä valmiuden, turvallisuuden, ja turvallisuusverkon palvelutuotannon ohjauksesta ja valvonnasta (Laki julkisen hallinnon turvallisuusverkkotoiminnasta 10/2015).

Verkko- ja infrastruktuuripalvelujen palveluntuottaja tai palveluntuottajan alihankkijan työntekijä, joka käsittelee turvallisuusverkkotoimintaan liittyviä salassa pidettäviä tietoja, sitoo Laki viranomaisten toiminnan julkisuudesta (621/1999). Valtiovarainministeriöllä on oikeus saada turvallisuusverkkotoimintaan osallistuvilta viranomaisilta ja muilta toimijoilta lain mukaisen tehtävän hoitamiseen välittömästi tarvittavat tiedot ministeriölle. Salassapitosäännökset eivät tätä oikeutta estä. (FINLEX 1999.)

4.2 Laki julkisen hallinnon tiedonhallinnasta 906/2019

Laki julkisen hallinnon tiedonhallinnasta (906/2019) -lain tarkoituksena on varmistaa viranomaisten tietoaineistojen hallinta ja käsittely, jossa huomioidaan laatu, yhdenmukaisuus, tietojen turvallisuus ja julkisuusperiaatteet. Lain tarkoituksena on myös edistää eri tietovarantojen ja -järjestelmien välistä yhteen toimivuutta. Näin viranomaiset voivat tehokkaasti ja turvallisesti hyödyntää tietoaineistoja ja tarjota asiakkaille laadukkaita palveluita myös tuloksellisuus huomioiden. Lakia käytetään myös kyberturvallisuuden korkean tason varmistamiseen Euroopan Unionin alueella (Laki julkisen hallinnon tiedonhallinnasta 906/2019).

Lakia sovelletaan tiedonhallintaan ja tietojärjestelmien käyttöön, kun viranomaiset käsittelevät tietoaineistoja (LIITE 1, LIITE 2). Mikäli yksityiset henkilöt tai yhteisöt hoitavat julkisia hallintotehtäviä, niin myös heihin sovelletaan edellä mainittua lakia kyseisten tehtävien osalta.
Lakia sovelletaan myös yliopistolaissa (558/2009) määriteltyihin yliopistoihin ja ammattikorkeakoululaissa (932/2014) määriteltyihin ammattikorkeakouluihin (Laki julkisen hallinnon tiedonhallinnasta 906/2019).

Laissa on myös poikkeuksia, joista esimerkkinä Kyberturvallisuutta koskevat velvollisuudet ja niiden noudattamisen valvonta -luku, mitä ei sovelleta:

- valtion hallinnon virastoihin ja laitoksiin esimerkiksi eduskunnan virastoihin, Puolustusvoimiin, poliisiyksiköihin, Rajavartiolaitokseen, tuomioistuimiin
- kuntien viranomaisiin pois lukien Helsingin kaupunki, johon lakia sovelletaan
- pankkisektorin osalta Suomen Pankkiin
- valtion oppilaitoksiin esimerkiksi yliopistoihin, ammattikorkeakouluihin
- turvallisuusverkon palvelutuotantoon ja palvelujen käyttöön
- diplomaatti- ja konsuliedustustoihin ja niiden verkko- ja tietojärjestelmiin (jos ne sijaitsevat edustuston tiloissa tai niitä ylläpidetään maiden käyttäjiä varten), eikä valtion viranomaisiin Ahvenanmaalla (Laki julkisen hallinnon tiedonhallinnasta 906/2019).

4.2.1 Tiedonhallinnan yleinen ohjaus ja tiedonhallintamalli

Laki velvoittaa viranomaisen tiedonhallintayksikön ylläpitämään tiedonhallintamallia, joka kuvaa ja määrittelee viranomaisen toimintaympäristön tiedonhallintaa. Tiedonhallintayksiköitä ovat muun muassa valtion virastot ja laitokset, tuomioistuimet ja ammattikorkeakoulut (Laki julkisen hallinnon tiedonhallinnasta 906/2019).

Tiedonhallintamallista saadaan pohjatietoja ja materiaalia tiedonsaantia koskevien rajoituksien ja oikeuksien toteuttamiseen. Mallia voidaan käyttää suunnitteluun ja toteutukseen, jotka koskevat palvelujen tuottamista, asiakäsittelyä ja tietoaineistojen hallintaa, sekä toteuttaa ja varmistaa tietojärjestelmien ja -varantojen yhteen toimivuuden ja tietoturvallisuuden ylläpidon. Tiedonhallintamallilla saadaan myös vähennettyä organisaation moninkertaista tiedonkeruuta (Laki julkisen hallinnon tiedonhallinnasta 906/2019).

Tiedonhallintamallin on sisällytettävä vähintään tiedot toimintaprosesseista, tietovarannoista- ja aineistoista, tietojärjestelmistä ja turvallisuustoimenpiteistä. Alla olevassa taulukossa (TAULUKKO 2) on esimerkkejä tiedonhallintamalliin sisällytettävistä tiedoista (Laki julkisen hallinnon tiedonhallinnasta 906/2019.

TAULUKKO 2: Esimerkki tiedonhallintamalliin sisällytettävistä tiedoista

Esimerkki toimintaprosessista löytyvistä tiedoista:	
Prosessia kuvaava nimi	Henkilöstön rekrytointi prosessi
Prosessin vastuu henkilö(t)	Maija Meikäläinen
Prosessin tarkoitus	Kuvaa työntekijän työhönoton eri vaiheet, roolit, tehtävät
Prosessin sidokset muihin prosesseihin	Palkanmaksuprosessi, perehdytysprosessi jne.
Esimerkki tietovarannosta löytyvistä tiedoista:	
Tietovarantoa kuvaava nimi	Henkilöstötietovaranto
Tietovarannon sidokset toimintaprosesseihin ja tietojärjestelmiin	- Rekrytointiprosessi, palkanmaksuprosessi jne. - Toiminnanohjausjärjestelmä, työajanseurantajärjestelmä jne.
Henkilötietojen käsittely ja tietojen liikkuvuus	Henkilötietojen käsittelyssä noudatetaan luonnollisen henkilön suojelussa..
Tietovaraanon/tietosuojaselosteen vastuu henkilö(t)	Maija Meikäläinen
Tietovarannon käyttötarkoitus	Henkilöstöhallintoon liittyvä asiankäsittely muun muassa palvelussuhdeasiat
Tietoaineiston keskeiset tietoryhmät	Henkilötiedot, yhteystiedot, terveystiedot jne.

Tietojen luovutus	Henkilötietoja luovutetaan viranomaistoiminnan..
Tietojen säilytysaika	Henkilötietoja säilytetään x vuotta
Esimerkki tietoaineistosta löytyvistä tiedoista:	
Tietoaineiston arkistoon siirtäminen	Säilytysvaiheen jälkeen tietoaineistot arkistoidaan arkistonmuodostussuunnitelman mukaisesti..
Tietoaineiston arkistointitapa ja arkistointipaikka	Tietoaineistot tallennetaan sähköiseen muotoon, ja pääasialliset tietoaineiston tallennuspaikat ovat asiahallintajärjestelmä x, toimialasidonnainen järjestelmä y, viranomaisten yhteiset tietojärjestelmät, verkkolevyt a, b, c jne.
Tietoaineiston tuhoaminen	Säilytysvaiheen jälkeen tietoaineistot tuhotaan arkistonmuodostussuunnitelman mukaisesti..
Esimerkki tietojärjestelmästä löytyvistä tiedoista:	
Tietojärjestelmää kuvaava nimi	HR-työpöytä
Tietojärjestelmän vastuu henkilö(t)	Maija Meikäläinen
Tietojärjestelmän käyttötarkoitus	Poissaolojen, lomien, koulutuksien haku ja ilmoitus järjestelmä
Tietojärjestelmän liittyminen muihin tietojärjestelmiin ja liittymien tiedonsiirtotavat	Palkanmaksujärjestelmä, toiminnanohjausjärjestelmä jne. Tiedonsiirto järjestelmästä virtuaalipalvelimen x kautta..
Esimerkki turvallisuustoimenpiteiden tiedoista: suunniteltaessa tiedonhallintamalliin hallinnollisia uudistuksia ja tietojärjestelmien käyttöönottoa, arviointi muutoksista ja niiden vaikutuksista suhteessa	
Tiedonhallinnan vastuisiin	Vastuuhenkilöksi nimitetty Erkki Esimerkki
Vaatimuksiin tietoturvallisuudesta ja tietoturvallisuustoimenpiteistä	Turvallisuusvaatimuksissa huomioitu tietojärjestelmän x käyttöönotto ja kyberturvallisuusdirektiivi NIS2:n vaatimukset
Vaatimuksiin tietoaineistojen muodostamista ja luovutustavasta	Osittaisesta analogisesta tietoaineistojen muodostamisesta siirrytty digitaaliseen tietoaineistojen muodostamiseen tietojärjestelmän x käyttöönoton yhteydessä
Vaatimuksiin asianhallinnasta ja palvelujen tiedonhallinnasta	Asianhallinnassa huomioitu siirtyminen tietoaineistojen digitaaliseen muodostamiseen. Palvelujen tiedonhallinnassa huomioitu huomioitu kyberturvallisuusdirektiivi NIS2:n vaatimukset
Asiakirjojen julkisuuteen, salassapitoon, suojaan ja tiedonsaantioikeuksiin, jotka on säädetty muualla laissa	Asiakirjojen tiedonsaantioikeuksia päivitetty tarvittavilta osin

Tiedonhallinnan muutosten arvioinnissa tiedonhallintayksikön on lisäksi otettava huomioon tietovarantojen yhteen toimivuus ja hyödynnettävyys. Kun arviointi on suoritettu, tiedonhallintayksikkö tekee ja toimeenpanee tarvittavat muutokset tiedonhallintamalliin. Tietosuojaa koskevaa muutos- ja vaikutustenarviointia ei ole sisällytetty yllä mainittuihin tiedonhallinnan muutosten varviointiin, vaan siitä on säädetty erikseen. (Laki julkisen hallinnon tiedonhallinnasta 906/2019).

4.2.2 Tietovarantojen yhteen toimivuuden yleinen ohjaus ja palvelujen tuottamisen yhteistyö

Valtiovaranministeriön tehtävänä on ylläpitää julkisen hallinnon tiedonhallintakarttaa, mikä ohjaa julkisen hallinnon yhteisten tietovarantojen yhteen toimivuutta. Valtiovaranministeriön tehtävänä on myös ylläpitää julkisen hallinnon tiedonhallinnan kehittämisen yleisiä linjauksia pyrkien näin edistämään tietovarantojen ja tietojärjestelmien yhteen toimivuutta. Edellä mainitut ylläpito tehtävät kuuluvat myös jokaiselle ministeriölle toimialoittain (Laki julkisen hallinnon tiedonhallinnasta 906/2019).

Valtiovarainministeriö huolehtii myös eri viranomaisten yhteistyön koordinoinnista varmistamalla, että yhteistyön koordinointia varten on yhteistyötavat ja -menettelyt järjestetty koskien julkisen hallinnon tiedonhallintaan sekä tieto- ja viestintäteknisten palvelujen tuottamista. Yhteistyön tarkoituksena on tietovarantoja, sekä tieto- ja viestintätekniikkaa hyödyntämällä edistää tämän lain tarkoitusten toteutuminen sekä julkisen hallinnon ja palvelujen tuotantotapojen kehittäminen. (Laki julkisen hallinnon tiedonhallinnasta 906/2019).

4.3 Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta 1109/2015

Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta on säädetty turvallisuusverkon palvelujen jatkuvuuden turvaamiseksi:

- normaali oloissa
- häiriötilanteissa normaali oloissa sekä
- poikkeus oloissa

korkean varautumisen ja turvallisuuden vaatimusten edellyttämässä laajuudessa, tarvittaessa yhteistyössä muiden palveluntuottajien ja käyttäjien kanssa (Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta 1109/2015).

Turvallisuusverkon palvelujen jatkuvuuden turvaamisessa tehtävät jaetaan tieto- ja viestintäteknisten palvelujen tuottajan, integraatiopalvelujen tuottajan ja muiden palvelutuottajien kesken (LIITE 1, LIITE 2).

Tieto- ja viestintäteknisten palvelujen tuottajan:

1. verkkopalveluja ovat:

    a. turvallisuusverkon runkoverkkopalvelu ja
    b. fyysisen liityntäpalvelun tarjoaminen turvallisuusverkon runkoverkkoon.

2. infrastruktuuripalveluja ovat:

    a. laitetilojen sekä laite- ja antennipaikkojen tarjoaminen käyttäjille ja palveluntuottajille.

3. yhteisiä tieto- ja viestintäteknisiä palveluja ovat:

    a. käyttäjätuki- ja päätelaitepalvelut sekä viestintätekniset palvelut
    b. muut tietoliikenne- ja tietoturvapalvelut
    c. konesali- ja kapasiteettipalvelut
    d. integraatio- ja sanomanvälityspalvelut
    e. a–d kohdissa tarkoitettuihin palveluihin yhteiset tietojärjestelmäpalvelut
    f. a–e kohdissa tarkoitettuihin palveluihin liittyvät omaisuudenhallintapalvelut
    g. turvallisuusverkon laitetiloihin sijoitettujen laitteiden ja tietojärjestelmien käyttöä tukevat palvelut.

Integraatiopalvelujen tuottajan tehtävänä on:

- muodostaa palvelukokonaisuudet turvallisuusverkolle
- vastata palvelukokonaisuuksiin liittyvästä sopimus- ja asiakkuudenhallinnasta
- järjestää turvallisuusverkon palvelujen yhdistäminen käyttäjien viestintäteknisiin palveluihin (Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta 1109/2015).

Huolehtiessaan turvallisuusverkon palvelujen ja tehtävien laadusta ja kustannustehokkuudesta, palvelutuottajan on erityisesti huolehdittava:

- ympärivuorokautisesta valvonnasta liittyen palvelujen toimivuuteen ja tietoturvallisuuteen

- häiritsevien tai uhkaavien tilanteiden havaitsemisesta, selvittämisestä ja raportoinnista liittyen palvelun toimivuuteen tai tietoturvallisuuteen (Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta 1109/2015).

Palvelutuottajan on laadittava ja ylläpidettävä palveluistaan myös:

- palveluluettelo, palvelukuvaukset ja hinnasto
- menettelyohjeet normaali oloihin, niiden häiriötilanteisiin ja poikkeus
- palvelujen toimivuutta ja turvallisuutta häiritsevien tai uhkaavien tilanteiden selvittämiseksi, vaikutusten minimoimiseksi ja poistamiseksi (Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta 1109/2015).

Jos toiminnassa on noudatettava korkean varautumisen tai turvallisuuden vaatimuksia, voidaan valtiovarainministeriön päätöksellä laitetiloihin sijoittaa valtion ylimmän johdon ja yhteiskunnan turvallisuuden kannalta tärkeiden viranomaisten ja muiden toimijoiden yhteistoiminnassa käytettäviä laitteita ja tietojärjestelmiä (Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta 1109/2015).

Palvelujen jatkuvuuden turvaamiseksi kaikissa olosuhteissa varautumisen ja turvallisuuden näkökulmasta palvelutuottajan on vastuutettava johtaminen organisaation eri tasoilla, suunniteltava ja järjestettävä palvelutuotanto huomioimalla jatkuvuus, häiriöttömyys ja uhkatekijät, varmistettava yhteistyön jatkuminen alihankkijoiden kanssa, tietoliikenteen toimivuus, tiedon, palvelujen, ylläpidon ja osaamisen saatavuus ja toiminta, resurssit ja huolehdittava koulutuksesta, häiriötilanneharjoittelusta (Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta 1109/2015).

Palvelutuottajan on kehitettävä ja tuotettava turvallisuusverkon palvelut siten, että palvelukohtaisesti on mahdollista täyttää suojaus tasojen II, III tai IV tietoturvavaatimukset sekä erityssuojattavalle tietoaineistolle asetetut tietoturvallisuusvaatimukset. Turvallisuusverkon palveluja koskevien tietoturvallisuus- ja varautumisvaatimusten täyttymisen toteamisessa käytetään arviointiperusteina tätä asetusta ja valtiovarainministeriön turvallisuusverkkolain antamia määräyksiä (Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta 1109/2015).

4.4 Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri)

Tämän suosituksen tarkoitus on kuvata julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) ja ohjeistaa Julkri'n käyttöä. Julkri'a käytetään koko julkishallinnon tietoturvallisuuden kehittämisen ja tarpeiden arvioinnin tukena. (VM 2023.)

Arvioitaessa tietoturvallisuutta koskevien vaatimusten täyttymistä tiedonhallintalaissa, turvallisuusluokitteluasetuksessa ja osin myös tietosuoja-asetuksessa voidaan Julkri'a käyttää apuna. Organisaatio voi käyttää Julkri'a esimerkiksi palvelulle asetettavien vaatimusten tunnistamiseen palvelun suunnittelussa ja vaatimusmäärittelyssä, sekä palvelun arvioinnissa verrattaessa tehtyyn hankintaan ja palvelusopimuksen vaatimuksiin. Julkri'a voidaan käyttää myös toimittajan vaatimusten tunnistamiseen toimittajaa arvioitaessa ja vaatimusten toteutumiseen toimittajan toiminnassa, sekä tietosuojaan liittyvien vaatimusten toteutumisessa ja arvioinnissa. (VM 2023.)

