

Matias Laiho

SUOMEN KUNTIEN KYBERTURVALLISUUS

Katsaus tapahtuneisiin kyberhyökkäyksiin

Kandidaatintyö
Johtamisen ja talouden tiedekunta
Tarkastaja: Maija Lampu
Huhtikuu 2025

TIIVISTELMÄ

Matias Laiho: Suomen kuntien kyberturvallisuus: Katsaus tapahtuneisiin kyberhyökkäyksiin
(Cybersecurity in Finnish Municipalities: A Review of Cyberattacks)

Kandidaatintyö

Tampereen yliopisto

Tietojohtamisen tutkinto-ohjelma

Huhtikuu 2025

Tässä työssä tarkastellaan Suomen kuntien kyberturvallisuutta ja sen haasteita. Työn tutkimuskysymys on ”Mitä haasteita Suomen kunnilla on kyberturvallisuudessa, ja miten kyberturvallisuutta tulisi kehittää?”. Työssä tarkastellaan myös Suomessa olevia julkisen sektorin kyberturvallisuuden kehittämisstrategioita ja mahdollisia ratkaisuja tunnistettuihin haasteisiin. Aihe on tutkimuksen arvoinen, koska Suomen kuntien kyberturvallisuudesta ei ole tehty tarpeeksi tutkimusta sen yhteiskunnalliseen merkitykseen nähden.

Työ on toteutettu kirjallisuuskatsauksena, joka kohdistuu tieteelliseen ja Suomen julkisen sektorin tietokannoissa olevaan aineistoon. Työssä aihetta tarkastellaan johtamisen ja hallinnollisen tason näkökulmasta, eikä työssä näin ollen oteta kantaa yksityiskohtaisiin teknisiin ratkaisuihin. Tämän lisäksi työssä hyödynnetään lehdissä ollutta tai organisaatioiden itsensä ilmoittamaa tietoa tapahtuneista kyberhyökkäyksistä.

Työssä havaitaan, millaisia erilaisia kyberhyökkäyksiä Suomen kuntia ja julkista sektoria kohtaan on kohdistunut. Työssä havaitaan Suomen kuntien kohdistuneita raportoituja kyberhyökkäyksiä yhteensä 14 kappaletta, joista yleisimpänä oli tietomurto, joita oli 6 tapausta, sekä 1 törkeä tietomurto. Suomen julkiseen sektoriin havaitaan kohdistuneen 10 tapausta, joista yleisimpiä olivat palvelunestohyökkäykset 6 tapauksella. Lisäksi työssä tunnistettiin ainakin 3 tapausta, jotka liittyivät vakoiluun. Suomen kuntien kyberturvallisuuden haasteiksi havaitaan resurssien puute, tiedon jakamisen puutteet, tiedon siiloutuminen toimialoittain, mittaamisen puutteet, selkeiden toimintamallien ja prosessien puutteet. Suomessa on laadittu useita kehittämisstrategioita kyberturvallisuuden suhteen ja niissä on tunnistettu erilaisia kehittämistapoja. Selkeästi kuntiin kohdistuvia kehittämisehdotuksia on julkisissa kehittämisstrategioita vain vähän.

Avainsanat: Kyberturvallisuus, kunta, kyberhyökkäys, julkinen sektori

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin Originality Check -ohjelmalla.

TEKOÄLYN KÄYTTÖ OPINNÄYTTEESSÄ

Opinnäytteessäni on käytetty tekoälysovelluksia:

- Ei
- Kyllä

Ilmoitukseni mukaan olen käyttänyt opinnäytteessäni tutkielmaprosessin aikana seuraavia tekoälysovelluksia:

Tekoälysovellusten nimet ja versiot:
OpenAI ChatGPT 4o.

Käyttötarkoitus:
ChatGPT 4o:ta on käytetty oikeinkirjoituksen ja lauserakenteiden tarkistamiseen.

Osiot, joissa tekoälyä on käytetty:
ChatGPT 4o:ta on käytetty kirjoitus- ja tarkistusvaiheessa. ChatGPT 4o:ta on käytetty kaikissa työn luvuissa 1–6 sekä lähdeluettelossa.

Olen tietoinen siitä, että olen täysin vastuussa koko opinnäytteeni sisällöstä, mukaan lukien osat, joissa on hyödynnetty tekoälyä, ja hyväksyn vastuun mahdollisista eettisten ohjeiden rikkomuksista.

ALKUSANAT

Haluan kiittää kandidaatintyön ohjaajaa tarkoista korjausehdotuksista. Haluan kiittää myös jokaista pienryhmäni jäsentä ja seminaarien opponentteja hyvistä huomioista ja tarkentavista kommentteista.

Tampereella, 30.4.2025

Matias Laiho

SISÄLLYSLUETTELO

| | |
|--|----|
| 1. JOHDANTO | 1 |
| 1.1 Tutkimuksen tausta ja merkitys | 1 |
| 1.2 Tutkimuskysymys ja rajaukset | 2 |
| 1.3 Tutkimuksen rakenne | 3 |
| 2. KYBERTURVALLISUUS JA KYBERUHAT | 4 |
| 2.1 Kyberturvallisuus | 4 |
| 2.2 Kyberuhat, uhkatoimijat ja haastekategoriat | 4 |
| 2.3 Kuntien tietohallintojen mallit | 6 |
| 2.4 Regulaatio kyberturvallisuudessa | 6 |
| 3. TUTKIMUKSEN TOTEUTTAMINEN | 9 |
| 3.1 Tutkimusmenetelmä | 9 |
| 3.1.1 Tieteellinen aineistohaku | 9 |
| 3.1.2 Julkisen sektorin aineistohaku | 10 |
| 3.2 Tutkimusaineisto | 11 |
| 4. SUOMESSA RAPORTOIDUT KYBERHYÖKKÄYKSET | 14 |
| 4.1 Suomen kuntiin kohdistuneet kyberhyökkäykset | 14 |
| 4.2 Suomen julkiseen sektoriin kohdistuneet merkittävimmät kyberhyökkäykset | 18 |
| 5. KUNTIEN KYBERTURVALLISUUDEN HAASTEET JA RATKAISUT | 22 |
| 5.1 Kyberturvallisuuden haasteet | 22 |
| 5.1.1 Kyberturvallisuuden haasteet Ruotsissa, Norjassa ja Yhdysvalloissa | 22 |
| 5.1.2 Kyberturvallisuuden haasteet Suomessa | 24 |
| 5.1.3 Tiedon jakaminen ja siiloutuminen | 25 |
| 5.2 Kyberturvallisuuden kehittäminen | 27 |
| 5.2.1 Kehittämisstrategiat | 27 |
| 5.2.2 Auditoinnit ja sertifiointit | 28 |
| 5.2.3 Seuraamusmaksujen vaikutus toimintaan | 28 |
| 5.2.4 Muut kyberturvallisuuden kehittämistavat | 30 |
| 6. YHTEENVETO | 32 |
| 6.1 Tutkimuksen tulokset | 32 |
| 6.2 Tulosten arviointi | 34 |
| 6.3 Tarve jatkotutkimukselle | 35 |
| LÄHTEET | 37 |

LYHENTEET JA MERKINNÄT

| | |
|-----------------|---|
| DVV | Digi- ja väestötietovirasto |
| EU | Euroopan unioni |
| ENISA | Euroopan unionin verkko- ja tietoturvavirasto |
| GDPR | Euroopan unionin yleinen tietosuoja-asetus |
| MSB | Ruotsin valmiusvirasto |
| Nato | Pohjois-Atlantin puolustusliitto |
| NIST | Yhdysvaltain standardisointi- ja teknologianstituutti |
| NIS2-direktiivi | Euroopan unionin kyberturvallisuusdirektiivi |

1. JOHDANTO

1.1 Tutkimuksen tausta ja merkitys

Kuntien toiminnalla ja toiminnan kyberturvallisuudella on vaikutuksia koko suomalaiseen yhteiskuntaan. Kunnat tuottavat kansalaisille tärkeitä palveluja, kuten koulutusta, vesi- ja jätehuoltoa, liikennettä ja joukkoliikennettä, turvallisuus- ja varautumispalveluita, työllisyyspalveluja sekä järjestävät vaaleja (Valtiovarainministeriö n.d.). Häiriön sattuessa nämä palvelut, kuten elintärkeät vesi- ja energiahuolto, voisivat vaarantua. Kriittisten toimialojen häiriöt voivat aiheuttaa hyvin merkittäviä häiriöitä myös muille yhteiskunnan toimialoille (Lehtilä et al. 2021). Kuntien kyberturvallisuuteen keskittyvän tutkimuksen vähäinen määrä ja tarve lisätutkimukselle on tunnustettu Yhdysvalloissa. Tutkimuksen avulla voidaan edistää organisaatioiden resilienssin kasvamista ja kyberturvallisuuden käytäntöjä. (Preis & Susskind 2021) Haasteen tutkimukselle Suomen kontekstissa aiheuttaa kuntien erilaisuus esimerkiksi niiden koon suhteen.

On esitetty väitteitä, että ennen Suomen ulkoministeriöön 2013 tapahtunutta tietomurtoa Suomen julkisen sektorin tietoturvallisuuden taso on ollut merkittävän puutteellista (Raiio 2013). Ennen ulkoministeriön vuoden 2013 tietomurtoa olevaa aikaa kuvastaa Martti J. Karin toteamus ”Meillä hoettiin mantraa, jonka mukaan Suomessa on maailman puhaimmat tietoverkot. Näin ei valitettavasti kuitenkaan ollut, kuten myöhemmin kävi ilmi” (Halminen 2024 s. 221). Myös kuntien kohdilla on viimevuosina havaittu merkittäviä kyberhyökkäyksiä.

Suomeen kohdistuu päivittäin kybervakoilua, kyberrikollisuutta ja kybervaikuttamista (Valtioneuvosto 2023 s. 7). Suomessa kyberturvallisuuden merkitystä korostaviksi asioiksi on tunnustettu COVID-19-pandemia ja sen kiihdyttämä digitalisaatio, Venäjän hyökkäyssota Ukrainassa, Suomen Nato-jäsenyys, Euroopan unionin (lyh. EU) tiukentuva kybersäätely ja maailmanlaajuisesti kiristynyt geopoliittinen tilanne (Paananen et al. 2024 s. 13). Tämä korostaa aiheen käsittelyn merkitystä ja ajankohtaisuutta. Aiemmissa raporteissa ja tutkimuksissa esitetyistä huomioista voidaan päätellä, että aihe on merkityksellinen ja tutkimuksen arvoinen.

1.2 Tutkimuskysymys ja rajaukset

Työn tutkimuskysymys on ”Mitä haasteita Suomen kunnilla on kyberturvallisuudessa, ja miten kyberturvallisuutta tulisi kehittää?”. Tämä tutkimuskysymys valittiin, koska Suomen kuntiin kohdistuneista kyberuhista ja -haasteista vaikutti olevan vain vähän tieteellistä tutkimusta saatavilla. Aiheen tarkastelun merkitystä korostaa erilaisten kyberhyökkäysten määrä viime vuosina ja niiden kohdistuminen yhä enemmän Suomen kuntasektoriin.

Alatutkimuskysymykset ovat seuraavat:

- Mitkä ovat Suomen kuntien kyberturvallisuushaasteet, ja millaisia uhkia on realisoitunut?
- Millaisia kyberturvallisuushaasteita on tunnistettu toisissa maissa?

Tutkimuksen tavoitteena on luoda yhtenäinen kokonaiskuva kirjallisuuskatsauksen avulla raportoiduista kyberhyökkäyksistä, kyberturvallisuuden haasteista, jotka on tunnistettu ja mahdollisista ratkaisuista haasteisiin. Tavoitteena on myös tutkia, millaisia strategioita on laadittu kyberturvallisuuden suhteen Suomessa. Tutkimuksessa tarkastellaan Suomen kuntien kyberturvallisuutta johtamisen ja hallinnollisen tason näkökulmasta. Suomen kuntia tarkasteltaessa tulee huomioida, että sosiaali- ja terveydenhuolto sekä pelastustoimi eivät enää kuulu kuntien tai kuntayhtymien vastuualueelle 1.1.2023 voimaan tulleen sosiaali- ja terveydenhuollon uudistuksen jälkeen (Sosiaali- ja terveystoimi 2023). Tämä korostuu ulkomaisia tai ennen vuotta 2023 julkaistuja lähdeaineistoja tarkasteltaessa. Työssä ei tarkastella spesifisti terveydenhuoltoa, koska sitä tarkastellaan usein omana kokonaisuutenaan ja koska se ei enää kuulu Suomessa kuntien vastuualueelle.