Julkri tukee organisaation turvallisuusjohtamista, joka on riskilähtöistä. Kriteeristöä voidaan käyttää arvioitaessa salassa pidettävän tiedon, henkilötiedon ja turvallisuusluokitellun tiedon käsittelyä. Jos organisaatiossa käsitellään turvallisuusluokka I (TL I – erittäin salainen) luokan tietoa, on edellä mainitun lisäksi huomioitava tapauskohtaiset käsittelyn vaatimukset. (VM 2023.)

Kriteeristön hallinnollinen ja tekninen turvallisuus ja osa-alueissa saavutettavuus on yleisenä kriteerinä. Kriteeristön ulkopuolelle on rajattu toiminnan jatkuvuutta poikkeus oloissa koskevat toimenpiteet. Julkri ei myöskään sisällä tietoturvallisuuden arviointia kansainväliselle turvallisuusluokitellulle tiedolle, eikä toimialakohtaisesta lainsäädännöstä johtuvia vaatimuksia. Organisaatioiden tulee kumminkin tunnistaa ja huomioida toiminnassaan vaatimukset, jotka tulevat toimialakohtaisesta tai kansainvälisestä lainsäädännöstä tai EU-sääntelystä. (VM 2023.)

Julkisen hallinnon tietoturvallisuuden arviointikriteeristö ja käyttösuositukset on jaettu viiteen osa-alueeseen, jotka ovat fyysinen turvallisuus (FYY), tekninen turvallisuus (TEK), hallinnollinen turvallisuus (HAL), varautuminen ja jatkuvuudenhallinta (VAR) ja tietosuoja (TSU). Ja osa-alue on edelleen jaettu pääkriteeriin ja pääkriteeriä täydentäviin alikriteereihin (VM 2023.). Kriteereitä on yhteensä yli kaksi sataa, ja jokainen kriteeri on luokiteltu eri tasoille luottamuksellisuuden, eheyden, saatavuuden ja tietosuojan mukaan. Kriteeriin liittyviä näkökulmia voi olla useampia kriteeristä riippuen. (VM 2023.)

Arvioitavan kohteen turvallisuusvaatimusten ja valitun käyttötapauksen perusteella Julkri poimii olennaiset ja valinnaiset kriteerit arviointiin. Kaikki olennaiset kriteerit tulisi sisällyttää arviointiin. Organisaatio voi päättää sisällyttää arviointiin myös valinnaisia kriteerejä riskiarvioinnin sekä tapauskohtaisen harkinnan perusteella, sekä päättää, mitkä valinnaisista kriteereistä otetaan mukaan arviointiin. (VM 2023.)

4.5 Tietoturvallisuuden arviointityökalu Katakri

Katakri on viranomaisten tietoturvallisuuden auditointityökalu (UM 2020). Katakri'a voidaan käyttää, kun halutaan arvioida organisaation kykyä suojata viranomaisen salassa pidettävää tietoa. Katakri'a voidaan käyttää auditointityökaluna myös viranomaisten tietojärjestelmien arviointiin, yrityksen turvallisuusjärjestelyjen arviointiin yritysturvallisuusselvityksissä, kansallisten ja kansainvälistenkin hankkeiden turvallisuusselvitykseen, sekä viranomaisten, yhteisöjen ja yrityksien muussa turvallisuustyössä ja sen kehittämisessä (UM 2020).

Käyttämällä Katakri'a pyritään varmistamaan kohdeorganisaation turvallisuusjärjestelyjen riittävyys viranomaisten salassa pidettävien tietojen paljastumisen ehkäisemiseksi niiden käsittely-ympäristöissä. Katakri sisältää vähimmäisvaatimukset kansallisista säädöksistä ja kansainvälisistä velvoitteista, eikä se sisällä tietoturvallisuudelle ehdottomia vaatimuksia. Katakri'n sisältämät vaatimukset pohjautuvat lainsäädäntöön ja kansainvälisiin tietoturvallisuusvelvoitteisiin, jotka sitovat Suomea. (UM 2020.)

Kun Katakri'a sovelletaan turvallisuusluokitellun tiedon käsittelyyn, jaetaan käyttötapaukset tuettuihin ja erityistapauksiin. Tuetuissa käyttötapauksissa tulee edellä mainitun tiedon käsittely tapahtua kokonaisuudessaan toimivaltaisten viranomaisten toimivallan piirissä. Erityistapauksissa, joita ovat muun muassa kansainväliseen viranomaisyhteistyöhön liittyvät hankkeet, voidaan käsiteltävät tiedot luovuttaa kyseisen kansainvälisen viranomaisyhteisön jäsenmaille. Toimivalta- ja tarkastusvastuista on kyseisten maiden turvallisuusviranomaisten kesken erikseen sovittu, mitkä liittyvät kyseessä olevana erityistapaukseen. (UM 2020.)

Katakri on normaali olojen työkalu, jota ei käytetä poikkeus olojen toimintaan. Katakri'a voidaan soveltaa myös normaalioloista poikkeaviin olosuhteisiin, jos tiedon omistavan viranomaisen on sen erillishyväksynyt, esimerkiksi toimintaan viruspandemian tai sotilaallisen konfliktin olosuhteissa. (UM 2020.)

Katakri on jaettu kolmeen eri osa-alueeseen, joita ovat turvallisuusjohtaminen (T), fyysinen turvallisuus (F) ja tekninen turvallisuus (I) (UM 2020.). Turvallisuusjohtamisen osa-alueessa pyritään varmistumaan organisaation tietoturvallisuuden hallintajärjestelmän toimivuudesta ja riittävistä henkilöstöturvallisuuden menettelyistä, joita käytetään turvallisusluokiteltujen tietojen suojaamiseen.
Fyysistä turvallisuutta koskevassa osa-alueessa kuvataan turvallisuusvaatimukset, jotka koskevat turvallisuusluokiteltujen tietojen fyysistä käyttöympäristöä. Teknistä tietoturvallisuutta koskevassa osa-alueessa kuvataan puolestaan turvallisuusvaatimukset, jotka on asetettu tekniselle tietojenkäsittely-ympäristölle. (UM 2020.)

Vaatimus -kentän kuvaus mahdollistaa erilaisia toteutustapoja. Lisätietoja -kenttien toteutusesimerkit on koottu tulkinnan tueksi, eivätkä ne ole sitovia. Nämä esimerkit on mahdollista korvata myös muilla vastaavan tasoisilla suojauksilla. Toteutusesimerkkien lähteinä on käytetty eri tahojen suosituksia ja ohjeita esimerkiksi tiedonhallintalautakunnan julkaisemia suosituksia ja EU:n turvallisuussääntöjä täydentäviä ohjeita. (UM 2020.)

T-05 - Työturvallisuustyön resurssit		
Vaatimus	§ Lähde (906/2019 ja/ tai 1101/2019)	§ Lähde (2013/488/ EU)
Organisaatiolla on käytössä riittävä asiantuntemus turvallisuusperiaatteiden varmistamiseksil	906/2019 4 § 2 mom	IV liitteen 4 kohta
Lisätietoja		

Yleistä: Riittävällä asiantuntemuksella pyritään varmistamaan, että turvallisuusperiaatteiden tarkoitus toteutuu ja toimet mitoitetaan suhteessa riskeihin. Resurssien riittävyyttä arvioidaan säännöllisesti.

Yleisenä vaatimuksena voidaan pitää, että organisaatiolla tulee olla riittävästi henkilöitä, henkilöllä riittävästi osaamista turvallisuudesta, ajantasaiset ohjeet, turvallisuuskoulutusta, asianmukaiset työvälineet sekä turvallisuustoimenpiteiden toimeenpanon valvonta ja tarkastukset järjestetty.

Toteutusesimerkki:
1. Turvallisuustehtävät hoitavalla on riittävä asiantuntemus sekä näistä on näyttöä.
2. Turvallisuustyön resurssit, tehtävät, vastuut ja valtuudet on määritelty organisaation toimintaan, kokoon ja riskeihin nähden riittävän kattavasti.
3. Resurssit riittävät tietoturvallisuuden hallintajärjestelmän luomiseen, toteuttamiseen, ylläpitoon ja jatkuvaan parantamiseen.
4. Resurssien riittävyyttä arvioidaan säännöllisesti.

Muita lisätietoja: SFS-EN ISO/IEC 27001:2017 7.1 7.2 5.1

KUVIO 4. Turvallisuustyön resurssit -vaatimus (UM 2020, mukaillen)

Kuvio 4 kuuluu kategoriaan Turvallisuusjohtaminen, Hallinnollinen tietoturvallisuus; T-05 – Turvallisuustyön resurssi (UM 2020.).

Kansallisessa yritysturvallisuusselvityksen T- ja F-osa-alueissa toimivaltainen viranomainen on Suojelupoliisi tai Pääesikunta, ja I-osa-alueessa toimivaltainen viranomainen on Liikenne- ja viestintävirasto (UM 2020.).

Kansainvälisen turvallisuusluokitellun tiedon suojaamiseen liittyvissä Katakri'n käyttötapauksissa toimivaltainen viranomainen on henkilöstö-, yritys- ja toimitilaturvallisuutta sekä Liikenne- ja viestintäviraston tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevat asioissa puolustusministeriö, Pääesikunta ja Suojelupoliisi (UM 2020.).

Kansainvälisessä yritysturvallisuusselvitysprosessissa (FSC, Facility Security Clearance) on toimivaltainen viranomainen T- ja F-osa-alueissa Suojelupoliisi tai Pääesikunta, ja I-osa-alueessa Liikenne- ja viestintävirasto (UM 2020.).

4.6 Euroopan unionin kyberturvallisuusdirektiivi NIS2

Euroopan Unionin (EU) kyberturvallisuusdirektiivin (NIS2) tarkoitus on Euroopan yhteisen kyberturvallisuuden tason varmistaminen. Direktiivissä vahvistettaan kyberturvallisuusriskien hallintatoimenpiteiden ja raportointivelvoitteiden perustason toimialoilla, jotka kuuluvat direktiivin piiriin. Direktiivi vaatii Euroopan Unionin jäsenvaltioita vahvistamaan valmiuksiaan kyberturvallisuuteen liittyen, ja ottamaan käyttöön direktiivin täytäntöönpanon sääntöjä ja kyberturvallisuusriskien hallintaan liittyviä toimenpiteitä. Direktiivin käyttöönotto edellyttää myös valvontaa ja raportointia kriittisillä toimialoilla unohtamatta toimialojen välistä tietojen vaihtamista ja yhteistyötä. Kansallisella tasolla toimijoilta edellytetään viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvien kyberriskien hallintaa ja pyrkien niiden haitallisten vaikutusten poistamiseen tai niiden vähentämiseen (LIITE 1, LIITE 2). (NIS 2 -direktiivi 2022/2555)

Direktiiviä sovelletaan pääasiassa keskisuuriin ja suuriin erittäin kriittisillä toimialoilla toimiviin toimijoihin, joihin kuuluu esimerkiksi eri infrastruktuurien toimijoita, kuten energian (sähkö, kaukolämpö, öljy, vety), vesi- ja jätehuollon, liikenteen (ilma, raide, vesi, tie) ja digitaalisten verkkojen toimijat. Myös julkisen hallinnon keskus- ja alue taso sekä terveyden huolto kuuluvat yllä rajattuihin toimijoihin. Direktiiviä sovelletaan käytäntöön myös muihin kriittisiin aloihin kuten esimerkiksi jätteiden huoltoon, elintarvikkeiden ja kemikaalien tuotantoon, jalostukseen ja jakelu ketjuihin, eri tutkimusorganisaatioiden toimintaan ja niin edelleen. (NIS 2 -direktiivi 2022/2555)

Jokaisella jäsenvaltiolla on oltava hyväksyttynä kansallinen strategia vaaditun kyberturvallisuuden korkean tason saavuttamiseksi ja ylläpitämiseksi kriittisillä toimialoilla. Jäsenvaltion kansallinen strategia sisältää eri sidosryhmien tehtäviä ja vastuita selventävän hallintokehyksen, toimintapolitiikan helpottamaan ja edelleen kehittämään kyberturvallisuuskoulutuksia, toimintaperiaatteet eri toimitusketjujen suojaamiseksi ja mahdollisten haavoittuvuuksien kontrolloimiseksi, sekä käytännön toimenpiteet lisäämään kansalaisten tietoisuutta kyberturvallisuuteen liittyvissä asioissa. (NIS 2 -direktiivi 2022/2555)

Jäsenvaltioiden on myös ylläpidettävä toimijaluetteloa eri toimijoista. Luetteloon listattavien toimijoiden kriteerinä on, että toimijat toiminnan kannalta keskeisiä ja tärkeitä. Luettelosta löytyvät myös verkkotunnusten rekisteröintipalveluja tarjoavat toimijat. Jäsenvaltioiden on myös perustettava kansallinen CSIRT -yksiköiden verkosto edistämään nopean toiminnan operatiivista yhteistyötä. Yksi perustetuista CSIRT -yksiköistä koordinoi havaittujen haavoittuvuuksien julkistamista TVT-tuotteissa tai -palveluissa. Kyseisen yksikön tehtävä on myös mahdollistaa ja varmistaa mahdollisuus haavoittuvuuksien nimettömään ilmoittamiseen. (NIS 2 -direktiivi 2022/2555)
Edellä mainittujen tehtävien lisäksi Euroopan Unionin jäsenvaltiot, Euroopan komissio ja Euroopan Unionin (EU) kyberturvallisuusviraston edustajat perustavat yhteistyöryhmän strategisen yhteistyön ja tietojenvaihdon edistämiseksi ja helpottamiseksi. (NIS 2 -direktiivi 2022/2555)

Meneillään olevan tai mahdollisen laajamittaisen kyberturvallisuuspoikkeaman tapauksessa, millä on todennäköisesti laaja vaikutus direktiivissä mainittuihin kriittisiin toimialoihin, kokoontuu Euroopan kyberkriisien yhteysorganisaatioiden verkosto (EU-CyCLONe). Verkosto koostuu jäsenvaltioiden kyberkriisinhallintaviranomaisten ja komission edustajista. Komission edustaja osallistuu verkoston toimintaan vain tapauksissa, joissa on kysymyksessä laajamittainen kyberturvallisuuspoikkeama, jolla on vaikutus direktiivin toimialoihin. Muussa tapauksessa komissio osallistuu toimintaan vain tarkkailijana. (NIS 2 -direktiivi 2022/2555)

Kansallisen toimijan on ilmoittauduttava toimialan valvovan viranomaisen ylläpitämään toimijaluetteloon ja ilmoitettava toimijaluetteloon tulleista muutoksista. Toimijalla on oltava käytössä ajantasainen kyberturvallisuuden riskienhallinnan toimintamalli ja toteutettava riskienhallinnan toimintamalliin perustuvia teknisiä, operatiivisia ja organisatorisia hallintatoimenpiteitä, ja ilmoitettava viipymättä merkittävistä poikkeamista valvovalle viranomaiselle. (NIS 2 -direktiivi 2022/2555)

Kaikki yritykset ja toimijat voivat ilmoittaa Traficom’in Kyberturvallisuuskeskuksen CSIRT -yksikölle tai vastaavalle viranomaiselle niihin kohdistuneista tietoturvaloukkauksista tai tapahtumista, jotka voivat aiheuttaa huomattavan palveluiden toimintahäiriön, taloudellista tappiota, aineellista tai aineetonta vahinkoa tai vaikuttavat muihin henkilöihin. (NIS 2 -direktiivi 2022/2555)

KUVIO 5. Merkittävien poikkeamien ilmoittaminen (NIS 2 -direktiivi 2022/2555, mukaillen)

CSIRT -yksikkö:

1. reagoi tietoturvaloukkauksiin ja avustaa tapauksissa
2. tutkii tietoturvaloukkauksia keräämällä ja analysoimalla tietoja, laatimalla analyysejä ja ylläpitämällä kyberturvallisuuden tilannekuvaa
3. antavat teknistä tukea toimijoille (NIS 2 -direktiivi 2022/2555).

Liikenne- ja viestintävirasto Traficom'in Kyberturvallisuuskeskus on laatinut Traficom'in suosituksen NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan NIS2-direktiivin mukaisten kyberturvallisuuden riskienhallinnan toimenpiteiden valvonnan tueksi (NIS 2 -direktiivi 2022/2555).

Euroopan komission täytäntöönpano asetuksella täsmennetään NIS2 -direktiivin riskienhallintavelvoitteiden sisältöä sekä sitä, milloin kyseessä on merkittävä poikkeama (NIS 2 -direktiivi 2022/2555).

4.7 Euroopan komission täytäntöönpano asetus 2024/2690

Euroopan komission täytäntöönpano asetuksella (2024/2690) täsmennetään NIS2 -direktiivin riskienhallintavelvoitteiden sisältöä sekä sitä, milloin kyseessä on merkittävä poikkeama (LIITE 1, LIITE 2) (KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2024/2690).

Asetuksen täsmennys tekniset ja menetelmiin liittyviin vaatimuksiin:

1. Direktiivin tarkoitettujen kyberturvallisuusriskien hallintatoimenpiteiden tekniset ja menetelmiin liittyvät vaatimukset vahvistetaan asianomaisten toimijoiden osalta tämän asetuksen liitteessä.

2. Toimijoiden on varmistuttava verkko- ja tietojärjestelmien turvallisuuden oikeasta tasosta suhteessa aiheutuviin riskeihin ennen kuin he alkavat toteuttavat ja soveltavat tämän asetuksen liitteessä vahvistettuja kyberturvallisuusriskien hallintatoimenpiteiden teknisiä ja menetelmiin liittyviä vaatimuksia (KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2024/2690).