Tutkimus rajataan koskemaan Suomen kuntia tutkimuksen laajuuden hallitsemiseksi. Koska Suomen kunnista tieteellisen tiedon ja muun raportoinnin saanti on rajallista, hyödynnetään kansainvälistä erityisesti kuntiin tai paikallishallintoihin kohdistunutta tutkimusta. Myös Suomen julkiseen sektoriin liittyviä tutkimuksia ja raportteja käytetään kuntien tarkastelun apuna. Internetissä tapahtuva kiusaaminen (engl. cyberbullying) ja yksityisten yritysten ja yksityishenkilöiden kyberturvallisuus rajattiin pois. Tutkimus toteutettiin kirjallisuuskatsauksena, jolloin esimerkiksi haastatteluja ei tehty. Tutkimuksessa ei oteta kantaa yksityiskohtaisiin teknisiin ratkaisuihin.

1.3 Tutkimuksen rakenne

Työn toisessa luvussa käsitellään kyberturvallisuuden käsitteitä, kyberuhkien tyyppejä ja kuntien kyberturvallisuuteen liittyviä toimintoja teorian tasolla. Tämä taustoitus auttaa lukijaa hahmottamaan työn keskeiset käsitteet ja toimintaympäristön, kuin ne tässä työssä on määritelty. Kolmannessa luvussa käsitellään tutkimusmenetelmää ja tarkastellaan tutkimusaineiston laatua.

Työn neljännessä luvussa siirrytään tutkimuksen tulosten esittelyyn. Luvussa tarkastellaan Suomen kuntiin ja julkiseen sektoriin kohdistuneita kyberhyökkäyksiä ja niiden seurauksia poliisin tiedote- ja lehtikatsauksen avulla. Kuntien kyberturvallisuuden haasteita ja niiden ratkaisuja käsitellään luvussa 5 käyttäen sekä tieteellistä että julkisen sektorin aineistoa. Viimeisessä luvussa käsitellään tutkimuksen tuloksia, tulosten arviointia ja mahdollisia jatkotutkimusten kohteita.

2. KYBERTURVALLISUUS JA KYBERUHAT

2.1 Kyberturvallisuus

Tietoturvallisuudella tarkoitetaan järjestelyitä, jotka takaavat tiedon luotettavuuden, eheyden ja saatavuuden. Kyberturvallisuus on tavoitetilä, jossa kybertoimintaympäristö on suojattu ja sen sisältöön voidaan luottaa. Kyberturvallisuuteen kuuluvat kyberuhkien ennakointi, hallinta ja vaikutusten sietäminen. Kybertoimintaympäristö on yhdestä tai useammasta tietojärjestelmästä koostuva ympäristö. (Sanastokeskus TSK 2018) Euroopan unionin verkko- ja tietoturvavirastoa (lyh. ENISA) koskevassa asetuksessa kyberturvallisuudella tarkoitetaan toimia, joilla suojataan verkko- ja tietojärjestelmiä ja näiden käyttäjiä sekä muita asianosaisia henkilöitä kyberuhilta (EU 2019/881 artikla 2). Yhdysvaltain standardisointi- ja teknologiainstituutti (lyh. NIST) puolestaan määrittelee kyberturvallisuuden seuraavanlaisesti. Kyberturvallisuus on tietokoneiden, sähköisten- ja langallisten viestintäjärjestelmien, sähköisten viestintäpalveluiden ja sähköisen viestinnän suojaamista ja vahingoilta estämistä, sekä palauttamista. Lisäksi kyberturvallisuus tarkoittaa näissä järjestelmissä olevan tiedon saatavuuden, eheyden, todennuksen luottamuksellisuuden ja kiistämättömyyden varmistamista. (NIST n.d.)

Tässä työssä käytetään termiä kyberturvallisuus, koska tarkastelun kohteena on tietojärjestelmien suojaamisen ja niihin kohdistuvat uhat ja Suomen julkisen sektorin suojaamisen suhteen käytetään usein terminä kyberturvallisuutta. Pääosin Suomen julkisen sektorin julkaisuissa on hyödynnetty Sanastokeskuksen julkaisemaa Kyberturvallisuuden sanastoa ja siksi sitä ja sen määritelmiä hyödynnetään tässä työssä. Kyberturvallisuutta haastavat erilaiset kyberuhat ja uhkatoimijat, joita käsitellään seuraavassa alaluvussa.

2.2 Kyberuhat, uhkatoimijat ja haastekategoriat

Kyberuhka määritellään sellaiseksi tilanteeksi, tapahtumaksi tai toiminnaksi, joka häiritsee tai vahingoittaa verkko- tai tietojärjestelmiä (EU 2019/881 artikla 2). Kyberhäiriö on toteutunut kyberuhka, joka aiheuttaa haittaa toiminnalle. Verkkohyökkäys on toiminta, jonka tavoitteena on pyrkiä vaurioittamaan tai saamaan luvattomasti käyttöön tietoverkko, tietojärjestelmä, data tai laite ja, se voidaan toteuttaa esimerkiksi palvelunestohyökkäyksenä tai haittaohjelman avulla. Kyberhyökkäyksellä viitataan verkkohyökkäykseen, mutta hyökkäystapa voi olla myös tietoverkon ulkopuolinen. Kybervakoilulla tarkoitetaan vakoilua, joka suoritetaan tietoverkkojen avulla ja se voi kohdistua valtioihin, yri-

tyksiin, yksityishenkilöihin tai erilaisiin organisaatioihin. Kiristyshaittaohjelma salaa tiedostoja käyttäjältä ja vaatii salauksen avaamisesta lunnaita. (Sanastokeskus TSK 2018) Tietomurrolla tarkoitetaan tunkeutumista suojattuun tietojärjestelmään tai tietojen oikeudetonta tarkastelemista (TEPA-termipankki n.d.). Palvelunestohyökkäyksessä tietojärjestelmä tai palvelu pyritään lamauttamaan kuormittamalla sitä suurella määrällä palvelupyyntöjä ja se toteutetaan usein hajautetusti bottiverkon avulla (Sanastokeskus TSK 2018).

Tietojenkalastelussa pyritään saamaan käyttäjä tekemään itselleen jokin haitallinen toimenpide, kuten antamaan pankkitunnukset, lataamaan haittaohjelma, lähettämään rahaa tai tietoa. Toteutustapa voi olla esimerkiksi sähköpostiviesti, tekstiviesti, puhelu tai valesivusto. (Kyberturvallisuuskeskus n.d.a) Kohdennetulla tietojenkalastelulla tarkoitetaan kehittyneempää tietojenkalastelua, jossa esimerkiksi sähköpostiviestiin on lisätty uskottavuutta lisääviä tekijöitä, kuten kohdehenkilön oikea nimi. (Norris et al. 2024)

Kohdistettu haittaohjelmahyökkäys tai APT-hyökkäys (engl. Advanced persistent threat attack) on monivaiheinen hyökkäys, jonka uhrit ovat kohdistettuja. Toteuttajat ovat usein valtiollisia tai niitä lähellä olevia APT-ryhmiä. (Sanastokeskus TSK 2018) Euroopan unionin alueella suurimmat kyberuhat muodostavat kirityshaittaohjelmat, haittaohjelmat, käyttäjien manipulointi, tietoturvaloukkaukset, tietovuodot, palvelunestohyökkäykset ja informaation manipulointi, joka vaikuttaa kansalaisten mielipiteisiin (ENISA 2024).

Erilaiset uhkatoimijat voidaan jakaa neljään pääryhmään: valtiosidonnaisiin toimijoihin, kyberrikollisiin, yksityisen sektorin kyberhyökkäystoimijoihin (engl. Private Sector Offensive Actors) ja haktivisteihin. Valtiosidonnaiset toimijat ovat hyvin rahoitettuja, ja nämä pyrkivät ajamaan oman maansa etuja, kuten suorittamaan vakoilua tai rahan hankintaa kyberrikollisuuden keinoin. Kyberrikollisten päämääränä on rahan hankkiminen, ja tämä saatetaan toteuttaa esimerkiksi kiristämällä uhreja tai myymällä kaapattua dataa eteenpäin. Tilaustöitä tekevät hakkerit, jotka tarjoavat rikollisia palveluita, voidaan katsoa kuuluvan kyberrikollisiin. Yksityisen sektorin kyberhyökkäystoimijat ovat yrityksiä, jotka kehittävät ja myyvät haavoittuvuuksia hyödyntäviä haittaohjelmia ja nollapäivähaavoittuvuuksia. Haktivistit pyrkivät ajamaan omia poliittisia tarkoituksiaan eteenpäin hakkeroinnin keinoilla. (ENISA 2024)

Kyberuhat aiheuttavat erilaisia haasteita organisaatioiden kyberturvallisuudelle. Kyberturvallisuuden haasteet voidaan tarkastella neljän eri kategorian avulla:

- Tekniset ja operatiiviset
- Vastuu ja käyttäytyminen
- Poliitikka ja sääntely

- Resurssit ja infrastruktuuri (Hossain et al. 2024).

Hossain et al. (2024) kategorioiden avulla voidaan seuraavissa kappaleissa helpommin tarkastella tunnistettuja haasteita ja luokitella ne kappaleessa 5. Hossain et al. (2024) esittelee myös artikkelissaan useita erilaisia ulkomaisia kuntia koskevia kyberhyökkäys-tapauksia, mutta ne ovat tämän työn rajauksen ulkopuolella.

2.3 Kuntien tietohallintojen mallit

Tarkastellaan Suomen kuntien tietohallintojen malleja, koska edellisessä alaluvussa Hossain et al. (2024) esittämänä resurssit ja infrastruktuuri havaittiin merkittäväksi kyberturvallisuuden haastekategoriaksi. Tarkastelu auttaa ymmärtämään Suomen kuntien kyberturvallisuuteen kiinteästi liittyvän tietohallinnon olosuhteita ja käytössä olevia resursseja. Suomen kuntien tietohallintojen malleiksi on esitelty neljä erilaista mallia:

- Tietohallinto järjestetään itse kunnan sisäisesti
- Inhouse-yhtiön käyttäminen, jossa palvelu ostetaan kunta- tai kuntayhtymäomisteiselta yhtiöltä
- Isäntäkunta-malli, jossa pienempi kunta ostaa palvelun suuremmalta kunnalta
- Ulkoistus, jossa palvelu ostetaan markkinoilta (Hillamo & Pesonen 2022).

Itse järjestetyssä tietohallinnossa ongelmaksi on havaittu asiantuntijoiden rekrytoinnin haasteet ja syväosaamisen saavuttaminen on vaikeaa (Hillamo & Pesonen 2022). Kunnista ja kuntayhtymistä 69 % järjesti tietoturvan sisäisesti, 32 % inhouse-yhtiön kautta, 22 % ulkoiselta palveluntarjoajalta ja 9 % kunta- tai kuntayhtymäyhteistyönä vuonna 2018 (Hyvärinen & Parviainen 2018). 70 % Suomen kunnissa on Kuntaliiton kyselyn perusteella henkilö, joka informoi kunnan johtoa tietoturvasta ja tehdyistä toimenpiteistä (Lyly et al. 2021). Voidaan pohtia, onko kaikilla Suomen kunnilla todellisuudessa tarvittavat resurssit ja tietotaidot sisäiseen toimintaan.

2.4 Regulaatio kyberturvallisuudessa

Hossain et al. (2024) tunnistavat politiikan ja sääntelyn merkittäväksi kyberturvallisuuden haastekategoriaksi, joten tarkastellaan aihetta tarkemmin. Tietoihin kohdistuva sääntely tulee lisääntymään ja pienillä kunnilla ei ole riittävästi osaamista uusien lakien käyttöönottoon (Lyly et al. 2021). Esimerkiksi vaatimalla korkeampaa tietoturvan tasoa voidaan ohjata organisaatioiden toimintaa (Lehtilä et al. 2021) ja näin näyttää tapahtuvan yhä enenemissä määrin niin EU:n kuin myös Suomen tasolla. Tämän takia tietoihin ja

kyberturvallisuuteen liittyvän regulaation tarkastelu on merkityksellistä. EU-asetukset tulevat voimaan kaikissa jäsenmaissa samanaikaisesti ja samalla tavalla. EU-direktiivit asettavat vaatimuksen muuttaa kansallista lainsäädäntöä direktiivin mukaiseksi tietyssä määräajassa, tyypillisesti 2 vuodessa. (Euroopan komissio n.d.) Koska EU-direktiivien vaikutus tulee kansalliseen lainsäädäntöön viiveellä, tarkastelemalla direktiivien ehtoja voidaan varautua tuleviin lainsäädännöllisiin muutoksiin ennakoivasti.

Suomessa valtioneuvosto (2024a) on esittänyt NIS2-direktiivin vähimmäisvaatimusten pohjalta kokonaan uuden kyberturvallisuuslain luomista. Kuntien tärkeitä suojattavia kohteita tarkasteltaessa voitaisiin käyttää hyväksi NIS2-direktiivin vaatimuksia. Kuntien NIS2-direktiivin alaisiin kohteisiin kuuluisi muun muassa juoma- ja jätevesihuolto, energiasektori (esimerkiksi sähkö ja kaukolämpö), jätehuolto ja satamat (Kuntaliitto 2023). Kunnilla voi olla omistuksessa myös lentokenttiä, yksityisraiteita ja tietoverkkopalveluita, jotka kuuluisivat direktiivin piiriin (Kuntaliitto 2023).

Euroopan unionin yleinen tietosuojasetus eli GDPR asettaa vaatimuksia yksityisten ihmisten henkilötietojen käsittelyyn ja omien tietojen saatavuuteen (EU 2022). EU:n jäsenmaat voivat itse päättää, voivatko viranomaiset tai julkishallinnon elimet saada GDPR:n mukaisia hallinnollisia seuraamusmaksuja. (EU 2016/679 artikla 83) NIS2- eli kyberturvallisuusdirektiivin tarkoituksena on vahvistaa kriittisten toimijoiden kyberturvallisuutta Euroopan unionin ja sen jäsenvaltioiden tasolla sekä säätää tietoturva-, riskienhallinta- ja raportointivelvoitteista (Kyberturvallisuuskeskus n.d.b). Suomen kansallisessa lainsäädännössä, kuten Tietosuoja-laissa (2018), käytetään termiä hallinnollinen seuraamusmaksu toisin kuin EU:n GDPR:n ja NIS2 suomenkielisissä käännöksissä, joissa käytetään termiä hallinnollinen sakko. Tässä työssä käytetään kansallista termiä hallinnollinen seuraamusmaksu. NIS2-direktiivissä julkishallinto on määritetty direktiivin soveltamisalaksi, pois lukien kansallisen turvallisuuden ja lainvalvonnan toimijat. EU:n jäsenmaa voi päättää, sovelletaanko NIS2-direktiiviä paikallistason julkishallinnon toimijoihin. (EU 2022/2555 artikla 2) EU:n jäsenvaltiot voivat päättää, voivatko julkishallinnolliset toimijat saada NIS2-direktiivin mukaisia hallinnollisia seuraamusmaksuja (EU 2022/2555 artikla 34). Taulukossa 1 on esitetty GDPR:n ja NIS2-direktiivin seuraamusmaksujen määrät taulukkomuodossa niiden vertailun selventämiseksi.

Taulukko 1. GDPR ja NIS2-direktiivin seuraamusmaksujen määrät

| Säädöstyyppe | Seuraamusmaksun enimmäismäärä euroina | TAI | Seuraamusmaksun enimmäismäärä prosentteina edellisen tilikauden globaalisti liikevaihdosta | Lähde |
|-------------------------|---------------------------------------|-----|--|---------------------------|
| GDPR rikkomus | 10 000 000 € | TAI | 2 % | (EU 2016/679 artikla 83) |
| GDPR vakavampi rikkomus | 20 000 000 € | TAI | 4 % | (EU 2016/679 artikla 83) |
| NIS2 rikkomus | 7 000 000 € | TAI | 1,4 % | (EU 2022/2555 artikla 34) |
| NIS2 vakavampi rikkomus | 10 000 000 € | TAI | 2 % | (EU 2022/2555 artikla 34) |

Sekä GDPR:n että NIS2-direktiivin mukaan euromääräisestä tai prosentuaalisesta summasta tuomitaan maksettavaksi se, joka niistä on suurempi (EU 2016/679 artikla 83; EU 2022/2555 artikla 34). Havaitaan, että hallinnolliset seuraamusmaksut voivat nousta hyvinkin suuriksi sekä GDPR:n että NIS2:n kohdalla.

3. TUTKIMUKSEN TOTEUTTAMINEN

3.1 Tutkimusmenetelmä

Tutkimusmenetelmänä tässä tutkimuksessa käytetään kirjallisuuskatsausta. Menetelmänä käytetään integroivaa mallia, jotka voidaan Cooperin (1989 s.15) mukaan jakaa 5 kohtaan:

- Tutkimusongelman asettelu
- Aineiston hankkiminen
- Arviointi
- Analyysi
- Tulkinta ja tulosten esittäminen (Salminen 2011 s.8).

Torracon (2005 s. 356) mukaan integroivan kirjallisuuskatsauksen avulla voidaan tuottaa aiheesta uutta tietoa ja tarkastella asiaa monipuolisesti (Salminen 2011 s. 8). Integroiva kirjallisuuskatsaus ei seulo aineisto yhtä tarkasti, kuin systemaattinen kirjallisuuskatsaus ja näin ollen sen avulla voidaan käyttää laajempaa aineistoa (Salminen 2011 s. 8).

3.1.1 Tieteellinen aineistohaku

Tavoitteena tieteellisellä haulla on luoda työlle tieteellinen pohja, johon esimerkiksi julkisen sektorin tarkastelussa saatuja tuloksia voidaan verrata. Tietoa haetaan Tampereen yliopiston tietokantapalvelu Andorista ja Elsevierin Scopuksesta. Tutkimuksen tieteellisessä haussa etsitään vertaisarvioituja tieteellisiä artikkeleja. Aineistoa haetaan Andorista englanninkielisillä termeillä, koska suurin osa tieteellisestä aineistosta on englanninkielistä ja koska suomenkielisillä termeillä löytyy lähes pelkästään opinnäytetöitä. Aineistoa etsitään myös helmenkasvatusmenetelmällä.

Aineistoa etsittäessä tulee huomioida käsitteiden määritelmien epäselvyydet ja erilaiset tulkinnat. Samoilla käsitteillä on useita erilaisia määritelmiä riippuen määrittelevästä organisaatiosta. Haasteen käsitteiden hakemiselle aiheuttavat erilaiset kirjoitusasut, esimerkiksi kyberhyökkäyksen englanninkielisiä termejä ovat ”cyberattack”, ”cyber attack” ja ”cyber-attack”. Samanlaista termien vakiintumattomuutta esiintyy myös runsaasti suomenkielisessä termistössä tai joillekin käsitteille ei ole olemassa suomenkielisiä vastineita. Yhdysvaltoja käsittelevän aineiston kohdalla tulee huomioida termien kunta (engl. municipality) ja paikallishallinnon (engl. local government) eroavaisuus. Yhdysvaltoja koskeva lähdeaineisto käyttää pääosin termiä ”local government”, joka käsittää sekä kunnat,

että niitä suuremmat piirikunnat. Tässä työssä käytetään pääsääntöisesti lähdeaineiston mukaista termiä paikallishallinto, paitsi silloin, kun Ruotsin ja Norjan kuntien käsittelyn kohdalla olisi lukemisen kannalta vaivalloista.

3.1.2 Julkisen sektorin aineistohaku

Tieteellisen aineiston lisäksi hyödynnetään Suomen julkisen sektorin aineistoja, jotta aihetta pystytään tarkastelemaan Suomen kontekstissa. Julkisen sektorin aineistona käytetään suomalaisten viranomaisten, Kyberturvallisuuskeskuksen, ministeriöiden tai valtioneuvoston tekemiä julkaisuja, raportteja ja toimintaohjeita. Tavoitteena tällä on tarkastella Suomen julkisen sektorin kyberturvallisuuden haasteita, erityispiirteitä ja kehittämisstrategioita. Haku suoritetaan valtioneuvoston julkaisuarkisto Valtoon, joka sisältää eri ministeriöiden julkaisuja. Aineistoa etsitään poliisin uutisarkistosta hakusanoilla ”kyber”, ”tietomurto” ja ”palvelunesto”. Julkisen sektorin aineistojen hakemiseen käytetään suomenkielisiä hakutermejä, koska aineisto on suomenkielistä. Osin ongelmallista julkisen sektorin julkaisuissa on, että Valto ei kuitenkaan sisällä kaikkia mahdollisia julkaisuja, vaan esimerkiksi Digi- ja viestintäviraston (lyh. DVV) julkaisuja jouduttiin hakemaan viraston omalta verkkosivulta. Julkisen hallinnon julkaisut eivät myöskään usein sisällä lähdeviitteitä, jolloin julkaisujen luotettavuutta ja niissä esitettyjä väitteitä olisi helpompi arvioida.

Poliisin raportoihin ja muihin mahdollisiin tapauksiin etsitään lisätietoa iteratiivisesti Google ja DuckDuckGo -hakukoneiden avulla lehtien, viranomaisten ja asianosaisten organisaatioiden julkaisuista. Haku toteutettiin käyttämällä hakutermeinä raportoitujen tapauksien nimiä tai halulausekkeita ”kunta tietomurto”, ”kunta kyberhyökkäys”, ”kunta palvelunestohyökkäys”, ”kunta verkkohyökkäys”. Lehtiaineistoon kohdistunut haku toteutettiin, koska Suomessa ei ole julkaistu kokoelmaa tai aikajanaa kuntiin tai julkiseen sektoriin kohdistuneista kyberuhista ja aiheen tarkastelu on tästä johtuen haastavaa. Osaltaan kuntiin ja julkiseen sektoriin kohdistuneiden uhkien selvittämistä hankaloittaa, että osasta tapauksista on vain poliisin lyhyt tiedote, uutismaininta ja ehkä lehtihaastatteluita kyseisen kunnan päättäviltä henkilöiltä. Lehtiaineistojen kohdalla tulee huomioida, että niiden kirjoittajat eivät useinkaan ole olleet kyberturvallisuuden ammattilaisia ja näiden aineiston luotettavuus on näin ollen alempi kuin tieteellisten aineistojen. Joistain tapauksista saattaa löytyä tapauksissa mukana olleiden asiantuntijoiden haastatteluja Pro Gradu- tai maisteritutkielmista ja niiden käyttö edellyttää harkintaa.

3.2 Tutkimusaineisto

Luotettavuuden takia aineistoksi valittiin vertaisarvioituja tieteellisiä artikkeleja. Näistä artikkeleista vain osa käsittelee aihetta tässä työssä hyödynnettävällä tavalla. Suuri osa hakulausekkeilla löydetyistä aineistosta käsittelee teknisiä kyberturvallisuuden ratkaisuja tai sellaisia maita, joiden julkinen sektori eroaa merkittävästi suomalaisesta ja ei siten ollut tässä työssä hyödyllistä. Työssä käytetty ulkomainen aineisto käsittelee käytännössä Yhdysvaltoja, Ruotsia ja Norjaa. Voidaan pohtia, olisiko ainoastaan Pohjoismaihin kohdistunut rajausta ollut tutkimuksen kannalta hyödyllisempi, mutta silloin ongelmaksi olisi muodostunut englannin- ja suomenkielisen aineiston rajallinen määrä. Taulukossa 2 on esitetty tieteelliseen aineistoon kohdistuneet haut, jotka on rajattu vertaisarvioituihin artikkeleihin. Tarkasteltaessa taulukkoa 2 havaitaan, että lopulliseen työhön päätyi 11 tieteellistä artikkelia yhteensä 730 hakutuloksesta.

Taulukko 2. *Vertaisarvioinnilla rajatut hakulausekkeet*

| Vertaisarvioitu | Andor | Scopus | Helmenkasvatus | Päätyi työhön |
|---|-------|--------|----------------|---------------|
| cyber AND municipality AND risk NOT bullying | 32 | 22 | - | 2 |
| cyber AND municipal* AND (risk* OR "risk management") AND (information OR knowledge) NOT bullying | 53 | 26 | - | 2 |
| cyber AND (challenge OR problem OR difficulty) AND ("public sector" OR municipal* OR "local government") NOT bullying | 328 | 186 | 2 | 5 |
| (cyberthreat OR "cyber threat") AND ("public sector" OR municipal* OR "local government") NOT bullying | 19 | 64 | - | 2 |

Poliisin uutisarkisto osoittautui työn kannalta vain osin hyödylliseksi, koska osasta merkittävistäkään kybertapahtumista ei löydy tietoa. Osaltaan poliisin uutisarkistosta tiedon hakemista ja löytymistä haittasi vaikeakäyttöinen käyttöliittymä. Osasta suurista tapahtumista ei löytynyt tietoa poliisin uutisarkistosta kuin lyhyitä tiedotteita, kun taas joistakin

suhteellisen vähäisistä tapauksista saattoi löytyä tietoa. Poliisin julkaisuarkistosta puolestaan löytyi lähes ainoastaan poliisin sisäistä toimintaa kuvaavia raportteja, eivätkä nämä julkaisut näin olleet työn kannalta hyödyllisiä. Valtioneuvoston julkaisuarkisto Valto osoittautui työn kannalta hyödylliseksi, koska se sisältää eri ministeriöiden ja virastojen julkaisuja helposti haettavassa muodossa. Nämä käsittelevät lisäksi spesifisti Suomea ja Suomen julkisen sektorin toimijoita. Taulukossa 3 esitetään julkisen sektorin julkaisuihin kohdistuneet haut. Taulukkoa 3 tarkasteltaessa havaitaan, että Valtosta löytyi useita työssä käytettyjä julkaisuja ja haun tulokset olivat hyvät tulosten määrän ja niiden käytettävyyden suhteen. Taulukossa 3 esitetään myös Poliisin uutisarkiston hakujen kautta löydetty kyberhyökkäykset, joista etsittiin sen jälkeen tietoa muista lähteistä. Taulukko 3 tarkasteltaessa havaitaan, että julkiseen sektoriin kohdistuneen haun seurauksena työhön päätyi 16 lähdeä 184 hakutuloksesta.