   Tätä varten asianomaisten toimijoiden on otettava huomioon mikä on poikkeamien esiintymisen todennäköisyys ja sen vakavuus, ja missä määrin he altistuvat riskeille kokonsa huomioiden. Myös taloudelliset ja yhteiskunnalliset vaikutukset on otettava huomioon noudattaessaan tämän asetuksen liitteessä vahvistettuja kyberturvallisuusriskien hallintatoimenpiteiden teknisiä ja menetelmiin liittyviä vaatimuksia (KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2024/2690).

3. Jos tämän asetuksen liitteessä säädetään, että jotakin kyberturvallisuusriskien hallintatoimenpiteen teknistä tai menetelmiin liittyvää vaatimusta on sovellettava:

   a. ”tarvittaessa”,
   b. ”tapauksen mukaan” tai
   c. ”mahdollisuuksien mukaan” ja
   d. jos asianomainen toimija katsoo, että joidenkin tällaisten teknisten ja menetelmiin liittyvien vaatimusten soveltaminen ei ole tarpeellista, asianmukaista tai mahdollista,

asianomaisen toimijan on dokumentoitava tätä koskevat perustelunsa ymmärrettävällä tavalla (KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2024/2690).

Asetuksen täsmennys milloin poikkeama katsotaan merkittäväksi asianomaisten toimijoiden osalta. Poikkeama on merkittävä, jos yksi tai useampi seuraavista kriteereistä täyttyy (KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2024/2690).

1. Poikkeama on aiheuttanut tai voinut aiheuttaa:

    a. toimijalle välittömiä taloudellisia tappioita, jotka ylittävät 500 000 euroa tai 5 prosenttia edeltävän tilikauden vuotuisesta kokonaisliikevaihdosta pienempi huomioiden
    b. luonnollisen henkilön kuoleman
    c. huomattavaa vahinkoa luonnollisen henkilön terveydelle

2. Poikkeama on mahdollistanut tai voi mahdollistaa asianomaisen toimijan liikesalaisuuden, sellaisena kuin se on määritetty varastamisen
3. on tapahtunut onnistunut, epäilty vihamielinen ja luvaton tunkeutuminen verkko- ja tietojärjestelmiin, mikä voi aiheuttaa vakavia toimintahäiriöitä
4. poikkeama täyttää 4 artiklassa säädetyt kriteerit
5. poikkeama täyttää yhden tai useamman 5–14 artiklassa säädetyistä kriteereistä (KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2024/2690).

4.8 Liikenne- ja viestintäviraston Traficom’in NCSA -toiminnon hyväksymät salausratkaisut

Liikenne- ja viestintäviraston Traficom’in NCSA -toiminnon lakisääteisenä tehtävänä on tarjota arviointi- ja hyväksyntäpalveluita ja tietoturvaneuvontaa valtionhallinnolle sekä huoltovarmuuskriittisille toimijoille (Traficom 2025b.). NCSA -toiminto vastaa turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioista. NCSA -toiminnon palvelut tukevat organisaatioiden ennalta ehkäisevää turvallisuustyötä sekä toimintamahdollisuuksia. (Traficom 2025b.)
Liikenne- ja viestintävirasto Traficom’in Kyberturvallisuuskeskuksen kansainvälisiin tietoturvavelvoitteisiin liittyviin tehtäviin kuuluu salaustuotteiden hyväksyntä kansainvälisen turvallisuusluokitellun tiedon suojaamiseksi Suomessa.

Salaustuotteiden hyväksyntäviranomaisesta käytetään EU:ssa lyhennettä CAA (Crypto Approval Authority). Traficom'in Kyberturvallisuuskeskuksen NCSA-toiminto huolehtii CAA-vastuista Suomessa. (Traficom 2025b.)

Traficom'in Kyberturvallisuuskeskuksen hyväksymiä salaustuotteita voi käyttää sekä kansallisten että Euroopan Unionin (EU) turvallisuusluokiteltujen tietojen suojaamiseen. Tuotteet on hyväksytty käytettäväksi korkean uhka tason ympäristöissä tiedon luottamuksellisuuden ja eheyden suojaamiseen. Korkea uhka taso tarkoittaa esimerkiksi järjestelmää, joka on hyväksytty lähetettävän tiedon turvallisuusluokkaa matalammalle turvallisuusluokalle tai viestintää avointen verkkojen, kuten Internetin yli. (Traficom 2025b.)

Ttaficom'in turvallisuusluokat koskevat vain viranomaisen turvallisuusluokittelemaa tietoa, mutta niitä voi käyttää myös suosituksina muihin tarpeisiin. Korkeammalle turvallisuusluokalle hyväksyttyjä tuotteita voidaan käyttää myös alempien turvallisuusluokkien tietojen suojaamiseen ja niiden käytön ehdot saattavat erota turvallisuusluokittain. (Traficom 2025b.)

Traficom'in käyttämät turvallisuusluokat ovat:

- TLII
- TLIII
- TL IV (Traficom 2025b.).

Kun haetaan hyväksyntää tietojärjestelmälle tai tietoliikennejärjestelyille, perustuen kansainvälisten tietoturvavelvoitteiden täyttämiseen, edellytetään hyväksyntää salaustuotteiden hyväksyntäviranomaisen. Tapauksissa, kun hyväksyntäprosessin perustana on laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista, hyväksyntää voidaan myös edellyttää. (Traficom 2025b.)

Euroopan Unionin (EU) neuvosto ja sen pääsihteeristö ylläpitävät myös listaa hyväksymistään salaustuotteista käytettäväksi myös kansainvälisen tai kansallisen turvallisuusluokitellun tiedon suojaamiseen. Euroopan Unionin (EU) turvallisuusluokiteltujen tietojen suojaamiseen käytettävien salaustuotteiden tulee olla hyväksyttyjä EU:n turvallisuussääntöjen 10 artiklan 6 kohdan mukaisesti. (Traficom 2025b.)

Kyseisen kohdan mukaan Euroopan Unionin (EU):

- CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C) tai
- RESTREINT UE/EU RESTRICTED (R-UE/EU-R)

turvallisuusluokiteltujen tietojen luottamuksellisuus voidaan suojata jäsenvaltioiden kansallisissa järjestelmissä salaustuotteilla, jotka on hyväksynyt jäsenvaltion salaustuotteiden hyväksyntäviranomainen (CAA). Suomen salaustuotteiden hyväksyntäviranomaisen (CAA) Traficom'in NCSA-toiminnon hyväksynnän perusteena on salaustuotteen tietoturva-arviointi, jonka on EU-maan toimivaltainen salaustuotteiden hyväksyntäviranomainen (CAA) tehnyt tai valvonut. (Traficom 2025b.)

SECRET UE/EU SECRET (S-UE/EU-S) tai sitä korkeamman turvallisuusluokan tietojen luottamuksellisuus, ja kansallisten järjestelmien ulkopuolella C-UE/EU-C ja R-UE/EU-R turvallisuusluokan tietojen luottamuksellisuus, on suojattava salaustuotteilla, jotka on hyväksynyt salaustuotteiden hyväksyntäviranomaisena toimiva neuvosto tai vastaavasti neuvoston pääsihteeristö. Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa määrittelee turvallisuusluokittelun valtionhallinnossa. (Traficom 2025b.)

Lisäksi Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa -asetuksessa säädetään julkisen hallinnon tiedonhallinnasta annetussa laissa tarkoitettujen asiakirjojen turvallisuusluokittelusta, turvallisuusluokiteltaviin asiakirjoihin tehtävistä merkinnöistä sekä turvallisuusluokiteltujen asiakirjojen käsittelyä koskevista tietoturvallisuustoimenpiteistä valtionhallinnon viranomaisille. (FINLEX 2019b.)

5 JULKISEN HALLINNON VERKKOJEN SUUNNITTELUN VAIHEET

Organisaation toimintaympäristö luo vaatimuksia tietoverkkoratkaisun teknologia- ja laitevalintoihin. Toimintaympäristö käsittää sekä ulkoisen että sisäisen toimintaympäristön. Ulkoinen toimintaympäristö käsittää toimipisteiden fyysisen sijainnin eri alueilla esimerkiksi kaupungeissa ja kunnissa. Suunnittelun lähtökohta on tavoitetilan asettaminen. Verkon suunnittelussa tärkeintä on toteuttaa verkko, joka vastaa julkisen sektorin tai yrityksen toimijan tarpeisiin, joista tärkein tarjottavat palvelut ja niiden saatavuus. Verkon on vastattava näiden palveluiden vaatimuksiin sekä laitteiden että kaapeloinnin osalta. Verkon on vastattava myös viranomaisvaateisiin ja niiden toteutumiseen. Suunnittelun lopputuloksena toteutuu toimiva verkko esimerkiksi lähiverkko, jota toimija pystyy hyödyntämään mahdollisimman tehokkaasti.

Tietoverkkoja suunniteltaessa on hallittava tietoverkkojen suunnittelun taustalla olevat lait, asetukset, ohjeet ja määräykset liittyen tietoverkkojen laatuun, häiriöttömyyteen, luotettavuuteen, viestintäsalaisuuteen ja sähköturvallisuuteen. Suunnittelussa on huomioitava erityisesti tietoturvallisuus ja varautuminen. Suunnitteluvaihe kattaa myös tietoverkkojen toteutusvaiheen materiaalivalinnat ja verkon toteutuksen dokumentointi.

Tietoverkon suunnittelun vaiheet voidaan jakaa verkon analysointiin, vaatimusten määrittelyyn, arkkitehtuuriin, suunnitteluun (LIITE 3) ja ylläpidon suunnitteluun. Tietoverkon suunnitelman toteuttaminen jakautuu verkon osien esim. laitteiden asentamiseen, toteutuksen dokumentointiin, sekä jatkossa tuotannossa olevan tietoverkon ylläpitoon.

Opinnäytetyössä käsitellään lähinnä LAN, WLAN ja MAN -verkkoja, joita tarvitaan tavallisimpien tietoverkkojen suunnittelussa.

5.1 Organisaation tietoverkon vaatimusten määrittäminen

Tietoverkon määrittelyvaiheessa suunnitellaan tietoverkolta vaadittavat ominaisuudet esimerkiksi verkon eri osien tiedonsiirronkapasiteetti, skaalautuvuus, häiriöttömyys sekä luottamuksellisuus. Lopputuloksena syntyy määrittelydokumentti, johon kirjataan järjestelmältä edellytettävät ominaisuudet, ja ne hyväksytetään esimerkiksi organisaation ohjausryhmällä. (Kari Ainonen. 2013, 12.)

Määrittelyvaiheen sisältöön vaikuttaa tavoite, eli rakennetaanko uutta tietoverkkoa vai uusitaanko aiempaa verkkoa uudella ja tehokkaammalla verkolla. Määrittely aloitetaan usein tarvekartoituksilla, joissa kysytään käyttäjien tarpeita ja toiveita. Määrittelyn työkaluna käytetään myös erityyppisiä analyysejä esimerkiksi tietotarveanalyysit tai tietovuoanalyysejä. Näitä verrataan organisaation aiemmin toteutettuihin tietoverkkojen suunnitelmiin. Tarvekartoituksiin ja analysointeihin tarvitaan erityisesti organisaation johdon sitoutumista ja mukanaoloa sekä käyttäjien ja tietohallinnon asiantuntijoiden kokemuksia ja näkemyksiä aikaisemmasta toteutuksesta. Organisaation eri henkilöstöryhmien mukaan ottaminen auttaa myös lisäämään ymmärrystä muutosten ja uudistusten taustalla ja sitoutumaan tuleviin muutoksiin. (Kari Ainonen. 2013, 12.)

Kun suunnitellaan ja rakennetaan täysin uutta tietoverkkoa, käytetään määrittelyvaiheen analyyseinä ovat tietotarve-, tietovarasto- ja tietovuo- ja tarpeen mukaan myös verkon liikenneanalyysi. Mikäli uusitaan vanhaa verkkoa tehokkaammalla ja nopeammalla verkolla, tehdään yleensä edellisten lisäksi myös ongelma- ja syy-seuraus-analyysit. (Kari Ainonen. 2013, 12.)

5.2 Organisaation toiminnassa ja tietoverkoissa käsiteltävien tietojen analysointi

Organisaation toiminnassa ja tietoverkoissa käsiteltävien tietojen analysointiin kuuluu tietotarve- ja tietovarastoanalyysit. Organisaation eri toimintaprosessien tarvitsemat tiedot kartoitetaan ja määritellään tietotarveanalyysissä, jossa luokitellaan tiedot syöttö- ja tulostustietoihin. Syöttötiedot ovat tietojärjestelmään syötettäviä tietoja, esimerkiksi työntekijän yhteystiedot, osoitetiedot tai terveystiedot. Tulostustietoja ovat järjestelmään sisälle syötettyjen tietojen tietojenkäsittelyn kautta johdetut raportit, analyysit, yhteenvedot ja niin edelleen. Tietotarveanalyysin seuraavassa vaiheessa jaetaan tiedot organisaation tietoturvaluokituksen mukaisiin tietoturvaluokkiin. Tietoturvaluokitus määrittelee tietojen luottamuksellisuuden ja saatavuuden huomioiden toiminnan jatkuvuuden. (Kari Ainonen 2013, 12-13.) Tietovarastoanalyysissä suunnitellaan tietotarveanalyysissä kartoitettujen tietojen säilyttäminen, ja määritellään tietojen tallennusmuoto, joka määräytyy tietojen luonteen mukaan. Tallennusmuoto voi olla relaatio- tai dokumenttitietokanta tai tiedostomuotoinen tallennus tai tulostus paperille, ja samalla tarkistetaan ja varmistetaan säilytystavan soveltuvuus tiedolle tietojen saatavuuden ja luottamuksellisuuden näkökulmasta. (Kari Ainonen 2013, 12-13.)

5.3 Organisaation tietoverkossa liikkuvan tiedon selvittäminen ja analysointi

Organisaation tietovuoanalyysissä kartoitetaan, miten tiedot kulkevat organisaation eri toimintaprosessien sisällä ja niiden välillä. Analyysissä tiedot luokitellaan raportoivaan tietoon, jossa tieto kulkee alhaalta ylöspäin, ja ohjaavaan tietoon, jossa tieto kulkee ylhäältä alas päin sekä rutiinitietoon. Tilanteissa, missä tieto ei kulje edellä mainitulla tavalla virallisen organisaatiokaavion mukaisesti tiedonkulun luokittelu edellyttää niin sanotun epävirallisen organisaationkaavion selvittämistä. Tietovuoanalyysissä pitäisi myös pohtia, miten tarvittava tieto saadaan eri tietovarastoista. Tehdäänkö säännöllisiä tietokanta kyselyitä vai tarvitaanko automaattista ilmoitusta tiedon syntymisestä. (Kari Ainonen 2013,13.)

Syy-seuraus-analyysillä selvitetään aiemman tietojärjestelmän puutteet ja heikkoudet. Ongelma-analyysillä selvitetään vanhan tietojärjestelmän puutteita, jotka liittyvät järjestelmän tehokkuuteen, tietojen ylläpidon puutteisiin, tietoturvaongelmiin ja niin edelleen. (Kari Ainonen 2013,13.)

Tietoverkkosuunnittelussa erityisesti vanhan tietoverkon uusimisessa määrittelyvaiheen analyyseihin kuuluvat myös verkon liikenneanalyysit, jossa nykyisen olemassa olevan verkon liikennemäärät mitataan ja luokitellaan toimintaprosesseittain ja sovelluksittain. Tietotarve-, tietovarasto- ja tietovuoanalyyseistä saatujen tietojen pohjalta arvioidaan uuden verkon liikenteen määrä, josta saadaan arviot verkon eri osien kapasiteettivaatimuksien määrittelylle. (Kari Ainonen 2013,13.)

5.3.1 Organisaation varautumisen tason määrittäminen

Kansallinen turvallisuustilanteen muuttuminen on aiheuttanut myös varautumisen tilannearviointia. Varautumista vaativia tilanteita ovat:

- pitkät sähkö-, tietoliikenne- ja puhtaan veden jakelun katkot
- pitkät häiriöt pankkipalveluiden saatavuudessa
- luonnonilmiöt (myrskyt ja maastopalot)
- pitkäkestoisemmat kriisit (pandemiat tai sotilaalliset konfliktit) (Suomi.fi.2024b.).

Organisaatioiden tiedonhallinnassa varautuminen tämä näkyy myös tietokantojen, tietoverkkojen, verkon laitteiden suunnittelussa ja ylläpidossa. Normaali olojen poikkeustilanteisiin ja poikkeusolosuhteisiin varaudutaan muun muassa:

- kahdentamalla verkkoja ja internet liittymiä
- hyödyntämällä mobiililaitteita ja satelliittiyhteyksiä
- varayhteyksien rakentamisella ja varalaitteilla
- varavoimajärjestelmillä (aggregaatti)
- koneiden etäkäytön ja pilvipalveluiden tietoturvan varmistamisella
- tietojen ja tiedostojen varmuuskopioinneilla
- laitteiden tallennettujen konfiguraatiotietojen saatavuuden varmistamisella
- riittävillä palvelutason määrittelyillä SLA (Service Level Agreement) sopimuksissa
- viranomaisverkolla ja -kenttäjärjestelmällä ja hätäkeskustietojärjestelmällä
- viranomaisten julkisen hallinnon turvallisuusverkolla.