Taulukko 3. *Julkisen sektorin hakulausekkeet*

| Hakulauseke | Tietokanta | Rajoite | Tulokset | Helmenkasvatus | Avulla löydettyt | Päätyi työhön |
|-------------------------|-----------------------|---------------|----------|----------------|------------------|---------------|
| kyber AND tietoturva | Valto | 2020– 2025 | 46 | 4 | - | 8 |
| kyber | Poliisin uutisarkisto | - | 35 | - | 1 | 1 |
| tietomurto | Poliisin uutisarkisto | - | 81 | - | 2 | 4 |
| palvelunesto | Poliisin uutisarkisto | - | 7 | - | - | 2 |
| kyber AND kunta | DVV | tiedostot | 15 | - | - | 1 |

Työssä käytetään myös Kuntaliiton julkaisuja, jotka löydettiin Kuntaliiton verkkosivuilta kuntien digitaalisia asioita ja kyberturvallisuutta käsittelevistä kohdista, joista löytyi 4 työssä käytettyä lähdeä ja lisäksi helmenkasvatuksella tätä kautta löytyi myös suomi.fi palvelussa ollut DVV:n vuoden 2021 selvitys, jota ei ollut DVV:n omilla verkkosivuilla. Kuntaliiton materiaalit tarjoavat tarkempaa tietoa Suomen kuntien toiminnasta. Työhön

valikoitui 20 lehtiartikkeliä, jotka koskivat tapahtuneita kyberhyökkäyksiä. Näistä 17 löytyi Google-haun ja 3 DuckDuckGo-haun avulla. Muuramen ja Kärkölen kuntaan kohdistuneet kyberhyökkäykset löytyivät myös näiden hakujen yhteydessä kyseisten kuntien verkkosivuilta. Onnettomuustutkintakeskuksen raportit koskien Helsingin kaupungin tietomurtoa löytyivät puolestaan lehtiartikkelin kautta helmenkasvatuksena.

Tutkimusaineistoa etsittäessä havaittiin, että täsmälleen Suomen kuntien kyberturvallisuutta koskettavaa aineistoa on saatavissa rajallinen määrä. Tämän takia joudutaan soveltamaan ulkomaista aineistoa Suomen kuntien kyberturvallisuuden tarkastelussa. Työhön valittuja aineistoja yhdistää keskittyminen kuntien tai Suomen julkisen sektorin kyberturvallisuuteen. Työhön valituista tieteellisistä artikkeleista suurin osa oli julkaistu 2020-luvulle. Julkisen sektorin aineistoista suurin osa oli alle 10 vuotta vanhaa. Aineiston uutuus korostuu etenkin nopeasti kehittyvän kyberturvallisuuden alalla. Isossa osassa tieteellistä ja julkista hakua kunnat olivat ainoastaan sivuroolissa kyberturvallisuuden käsitteilyn kohdistuessa toisenlaisiin organisaatioihin kuten yrityksiin, eivätkä nämä artikkelit sen takia olleet hyödyllisiä tätä työtä varten.

4. SUOMESSA RAPORTOIDUT KYBERHYÖKKÄYKSET

4.1 Suomen kuntiin kohdistuneet kyberhyökkäykset

Tässä kappaleessa siirrytään tutkimuksen tulosten esittelyyn. Jotta saadaan ymmärrys Suomen kuntasektorin kyberturvallisuudesta, tarkastellaan Suomen kuntiin kohdistuneita kyberhyökkäyksiä. Tarkastelemalla aikaisempia tapahtumia voidaan havaita yhteisiä ongelmakohtia, millaisilla tavoilla kuntiin on hyökätty ja millaisia vaikutuksia hyökkäyksillä on ollut. Raportoituja kyberuhkia tarkasteltaessa rajataan tarkastelu koskemaan pelkästään Suomen kuntia ja julkista sektoria laajuuden hallitsemiseksi. Tämän lisäksi ulkomaisista tapauksista löytyy jo valmiiksi tutkimusta. Taulukossa 4 käytetään tapahtumien kuvauksessa lähteissä olleita termejä. Tarkasteltaessa taulukkoa 4 havaitaan, että Suomen kunnat ovat olleet viime vuosina usein erilaisten kyberuhkien kohteena.

Taulukko 4. Suomen kuntiin kohdistuneita kyberhyökkäyksiä

| Tapahtumatyyppi | Kohde | Milloin | Lähde |
|-----------------------------------|---|----------------|--|
| Verkkohyökkäys | Kunnat Askola, Brändö, Kerimäki, Myrskylä, Pernaja ja Vesanto | 2009 | (Linnake 2009) |
| Tietomurto | Espoon kaupunki | 2010 | (Yle 2010) |
| Haitallinen kryptolouhija | Lahden kaupunki | 2018 | (Hannula 2020) |
| Kirstyshaittaohjelma | Kokemäen kaupunki | 2019 | (Poliisi 2019) |
| Tietomurto | Porin kaupunki | 2019 | (Joensuu 2019) |
| Törkeä tietojärjestelmän häirintä | Lahden kaupunki | 2019 | (STT 2019a) |
| Tietomurto | Siuntion kunta | 2019 | (Savonen 2019) |
| Tietomurto | Muuramen kunta | 2022 | (Muuramen kunta 2022) |
| Tietomurto | Säkylän kaupunki | 2022 | (Ylä-Tuuhonen 2023) |
| Verkkohyökkäys | Vesannon kunta | 2023 | (Lampinen 2023) |
| Kirstyshaittaohjelma | Rautavaaran kunta | 2023 | (Moliis 2023) |
| Tietomurto | Kärkölän kunta | 2023 | (Kärkölän kunta 2023) |
| Palvelunestohyökkäys | Kaupungit Espoo, Helsinki, Jyväskylä, Kotka, Kuopio, Lahti, Pori, Tampere, Turku ja Vaasa | 2024 | (Hanhinen et al. 2024; Rantanen et al. 2024) |
| Törkeä tietomurto | Helsingin kaupunki | 2024 | (Poliisi 2024) |

Taulukosta 4 havaitaan 14 erilaista kyberhyökkäystapausta. Taulukon 4 perusteella vaikuttaisi siltä, että Suomen kuntiin kohdistuneiden kyberhyökkäysten määrä on noussut

tai niistä on ainakin tiedotettu aiempaa enemmän. Havaitaan myös, että suurin osa kyberhyökkäyksistä on tietomurtoja, 6 kappaletta ja 1 törkeä tietomurto. Taulukossa 4 on myös hyvin erikokoisia kuntia, pienistä keskisuuriin ja suuriin, joten ongelma on selvästi koko Suomen kuntasektoria koskeva. Suurinta osaa tapauksia vaikuttaisi yhdistävän, että hyökkääjänä olisi kyberrikollistoimija, jonka toiminnan vaikuttimena olisi taloudelliset motiivit. Tätä ei voida kuitenkaan varmasti sanoa. Vuoden 2024 suuriin kaupunkeihin kohdistuneessa palvelunestohyökkäyksessä (Hanhinen et al. 2024; Rantanen et al. 2024) motiivina vaikuttaisi olevan poliittisesti motivoitunut häiriköinti.

Säkylään kohdistunut kyberhyökkäys aiheutti häiriöitä muun muassa suun terveydenhuollossa, jossa vuoroja jouduttiin siirtämään ja sosiaalihuollossa jouduttiin siirtymään varajärjestelmään. Säkylään kohdistunut hyökkäys aiheutti useiden satojen tuhansien euron vahingot. (Ylä-Tuuhonen 2023) Sekä Lahden että Säkylän tapauksia ennen kunnissa oli harjoiteltu toimia kyberhyökkäyksiä vastaan ja harjoittelusta kerrotaan olleen hyötyä kyberhyökkäysten aikaisessa toiminnassa (STT 2019b; Ylä-Tuuhonen 2023).

Säkylän kunnan tasolta on arvioitu Säkylään kohdistuneen kyberhyökkäyksen taustalla olleen jotakin valtiota lähellä oleva ammattimainen toimija. Säkylän kuntaan kohdistuneesta kyberhyökkäyksestä ei kerrota, johtuiko hyökkäys kunnassa sijaitsevasta Porin prikaatin varuskunnasta, mutta sen on arveltu vaikuttaneen asiaan. Puolustusvoimien tietojärjestelmät ovat erillisiä Säkylän kunnan tietojärjestelmistä. (Rantala 2023)

Lahdessa kyberhyökkäyksen aiheutti haavoittuva etäkäyttöohjelmisto yksittäisessä tietokoneessa, jonka kautta hyökkääjä pääsi Lahden kaupungin sisäverkkoon. Hyökkäyksen esto- ja korjaustoimenpiteet aiheuttivat merkittävää haittaa tietojärjestelmien käytölle ja hetkellisesti ne kaikki olivat pois käytöstä. Lahdessa on otettu kyberhyökkäyksen jälkeeseen käyttöön tietoturvalvomo, verkko on segmentoitu uudestaan ja on otettu käyttöön sekä tietoturvatestaukset sekä auditoinnit. Hyökkäyksen motiivia ei voida varmuudella tietää. (Ollila 2021) Lahden kaupunkiin vuonna 2019 kohdistuneen kyberhyökkäyksen suorat kustannukset olivat noin 700 000 €. Lahden tapauksen epäsuorien kustannusten arviointi on haastavaa. (Lehtilä et al. 2021)

Kokemäellä kyberhyökkäys rajautui kaupungin hallinnon ja vesihuollon verkkosegmenttiin, jossa kiristyshaittaohjelma salasi tietokoneiden tiedostoja ja vaati lunnaita niiden avaamisesta. Joitakin tietoja menetettiin pysyvästi ja osa varmuuskopioista oli vanhentuneita. Hyökkäys haittasi kyseiseen verkkosegmenttiin kuuluneiden työskentelyä ja sähköpostiviestintää. Kokemäen tapauksen suorat kustannukset olivat noin 25 000 € ja tie-

toturvan parantamiseen käytetyt välilliset kustannukset olivat 75 000 €. Kokemäen tapaukseen käytettyjen henkilöstöresurssien määrän arviointi on hankalaa. (Tammelin 2021)

Lahden tapauksessa hyökkäyksen jälkeen lisättiin toimia muun muassa teknisen tietoturvan konfiguraatioiden ja valvonnan tehostamiseksi. Kokemäen tapauksessa havaittiin, että henkilöstöllä ei ollut tarvittavaa osaamista kaikista verkkoon liittyvistä osista. Hyökkäyksen jälkeen Kokemäellä muutettiin verkon ja käyttövaltuuksien dokumentointia, varmuuskopiointia, ohjeita ja ylläpitoa. Lahden tapauksessa oli tietoturvapoliitikassa mainittu ulkopuolisten suorittamat tietoturvatarkastukset, mutta niitä ei toteutettu. (Tammelin 2021) Sekä kuntien Askola, Brändö, Kerimäki, Myrskylä, Pernaja ja Vesannon tapauksessa, että Säskylän tapauksessa hyökkäys tapahtui ulkopuolisen palveluntuottajan kautta (Linnake 2009; Ylä-Tuuhonen 2023). Tämä korostanee kunnan käyttämien kokonaan tai osin ulkoistettujen palveluntarjoajien kyberturvallisuuden arvioinnin ja valvonnan tärkeyttä.