ICT -Palvelutuotannon varautuminen -suosituksessa ohjeistetaan organisaatioita huoltovarmuuteen. (Huoltovarmuusorganisaatio 2024).

ICT-palvelutuotannon varautuminen:

- tunnista ja kuvaa kriittiset organisaation tuottamat palvelut ja tärkeät toiminnot sekä tuotannontekijät
- tee suunnittelu ja toteutus eri vaiheissa aloittaen kaikkein kriittisimmistä palveluista ja riskialttiimmista tuotannontekijöistä.
- varmista, että eri osapuolten varautumissuunnitelmat ovat yhdenmukaiset. (Huoltovarmuusorganisaatio 2024).

5.3.2 Organisaation laitetilaturvallisuuden tasojen määrittäminen

Liikenne- ja viestintäviraston Traficom'in NCSA -toiminnon hyväksymät salausratkaisut määrittelevät myös tietoturvallisuuden varmistamisen toimenpiteitä (Traficom. 2025b.).
Laitetilaturvallisuuden arviointikriteeristönä käytetään Julkisen hallinnon tietoturvallisuuden arviointikriteeristöä Julkri'a. (VM. 2023.)

5.3.3 Organisaation tietoturvallisuuden varmistavien toimenpiteiden määrittäminen

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa -asetuksessa (FIN-LEX 2019b) määrätään organisaatioiden tietoturvallisuuden varmistamisesta ja siihen liittyvistä toimenpiteistä asiakirjojen osalta. Tämän lisäksi Liikenne- ja viestintäviraston Traficom'in NCSA -toiminnon hyväksymät salausratkaisut määrittelevät myös tietoturvallisuuden varmistamisen toimenpiteitä (Traficom).
Tietoturvallisuuden arviointikriteeristönä käytetään Julkisen hallinnon tietoturvallisuuden arviointikriteeristöä Julkri'a. (VM. 2023.)

5.3.4 Organisaation tietoverkossa liikkuvan tiedon suojauksen tasojen määrittäminen

Liikenne- ja viestintävirasto Traficomin suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä (Traficom 2025), ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista (Traficom 2021) ja NCSA-toiminnon hyväksymät salausratkaisut (Traficom 2025b) määrittelevät liikkuvan tiedon suojauksen vaateet.
Tietoverkossa liikkuvan tiedon suojauksen tasojen arviointikriteeristönä käytetään Julkisen hallinnon tietoturvallisuuden arviointikriteeristöä Julkri'a. (VM. 2023.)

5.4 Tietoverkkojen arkkitehtuurin suunnittelu

Tietojärjestelmän arkkitehtuuri kuvaa tietoverkon rakenneosat, joita ovat verkko ja verkkoon liitetyt laitteet, ja niiden väliset yhteydet ja riippuvuudet. Järjestelmän suunnittelu ja toteutus pohjautuu tietojärjestelmän arkkitehtuuriin tukien ja ohjaten rakenteen kehittämistä järjestelmän elinkaaren ajan. Myös järjestelmän kehittämiseen ja ylläpitämiseen liittyviin keskusteluihin eri sidosryhmien välillä voidaan käyttää arkkitehtuurikuvauksia. (Valtteri Aalto 2019, 16.)

Tietojärjestelmällä tarkoitetaan järjestelmää, jonka tarkoituksena on tietojen käsittelyn avulla tehostaa tai helpottaa tai mahdollistaa jokin toiminta. Tietojärjestelmä koostuu eri tyyppisistä tiedoista, niitä käsittelevistä ihmisistä, tietojenkäsittely- ja tiedonsiirtolaitteista, ohjelmistoista ja tiedonkäsittelysäännöistä. (Valtteri Aalto 2019, 16.)

5.4.1 Lähiverkkostandardit

Lähiverkkostandardit kostuvat IEEE:n 802-standardeista ja yleiskaapelointistandardeista. Langattomat verkot on rajattu opinnäytetyön ulkopuolelle (Jodi Haasz 2020).

IEEE:n 802-standardit:

The Institute of Electrical and Electronics Engineers (IEEE) kehittää verkkostandardeja, jotka ovat hallitsevia lähiverkkostandardeja tällä hetkellä. IEEE on myös kehittänyt (1980 -luvun puolessavälissä) uusia standardeja Ethernet -verkoille eli lähiverkoille esimerkiksi Ethernet 802.3, jota edelleenkin käytetään ja kehitetään. (Jodi Haasz 2020).

802.1X -standardi kehitettiin vastaamaan heikon tietoturvan parantamisen, tietoturvavaatimusten lisääntymisen ja 802.11-verkkojen yleistymisen tarpeisiin. Internet -palveluiden lisääntyessä kirjautumistunnusten hallinnointiin on haettu keskitettyä ratkaisua Authentication, Authorization ja Accounting (AAA-protokolla) -palvelun toteuttavista protokollista esimerkiksi Remote Authentication Dial-In User Service (RADIUS) -protokolla, jonka ideana on tuottaa keskitetty tietokanta, joka mahdollistaa käyttäjien turvallisen tunnistautuminen kaikissa olosuhteissa. Ratkaisussa AAA -protokollan tehtävänä on kuljettavat autentikointiliikenne verkon reunalta turvallisesti verkon autentikointipalvelimelle. 802.1X:n -standardia on esitetty käytettäväksi myös langattomille verkoille, minkä avulla avainten jakelu voidaan toteuttaa turvallisesti liityntäpisteelle ja päätelaitteille. (Ville Leppäniemi, Daniel Nygård 2016, 10.)

802.1X-standardia käytetään IEEE 802 Ethernet- ja WLAN -verkoissa. Standardin tarkoituksena on estää lähiverkon liityntäpisteen kautta luvattoman asiakaslaitteen kommunikointi. Verkossa liityntäpiste voi olla esimerkiksi kytkimen portti (IEEE 802.3 ja 802.5) tai tukiaseman looginen portti (IEEE 802.11). Standardissa käytetään käyttäjän todentamiseen ensimmäisessä vaiheessa todennusprotokollana Protected EAP (PEAP) todennusprotokolla ja toisessa vaiheessa Extensible Authentication Protocol (EAP) – Transport Layer Security (TLS) metodia. Kun palvelin on hyväksynyt käyttäjän todentamisen, muodostetaan yhteysavaimella WEP -tunneli, minkä jälkeen voidaan aloittaa dataliikenteen välittäminen. Myös EAP Tunneled TLS Authentication Protocol (EAP-TTLS) -menetelmää voidaan käyttää autentikointitietojen välittämisessä. Menetelmässä sertifikaatit sijaitsevat keskitetysti RADIUS-palvelimella, mikä säästää hallinnointikustannuksia.

802.1X -standardin etuja ovat avoin standardi, käyttäjän todentaminen verkon reunalla, tietoturvan vahvistaminen salausavaimen vaihtamisella määräajan tai tapahtuman jälkeen ja datapaketin koko. Standardi voidaan toteuttaa olemassa oleviin verkkoihin, joihin on rakennettu esimerkiksi VPN- ja etäkäyttöyhteyksiä. (Ville Leppäniemi, Daniel Nygård 2016, 10.)

Yleiskaapelointistandardi:

Yleiskaapelointijärjestelmä toimii kaikkien yleisesti käytössä olevien sovellusten kanssa täyttäen niiden vaatimukset. Yleiskaapelointistandardi koostuu kolmesta eri osasta:

- EN-50173-1 (määrittelee toimistorakennusten tele ja datakaapeloinnin)
- EN-50173-2 (määrittelee teollisuusrakennusten kaapeloinnin)
- EN-50173 (määrittelee asukasrakennusten kaapeloinnin). (Ville Leppäniemi, Daniel Nygård 2016, 10.)

EN 50173-1 - standardissa määritellään tietoliikenteeseen liittyvien järjestelmien yleiskaapelointijärjestelmien runkokaapelointien osajärjestelmien rakenne ja kokoonpano yhden tai useamman rakennuksen toimitilakiinteistöille tietyllä alueella (SFS 2018). Standardia sovelletaan kiinteistöissä, joissa tietoliikenneverkkojen alueellinen laajuus on max. 2000 m. Standardia suositellaan myös suurempiin asennuksiin toimitilakiinteistöissä. Myös teollisuus- ja asuinkiinteistöissä standardin periaatteita voidaan hyvin soveltaa. (Ville Leppäniemi, Daniel Nygård 2016, 10.)

EN 50173-1 – standardia sovellettaessa kaapelointiin etuna on toimittajariippumattomuus. Standardi tukee puhetta, tekstiä, dataa, kuvaa, videokuvaa ja tietoliikennesovelluksia. Standardissa määritellään suorituskykyvaatimukset kanaville, siirtoteille ja kaapeleille, kytkentäkaapeleille ja liittymätarvikkeille, sekä kaapeloinnin rakenne ja kokoonpano ja toteutusvaihtoehdot. (Ville Leppäniemi, Daniel Nygård 2016, 10.)

5.4.2 Verkkotyypit

Tietokoneverkko voidaan luokitella yksityiseen ja julkiseen luokkaan (Word Wide Technology 2021). Edellä mainitun lisäksi tietokoneverkot voidaan luokitella koon, fyysisen arkkitehtuurin ja peittoalueen

perusteella. Verkon rakenteen ja kaapeloinnin kuvaamiseen käytettyjä yleisimpiä typologioita ovat tähti-, laajennettu tähti, väylä-, rengas-, mesh- ja hierarkkinen typologia. (education-wiki 2025.)

Yleisimpiä luokituksia koon mukaan ovat:

1. henkilökohtainen verkko (Personal Area Network, PAN)
2. langaton henkilökohtainen verkko (Wireless Personal Area Network, WPAN)
3. lähiverkko (Local Area Network, LAN)
4. langaton lähiverkko (Wireless Local Area Network, WLAN)
5. metropolitan verkko (Metropolitan Area Network, MAN)
6. suuralueverkko (Wide Area Network, WAN)
7. globaali verkko (Global Area Network, GAN) (IT PLANET).
8. satelliittiverkko
9. mobiilidataverkko. (education-wiki 2025.)

Edellä luetelluista langattomia tai osittain langattomia verkkoja ovat WPAN, WLAN, WAN, GAN, satelliittiverkko ja mobiilidataverkko, jotka on rajattu opinnäytetyön ulkopuolelle.

Personal Area Network, PAN:

Henkilökohtainen verkko (Personal Area Network, PAN) on verkko, jossa käyttäjän henkilökohtaiset laitteet esimerkiksi tietokone, tulostin, matkapuhelin, kuvanlukija ja muut laitteet voidaan yhdistää toisiinsa käyttämällä USB-kaapeleita ja porttitoistimia, langattomia Bluetooth-laitteilla, FireWire-liitäntöjä tai infrapunaa ja niin edelleen. Yhdyskäytävänä lähiverkkoon tai Internetiin voidaan käyttää puhelinta tai tietokoneen verkkoliitäntää. (education-wiki 2025.)

Wireless Personal Area Network, WPAN:

Langaton henkilökohtainen verkko (Wireless Personal Area Network, WPAN) on verkko, jossa käyttäjän henkilökohtaiset laitteet esimerkiksi tietokone, tulostin, matkapuhelin, kuvanlukija ja muut laitteet voidaan yhdistää toisiinsa langattomasti. Verkkoa on mahdollista käyttää rajatulla alueella, joka on metristä muutamaan kymmeneen metriin ilman signaalinvahvistimia. (education-wiki 2025.)

Local Area Network, LAN:

Lähiverkko (Local Area Network, LAN) on verkko, joka toimii rajatulla maantieteellisellä alueella. LAN -verkko voi olla esimerkiksi talon tai yrityksen toimipisteen eri laitteiden muodostama verkko, joka voidaan toteuttaa käyttämällä kytkimiä ja toistimia siirtämään tietoa lähiverkon sisällä, sekä reititintä siirtämään tietoa laajaverkkoon (WAN). Lähiverkon tiedonsiirtonopeutena käytetään 10 – 1 000 megabittiä sekunnissa. Verkko Langaton lähiverkko (WLAN) rakennetaan usein täydentämään langallista lähiverkkoa. (education-wiki 2025.)

Lähiverkot voidaan jakaa verkon tyypin mukaan asiakaspalvelin lähiverkkoihin sekä vertaislähiverkkoihin. Asiakaspalvelin lähiverkoissa laitteet esimerkiksi tietokoneet on yhdistetty verkon kautta erilliseen keskitettyyn palvelimeen, jonka kautta laitteet saavat dataa, sovelluksia ja resursseja käyttöönsä. Vertaislähiverkot ovat asiakaspalvelin verkkoja pienempiä, eivätkä ne pysty käsittelemään suurta määrää dataa tai työkuormia. Vertaislähiverkossa ei ole erillistä keskitettyä palvelinta vaan kaikki laitteet ovat asiakkaan ja palvelimen roolissa, esimerkiksi kotiverkot ovat vertaislähiverkkoja. Lähiverkkoja yhdistetään toisiinsa laajaverkoilla (alueverkko) toteutettuina esimerkiksi kuitu-Ethernet-tekniikalla (1GE ja 10GE-Ethernet) (Cisco 2025).

Metropolitan Area Network, MAN:

Metropolitan verkko (Metropolitan Area Network, MAN) eli kaupunkiverkko verkko, joka toimii yhden tai useamman kaupungin alueella esimerkiksi jokin kaupunki ja sen pienemmät lähikunnat tai muut yhteen kasvaneet lähekkäin olevat kaupungit tai yliopistot voivat muodostaa tällaisen. MAN -verkko muodostuu useasta lähiverkosta. (education-wiki 2025.)

Wide Area Network, WAN:

Suuralueverkko (Wide Area Network, WAN) on verkko, joka kattaa isoja maantieteellisiä yhdistäen lähiverkot sekä kaupunkiverkot yhdeksi suureksi verkoksi, esimerkkinä Internet. Kaupunkiverkkojen ja lähiverkkojen nopeiden verkkoyhteyksien tarpeisiin käytettään WAN -verkoissa rinnakkaisia linjoja nopeaan tiedon siirtoon paikasta toiseen. Tietoliikenteen määrän rajoittamiseen käytetään tarvittaessa IP -osoitteita ja -alueita. (education-wiki 2025.)

Kiinteässä verkossa nettiyhteyden nopeuteen ja toimivuuteen vaikuttavat muun muassa käytetty tiedonsiirtotekniikka (valokuitu, kaapeliverkko, puhelinverkko), sijainti (päätelaitteen sijainti verkon keskittimeen) esimerkiksi mitä kauempana asut operaattorin laajakaistakeskittimestä sitä enemmän se vaikuttaa liittymän nopeuteen, monenko muun käyttäjän kesken yhteys on jaettu, laite. (education-wiki 2025.)

Global Area Network, GAN:

Globaali verkko (Global Area Network, GAN) on maantieteellisesti hajautettu tietokoneverkko, mikä mahdollistaa tiedonvaihdon ja viestinnän käyttäjien välillä eri puolilla maailmaa, esimerkiksi WWW (Word Wide Web) -verkko. Verkko mahdollistaa datan, resurssien ja sovellusten käytön eri sijainneissa. GAN -verkko on lähiverkon ja suuralueverkon sekoitus, joka käyttää satelliitteja tai laaja-alueverkkojen valokuiturakennetta tiedonsiirrossa.
Globaaleja alueverkkoja käytetään pääasiassa yritysyhteistyöhön, puhelinneuvotteluihin tai Online -peleihin. GAN -verkkoja voidaan käyttää myös suurten tiedostojen jakamiseen tai etätietokantojen käyttämiseen. Verkko on joustava, skaalautuva ja kustannustehokas. (IT PLANET.)

Satelliittiverkko on langaton verkko, jossa radioyhteyttä käytetään satelliittien, maa-asemien ja satelliittipäätelaitteiden välillä (Suomi.fi 2024a), esimerkiksi Starlink satelliitti-internet, latausnopeus 25 – 220 Mbps.

Mobiilidataverkko:

Mobiilidataverkko eli matkapuhelinverkko muodostuu maan sisällä kulkevasta valokuitukaapelista rakennetusta runkoverkosta sekä runkoverkkoon mekaanisesti kytketyistä jatkuvaa mikroaaltosäteilyä kaikkiin ilmansuuntiin lähettävistä tukiasemista eli soluista. Puhelut kulkevat suurimman osan matkastaan mobiilioperaattorien valokuituverkossa, vain alku- ja/tai loppumatka tapahtuu ilmateitse. (education-wiki 2025.)

Verkkoja voidaan luokitella myös käyttäjäryhmän mukaan:

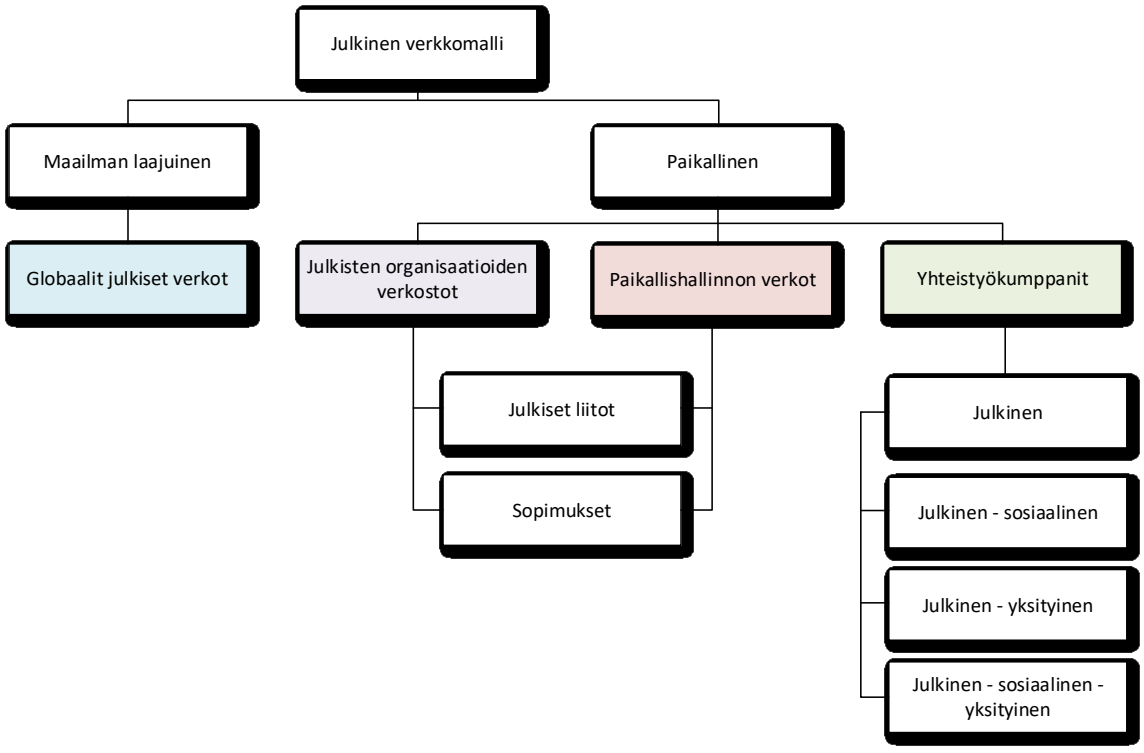
1. Tietyn ryhmän käyttöön rajattu intranet verkko, esimerkiksi yrityksen sisäinen verkko
2. Yhteisöjen välinen suljettu extranet verkko
3. Maailmanlaajuinen avoin Internet tietoverkko. (education-wiki 2025.)

5.4.3 Julkisten verkkomallit

Julkiset verkot esimerkiksi julkisen hallinnon verkot eroavat muista verkoista, kuten yritysverkoista. Julkisten verkkomallien erittely on monitasoista ja voi sisältää erilaisia kriteerejä (Beata Barczak 2023, 39).

Julkiset verkkomallit voidaan jakaa neljään eri tyyppiin (KUVIO 6):

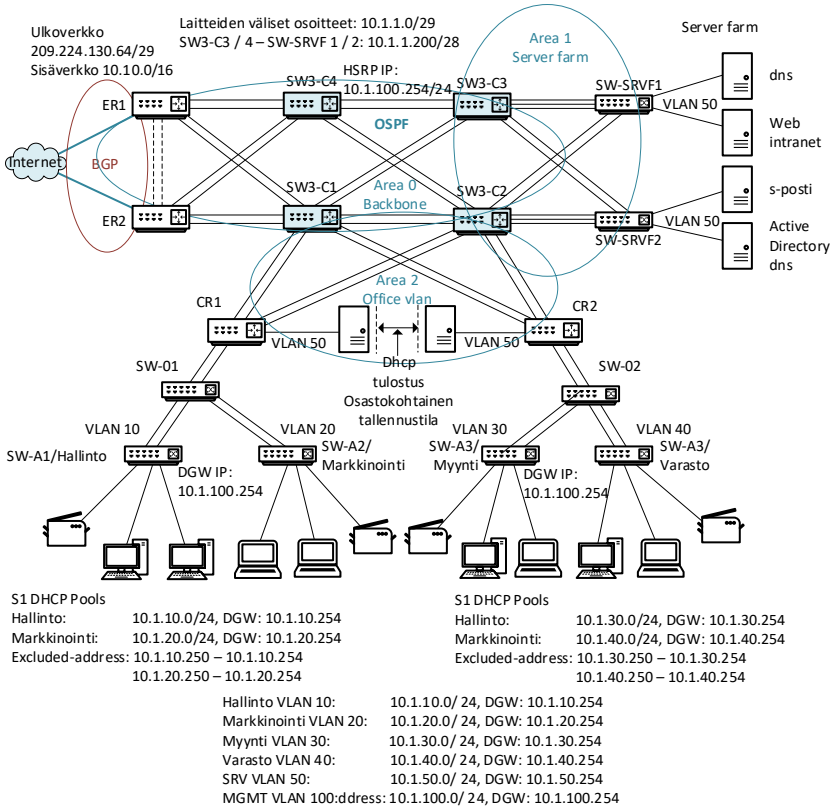
1. globaalit julkiset verkostot
2. julkisten organisaatioiden verkostot
3. paikallishallinnon verkostot ja
4. kumppanuussuhteet. (Beata Barczak 2023, 39.)



KUVIO 6. Julkisten verkkomallien jako neljään eri tyyppiin (Mukaillen Beata Barczak 2023, 39, mukaillen).

5.4.4 Lähiverkkojen topologiat

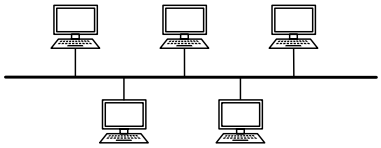
Laitteiden välistä verkon kautta tapahtuvaa tietoliikennettä tarkastellaan loogisen ja fyysisen topologian tasoilla. Looginen topologia määrittelee ja hahmottaa reitit ja polut, mitä pitkin datapaketit kulkevat laitteelta toiselle ja miten laitteiden välinen tiedonsiirto tapahtuu. Fyysinen topologia määrittelee, kuinka koneita yhdistävät kaapelit, tietokoneet, kytkimet, reitittimet ja muut laitteet on fyysisesti kytketty ja sijoiteltu. Kun halutaan tietää, miten datapaketti liikkuu esimerkiksi palvelimelta käyttäjän koneelle, käytetään loogista topologiaa, ja kun halutaan tietää, kuinka monen kytkimen kautta datapaketti liikkuu palvelimelta käyttäjän koneelle, käytetään fyysistä topologiaa asian selvittämiseen. Verkon fyysisessä ja loogisessa rakenteessa voi olla eroavaisuuksia. Sekä fyysinen että looginen topologia ovat ratkaisevan tärkeitä erityyppisten järjestelmien esimerkiksi lähiverkkojen suunnittelussa ja rakentamisessa. (Bryce Leo 2024.)



KUVIO 7. Verkon loogisen topologian perusmalli (Kari Ainonen 2013)

Verkon rakenteen ja kaapeloinnin kuvaamiseen käytettyjä yleisimpiä topologioita ovat väylä-, tähti-, laajennettu tähti, hierarkkinen-, rengas- ja mesh -topologia. (Bryce Leo 2024.)

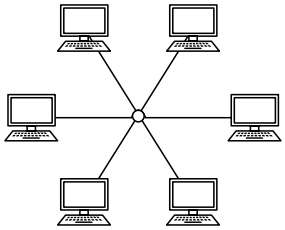
Väylätopologia:



KUVIO 8. Väylätopologia (Bryce Leo 2024, mukaillen)

Vanhin käytössä olevista topologioista on väylätopologia. Väylätopologiassa verkon laitteet on kytketty laitteiden välillä kulkevaan yhdistävään kaapeliin, jonka on kummastakin päästä kytketty vastukseen (terminaattoriin). Väylätopologian heikkous on siinä, että verkkoa voi käyttää vain yksi laite kerrallaan. Verkon käyttö perustuu kilpavarausmenettelyyn (CSMA/CD), jossa kaikki verkon laitteet yrittävät lähettää dataa yhtä aikaa aiheuttaen törmäyksiä ja ruuhkauttaen verkkoa. Kilpavarausmenettely rajoittaa laitteiden määrää verkossa. Väylärakenteessa verkossa kaikki verkon laitteet saavat sanoman samanaikaisesti. Verkon kaapelointi on toteutettu joko koaksiaali- tai valokuitukaapelilla. Kaapelin mennessä epäkuntoon verkko jakautuu kahteen osaan ja lakkaa toimimasta. (Bryce Leo 2024.)

Tähtitopologia:



KUVIO 9. Tähtitopologia (Bryce Leo 2024, mukaillen)

Tähtitopologiassa verkon laitteet kytketään verkon keskellä sijaitsevaan keskuslaitteeseen esimerkiksi kytkimeen tai keskittimeen, jota kautta verkon kaikki liikenne kulkee. Keskuslaitteeseen voi olla kytkettynä 12 tai 24 eri verkkolaitetta. Kytkin tai keskitin, voidaan linkittää toiseen kytkimeen tai reitittimeen, ja näin saada yhteys toisille laitteille. Keskittimiä käytetään yhä vähenevässä määrin, koska ne voivat ruuhkauttaa liikennettä kaiuttaessaan kaiken liikenteen jokaiseen keskittimessä kiinni olevaan verkon laitteeseen. Kytkintä käytettäessä verkko ei ruuhkaannu, koska kytkin ohjaa datan vain tarkoitettuun osoitteeseen. Yhden kaapelivälin rikkoutuminen vaikuta muun verkon toimivuuteen. Verkon

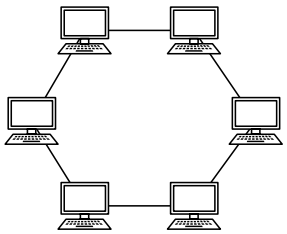
kaapelointi on toteutettu käyttämällä kierrettyä parikaapelia, koaksiaali- tai valokuitukaapelia. Käytössä olevista Ethernet -verkkotopologioista on tähtitopologia yleisin, esimerkkinä lankapuhelinverkko. (Bryce Leo 2024.)

Laajennettu tähti yhdistää yksittäiset tähdet toisiinsa hierarkkisesti, joko eteen, viereen tai jälkeen. Rakennetta käytetään reititysprotokollien yhteydessä, jotka vaativat tiukkaa hierarkiaa, esimerkiksi TCP/IP -verkkojen reititysprotokolla OSPF. (Bryce Leo 2024.)

Hierarkkinen topologia:

Hierarkkinen topologia eli puutopologia (Global YO 2023) yhdistää sekä tähti- että väylätopologian ominaisuudet luoden kerroksellisen, haarautuvan verkkorakenteen. Verkossa laitteet on järjestetty puumaiseen muodostelmaan, jossa useita tähtiverkkoja on kytketty keskeiseen runkoverkkoon (väylään). Rakennetta käytetään suurissa skaalautuvuutta vaativissa verkoissa, kuten organisaatioiden infrastruktuureissa ja yritysten verkoissa. Verkon suunnittelu puutopologialla yhdistämällä tähtitopologioita parantaa verkon skaalautuvuutta, joustavuutta ja hallittavuutta vaikuttamatta koko järjestelmään. (Bryce Leo 2024.)

Rengastopologia:

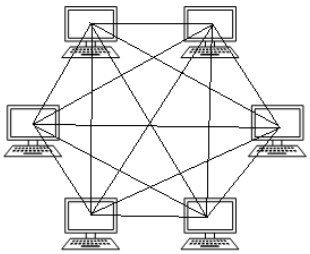


KUVIO 10. Rengastopologia (Bryce Leo 2024, mukaillen)

Rengastopologiassa verkon laitteet kytketään toisiinsa fyysisesti renkaan muotoon niin, että verkon laitteet ovat kytkettynä niin sanottuihin solmukohtiin. MAU-yksiköitä (Multistation Access Unit) on käytetty verkkolaitteiden verkkoon yhdistämiseen. Topologian rengasrakenteessa verkon jokaisella laitteella on kummallakin puolella naapuri niin, että toiselle lähetetään dataa ja toiselta saadaan dataa, ja vain yksi verkkolaite saa datan kerrallaan. Verkossa niin sanottu ”haltijalaite” saa lähettää dataa, ja

muut laitteet eivät lähetä mitään. Jos laitteella ei ole mitään lähetettävää, siirtyy vuoro seuraavalle laitteelle myötäpäivään kiertäen esimerkkinä IBM:n Token Ring -verkko. (Bryce Leo 2024.)

MESH -topologia:



KUVIO 11. MESH -topologia (Bryce Leo 2024, mukaillen)

Mesh-topologiassa kaikki verkon laitteet ovat suorassa yhteydessä toisiinsa. Mesh-topologiaa kutsutaan myös silmukkatopologiaksi, ja sitä käytetään langattomissa verkoissa, missä kaikki verkon laitteet voivat vapaasti viestiä keskenään kaapeloinnin sitä rajoittamatta. (Bryce Leo 2024.)

Ethernet -verkkotopologioista yleisin on tähtitopologia ja laajennettu tähtitopologia, ja puutypologia ja Mesh -topologia langattomissa verkoissa. Näitä typologioita käytetään yleisimmin suunniteltaessa tietokoneverkon perusrakennetta. (Bryce Leo 2024.)

5.4.5 Tiedon siirtäminen verkossa eri toimijoille salausvaatimukset huomioiden ja eri toimijoiden väliset yhdyskäytäväratkaisut

Osiossa käydään läpi yleisimmät edellytykset hyväksyttävissä oleville yhdyskäytäväratkaisuille, eri yhdyskäytäväratkaisujen keskeiset ominaispiirteet sekä esimerkein eri vaihtoehdot turvaluokitellun TLII, TLIII, TLVI ja salattu tiedon siirtämiseen tietoverkossa toimijalta toiselle (Traficom 2021).

Kun suunnitellaan yhdyskäytäväratkaisuja, niin periaate on, että hyväksyttävän yhdyskäytäväratkaisun pitää estää ylemmän turvallisuusluokan tiedon kulkeutuminen matalamman turvallisuusluokan ympäristöön (Bell-LaPadula -mallin säännöt). (Traficom 2021).

Bell-LaPadula -malli toteutetaan usein yksisuuntaisella suodatusratkaisulla, jossa sallitaan liikennöinti vain matalamman luokan ympäristöstä ylemmän luokan ympäristöön, sekä sisältösuodatusratkaisulla, jossa sallitaan vain matalamman luokan tiedon siirtyminen ylemmän luokan ympäristöstä matalamman luokan ympäristöön. Siirrettävä tieto tunnistetaan ennen siirtämistä ylemmän luokan ympäristössä. Suodatus tulee toteuttaa luotetun ohjelmisto- ja rauta-alustan päällä. (Traficom 2021).

Hyväksyttävältä yhdyskäytäväratkaisun edellytetään myös monikerrossuojaamista, vikaturvallisuutta, vähimpien oikeuksien ja haavoittuvuusavaruuden minimointia. Yhdyskäytäväratkaisun tulee myös pystyä suojaamaan itseään käyttöympäristönsä uhkia vastaan ja turvallisuustoteutuksen oikeellisen toiminnan tulee olla luotettavasti todennettavissa. Myös turvallisuuden hallinnoinnille sekä valvonnalle edellytetään luotettavaa toteutusta yhdyskäytäväratkaisulta, mukaan lukien kyky havainnoida hyökkäyksiä yhdyskäytäväratkaisua ja/tai sen suojaamaa ympäristöä vastaan. (Traficom 2021).

Yleisimmät hyväksyttävät yhdyskäytäväratkaisut jakautuvat:

1. yksisuuntaisiin suodatusratkaisuihin, jotka jakautuvat edelleen:
    - datadiodiratkaisuihin
    - muihin yksisuuntaisiin suodatusratkaisuihin.
2. alkiotunnistuksen sisältösuodatusratkaisuihin. (Traficom 2021).

Yksisuuntaiset suodatusratkaisun datadiodiratkaisussa liikennöinti tapahtuu matalamman luokan ympäristöstä ylemmän luokan ympäristöön, esimerkiksi matalamman turvallisuusluokan ympäristön sähköpostien välitys ylemmän luokan turvallisuusluokan ympäristöön.
Yksisuuntaiset suodatusratkaisun datadiodiratkaisussa hyväksytään yhden tai useamman turvallisuusluokan ylittävä yhdyskäytäväratkaisu välillä TL IV -> TL III, TL III -> TL II, TL IV -> TL II ja TL II -> TL I (moniportaisena toteutuksena erityisehdoin). (Traficom 2021).

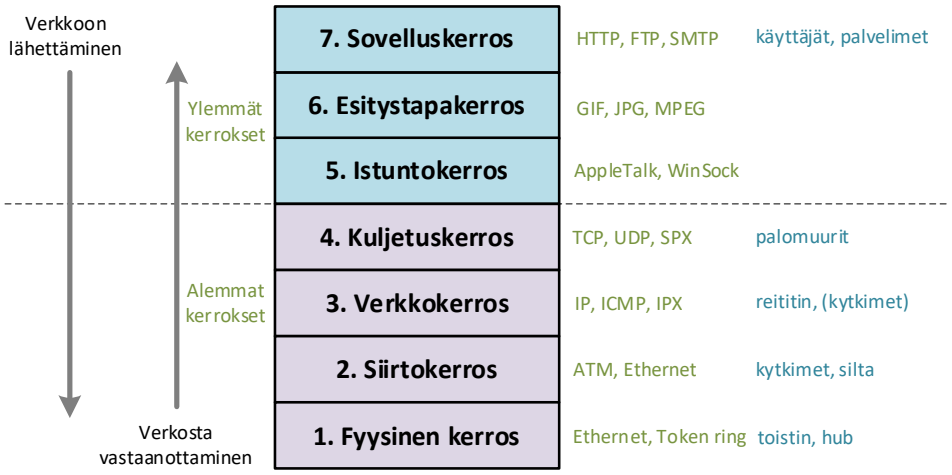
Yksisuuntaiset suodatusratkaisun muu yksi suuntaisessa suodatusratkaisussa liikennöinti tapahtuu matalamman luokan ympäristöstä ylemmän luokan ympäristöön, esimerkiksi matalamman luokan paikkatiedon tuonti tilannekuvatiedon tarkkuuden parantamiseksi.
Yksisuuntaiset suodatusratkaisun muu yksi suuntaisessa suodatusratkaisussa hyväksytään yhden turvallisuusluokan ylittävä yhdyskäytäväratkaisu välillä TL IV -> TL III. (Traficom 2021).