Helsingin kaupungin tietomurron kohdalla noin 300 000 ihmisen tiedot vaarantuivat. Helsingin kaupungin tapaukseen on valtioneuvoston toimesta asetettu riippumaton Onnettomuustutkintakeskuksen tutkintaryhmän tutkimaan asiaa tapahtuman poikkeuksellisuuden vuoksi. (Onnettomuustutkintakeskus 2024) Helsingin kaupungin tietomurron vakavuudesta kertonee se, että muut Onnettomuustutkintakeskuksen tutkimat poikkeukselliset tapahtumat ovat COVID-19-pandemia sekä vakavia henkirikoksia, jotka ovat herättäneet merkittävää yhteiskunnallista keskustelua (Onnettomuustutkintakeskus n.d.). Helsingin kaupungin tietomurron laajuutta voidaan verrata Suomessa aiemmin tapahtuneisiin laajoihin tietomurtoihin, kuten Psykoterapiakeskus Vastaamon vuoden 2020 tietomurron 30 000 uhriin (Poliisi 2023) ja Valion vuoden 2024 tietomurron 70 000 uhriin (Valio 2025). Vastaamon tapauksen kohdalla tulee kuitenkin huomioida varastettujen terveystietojen vakavuusaste. Helsingin kaupungin tietomurron kohdalla epäillään myös tietosuojarikosta kaupungin toiminnassa (Rita 2025).

Vuoden 2024 laajasta suuriin Suomen kaupunkeihin kohdistuneesta palvelunestohyökkäysten sarjasta ei ole saatavilla tietoa poliisin tiedotteista. Voidaan pohtia, onko palvelunestohyökkäyksistä tarkemmin tiedottaminen edes tarpeellista, koska näissä hyökkäyksillä on tarkoitus usein hakea huomiota tai tuoda esille omia poliittisia päämääriään. Toisaalta avoimuuden, yhteiskunnallisen keskustelun, ja aiheen tarkastelun kannalta on jokseenkin poikkeuksellista, että poliisi ei tiedota asiasta.

Vuosi 2019 näyttäyty käänteentekeväna vuotena, jolloin kolmeen eri kaupunkiin kohdistui merkittäviä ja kansallisen uutiskynnyksen ylittäviä kyberhyökkäyksiä. Herää kysymys, eikö aiemmin ole ollut kyberhäiriöitä vai eivätkö ne ole vain tulleet yleiseen tietoon. Raportoidut kyberhäiriöt kattavat ainoastaan 30 % kaikista kyberhäiriöistä (Online Trust Alliance 2017; Institute of Directors 2016; Kesan & Zhang 2021 mukaan). Olisi hyödyllisempää, jos tietojärjestelmien haavoittuvuudet, kyberhyökkäykset ja niiden aiheuttamat haitat olisi voitu välttää etukäteen tehdyillä toimenpiteillä.

4.2 Suomen julkiseen sektoriin kohdistuneet merkittävimmät kyberhyökkäykset

Tarkastellaan Suomen julkiseen sektoriin kohdistuneita merkittäviä kyberhyökkäyksiä. Taulukossa 5 esitetään työssä löydetyt Suomen julkiseen sektoriin kohdistuneet kyberhyökkäykset.

Taulukko 5. Suomen julkiseen sektoriin kohdistuneita kyberhyökkäyksiä

| Tapahtumatyyppe | Kohde | Milloin | Lähde |
|---------------------------|---------------------------------------|------------------------|---------------------------------|
| Vakoilu ja törkeä vakoilu | Ulkoministeriö | 2013 (mahd. 2009–2013) | (Rajamäki 2013; Hiltunen 2014) |
| Palvelunestohyökkäys | Valtionhallinto | 2016 | (Poliisi 2016) |
| Palvelunestohyökkäys | suomi.fi | 2018 | (Poliisi 2018) |
| Palvelunestohyökkäys | Vaalijärjestelmä | 2019 | (CSIS 2025) |
| APT-hyökkäys | Eduskunta | 2020–2021 | (Poliisi 2021; CSIS 2025) |
| Pegasus-vakoiluohjelma | Ulkoministeriö | 2021–2022 | (Ulkoministeriö 2022; STT 2022) |
| Palvelunestohyökkäys | Ulkoministeriö ja puolustusministeriö | 2022 | (CSIS 2025) |
| Palvelunestohyökkäys | Eduskunta | 2022 | (CSIS 2025) |
| Palvelunestohyökkäys | Suomen Pankki | 2024 | (Hanhinen et al. 2024) |
| Epäilty törkeä tietomurto | Ulkoministeriö | 2025 | (STT 2025) |

Taulukosta 5 havaitaan 10 erilaista kyberhyökkäystapausta. Havaitaan, että raportoiduista kyberhyökkäyksistä yleisin on palvelunestohyökkäys, joka esiintyy 6 kertaa. Toiseksi yleisimpiä ovat erilaiset vakoilutapaukset, joita on ainakin 3 kappaletta, tosin eri toteutustavoilla. Ulkoministeriön vuoden 2025 tietomurrosta ei vielä tiedetä tarpeeksi, joten sitä ei ole laskettu tähän mukaan. Havaitaan, että merkittävien kansainvälisten kyberhyökkäysten listalle on Suomen julkista sektoria koskien päätynyt useita tapauksia (CSIS 2025).

Suomen ulkoministeriöön kohdistui vieraiden valtioiden suorittamaa vakoilua, joka havaittiin vuonna 2013. Suojelupoliisi kuvailee hyökkääjää erittäin edistyneeksi ja vaikeasti havaittavaksi. Tapauksia tutkittiin vakoiluna ja törkeänä vakoiluna. (Hiltunen 2014) CSIS (2025) väittää, että Suomen ulkoministeriö olisi havainnut vuonna 2016 neljä vuotta kestäneen tietomurron. Tästä ei löydy lisätietoa ja vaikuttaisi, että tämä tieto on virheellinen ja että tämä liittyy vuonna 2013 ulkoministeriöön kohdistuneeseen tietomurtoon ja vakoiluun. Tässä lienee kysymys virheellisestä vuosiluvusta, sillä silloinen ulkoministeri Erkki Tuomioja kertoi vuonna 2013 ulkoministeriön vakoilun kestäneen neljä vuotta (Rajamäki 2013). Tämä korostaa tarvetta tapahtuneiden kyberhyökkäysten paremmalle raportoinnille, tilastoinnille ja julkaisulle esimerkiksi suomalaisten viranomaisien tai Kyberturvallisuuskeskuksen toimesta, jotta luotettavaa ja oikeellista tietoa tapahtumista olisi saatavilla.

Suomen ulkoministeriön työntekijöiden puhelimiin kohdistui vuosina 2021–2022 kybervakoilua kaupallisella Pegasus-vakoiluohjelmalla. Pegasuksen avulla hyökkääjä on mahdollisesti saanut haltuunsa julkista ja alimman turvaluokitustason tietoa. (Ulkoministeriö 2022) Pegasus-vakoiluohjelmaa myydään ainoastaan valtiollisille tahoille ja hyökkääjä on todennäköisesti myös ollut valtiollinen taho (STT 2022).

Suomen ulkoministeriöön kohdistui vuonna 2025 epäilty törkeä tietomurto, jossa etäyhteyspalvelussa oli poikkeavaa toimintaa (STT 2025). Suuriin suomalaisiin kaupunkeihin kohdistuneen palvelunestohyökkäyksen kohteena oli myös Suomen Pankki (Hanhinen et al. 2024). Vuonna 2016 valtionhallintoon kohdistui palvelunestohyökkäys, jonka kolme epäiltyä poliisi pystyi tunnistamaan (Poliisi 2016). Julkiseen hallintoon sekä suomi.fi palveluun kohdistui vuonna 2018 palvelunestohyökkäyksiä, joista epäillyn poliisi pystyi tunnistamaan (Poliisi 2018). Eduskuntaan vuosina 2020–2021 kohdistunutta APT-hyökkäystä tutkitaan törkeänä vakoiluna, törkeänä tietomurtona ja törkeänä viestintäsalaisuuden loukkauksena (Poliisi 2021).

Havaitaan, että Suomen kunta- ja julkiseen sektoriin on kohdistunut säännöllisesti kyberhyökkäyksiä. Julkiseen sektoriin kohdistuneita kyberhyökkäyksiä kuntiin kohdistuneista erottaa esille tulleiden vakoilutapausten määrä, joissa hyökkääjänä on ollut valtiollinen taho. Havaitaan, että sekä kuntien että valtionhallinnon kohdalla tietyt organisaatiot, kuten ulkoministeriö ja Lahden kaupunki, toistuvat löydettyissä tapauksissa useamman kerran. Voidaan pohtia, johtuuko tämä niiden hallinnoimien asioiden ja tietojen kiinnostavuudesta, siitä että ne ovat olleet kyberturvallisesti haavoittuvia vai siitä, että ne ovat noudattaneet muita organisaatioita avoimempia tiedotuskäytäntöjä.

Ulkoministeriö on kuvaillut siihen kohdistuneita kybertapahtumia jokseenkin vähättelevästi, ”laittomalta tiedustelulta ei voida suojautua täysin” (Ulkoministeriö 2022) ja vuoden 2025 epäilyssä törkeässä tietomurrossa ulkoministeriö oli käyttänyt tietoisesti haavoittuvaa etäyhteyspalvelinta ja ainoastaan lisännyt sen valvontaa (STT 2025). Voidaan pohtia, onko tällainen suhtautuminen ja varautumisen taso kyberturvallisuudessa yleistä myös muualla Suomen julkisella sektorilla, mikäli näin merkittävän ja kriittisen toimijan toiminnan taso on edellä kuvatun kaltaista.

Osissa tapauksissa kyberhäiriötilanteet ovat olleet niin laajoja, että ne ovat näkyneet organisaatiosta ulospäin esimerkiksi verkkosivujen toimimattomuuden vuoksi, jolloin asian piilottelu ei olisi ollut mahdollista. Voidaan pohtia, myös regulaation merkitystä tähän. Suomen kuntia ja julkista sektoria kohtaan tapahtuneita kyberhyökkäyksiä tarkasteltaessa on hyvä havaita, että vaikka erityyppisiä hyökkäyksiä on tapahtunut, ilmi tulleiden hyökkäysten ja niistä jaetun tiedon määrä on suhteellisen rajallinen. Tämä saattaa aiheuttaa virhepäätelmiä, jos tämän perusteella aiheen tarkastelu kohdistuisi ainoastaan edellisen kaltaisiin tapauksiin, sivuuttaen muut mahdolliset hyökkäystavat ja uhat. Tämän takia ulkomaisen lähdeaineiston tarkasteleminen olisi myös hyödyllistä.

5. KUNTIEN KYBERTURVALLISUUDEN HAASTEET JA RATKAISUT

5.1 Kyberturvallisuuden haasteet

5.1.1 Kyberturvallisuuden haasteet Ruotsissa, Norjassa ja Yhdysvalloissa

Aineistossa kuntiin kohdistuneita kyberturvallisuuden haasteita Ruotsin, Norjan ja Yhdysvaltojen kuntien kohdalta. Taulukossa 6 esitellään aineiston perusteella tunnistettuja kyberturvallisuuden haasteita ulkomailta Hossain et al. (2024) esittämien kategorioiden mukaisesti, jotka on esitelty alaluvussa 2.2.

Taulukko 6. *Kyberturvallisuuden haasteet kategorioittain Ruotsin, Norjan ja Yhdysvaltojen kunnissa*

| Kategoriat | Kyberturvallisuuden haasteet |
|------------------------------|---|
| Tekniset ja operatiiviset | – Datan jakamisessa on epäselvyyksiä ja virheitä (Caldarulo et al. 2024) |
| Vastuu ja käyttäytyminen | – Haluttomuus jakaa tietoa tietoturvatapahtumista (Andreasson et al. 2024) – Kyberturvallisuudesta ei oteta vastuuta (Norris et al. 2024) – Kansalaisten organisaatioon kohdistamat paineet (Preis & Susskind 2021) – Yhteisen kielen puute muiden kuin IT-alan ihmisten kanssa (Skjelvik & Verkstad 2023) |
| Politiikka ja sääntely | – Standardeita ei noudateta (Magnusson et al. 2023) – Johtajat eivät ymmärrä perusteita kyberturvallisuudesta (Norris et al. 2024) |
| Resurssit ja infrastruktuuri | – Riittämättömät resurssit (Norris et al. 2024) |

Taulukosta 6 voidaan havaita, että suurin osa tunnistetuista haasteista sijoittuu vastuun ja käyttäytymisen kategoriaan. Ruotsissa kuntien kyberturvallisuuden haasteiksi on tunnistettu, että tietoturvaluus on muodostunut liian monimutkaiseksi pienille organisaatioille. Kyseisissä organisaatioissa on keskitytty ainoastaan ISO/IEC 27001 -standardin vähimmäisvaatimusten täyttämiseen. (Magnusson et al. 2023) Kyseisessä standardissa on tietoturvaluuden hallintajärjestelmään liittyviä vaatimuksia sen suunnittelun, toteuttamisen, ylläpidon ja kehittämisen suhteen (SFS Suomen Standardit n.d.) Ruotsin kunnista ainoastaan 6 % läpäisi tietoturvatarkistuksen täysin, 28 % osittain, 34 % ei läpäissyt tätä ja 31 % tarkistuksista ei ollut saatavilla tietoja. Ruotsalaisten maakuntien tietoturva oli tarkistusten mukaan parempi kuin kunnilla. Muista Pohjoismaista ainoastaan Norjasta löytyi kahden julkisen toimijan tietoturvatarkastuksen tulokset, kun taas Ruotsissa vastaavia tarkastuksia oli tehty 62 kunnassa ja 10 maakunnassa. (Magnusson et al. 2023) Vastaavan tarkastustiedon saaminen suomalaisista kunnista olisi hyödyllistä niiden tutkimukselle, huomioiden kuitenkin, että kuntien turvallisuutta ei tällä vaarannettaisi. Ruotsissa on havaittu, että 71 % kunnista vastuu kyberturvallisuudesta on henkilöllä, joka tekee kyberturvallisuuden töitä muun työn ohessa (Andreasson et al. 2021).

Yhdysvalloissa paikallishallinnon kyberturvallisuushaasteiksi on tunnistettu liian vähäiset investoinnit, parhaita työkaluja ei ole otettu käyttöön, koulutusta ei ole tarjottu tarpeeksi, sopivimpia kyberturvallisuuspolitiikkoja ei ole otettu käyttöön ja parhaita käytäntöjä ei ole noudatettu. Lisäksi teknologia, käytännöt ja politiikka olivat vanhentuneita. Tämän lisäksi kyberpoikkeamien määrää ei tiedetty ja ylin johto ei tuntenut kyberturvallisuuden vaatimuksia. Päättävät henkilöt tarjosivat liian vähän resursseja kyberturvallisuuteen eivätkä ottaneet siitä vastuuta. (Norris et al. 2021) Yhdysvalloissa 55,14 % paikallishallintoihin kohdistuneista kyberuhista on tietomurtoja ja 20,12 % tahattomia tiedon paljastumisia (Kesan & Zhang 2021). Yhdysvaltojen paikallishallinnossa päättävät henkilöt eivät ota vastuuta kyberturvallisuudesta, vaikka se kuuluisi heille aseman mukaan, vaan kyberturvallisuus nähdään pelkästään tietohallinnon asiana. Kyberturvallisuuden asiantuntijat eivät pääse vaikuttamaan tarpeeksi budjetointiin ja resurssien ohjaamiseen, vaan joutuvat toimimaan usein riittämättömien resurssien varassa. Vastuun kantaminen eroaa yksityisestä sektorista, jossa toimitusjohtaja ja yhtiön hallitus kantavat lopullisen vastuun toiminnasta. (Norris et al. 2024)

Organisaatiot eivät välttämättä tunnista omia heikkouksiaan kyberturvallisuuden suhteen ennen kuin ne kohtaavat kyberhyökkäyksen. Laajamittainen paikallistasoon kohdistuva uutiskynnyksen ylittävä kyberhyökkäys aiheuttaa johtajille paineen toimia asian suhteen. Tällaisissa tilanteissa kyberturvallisuuteen kiinnitetään huomiota ja sen parantamiseen suunnataan resursseja (Norris et al. 2024) Paikallishallintoihin kohdistuvat poliittiset,

lainsäädännölliset ja eettiset paineet saattavat vaikeuttaa kyberturvallisuuden toimintaa verrattuna yrityksiin, joilla voi olla vähemmän näitä rajoitteita (Preis & Susskind 2021).

5.1.2 Kyberturvallisuuden haasteet Suomessa

Tarkastellaan kyberturvallisuuden haasteita Suomessa. Taulukossa 7 esitellään aineiston perusteella tunnistettuja kyberturvallisuuden haasteita Suomessa, Hossain et al. (2024) esittämien erilaisten kategorioiden perusteella jaoteltuna.

Taulukko 7. *Kyberturvallisuuden haasteet kategorioittain Suomessa*

| Kategoriat | Kyberturvallisuuden haasteet |
|------------------------------|---|
| Tekniset ja operatiiviset | – Mittarien puute (DVV 2023) |
| Vastuu ja käyttäytyminen | – Johto ei ymmärrä tai sitoudu (DVV 2021) – Tiedon jakaminen on heikkoa (Paananen et al. 2024 s. 21–22) |
| Politiikka ja sääntely | – Selkeiden prosessien puute (DVV 2023) – Lainsäädännön rajoitteet tiedonvaihdolle (Paananen et al. 2024 s. 33–34) |
| Resurssit ja infrastruktuuri | – Osaamisen puute (DVV 2021) – Eroavaisuudet resurssien suhteen (Paananen et al. 2024 s. 18) |

Suomen kunnilla on keskimäärin valtion- ja aluehallintoa heikompi kyberturvallisuuden taso. Eri kuntien välillä on havaittu olevan eroja resurssien suhteen. (Paananen et al. 2024 s. 18) Suomessa on ongelmia viranomaisten välisessä kommunikaatiossa ja sääntelyssä kyberuhkien torjunnassa. Kyberturvallisuustietoja ei jaeta tehokkaasti eri toimijoiden välillä. Kansallisesta kyberturvallisuuden tilannekuvasta vastaa Kyberturvallisuuskeskus tehden yhteistyötä muiden tahojen kanssa. (Paananen et al. 2024 s. 21–22) Puolustusliitto Nato asettaa vaatimuksia Suomen resilienssille, mikä puolestaan vaikuttaa myös kansalliselle kyberturvallisuuden resilienssin kehittämiseen. Tiedonvaihto on tunnistettu hyvin tärkeäksi osa-alueeksi kyberturvallisuudessa. Nykyisellään lainsäädäntö ja muut rajoitteet estävät tehokasta tiedonvaihtoa ja niiden muuttamista on ehdotettu. Lisäksi aiheeseen liittyviä laintulkintoja on ehdotettu yhdenmukaistettavaksi. (Paananen et al. 2024 s. 33–34)

Suomen kunnissa on havaittu, että organisaation ylimmässä johdossa ei ole tietohallinnon tai tietoturvan asiantuntijoita, eikä johto ymmärrä tietoturvasta tai sitoudu siihen. 80 % edelläkävijäkuntien mukaan heillä ei ollut tarpeeksi osaamista organisaatiossa. (DVV 2021) Kuntien kohdalla erityiseksi ongelmaksi oli digitaalisen turvallisuuden mittarien puute. Selkeiden prosessien ja toimintamallien puute oli tunnistettu. Kunnat olivat arvioineet kyberturvallisuustilanteensa paremmaksi kuin hyvinvointialueet. (DVV 2023) Tämä eroaa Magnusson et al. (2023) tutkimuksesta Ruotsissa, jossa havaittiin maakunnilla parempi tietoturvan taso kuin kunnilla. On kuitenkin huomioitava, että Suomen kohdalla kyse oli itsearvioinnista. Kyberturvallisuuden puutteeksi oli myös kirjattu negatiivisilta vaikuttamiskampanjoilta varautumisen, jonka arvioitiin olevan kaikista heikoimmalla tasolla (DVV 2023), mutta voidaan pohtia kuuluisiko se jonkin toisen kategorian alle. Kyberturvallisuutensa suhteen kunnat arvioivat tilanteensa vuonna 2023 paremmaksi kuin vuonna 2021 (DVV 2023).

5.1.3 Tiedon jakaminen ja siiloutuminen

Useissa lähteissä (Ring 2014; Preis & Susskind 2022; Skjelvik & Verkstad 2023; Andreasson et al. 2024; Paananen et al. 2024 s. 33) tiedon jakaminen nousee esiin keskeisenä kyberturvallisuuden haasteena ja tärkeänä kehityskohteenä sekä Suomen että ulkomaiden kohdalla ja siksi sitä käsitellään muita haasteita perusteellisemmin. Yhdysvalloissa paikallishallintojen asiantuntijoilla ei välttämättä ole halua vastata kyberturvallisuuden ongelmia koskeviin tutkimuksiin, sillä he pelkäävät, että tiedon jakaminen voisi vaarantaa organisaation turvallisuuden (Norris et al. 2021). Ruotsin julkisen sektorin tutkimuksessa havaittiin myös haluttomuutta jakaa tietoa tapahtuneista tietoturvatapahtumista. Syynä tähän pidettiin tiedon salassapitoa tai pelkoa ammatillisen maineen menettämisestä. (Andreasson et al. 2024) Tässä voi havaita ongelman tiedon jakamisessa ja tutkimuksen tekemiselle. On syytä pohtia, koskeeko haluttomuus jakaa tietoa tapahtuneista häiriöistä ainoastaan tieteellisiä tutkimuksia vai koskeeko tämä myös luottamuksellisia tiedon jakamis- ja yhteistyöverkostoja. Olisiko tutkimuksen suorittajan pystyttävä todentamaan henkilöllisyytensä ja tarkoituksensa, jotta tätä ei sekoitettaisi vihamieliseen tietojenkalasteluun?

Suomessa on perustettu ISAC-tiedonvaihtoryhmiä, joiden avulla eri organisaatiot voivat jakaa tietoa kyberuhista kustannustehokkaasti. Esimerkiksi kunnilla on käytössä KUNTA-ISAC-tiedonvaihtoryhmä. (Kyberturvallisuuskeskus 2025) Tiedonvaihtoryhmissä voidaan myös jakaa sektorikohtaista- ja kybertyökalutietoa sekä mahdollistaa verkostoituminen (Norris et al. 2024). Ruotsin kuntasektorilla 83 % vastaajista piti epävirallista ammattilaisten tiedonvaihtoa kyberturvallisuudesta hyödyllisenä ja tärkeänä (Andreasson et al. 2021). Ruotsissa hyödyllisimmäksi kybertiedon lähteeksi ilmoitettiin MSB-

valmiusvirasto (ruots. Myndigheten för samhällsskydd och beredskaps), kun taas Europolia ja ENISAA ei pidetty juurikaan hyödyllisinä. Ruotsin puolustusvoimien toimijoita pidettiin ainoastaan hieman hyödyllisinä. (Andreasson et al. 2021) Tästä voitaisiin päätellä, että kuntatoimijoille on tärkeää organisaatiolle ja kansallisesti kohdennettu kyberturvallisuustieto.

Yhdysvaltojen kunnissa tahattomia ja tahallisia kyberhäiriöitä aiheuttavat epäselvyydet ja huolimattomuudet datan jakamiskäytännöissä. Datan säännöllinen vastaanottaminen lisää riskiä haitallisille toimenpiteille tietojärjestelmää kohtaan. (Caldarulo et al. 2024) Kuntien päättäjiltä ja johtajilta saattaa puuttua perustaidot kyberturvallisuudesta, jolloin he eivät pysty johtamaan hyvin kyseisiä aiheita käsitteleviä ohjelmia (Norris et al. 2024).

Tieto organisaatioiden haavoittuvuuksista voi aiheuttaa mainehaittaa tai altistaa ne uusille uhille. Tietoturvaan liittyvän tiedon salaaminen haittaa aiheen tieteellistä tutkimusta. (Magnusson et al. 2023) Lahden kaupunki on tuonut kattavasti esille tietoa siihen kohdistuneesta kyberhyökkäyksestä, teknisiä yksityiskohtia ja hyökkäyspolkua myöden (Ollila 2021) ja se näin ollen näyttäytyy poikkeuksena.

Suomen kyberturvallisuuden strategisen johtamisen suhteen johtamisvastuut ovat epäselvät ja pirstaloituneet usealle eri toimijalle. Eri ministeriöt toteuttavat kyberturvallisuuden strategista johtamista omilla hallinnollisilla aloillaan siiloutuneesti. Ministeriöt tarkastelevat aihetta omasta näkökulmastaan eivätkä hahmota kyberturvallisuuden kokonaiskuvaa. Strategisen kyberturvallisuuden johtamiseen ei ole käytössä toimivaa yhteistyömekanismia. Nopeasti eskaloituvassa kyberhäiriötilanteessa toimijoiden valtuuksien pitäisi olla selkeitä ja toimijoiden välisen tiedonvaihdon tulisi olla toimivaa ja nopeaa. (Limnell & Lehto 2019) Myös kuntien kohdalla on havaittu tiedon siiloutumista (Lyly et al. 2021). Ihmiset voivat olla jakamatta kyberuhkatietoa oman organisaation sisällä ja tämä vaikeutuu entisestään, kun tietoa pitäisi jakaa organisaation ulkopuolelle (Ring 2014).