Alkiotunnistuksen sisältösuodatusratkaisussa liikennöinti tapahtuu matalamman luokan ympäristöstä ylemmän luokan ympäristöön tai ylemmän luokan ympäristöstä matalamman luokan ympäristöön tai edellisten yhdistelmänä tai/ja saman turvallisuusluokan ympäristöstä toiseen saman turvallisuusluokan ympäristöön. Alkiotunnistuksen sisältösuodatusratkaisussa hyväksytään yhden turvallisuusluokan ylittävä yhdyskäytäväratkaisu välillä TL IV <- -> TL III. Kun ylemmän luokan ympäristöstä siirretään matalamman luokan tietoa matalamman luokan ympäristöön, hyväksytään toteutus datadiodiin yhdistettynä myös välillä TL II -> TL III ja TL II -> TL IV. (Traficom 2021). Myös muita ratkaisumalleja on mahdollista käyttää riskiarviointiin perustuen tilanteissa, missä ei voi soveltaa edellä mainittuja malleja. (Traficom 2021).

5.4.6 OSI -malli

The Open Systems Interconnection (OSI) -malli on kuvaus tietokonejärjestelmien verkon yli kommunikointiin käyttämästä seitsemästä kerroksesta. OSI -mallin tarkoitus on varmistaa kansainvälisten tietojärjestelmien välinen yhteensopivuus, ja näin helpottaa järjestelmien yhteensopivuutta ja kehitystä. OSI -malli oli ensimmäinen standardi malli verkkokommunikaatiolle. (Jarkko Leiviskä 2021.)

Nykyinen Internet perustuu Transmission Control Protocol/Internet Protocol (TCP/IP) -malliin, joka on OSI -mallia yksinkertaisempi rakenteeltaan. OSI-malli on kuitenkin vielä laajasti käytössä, koska se auttaa hahmottamaan verkon toimintaa sekä auttamaan verkkoon liittyvien ongelmien selvittämisessä ja vikojen etsinnässä. (Jarkko Leiviskä 2021.)



KUVIO 12. OSI -malli (Andrew L. Russell 2013, mukaillen)

OSI -malli (KUVIO 11) koostuu seitsemästä kerroksesta, joita ovat:

7. Sovelluskerros
    a. kerroksella toimivat sovellukset, jota käyttäjät käyttävät datan vaihtoon
6. Esitystapakerros
    b. kerros vastaa vaihdettavan datan muodosta
5. Istuntokerros
    c. kerros vastaa 7. ja 6. kerroksien yhteyksien avaamisesta ja sulkemisesta
4. Kuljetuskerros
    d. kerros pilkkoo datan segmenteiksi ja päättää datan lähettämisen tavan
3. Verkkokerros
    e. kerros vastaa Internetin ohjeistuksesta ja datan osoitteistamisesta
2. Siirtoyhteyskerros
    f. kerros valmistelee datan fyysiselle kerrokselle
1. Fyysinen kerros
    g. kerros määrittää 2. kerroksesta tulevan datan fyysisen siirtotavan. (Jarkko Leiviskä 2021.)

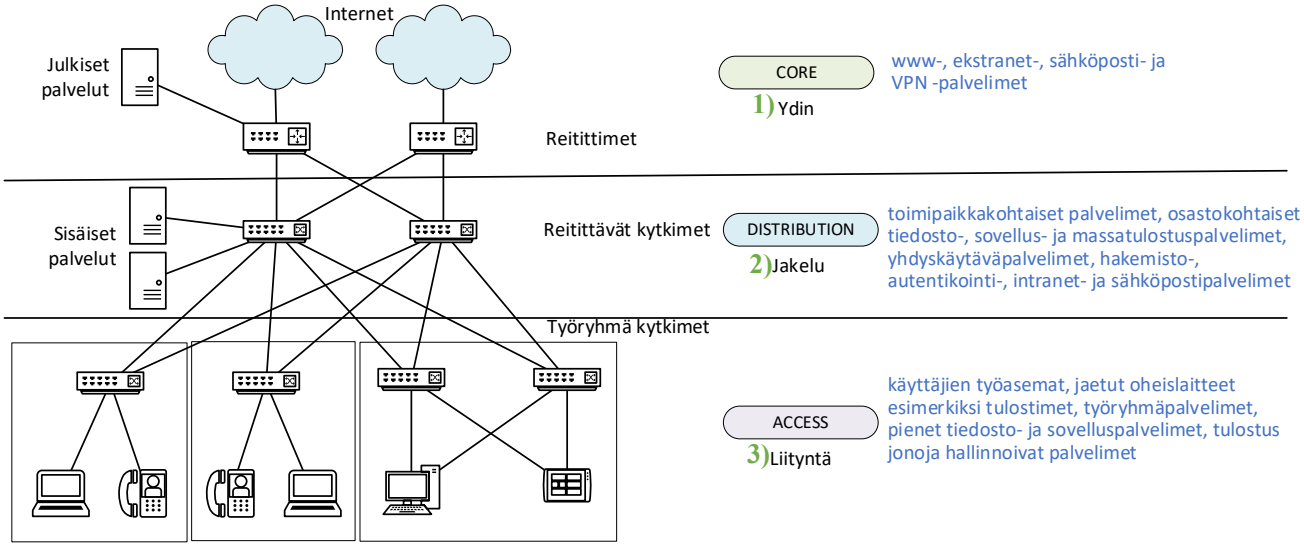
5.4.7 TCP-IP -malli

Internet protokollapaketti tarjoaa päästä – päähän tiedonsiirron määrittäen kuinka tiedot tulee paketoida, osoittaa, lähettää, reitittää ja vastaanottaa. TCP-IP mallia ei käsitellä tässä yhteydessä yksityiskohtaisemmin. Langattomat mobiiliverkot on rajattu opinnäytetyön ulkopuolelle. (Jarkko Leiviskä 2021.)

5.4.8 Hierarkkinen tietoverkko arkkitehtuuri

Tietoverkon segmentointi on organisaation tietoturvan kivijalka. Kun segmentointi suunniteltu ja toteutettu huolellisesti, tietoverkon tietoturvaa voidaan lähteä rakentamaan eteenpäin esimerkiksi suunnittelemalla ja lisäämällä verkkoon palomuurit ja niin edelleen. (Valtteri Aalto 2019, 16.)

Yleisin suunnitteluun käytetty malli on Ciscon kehittämä taso malli. Mallin avulla palvelut saadaan jaettua verkon eri tasoille, ja vähennetään näin verkon kuormitusta ja mahdollisia pullonkauloja. Mallissa jokaisella tasolla on omat tehtävänsä. Verkon rakenteen kuvaaminen on hyvä toteuttaa käyttämällä sekä fyysistä että loogista topologiaa. Topologiat on kuvattu tarkemmin osiossa 5.4.4. Yllä mainitut tasot löytyvät loogisesta topologiasta kerroksittain. (Kari Ainonen 2013).



KUVIO 13. Kolmitasoinen hierarkkinen tietoverkkoarkkitehtuuri (Kari Ainonen. 2013, mukaillen)

Taso -malli koostuu kolmesta tasosta:

1) ydin taso
   - tasolla liitytään Internetiin, palveluihin, organisaation toimipisteisiin
2) jakelu taso
   - tasolle sijoitetaan suuremmalle käyttäjäjoukolle yhteiset palvelimet
3) liityntä taso
   - tasolla liitytään organisaation lähiverkkoon (Kari Ainonen 2013).

Tasot käytännön suunnitellaan niin sanotulla ylhäältä-alas-menetelmällä. Määrittelyvaiheen tietojen perusteella suunnitellaan ydin tason palvelut laite- ja kaapelointiratkaisuineen. Tämän jälkeen suunnitellaan jakelu tason sisäiset palvelut ja viimeisenä liityntä tason julkiset palvelut.
Verkon segmentoinnissa käytetään PCI-DSS standardin suosituksia. (Kari Ainonen 2013).

Hierarkkisen tietoverkkoarkkitehtuurin hyötyjä on verkon erittäin hyvä suorituskyky, parempi hallittavuus, arkkitehtuurin skaalautuvuus ja vikasietoisuus.

5.4.9 Two-Tier Collapsed core tietoverkkoarkkitehtuuri

Two-Tier Collapsed core'ssa jakelu- ja runkokerroksen toiminnallisuudet ovat yhdistetty samaan laitteeseen. Käyttämällä mallia pienemmässä verkossa saadaan kustannussäästöjä, koska erillistä runkokerrosta ei välttämättä tarvita. Ja mallilla saavutetaan useimmat kolmikerroksisen mallin hyödyistä. (Valtteri Aalto 2019, 16.)

5.4.10 Tietoverkon segmentointi ja mikrosegmentointi

Tietoverkon segmentointi tarkoittaa tietoverkon jakamista pienempiin osiin. OSI-mallissa tietoverkkoa jako voidaan toteuttaa:

- virtuaalilähiverkkojen avulla siirtokerros-tasolla, jossa verkkosegmenttiä kutsutaan broadcast domainiksi ja
- aliverkotuksen avulla verkkokerros-tasolla, jossa verkkosegmenttiä kutsutaan aliverkoksi (kuluu IP -verkkoon). (Valtteri Aalto 2019, 16.)

Tietoverkon jaolla tavoitellaan verkon parempaa suorituskykyä ja tietoturvaa. Verkon broadcast liikennettä saadaan vähennettyä, kun tietoverkko jaetaan useampaan loogiseen broadcast domain'iin, mikä parantaa verkon suorituskykyä. Ja kun eri palvelut ovat omissa verkoissaan, myös tietoturva paranee. (Valtteri Aalto 2019, 16.)

Mikrosegmentointi on verkon virtualisointiin perustuva tekniikka. Tekniikassa virtuaalikone-tasolla jaetaan verkko omiin osioihin ja turvallisuusvyöhykkeisiin. Tietoturvasäännöstö voidaan määritellä virtuaalikone kohtaisesti, esimerkkinä VMware koneet. Mikrosegmentointi on vaihtoehto perinteiselle VLAN -segmentoinnille. Mikrosegmentoinnin VXLAN: eja voi olla jopa 16 miljoonaa, kun taas virtuaalilähiverkkosegmentoinnissa on rajoitteena virtuaalilähiverkkojen määrä, joka on maksimissaan 4096. Mikrosegmentoinnin liikennettä voidaan rajoittaa virtuaalikone-tasolla perinteisen aliverkkotason sijaan, mikä antaa paremman tietoturvan. (Valtteri Aalto 2019, 16.)

5.5 Tietoverkkojen laitteiden ja päätelaitteiden suunnittelu

OSI-mallin siirtoyhteyskerros- ja verkkokerros-tasoilla kytkimillä kytketään laitteita lähiverkkoon ja määritellään virtuaalilähiverkot. Reitittimiä tai palomuureja käytetään aliverkottamiseen ja reitittämään aliverkkojen välisen liikenteen. (Valtteri Aalto 2019, 16.)

Tässä osiossa esitellään pääpiirteittäin oleellisimmat verkoissa käytettävät verkkolaitteet (palvelin, palomuuri, reititin, kytkin, modeemi, kaapelit, valokuidut), niiden tehtävät, ja miten näitä verkkolaitteita käytetään osiossa 5.3.6 esitellyn OSI -mallin tasoissa. (Andrew L. Russell 2013.)

Palvelin on OSI -mallin seitsemännessä kerroksessa (sovelluskerros) toimiva tietokone, ohjelmisto tai näiden yhdistelmä. Palvelimen tehtävä on hoitaa tiettyjä tehtäviä, jotka tulevat palvelupyyntöinä muilta samaan verkkoon kytketyiltä tietokoneilta. Palomuuri on OSI -mallin neljännessä kerroksessa (kuljetuskerros) oleva tekninen järjestely. Palomuurin tehtävä on estää asiaton pääsy verkosta toiseen. Reititin on OSI -mallin kolmannessa kerroksessa (verkkokerros) sijaitseva verkkolaite, joka yhdistää tietoverkkoja toisiinsa, joko langattomasti (WiFi) tai kaapeleilla (esimerkiksi Ethernet). Reitittimen tehtävä on välittää datapaketteja. Reitittimen avulla voi luoda LAN -verkon. Reititin voi olla pelkkä reititin tai yhdistelmälaite, joissa on sekä reititin että modeemi samassa laitteessa. (Andrew L. Russell 2013.)

Modeemi on OSI -mallin kolmannessa kerroksessa (verkkkokerros) sijaitseva laite, joka ottaa vastaan liikenteen ja ohjaa sen oikeille laitteille langattomasti (WiFi). Modeemin tehtävä on muuntaa Internet -palveluntarjoajalta tuleva analoginen signaalin digitaaliseen muotoon ja päinvastoin. Modeemi voi olla kaapelimodeemi, joka käyttää kaapeli -TV verkkoa tai ADSL -modeemi, joka käyttää puhelinlinjaa. Kytkin on OSI -mallin toisessa kerroksessa (siirtokerros) sijaitseva laite, joka yhdistää eri päätelaitteet lähiverkossa. Kytkimen toimii verkossa ohjaajana mahdollistaen laitteiden välisen tiedon jakamisen ja kommunikoinnin. Kytkimet jaetaan ohjelmoitavaiin ja ei ohjelmoitaviin perustyyppeihin. Verkossa voi käyttää myös kolmannen kerroksen kytkintä eli L3-kytkintä, joka toimii reitittimen tavoin ilman WAN yhteyttä käyttäen IP -osoitteita. (Andrew L. Russell 2013.)

Kaapelit ja valokuidut ovat OSI -mallin ensimmäisessä kerroksessa verkon osa, jonka avulla eri päätelaitteet esimerkiksi tietokoneet liitetään verkkoon. Lähiverkoissa kaapelointi toteutetaan kierretyllä parikaapelilla tai optisilla kuitukaapeleilla eli valokaapeleilla. Kierrettyä parikaapelia kutsutaan Ethernet

kaapeliksi, josta löytyy suojaamaton UTP (Unprotected Twisted Pair) ja suojattu STP (Shielded Twisted Pair) versio. Myös optisista kuitukaapeleista löytyy kahta eri päätyyppiä eli monimuotokuitu MMF (Multi-Mode Fiber) ja yksimuotokuitu SMF (Single Mode Fiber). Kategoriasta riippuen monimuotokuidun siirtoetäisyys on 2 kilometriä ja yksimuotokuidut jopa 40 kilometriä. Pitkien yhteyksien rakentamisessa käyttää optisia vahvistimia. (Andrew L. Russell 2013.)

5.6 Tietoverkkoon liitettävien laitteiden turvallisuus ja hyväksyntämenettely

Julkisen hallinnon turvallisuusverkon (TUVE -verkko) käytöllä turvataan valtion ylimmän johdon ja turvallisuusviranomaisten yhteistyö ja kommunikointi kaikissa tilanteissa. TUVE -toiminta on lailla säädetty (FINLEX 2015a.). TUVE -verkko on viranomaisverkko, johon kuuluu viestintäverkko, laitetilat, laitteet sekä tieto- ja viestintätekniset palvelut. Valtio omistaa verkon ja hallinnoi sitä. Verkon palveluita tuotetaan, valvotaan ja hallitaan kellon ympäri. (VM. 2025b.)

5.7 Tietoverkkojen ylläpidon suunnittelu

Järjestelmien ja siihen kuuluvien verkkojen ylläpito alkaa, kun tietojärjestelmä ja -verkko projektit on saatu vietyä loppuun ja tietojärjestelmät ja -verkot ovat tuotannossa. Ylläpitovaiheen alussa järjestelmään tehdyistä muutoksista ja laajennuksista laaditaan dokumentit, johon kuuluvat muun muassa käyttäjä- ja käyttöoikeusasetukset, aktiivilaitteiden konfiguraatiomuutokset, ristiinkytkentätaulukot, verkon yhteyskaaviot, liikenne- ja kuormitusanalyysejä, lokitiedostojen kerääminen.
Ciscon kehittämää elinkaariajattelumallia on mahdollista ottaa käyttöön ylläpitovaiheen tehtäviin. Elinkaarimallin vaiheet ovat esitutkimus, määrittely, suunnittelu, toteutus, käyttöönotto ja optimointi. (Kari Ainonen. 2013b, 25-29.)

6 VERKKOJEN SUUNNITTELUN TULEVAISUUDEN TRENDIT, HAASTEET JA UHAT

Tulevaisuuden trendeinä ja kehityssuuntina ovat nousset pinnalle kyberturvallisuuteen liittyvät asiat, tehokkaampien tietoverkkoyhteyksien myötä laajempi kansainvälinen yhteistyö yhteiskunnan eri sektoreilla ja tekoälyn ”vallankumous” tietotekniikassa. Tässä osiossa käydään muutamin esimerkein läpi näitä kehityssuuntia.

6.1 Tietoverkkojen tulevaisuuden kehityssuunnat

NIS2 -direktiivin vaikutukset:

NIS2 -direktiivi on Euroopan Unionin päivitetty säädös, joka keskittyy kyberturvallisuuden parantamiseen kriittisen infrastruktuurin alueilla. NIS2 -direktiivin tavoitteena on turvallisuuskäytäntöjen harmonisointi tietoverkkojen ja tietojärjestelmien koko Euroopassa. Tämä tavoite on erityisen tärkeää tietoverkkojen asiantuntijoille ja IT -alan ammattilaisille. NIS2 -direktiivin vaikutukset tietoverkkojen hallintaan ja kyberturvalliuuskäytäntöihin ulottuvat pitkälle tulevaisuuden. Direktiivin asettamat vaatimukset kannustavat organisaatioita päivittämään ja kehittämään turvallisuuskäytäntöjään parantaen yleistä kybeturvallisuustasoa Euroopassa, minkä seurauksena voimme odottaa entistä turvallisempaa ja resilientimpää digitaalista infrastruktuuria. (Mintly 2025.)

Miten kaikki organisaatiot, erityisesti pienemmät ja keskisuuret yritykset, pystyvät noudattamaan direktiivin vaatimuksia, on kuitenkin varmistamisen näkökulmasta haaste. Tämä vaatii jatkuvaa kehitystä ja investointeja tietoturvaan. Kehityssuunnat näyttävätkin suuntautuvan kohti yhä tiiviimpää yhteistyötä julkisen ja yksityisen sektorin välillä, sekä uusien teknologioiden ja innovaatioiden hyödyntämistä kyberturvallisuuden parantamiseksi. (Mintly 2025.)

Bublic Sector Network -sosiaalinen oppimisalusta:

Kansainvälisistä trendeistä voidaan mainita Bublic Sector Network, joka on kehitetty kansalaiskeskeiseen muutokseen julkisella sektorilla. Bublic Sector Network on sosiaalinen oppimisalusta, joka auttaa hallituksia ympäri maailman hajottamaan siilot, tekemään yhteistyötä ja työskentelemään yhdessä kansalaisten kannalta parempien tulosten saavuttamiseksi. (Public Sector Network. 2025.)

Public Sector Network kokoaa yhteen oivalluksia ja innovaatioita eri puolilta maailmaa, mahdollistaa yhteen kokoontumisen, yhteistyön, yhteyksien luomisen ja kansalaiskeskeisen muutoksen julkisella sektorilla. Public Sector Network oppimisalustaan liittyen järjestetään tapahtumia, jotka ovat kaikille avoimia, esimerkiksi Hallituksen innovaatioviikko 2025 (Goverment innovation Week 2025 – Global Series). (Public Sector Network. 2025.)

Tekoälyn hyödyntäminen:

Tekoälyä voidaan hyödyntää fyysisen kuituverkon suunnittelussa. Tekoälyn voi laittaa analysoimaa uuden valokuitukaapelin asennusmahdollisuuksia jo käytössä olevaan vanhaan kaapelointia sisältävään putkeen. Tekoäly vertailee olemassa olevien kaapeleiden paksuuksia putken tilavuuteen ja analysoinnin kautta auttaa arvioimaan voiko uuden valokuitukaapeli asentaa jo käytössä olevaan putkeen vai onko asennettava uusi putki. (Igor Sokolov 2024, 15-18.)

Tekoälyn käyttö kuituverkkojen suunnittelussa on investointi tulevaisuuden infrastruktuurien ja yhteisöjen kehittämiseen. Nopea ja luotettava tiedonsiirtoyhteys on tärkeä osa tulevaisuuden tietoyhteiskuntaa ja elämäntapaa, joka mahdollistaa etätyön, sähköiset oppimisalustat ja digitaalisen viihde tarjonnan. Käyttämällä tekoälyä verkkojen suunnittelussa varmistetaan, että nämä digitaaliset palvelut ovat saatavilla nopeasti, tehokkaasti, luotettavasti ja skaalautuvasti. (Igor Sokolov 2024, 15-18.)

6.2 Tietoturvallisuuden, varautumisen ja toimintaympäristön muutosten haasteet

Merkittävät tietoturvallisuuden haasteet liittyvät tietoverkon puutteelliseen toteutukseen, ja tietosuoja ja tietoturvatoimenpiteiden laiminlyönteihin. Alla olevissa esimerkeissä käydään läpi tietomurron kohteeksi joutunut yhdysvaltalainen vähittäiskappaketju Target, Psykoterapiakeskus Vastaamo ja lainsäädäntöjohdannaisena riskinä Julkri.

Viime vuosien julkisuuteen tulleissa tietomurroissa yksi yhdistävä tekijä on ollut se, että tietomurron kohteeksi joutuneiden organisaation sisäverkko on monesti ollut puutteellisesti segmentoitu, mikä on mahdollistanut vapaan liikkumisen verkossa. Yhdysvaltalainen vähittäistavarakauppa Target joutui tietomurron kohteeksi vuonna 2013. Hakkerit varastivat tietoja noin 40 miljoonalta Target kaupassa käyneiden asiakkaiden luotto- ja pankkikorttitietoja, ja 70 miljoonan käyttäjän henkilötietoja. Tietomurron aiheutti hakkereiden pääsy kaupan tietoverkkoon varastetuilla kirjautumistiedoilla. Sisälle päästyään

hyökkääjät asensivat ”BlackPOS” -nimisen haittaohjelman Target’in kassajärjestelmään tallentaakseen salaamattomia luotto- ja pankkikorttitietoja aina, kun asiakkaat lukivat korttejaan kaupan kassalla. (StrongDM-tiimi. 2025.)

Toinen merkittävä tekijä on monissa esiin tulleissa tapauksissa ollut tietosuojan, tietoturvallisuuden ja henkilötietojen käsittelyn turvallisuuden laiminlyönti. Viime aikoina paljon julkisuutta saaneen Vastaamon potilastietojärjestelmään kohdistuneen tietomurron tapauksessa yhtiön järjestelmän salasanoja jaeltiin suojaamattomissa sähköpostiviesteissä, ja salasanat itsessään olivat liian yksinkertaisia. Lisäksi Skype-keskustelussa oli jaettu selkokielinen käyttäjätunnus ja salasana Vastaamon työasemille. Todennäköinen syy tietokanta vuodolle on ollut suojaamaton MySQL -portti, josta tietokanta on ladattu joskus marraskuun 2017 ja maaliskuun 2019 välisenä aikana (MTV 2021). Tietomurto tapahtui kaksi kertaa ja toista tietomurroista ei edes huomattu. Yhtiön järjestelmiin syntynyt tietoturva-aukko aiheutti sen, että 30 000 asiakkaan arkaluonteisia tietoja varastettiin 2017 syksyllä. (Jesse Mäntysalo 2023.)

Myös lainsäädäntöön saattaa liittyä riskejä. Esimerkiksi Julkri’n käytössä organisaation tulee tunnistaa lainsäädäntöjohdannaiset riskit. Tällä tarkoitetaan eri maiden lainsäädännössä olevia mahdollisuuksia, joilla velvoitetaan palveluntarjoaja toimimaan yhteistyössä kyseessä olevan maan viranomaisten kanssa. Ja yhteistyöhön liittyen tarjoamaan esimerkiksi suora tai epäsuora pääsy asiakkaiden salassa pidettäviin tietoihin palvelussa tai järjestelmässä, mikä voi aiheuttaa tietosuojariskin ja -poikkeaman. (VM 2023.)

Toimintaympäristön yleisiä kansallisia haasteita ovat turvallisuus ympäristön muutokset, hyvinvointialueiden muutokset, yhteistoiminta-alueet, organisaation omat tarpeet, eri toimijoiden yhteiset tarpeet, kuntien ja kaupunkien tarpeet.

7 JOHTOPÄÄTÖKSET

Aloitin opinnäytetyön tutustumalla saatavilla oleviin kansainvälisiin julkisen sektorin tietoverkkojen toteutuksiin ja kehitys suuntiin, ja suunnittelua sääteleviin kansainvälisiin ja kansallisiin lakeihin, asetuksiin ja ohjeisiin tavoitteena yleisen tietoverkkojen suunnittelun ohjeistuksen laatiminen kansallisen julkisen ja yritysten tietoverkkojen suunnitteluun.

Käytännöt verkkojen suunnittelussa ja ylläpidossa vaikuttivat eroavan maan ja toimijan sektorin mukaan. Yhtenäisten ohjeiden ja toteutuksen puuttuminen on johtanut esimerkiksi Englannissa siihen, että jokaisella julkisen sektorin toimijalla oli oma paikallinen ratkaisu verkkojen ja palvelujen toteuttamiseksi käyttäen eri teknologioita. Tietoverkkojen teknologioiden esimerkiksi pilvipalveluiden ja tekoälyn kehittymisen myötä vanhalla tekniikalla toteutettu tietoverkko ei enää taipunutkaan uusiin vaateisiin verkon skaalautuvuudesta, suorituskyvystä, kyberturvallisuuden vaateista asiakkaiden tarpeisiin. Myöskin Suomessa tietoverkkojen suunnittelun ja toteutuksen käytännöt vaihtelevat julkisella sektorilla, kaupungeissa, kunnissa ja myös yrityksissä.

Opinnäytetyötä tehdessäni opin lakien, asetusten ja viranomaisohjeiden roolin ja merkityksen tietoverkkojen suunnittelua, toteutusta, hallintaa ja ylläpitoa määräävänä ja ohjaavana tekijänä yhdessä tietoverkkojen suunnittelun teknisten ohjeiden rinnalla. Julkisella sektorilla on yhteisten tietoverkkojen suunnittelua ja toteutusta ohjaavien ohjeiden tarve ohjaamaan tietoverkkojen kehitystä harmonisoidumpaan lopputulokseen, mikä parantaa tietoverkkojen tietoturvallisuutta, ja varautumista tulevaisuuden tietoverkkojen kehityshaasteisiin vastaamiseen.

Opinnäytetyönä toteutui ohjeistus (LIITE 3), joka pohjautuu työlle asetettuihin tavoitteisiin eli luoda ohjeistus, joka selkeyttää tietoverkkojen taustalla olevaa lainsäädäntöä ja tarjoaa pelkistetyn selkeän perusohjeen tietoverkkojen tekniseen suunniteluun ja ylläpitoon kokoamalla samaan ohjeeseen keskeisemmät lainsäädännön vaateet ja tekniset ohjeet verkkojen suunnitteluun ja toteuttamiseen huomioiden tietoturvallisuuden ja varautumisen kasvavat haasteet.

LÄHTEET

Agency for Digital Government. 2017. *White Paper on a Common Public-Sector Digital Architecture.* Saatavissa: White Paper on a Common Public-Sector Digital Architecture. Viitattu: 18.4.2025.

Andrew L. Russell. 2013. *OSI: The Internet That Wasn't.* Saatavissa: https://spectrum.ieee.org/tech-history/cyberspace/osi-the-internet-that-wasnt. Viitattu 17.6.2018.

BDBOSa. 2025. *Networks of the federal government.* Saatavissa: https://www.bdbos.bund.de/EN/Our-tasks/Networksofthefederalgovernment/networksofthefederalgovernment_node.html. Viitattu: 18.4.2025.

BDBOSb. 2025. *Public administration information network – IVÖV.* Saatavissa: https://www.bdbos.bund.de/EN/Ourtasks/Publicadministrationinformationnetwork/ivoev_node.html. Viitattu: 18.4.2025.

BDBOSc. 2025. *Public Safety Digital Radio.* Saatavissa: https://www.bdbos.bund.de/EN/Our-tasks/PublicSafetyDigitalRadio/public_safety_digital_radio_node.html. Viitattu: 18.4.2025.

Beata Barczak. 2023, 39. *Public Network Models: A Typology Based on a Systematic Literature Review. Zesz. Nauk. UEK.* 3(1001), 27–45. Saatavissa: http://dx.doi.org/10.15678/ZNUEK.2023.1001.0302. Viitattu 30.4.2025.

Bryce Leo. 2024. *Verkkotopologian tyypit: väylä, rengas, tähti, verkko, puukaavio.* Saatavissa: https://www.guru99.com/fi/type-of-network-topology.html. Viitattu 30.12.2024.

Cisco. 2025. *What is LAN?* Saatavissa: https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html?dtid=osscdc000283&linkclickid=srch. Viitattu 2.5.2025.

education-wiki. 2025. *Tietokoneverkkojen tyypit Esimerkki tietokoneverkosta.* Saatavissa: https://education-wiki.com/1154609-types-of-computer-network. Viitattu 23.5.2025.

EU. 2025. *Digital connectivity in Germany.* Saatavissa: https://digital-strategy.ec.europa.eu/en/policies/digital-connectivity-germany. Viitattu 2.5.2025.

NIS 2 -direktiivi 2022/2555. Saatavissa: https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=fi.

KOMISSION TÄYTÄNTÖÖNPANOASETUS (EU) 2024/2690. Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32024R2690&qid=1741615462589#fnp_1.

European Commission. 2025. *Summary of digital connectivity development in Germany*. Saatavissa: https://digital-strategy.ec.europa.eu/fi/policies/digital-connectivity-germany. Viitattu 18.4.2025.

Laki viranomaisen toiminnan julkisuudesta 621/1999. Saatavissa: https://finlex.fi/fi/lainsaadanto/1999/621?language=fin&highlightId=626022&highlightParams=%7B%22type%22%3A%22BASIC%22%2C%22search%22%3A%22Laki+viranomaisen+toiminnan+julkisuudesta%22%7D.

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 1101/2019. Saatavissa: https://www.finlex.fi/fi/lainsaadanto/2019/1101.

Laki julkisen hallinnon turvallisuusverkkotoiminnasta 10/2015. Saatavissa: https://finlex.fi/fi/lainsaadanto/2015/10.

Laki julkisen hallinnon tiedonhallinnasta 906/2019. Saatavissa: https://finlex.fi/fi/lainsaadanto/saadoskokoelma/2019/906.

Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta 1109/2015. Saatavissa: https://finlex.fi/fi/lainsaadanto/saadoskokoelma/2015/1109#OT0.

Global YO. 2023. *Verkkotopologian selitys: tyypit, rakenteet ja oikea valitseminen.* Saatavissa: https://www.globalyo.com/fi/blog/exploring-the-different-types-of-network-topology-a-comprehensive-guide/. Viitattu 30.4.2025.

GOV.UKa. Public Services Network (PSN). Saatavissa: https://www.gov.uk/government/groups/public-services-network#contents Viitattu 18.4.2025.

GOV.UKb. 2022. *Future Networks for Government (FN4G).* Saatavissa: https://www.gov.uk/guidance/future-networks-for-government-fn4g Viitattu 21.4.2025.

GOV.UKc. 2015. *Guidance Network principles.* Luettavissa: https://www.gov.uk/government/publications/network-principles/network-principles Viitattu 21.4.2025.

GOV.UKd. 2025. *Research and analysis State of digital government review.* Saatavissa: https://www.gov.uk/government/publications/state-of-digital-government-review/state-of-digital-government-review#conclusion . Viitattu 21.4.2025.

Huoltovarmuusorganisaatio. 2024. *ICT-Palvelutuotannon varautuminen.* Saatavissa: ICT-Palvelutuotannon varautuminen – suositukset huoltovarmuusorganisaation yrityksille. Viitattu 2.5.2025.

Sokolov I. 2024. *Tekoälyn hyödyntäminen tietoverkon suunnittelussa.* Kouvola: Kaakkois-Suoman ammattikorkeakoulu. Opinnäytetyö. Saatavissa: https://www.theseus.fi/bitstream/handle/10024/819841/Sokolov_Igor.pdf?sequence=2. Viitattu 1.5.2025.

IT PLANET. *Globaali alueverkko (GAN) – Määritelmä.* Saatavissa: https://blog.it-planet.com/en/glossar/global-area-network/. Viitattu 30.4.2025.

Leiviskä J. 2021. *Tietoverkon anatomia.* Satakunta: Satakunnan ammattikorkeakoulu. Opinnäytetyö. Saatavissa: https://www.theseus.fi/bitstream/handle/10024/495330/Leiviska_Jarkko.pdf?sequence=2. Viitattu 1.5.2025.

Jodi Haasz. 2020. *IEEE SA - IEEE 802.1X-2020.* Saatavissa: https://standards.ieee.org/ieee/802.1X/7345/ IEEE SA - IEEE 802.1X-2020. Viitattu 28.2.2020.

Ainonen. K. 2013. *Lähiverkon suunnittelu yrityksille.* Tampere: Tampereen ammattikorkeakoulu. Opinnäytetyö. Saatavissa: https://www.theseus.fi/bitstream/handle/10024/59186/Ainonen_Kari.pdf;jsessionid=DC9C75B94E2A2A236FAFF96C524B3806?sequence=1.

Ainonen K. 2013b, 25-29. *Lähiverkon suunnittelu yrityksille.* Tampere: Tampereen ammattikorkeakoulu. Opinnäytetyö. Saatavissa: https://www.theseus.fi/bitstream/handle/10024/59186/Ainonen_Kari.pdf;jsessionid=DC9C75B94E2A2A236FAFF96C524B3806?sequence=1.

Mintly. 2025. *Ketkä ovat NIS2 -direktiivin piiriin kuuluvat?* Saatavissa: https://mintly.fi/uutiset/ketka-ovat-nis2-direktiivin-piiriin-kuuluvat/. Viitattu 2.5.2025.
MTV. 2021.Oikeuden paperit paljastavat: Näin Vastaamon tietomurto tapahtui – salainen kauppasumma paljatui. Saatavissa: https://www.mtvuutiset.fi/artikkeli/oikeuden-paperit-paljastavat-nain-vastaamon-tietomurto-tapahtui-salainen-kauppasumma-paljastui/8055050. Viitattu 2.5.2025.