Yhteisen kielen ja ymmärryksen puute kyberturvallisuuden suhteen on tunnistettu ongelmaksi. Norjan kuntasektorilla on havaittu, että terveydenhuollon ja IT-alan ammattilaiset eivät pystyneet kommunikoimaan tehokkaasti keskenään ja syyksi tähän on esitetty erilaisia osaamisaloja. Työntekijöiden tulee oppia koko ajan uusia asioita, mutta oman alan ulkopuolisista asioista ajan tasalla pysyminen oman työn ohella on havaittu haasteelliseksi. (Skjelvik & Verkstad 2023) Myös Suomen kuntien kohdalla on havaittu, että keskustelu on asiantuntijoiden välistä, jonka ymmärtämiseen vaaditaan tietyn tason ymmärrystä aiheesta ja alan termistön tuntemista (Lyly et al. 2021). Tälle yhteisen kielen ja

ymmärryksen puutteelle haasteen aiheuttanee kyberturvallisuuden käsitteiden moninaisuus ja joissakin tapauksissa vaikea hahmotettavuus. Tässä voisikin nähdä tietojohdattamisen suhteen kiinnostavan kehityskohteen.

5.2 Kyberturvallisuuden kehittäminen

5.2.1 Kehittämisstrategiat

Tarkastellaan Suomessa julkaistujen kansallisten kyberturvallisuusstrategioiden julkaisuaikojia, pituuksia ja tekijöitä. Vuonna 2013 julkaistu kyberturvallisuusstrategia on 11 sivua pitkä, julkisen taustamuistion ollessa 24 sivua pitkä (Turvallisuus- ja puolustusasiain komitean sihteeristö 2013), vuoden 2019 strategia on 5 sivua pitkä (Turvallisuuskomitean sihteeristö 2019) ja vuosien 2024–2035 strategia on 42 sivua pitkä (Paananen et al. 2024). EU:n NIS2-direktiivi asettaa vaatimuksen tarkastella kansallisen kyberturvallisuusstrategian päivitystarpeita 5 vuoden välein, mutta päivityksiä voidaan tarpeen vaatiessa tehdä useammin (Paananen et al. 2024 s. 42). On kuitenkin huomioitava, että pelkkien sivumäärien tarkastelu ei yksinään kerro sisällön merkitteväydestä, vaan sisällön laatu on tätä tärkeämpää. Voidaan pohtia, onko vuoden 2019 strategian lisäksi olemassa jonkinlainen taustamuistio. Havaitaan, että Suomessa julkaisuväli on ollut lähellä tätä jo ennen NIS2-direktiivin julkaisua. Osaltaan Suomen julkisen sektorin kyberturvallisuuden muutosta kuvastaa se, että kyberturvallisuusstrategian on jokaisella keralla laatinut eri toimija.

Kyberturvallisuuden kehittämisohjelma käsittelee Suomen kyberturvallisuuden kehittämistä ja se on laadittu yhteistyönä useiden eri tahojen kanssa. Kehittämisohjelman päätaavoitteena on luoda kyberturvallisuuden ekosysteemi, joka tuottaa monenlaisia itseään vahvistavia positiivisia vaikutuksia. Kehittämisohjelmassa on tunnistettu tarve lisätä soveltuvien kyberturvallisuusosaajien koulutusta ja nykyisten työntekijöiden jatkokoulutusta. (Paananen 2021 s. 10–11) Julkisen sektorin ja elinkeinoelämän yhteistyön edistäminen on tunnistettu merkittäväksi mahdollisuudeksi, ja eri toimijoiden yhteistyötä pyritään lisäämään. Kehittämisohjelman toimeenpanosuunnitelmassa eri toimenpiteille on merkitty selkeät vastuutahot ja resurssoinnit. (Paananen 2021 s. 21) Kuntien ja hyvinvointialueiden kyberturvallisuuteen on tunnistettu tarvittavan nykyistä enemmän tukea (Paananen et al. 2024 s. 18).

Paananen et al. (2024 s.18) ei määrittele tarkasti kuntien ja hyvinvointialueiden kyberturvallisuuteen vaatimaa tukea, mikä tekee sen tarpeen ja määrän arvioinnista haastavaa. Kuten Ruotsin kuntien kohdalla on esitetty (Magnusson et al. 2023), Suomessakin olisi hyödyllistä tarkastella aihetta lukujen, auditointien ja tutkimusten avulla, jotta ongelman laajuudesta saataisiin parempi kokonaiskuva. Kyberturvallisuuden strategisessa

johtamisessa avainasemassa on toimiva lainsäädäntö, riittävät valtuudet, yhteydet poliittisiin päätöksentekijöihin, kyvykkyydet ja tietotaito sekä taloudelliset resurssit (Limnell & Lehto 2019). Tässä voikin nähdä selvän yhtäläisyyden Hossain et al. (2024) esittämien eri kyberturvallisuuden haasteiden kategorioiden suhteen.

Kuntien toiminnan jatkuvuuden, valmiuden ja varautumisen menettelyjen ajantasaisuus ja käyttö kyberturvallisuuden suhteen on vuoden 2024 kyberturvallisuusstrategian toteuttamissuunnitelmassa arvioitu tärkeimpien toimintojen joukkoon. Näiden huoltovarmuskriittisten alojen vaikutus on arvioitu erittäin suureksi ja kansallisesti merkittäväksi. Suunnitelmassa on myös ehdotettu paikalliskyberpuolustuksen liittämistä entistä paremmin paikallis- ja aluetason varautumiseen ja toimintaan. Kuntien reaktiokyvyn kyberhäiriötilanteisiin on otettu huomioon ja siihen on esitetty ratkaisuksi esimerkiksi riskienhallinnan, jatkuvan kehittämisen ja turvallisten hankintojen kehittämistä. Kuntien ja muun julkisen sektorin kyberturvallisuuden resurssien suunnittelu, seuraaminen ja hyödyllisimmällä tavalla kohdentaminen oli myös tunnistettu tärkeäksi. (Valtioneuvosto 2024b)

5.2.2 Auditoinnit ja sertifiointit

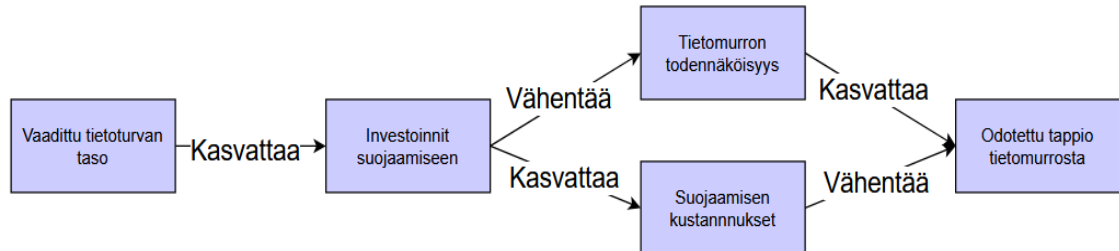
Sertifikaattien hankkimisen velvoittavuuden avulla voidaan ohjata toimintaa ja parantaa tietoturva, kun organisaatio joutuu täyttämään tietyt kriteerit. Suomen kunnissa on tehty vain vähän tietoturva-auditointeja, mikä on johtanut suuriin eroihin tietoturvallisuuden tasossa. Auditointi maksaa organisaatiolle sen laajuudesta ja yksityiskohtaisuudesta riippuen. Sertifiointin avulla voidaan mahdollisesti välttää organisaation toimintaa häiritseviä tapahtumia. (Lehtilä et al. 2021) Koska Suomen kuntien kontekstista ei löytynyt tarkastusten tuloksia hyödynnetään Ruotsin kuntia käsittelevää aineistoa.

Ruotsissa vain neljä kuntaa oli ottanut ISO/IEC-tietoturvamallin käyttöön, vaikka 22 oli päättänyt sen käyttöönotosta. Erityisesti tarkastuksissa havaittiin ongelmia käyttöoikeuksien ja pääsynhallinnassa. (Magnusson et al. 2023) Tämä korostaa ulkopuolisten vaatimusten ja tarkastusten merkitystä organisaation tietoturvallisuuden tasolle. Tulee huomioida, että sertifiointi ja auditointi eivät kuitenkaan yksin riitä, vaan tarvitaan myös muita ratkaisutapoja kuten Magnusson et al. (2023) ovat esittäneet.

5.2.3 Seuraamusmaksujen vaikutus toimintaan

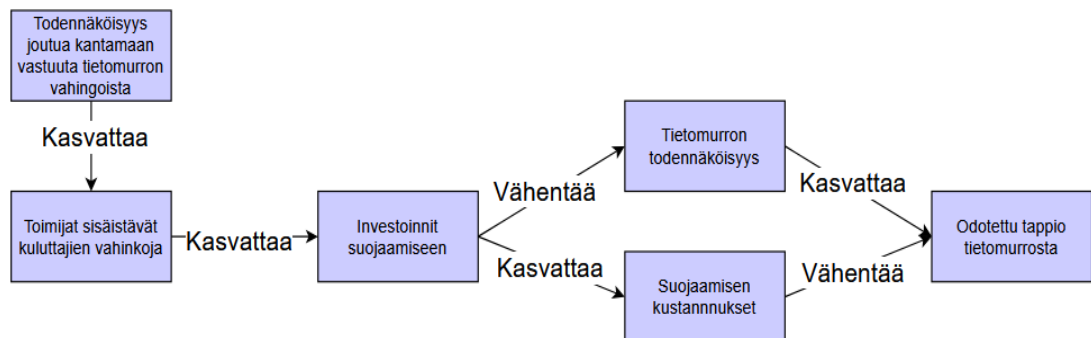
Tällä hetkellä julkisyhteisö tai uskonnollinen toimija ei voi Suomessa joutua maksamaan tietosuojarikkomuksesta GDPR:n mukaisia hallinnollisia seuraamusmaksuja (Tietosuojalaki 2018 4 luku 24 §). Sakkojen tulee olla tällaisissa tapauksissa tehokkaita, oikeasuhteisia ja varoittavia (EU 2016/679 artikla 83). Voidaan pohtia, onko tällaisessa tilanteessa ristiriita verrattuna yksityisiin yrityksiin, jotka voivat saada hyvin suuret seuraamusmaksut

ja ajautua tämän takia suuriin taloudellisiin vaikeuksiin tai jopa konkurssiin. Tarkastellaan aihetta sääntelyn näkökulmasta. Vaatimalla korkeampaa tietoturvan tasoa voidaan ohjata toimintaa ennaltaehkäisevästi (Lehtilä et al. 2021). Kuvassa 1 on kuvattu sääntelyn vaikutuksia tietoturvainvestointeihin ja niiden kustannuksiin. Nuolet kuvaavat vaikutussuhteita ja nuolen päällä olevat merkinnät vaikutuksen suunnan.



Kuva 1. Ennaltaehkäisevän sääntelyn vaikutus (Mukaiillen Romanosky & Acquisti 2009 s. 1069; Lehtilä et al. 2021)

Riski joutua vastuuseen tietomurron vahingoista kasvattaa organisaation halua torjua tätä riskiä ja näin ollen kannustaa investoimaan parempaan suojaamiseen. Jälkikäteistä sääntelyä voidaan toteuttaa myös valvonnalla ja sanktiomaksuilla, jos suojaamisen taso ei vastaa ennalta määrättyä. (Lehtilä et al. 2021) Kuvassa 2 on kuvattu jälkikäteisen sääntelyn vaikutuksia tietoturvainvestointeihin ja niiden kustannuksiin.



Kuva 2. Jälkikäteisen sääntelyn vaikutus (Mukaiillen Romanosky & Acquisti 2009 s. 1072; Lehtilä et al. 2021)

Romanosky & Acquisti (2009 s.1093) esittävät, että päätöksentekijöiden on huomattavasti helpompaa noudattaa ennalta määritettyä sääntelyä, kuin arvioida epävarmoja tietoturtoja ja niiden jälkeisiä korvauksia. Yksityishenkilölle datan vuotamisesta koituvat kustannukset voivat olla sekä rahallisia että psykologisia ja nämä seuraukset voivat olla yhdentekeviä tai elämää järkyttäviä (Romanosky & Acquisti 2009 s.1101). Näiden asioi-

den perusteella voidaan pohtia, olisiko seuraamusmaksujen uhka voinut ohjata esimerkiksi Suomen kuntasektorin toimijoiden investointeja tiedon suojaamisen parantamiseen ja näin ollen tämän avulla jotkin tietomurrot olisi saatettu mahdollisesti välttää.