Public Sector Network. 2025. *Learn from anywhere with Public Sector Network.* Saatavissa: Public Sector Network - Online network for public sector professionals. Viitattu 2.5.2025.

SFS. 2018. *SFS-EN 50173-1:2018.* Saatavissa: https://sales.sfs.fi/fi/index/tuotteet/SFSsahko/CENELEC/ID2/5/700958.html.stx. Viitattu 2.5.2025.

SSC. 2022. *The Government of Canada Enterprise Network — the Foundation of Digital Government.* Saatavissa: Network Modernization - Canada.ca. Viitattu: 18.4.2025.

STM. 2021. *Korkean varautumisen viestintä ja tietojärjestelmät, Hallinnan ja käytön toimintamalliohje.* Saatavissa: https://stm.fi/documents/1271139/1334666/Korkean%20varautumisen%20viestint%C3%A4-ja%20tietoj%C3%A4rjestelmien%20hallinnan%20ja%20k%C3%A4yt%C3%B6n%20toimintamalli%20ohje.pdf . Viitattu 24.4.2025.

StrongDM-tiimi. 2025. *Kohdetietomurto: Mitä tapahtui ja miten se estetään.* Saatavissa. https://www.strongdm.com/what-is/target-data-breach.Viitattu 2.5.2025.

Suomi.fi. 2024a. *Satelliittiverkko -määritelmä.* Saatavissa: https://sanastot.suomi.fi/terminology/teknisetverkot/concept/c35. Viitattu 30.4.2025.

Suomi.fi.2024b. *Häiriö- ja kriisitilanteisiin varautuminen.* Saatavissa: https://www.suomi.fi/oppaat/varautuminen. Viitattu 30.4.2025.

Tilastokeskus. 2019. *Hae käsitettä*. Saatavissa: https://stat.fi/meta/kas/julkinen_sektor.html
Viitattu: 18.4.2025.

Traficom. 2021. *Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista.* Saatavissa: Yhdyskäytäväratkaisuohje (v1_4 - Julkaisuversio- 2021-12-02). Viitattu 1.5.2025.

Traficom. 2025a. *Liikenne- ja viestintävirasto Traficomin suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä.* Saatavissa: Suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä.pdf. Viitattu 28.4.2025.

Traficom. 2025b. *Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut.* Saatavissa: Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut | Kyberturvallisuuskeskus. Viitattu 29.4.2025.

UM. 2020. *Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille.* Saatavissa: https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246. Viitattu 27.4.2025.

Aalto V. 2019, 16. *Suunnitelma yrityksen tietoverkon segmentointiin.* Helsinki: Haaga-Helia ammattikorkeakoulu. Opinnäytetyö. Saatavissa: https://www.theseus.fi/bitstream/handle/10024/172208/Opinn%C3%A4ytety%C3%B6%20-%20Valtteri%20Aalto.pdf?sequence=2.

Leppäniemi V. 2016. *Yrityksen tietoverkot ja tietoverkkojen hallinta.* Saatavissa: https://www.theseus.fi/bitstream/handle/10024/114818/Opinnaytetyo_final_Theseus_version.pdf?sequence=1.

VM. 2023. *Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri): Suositus ja kriteeristö.* Saatavissa: http://urn.fi/URN:ISBN:978-952-367-458-5. Viitattu 26.4.2025.

VM. 2025a. *Julkisen hallinnon ICT.* Saatavissa: https://vm.fi/en/public-sector-ict. Viitattu 24.4.2025.

VM. 2025b. *Julkisen hallinnon turvallisuusverkkotoiminta (TUVE -toiminta).* Saatavissa: https://vm.fi/turvallisuusverkkotoiminta. Viitattu 2.5.2025.

Word Wide Technology. 2021. *What Is a Data Network? Understanding the Types and Benefits of Data Networks.* Saatavissa: What Is a Data Network? Understanding the Types and Benefits of Data Networks - WWT. Viitattu 30.4.2025.

SA

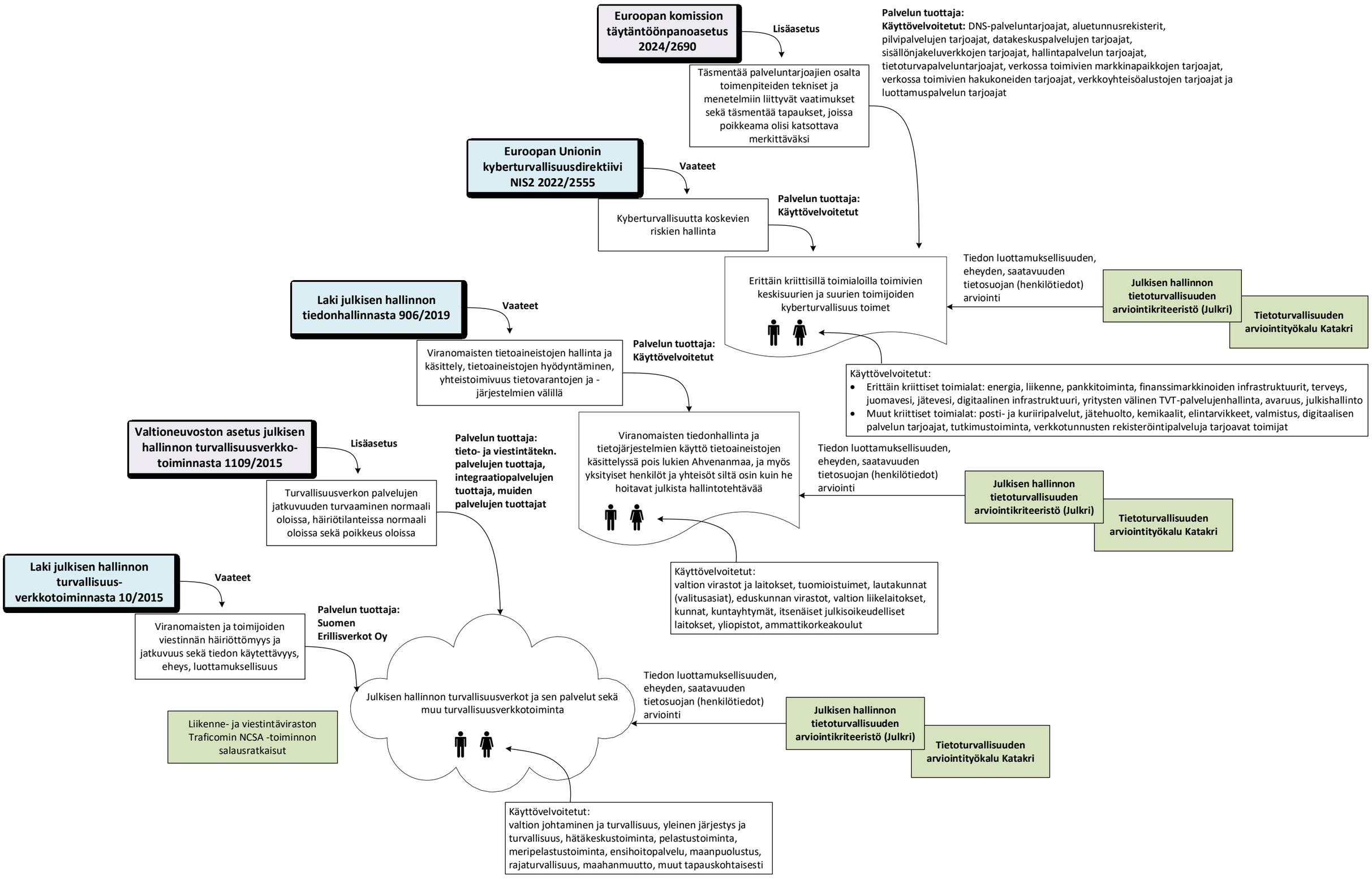
Jesse Mäntysalo. 2023. *Vastaamossa käytettiin yksinkertaisia salasanoja, kunnes tapahtui tuhoisa tietomurto -tuomio tietosuojarikoshaarassa annettiin tänään.* Saatavissa: https://yle.fi/a/74-20027486?utm_source=social-media-share&utm_medium=social&utm_campaign=ylefiapp. Viitattu 2.5.2025.

Liite 1

	Laki julkisen hallinnon turvallisuus-verkkotoiminnasta 10/2015	Laki julkisen hallinnon tiedonhallinnasta 906/2019	Valtioneuvoston asetus julkisen hallinnon turvallisuusverkko-toiminnasta 1109/2015	Euroopan Unionin (EU) kyberturvallisuusdirektiivi NIS2 2022/2555	Euroopan komission täytäntöönpanoasetus 2024/2690
Tarkoitus	Lain tarkoitus on kaikissa tilanteissa varmistaa viranomaisten ja toimijoiden viestinnän häiriöttömyys ja jatkuvuus sekä tiedon käytettävyys, eheys, luottamuksellisuus	Lain tarkoitus on varmistaa viranomaisten tietoaineistojen hallinta ja käsittely, mahdollistaa tietoaineistojen hyödyntäminen, edistää yhteistoimivuutta tietovarantojen ja -järjestelmien välillä	Asetus on säädetty turvallisuusverkon palvelujen jatkuvuuden turvaamiseksi normaali oloissa, häiriötilanteissa normaali oloissa sekä poikkeus oloissa	Direktiivillä vahvistetaan yhteinen kyberturvallisuuden sääntelykehys parantamaan kyberturvallisuuden tasoa Euroopan unionissa (EU). Sen tarkoituksena on vaatia EU:n jäsenvaltioita vahvistamaan kyberturvallisuusvalmiuksia ja ottamaan käyttöön kyberturvallisuusriskien hallintatoimenpiteitä ja raportointia kriittisillä toimialoilla sekä yhteistyötä, tietojen vaihtamista, valvontaa ja täytäntöönpanoa koskevia sääntöjä	Asetuksen tarkoituksena on täsmentää direktiivin 3 artiklan soveltamisalaan kuuluvien palveluntarjoajien osalta direktiivin 21 artiklan 2 kohdassa tarkoitettujen toimenpiteiden tekniset ja menetelmiin liittyvät vaatimukset sekä täsmentää tapaukset, joissa poikkeama olisi katsottava merkittäväksi direktiivin 23 artiklan 3 kohdan mukaisesti
Soveltaminen	Lakia sovelletaan julkisen hallinnon turvallisuusverkkotoimintaan ja sen palvelujen käyttöön sekä muuhun turvallisuusverkkotoimintaan	Lakia sovelletaan viranomaisten tiedonhallintaan ja tietojärjestelmien käyttöön tietoaineistojen käsittelyssä pois lukien Ahvenanmaa, ja myös yksityisiin henkilöihin, yhteisöihin ja yhteisöihin siltä osin kuin he hoitavat julkista hallintotehtävää		Sääntelyä sovelletaan erittäin kriittisillä toimialoilla toimiviin pääasiassa keskisuurien ja suurien toimijoiden kyberturvallisuus toimiin	
Käyttövelvoite	Viranomaisten sisäinen, välinen ja ulkoinen yhteistoiminta ja viestintä, joissa noudatetaan korkean varautumisen tai turvallisuuden vaatimuksia	Viranomaisen toimintaympäristön tiedonhallintaa määrittelevän ja kuvaavan tiedonhallintamallin ylläpito, ja valtiovarainministeriö; tiedonhallintakartan ylläpito, huomioiden tietoturvallisuus, tietoaineistojen muodostaminen ja sähköinen luovutustapa, asianhallinta ja palvelujen tiedonhallinta		Kyberturvallisuuden riskienhallinnan toimintamallin ylläpito ja riskienhallinnan toimenpiteet, merkittävien poikkeamien ilmoittaminen	
Käyttövelvoitetut	Valtion johtaminen ja turvallisuus, yleinen järjestys ja turvallisuus, hätäkeskustoiminta, pelastustoiminta, meripelastustoiminta, ensihoitopalvelu, maanpuolustus, rajaturvallisuus ja maahanmuutto, muut tapauskohtaisesti	Valtion virastot ja laitokset, tuomioistuimet, lautakunnat (valitusasiat), eduskunnan virastot, valtion liikelaitokset, kunnat, kuntayhtymät, itsenäiset julkisoikeudelliset laitokset, yliopistot, ammattikorkeakoulut		<u>Erittäin kriittiset toimialat:</u> energia, liikenne, pankkitoiminta, finanssimarkkinoiden infrastruktuurit, terveys, juomavesi, jätevesi, digitaalinen infrastruktuuri, yritysten välinen TVT-palvelujenhallinta, avaruus, julkishallinto <u>Muut kriittiset toimialat:</u> posti- ja kuriiripalvelut, jätehuolto, kemikaalit, elintarvikkeet, valmistus, digitaalisen palvelun tarjoajat, tutkimustoiminta, verkkotunnusten rekisteröintipalveluja tarjoavat toimijat	DNS-palveluntarjoajat, aluetunnusrekisterit, pilvipalvelujen tarjoajat, datakeskuspalvelujen tarjoajat, sisällönjakeluverkkojen tarjoajat, hallintapalvelun tarjoajat, tietoturvapalveluntarjoajat, verkossa toimivien markkinapaikkojen tarjoajat, verkossa toimivien hakukoneiden tarjoajat, verkkoyhteisöalustojen tarjoajat ja luottamuspalvelun tarjoajat
Palvelun tuottaja	Suomen Erillisverrkot Oy ja sen tytäryhtiö	Käyttövelvoitetut	1) tieto- ja viestintäteknisten palvelujen tuottaja, 2) integraatiopalvelujen tuottaja ja 3) muiden palvelujen tuottajat	Käyttövelvoitetut	Käyttövelvoitetut
Palvelun tuottajan tehtävät	Turvallisuusverkon verkkopalveluiden ja muiden yhteisten infrastruktuuripalvelujen tuottaminen, ylläpitäminen ja kehittäminen, laitetilojen ja laitteiden hallinnointi sekä verkon turvallisuus-, valmius-, varautumis- ja jatkuvuusvaatimusten toteutumisesta vastaaminen	Toimintaprosessien, tietovarantojen, -aineistojen ja -järjestelmien ylläpito tiedonhallintamallissa, ja arviointi hallinnollisissa uudistuksissa ja muutoksissa niiden vaikutuksista tiedonhallintamalliin. Tietosuojaa koskeva vaikutusten arviointi säädetään erikseen	1) verkkopalvelut (runkoverkko- ja liityntäpalvelu runkoverkkoon), infrastruktuuripalvelut (laitetilat, laite- ja antennipaikat), yhteiset tieto- ja viestintätekniset palvelut (käyttäjätuki- , päätelaite- , viestintä- , tietoliikenne- , tietoturva- , konesali- , kapasiteetti- , integraatio- ja sanomanvälityspalvelut, sekä em. liittyen yhteiset tietojärjestelmä- ja omaisuuden-hallintapalvelut 2) palvelukokonaisuuksien muodostaminen ja niiden sopimusten asiakkuushallinta, palvelujen yhdistäminen käyttäjien viestintäteknisiin palveluihin, koordinoida muutoksen- ja häiriötilannehallintaa, tietoturvauhkilta suojautumista, koota verkon tilannetietoa 3) asennus- , projekti- ja asiantuntijapalvelut	Toimialan valvovan viranomaisen ylläpitämään toimijaluetteloon ilmoittautuminen ja toimijaluetteloon tulleista muutoksista ilmoittaminen. Toimijalla on oltava käytössä ajantasainen kyberturvallisuuden riskienhallinnan toimintamalli ja toteutettava riskienhallinnan toimintamalliin perustuvia teknisiä, operatiivisia ja organisatorisia hallintatoimenpiteitä, ja ilmoitettava viipymättä merkittävistä poikkeamista valvovalle viranomaiselle. Kaikki yritykset ja toimijat voivat ilmoittaa niihin kohdistuneista tietoturvaloukkauksista Traficomin Kyberturvallisuuskeskuksen CSIRT -yksikölle.	
Strategia, linjaukset (yleinen), varautuminen, valmius, turvallisuus, ohjaus (yleinen), valvonta, arviointi	Valtiovarainministeriö	Valtiovarainministeriö, valtion virastot ja laitokset	Valtiovarainministeriö, turvallisuusverkkotoiminnan neuvottelukunta	Traficom / Verkkotunnukset, Traficom / Liikenne, Traficom / Julkishallinto ja tutkimus, Traficom / Digitaalinen infrastructuuri, digitaaliset palvelut ja TVT-palvelut, Traficom / Posti- ja kuriiripalvelut, Traficom / Avaruusd, Energiavirasto, Tukes, Valvira, Fimea, Etelä-Savon ELY-keskus, Ruokavirasto, Finanssivelvonta	Traficom / Verkkotunnukset, Traficom / Liikenne, Traficom / Julkishallinto ja tutkimus, Traficom / Digitaalinen infrastructuuri, digitaaliset palvelut ja TVT-palvelut, Traficom / Posti- ja kuriiripalvelut, Traficom / Avaruusd, Energiavirasto, Tukes, Valvira, Fimea, Etelä-Savon ELY-keskus, Ruokavirasto, Finanssivelvonta

Lakien ja asetusten vaikutus julkisten organisaatioiden tiedonhallintaan

Liite 2



Ohje julkisen sektorin tietoverkon suunnitteluun

Liite 3