5.2.4 Muut kyberturvallisuuden kehittämistavat

Kyberturvallisuus tarvitsee oman budjetin, jonka avulla pystytään ratkaisemaan resursseihin, kuten toiminnan rahoittamiseen sekä työntekijöiden palkkaamiseen ja kouluttamiseen liittyviä haasteita. Kyberturvallisuuspolitiikkojen käyttöönoton ja toteuttamisen avulla organisaatiolla on ohjeet tehokkaaseen ja turvalliseen toimintaan, mikä auttaa organisoimaan toimintaa järjestelmälliseksi. (Norris et al. 2024)

Tiedon siiloutumiseen liittyen on ehdotettu yhteisen tietovaraston luomista ja yhteistointarakenteen kehittämistä. Eri toimijoiden yhteinen tietovarasto voisi helpottaa suurten kyberhäiriöiden tiedon käsittelyä. Tämä mahdollistaisi tiedon analysoinnin eri toimijoiden kesken. Kybertilannekuvaan liittyen teknisiä ratkaisuja tulisi parantaa, ja niiden yhteiskäyttöä ja verkostopohjaista yhteistoimintaa tulisi lisätä. (Limnell & Lehto 2019). Yhdistyneessä kuningaskunnassa kyberuhkatiedonvaihtoryhmässä organisaatio voi päättää, haluaako se jakaa tiedon nimellään tai anonyymisti, ainoastaan viranomaisille, oman toimialan toimijoille vai kaikille tiedonvaihtoryhmässä oleville (Ring 2014).

Akateemiset toimijat voivat auttaa parantamaan paikallistason kyberturvallisuutta. Myös yliopistojen ja tutkijoiden yhteistyötä kuntien kanssa kyberturvallisuuteen liittyen on ehdotettu. Jotta yhteistyön avulla voidaan antaa syvällisiä parannusehdotuksia, yhteistyön pitää olla pitkäkestoista ja läheistä. Tutkimuksella voidaan parantaa sekä organisaatioiden resilienssiä että käytäntöjä. (Preis & Susskind 2021) Kyberresilienssiä voidaan kasvattaa harjoittelemalla kyberhäiriötilanteissa toimimista ja harjoituksia tulee kehittää vastaamaan todellista toimintaympäristöä. Harjoitustoiminnan avulla voidaan parantaa sekä yksilöiden että organisaatioiden osaamista ja valmiutta. (Paananen et al. 2024 s.30)

Julkisella sektorilla tarvitaan joustavampaa toimintaa ja avoimempaa tiedon vaihtoa ja kommunikaatiota. Investoinnit tietotekniikkaan auttavat vähentämään odotettua kyberhäiriön kustannusta. Pienten paikallishallintojen investoinnit tietotekniikkaan vähentävät kyberhäiriön odotettuja kustannuksia suhteessa vähemmän verrattuna suurten paikallishallintojen investointeihin. (Kesan & Zhang 2021)

DVV:n (2021) selvityksessä oli tunnistettu, että osa kunnista pystyy suorittamaan digitaalisen turvallisuuden hyvällä tasolla pienilläkin resursseilla. Selvityksessä myös tunnistettiin, että kaikkia edelläkävijäkuntia yhdisti tietosuoja- ja tietoturvaloukkausten hallintaa koskeviin harjoituksiin osallistuminen. Edelläkävijäkunnat myös hyödynsivät ulkoisia pal-

veluita. Selvityksessä on myös havaittu, että vuonna 2020 tapahtuneet negatiiviset tietoturvasuuteen liittyvät tapahtumat ovat vaikuttaneet toiminnan merkityksen korostumiseen. (DVV 2021) Tässä voi nähdä yhtymäkohdan Norris et al. (2024) esittämän negatiivisen tapahtuman vaikutuksen organisaation toiminnan tehostamiseen. DVV:n (2023) raportissa on esitelty erilaisia ratkaisutapoja ja kehitystapoja julkisen sektorin toimijoille. Siinäkin kaikkiin haasteisiin ei löydetty selkeitä ratkaisutapoja.

6. YHTEENVETO

6.1 Tutkimuksen tulokset

Työn tutkimuskysymys oli ”Mitä haasteita Suomen kunnilla on kyberturvallisuudessa, ja miten kyberturvallisuutta tulisi kehittää?”. Työn alatutkimuskysymykset olivat seuraavat:

- Mitkä ovat Suomen kuntien kyberturvallisuushaasteet, ja millaisia uhkia on realisoitunut?
- Millaisia kyberturvallisuushaasteita on tunnistettu toisissa maissa?

Työn tavoitteena oli tarkastella Suomen kuntien kyberturvallisuushaasteita ja millaisilla tavoilla kyberturvallisuutta voisi kehittää. Tutkimuksessa tunnistettiin erilaisia kyberhyökkäyksiä, jotka ovat kohdistuneet Suomen kuntiin ja julkiseen sektoriin. Kuntien osalta tarkasteltiin myös niiden kyberturvallisuuteen liittyviä haasteita ja mahdollisia ratkaisuja niihin.

Tarkastellaan ensimmäisen alatutkimuskysymyksen mukaisia Suomessa realisoituneita uhkia. Työssä havaittiin Suomen kuntien kohdistuneita raportoituja kyberhyökkäyksiä taulukon 4 perustella yhteensä 14 kappaletta, joista yleisimpänä oli tietomurto, joita oli 6 tapausta, sekä 1 törkeä tietomurto. Suomen julkiseen sektoriin havaitaan taulukon 5 perusteella kohdistuneen 10 tapausta, joista yleisimpiä olivat palvelunestohyökkäykset 6 tapauksella. Lisäksi tunnistettiin ainakin 3 tapausta, jotka liittyivät vakoiluun. Raportoiduista kyberhyökkäyksistä Suomen kunnissa tunnistettiin taulukon 4 perusteella muun muassa tietomurrot, kiristyshaittaohjelmat ja toimintaa häiritsevät palvelunestohyökkäykset. Raportoidussa kyberhyökkäyksissä julkisella sektorilla korostui vakavimmissa tapauksissa valtiollisten toimijoiden tekemät vakoilutapaukset, joiden kesto saattoi olla useita vuosia pitkä. Suomen kuntien kohdalla selkeästi valtiollisia toimijoita ei havaittu kuin mahdollisesti Säkylän tapauksen kohdalla. Suomalaiset viranomaiset nimesivät epäillyn tekijän selvemmin julkisen sektorin kuin kuntien tapauksissa. Osaltaan viranomaisten tiedottaminen oli vähäistä vakavistakin kyberhyökkäyksistä. Geopoliittisten jännitteiden kiristyessä ei voida todennäköisesti poissulkea valtiollisten tahojen kiinnostusta esimerkiksi kuntien hallussa olevaa tietoa tai kriittistä infrastruktuuria kohtaan. Osaltaan tapahtuneissa tietomurroissa voi olla hankalaa tunnistaa tekijää ja tämän motiivia. Joissakin tapauksissa viranomaiset ovat mahdollisesti voineet tunnistaa epäillyn, mutta eivät ole koskaan tiedottaneet asiasta. Yhdysvaltojen paikallishallintojen kohdalla suurin osa kyberhäiriöistä oli puolestaan tietomurtoja ja tahattomia tiedon paljastumisia väärille vastaanottajille (Kesan & Zhang 2021).

Ensimmäisen alatutkimuskysymyksen mukaan tarkastellaan Suomessa havaittuja kyberturvallisuuden haasteita. Suomen kuntien kyberturvallisuuden haasteiksi havaitaan resurssien puutteet, tiedon jakamisen puutteet, tiedon siiloutuminen toimialoittain, mitaamisen puutteet, selkeiden toimintamallien ja prosessien puutteet (DVV 2021; DVV 2023; Paananen et al. 2024 s. 18, 21–22, 33–34).

Toisen alatutkimuskysymyksen mukaisesti tarkastellaan ulkomaisissa kunnissa havaittuja kyberturvallisuuden haasteita. Ruotsin, Norjan ja Yhdysvaltojen kuntien kohdalla havaittiin haasteiksi kyberturvallisuudessa muun muassa resurssien puutteet, organisaatioiden johtajien puutteellinen ymmärrys kyberturvallisuudesta ja vastuun välttely siitä, standardien noudattamattomuus tai ainoastaan vähimmäistason täyttäminen, kommunikaation haasteet ja haluttomuus jakaa tietoa tietoturvatapahtumista (Magnusson et al. 2023; Skjelvik & Verkstad 2023; Andreasson et al. 2024; Norris et al. 2024). Ruotsin, Norjan, Yhdysvaltojen ja Suomen kuntien kyberturvallisuushaasteissa voidaan nähdä yhtäläisyyksiä erityisesti johdon heikossa tietämyksessä, resursseissa, kommunikaatiossa ja tiedon jakamisessa.

Tutkimuskysymyksen mukaisia kehittämistapoja tarkasteltaessa havaitaan, että Suomessa on laadittu useita kehittämisstrategioita kyberturvallisuuden suhteen ja niissä tunnistettu erilaisia kehittämistapoja. Selkeästi kuntiin kohdistuvia kehittämisohjelmia on julkisissa kehittämisstrategioissa vain vähän. Herää kysymys, ovatko kaikki strategiat julkisia vai onko kyseisillä sidosryhmillä lisää strategioita. Tarkastellaan kyberturvallisuuden mahdollisia kehittämistapoja Hossain et al. (2024) esittämässä kategorioissa taulukossa 8.

Taulukko 8. *Kyberturvallisuuden kehittämistapoja kategorioittain*

| Kategoriat | Kyberturvallisuuden kehittämistavat |
|------------------------------|---|
| Tekniset ja operatiiviset | <ul style="list-style-type: none"> – Investoinnit tietotekniikkaan (Kesan & Zhang 2021) – Yhteinen tietovarasto (Limnell & Lehto 2019) – Kyberuhkatilanteiden harjoittelu (Paananen et al. 2024 s.30) – Tieteellinen tutkimus, joka parantaa resilienssiä ja käytäntöjä (Preis & Susskind 2021) |
| Vastuu ja käyttäytyminen | <ul style="list-style-type: none"> – Yhteistyön lisääminen (Preis & Susskind 2021) |
| Politiikka ja sääntely | <ul style="list-style-type: none"> – Sertifiointit ja auditoinnit (Lehtilä et al. 2021) – Seuraamusmaksut (Romanosky & Acquisiti 2009; Lehtilä et al. 2021) – Kehittämisstrategiat |
| Resurssit ja infrastruktuuri | <ul style="list-style-type: none"> – Investoinnit tietotekniikkaan (Kesan & Zhang 2021) – Kyberturvallisuuden oma budjetti (Norris et al. 2024) |

Taulukon 8 perusteella havaitaan, miten eri kehittämistavat sijoittuvat eri kategorioihin suhteellisen tasaisesti. Tämän tutkimuksen perusteella vaikuttaisi siltä, että Suomen kuntien kyberturvallisuudessa tutkimuksen lisääminen olisi sellainen tapa, jolla pystyttäisiin tuottamaan aiheen käsittelyyn merkittävää lisäarvoa. Tutkimustoimintaa voitaisiin edistää niin akateemisen, kuin myös julkisen sektorin oman tutkimus- ja kehittämistyön suhteen.

6.2 Tulosten arviointi

Täsmällisesti Suomen kuntien kyberturvallisuuteen koskevaa aineistoa ei löytynyt kovinkaan paljoa, mikä osaltaan haittasi aiheen täsmällistä tarkastelua. Haasteen aiheutti myös eri organisaatioiden ja aineistoissa osin eroavat käsitteet. Raportoitujen kuntiin kohdistuneiden kyberhyökkäysten kohdalla tulee huomioida, että välttämättä kaikki ky-

berhyökkäykset eivät ole tulleet julkiseen tietoon. Osaltaan kyberhyökkäysten hakemisessa myös kyseisten tapausten otsikointi saattaa vaikuttaa hakutuloksiin. Vanhoissa tapauksissa verkkosivut ovat saattaneet myös muuttua ja tieto näin poistua. Näin ollen niissä esiintyvien organisaatioiden tuomitseminen kyberturvallisuudeltaan vastuuttomiksi on epäsuhtaista. Tässä tulee huomioida, ovatko omista kybervahingoistaan ilmoittaneet organisaatiot ainoastaan noudattaneet muita avoimempia tiedotuskäytäntöjä vai onko niihin kohdistuneet hyökkäykset olleet sellaisia, joita ei olisi ollut mahdollista salata. Tämän työn toteutukseen vaikutti se, että kyseisistä kyberhyökkäyksistä oli tietoa saatavilla. Raportoituja kyberhyökkäyksiä on Suomen kuntien suhteen kuitenkin suhteellisen vähän ja näistä yleistyksen tekeminen saattaisi aiheuttaa vääristymiä potentiaalisten kyberhyökkäysten todennäköisyyksien arvioinnissa.

Selkein vertailukohta tälle tutkimukselle on Hossain et al. (2024). Hossain et al. (2024) ovat pystyneet tunnistamaan hyvin laajasti erilaisia Yhdysvaltojen paikallishallintojen kyberturvallisuuteen vaikuttavia haasteita, ratkaisuja haasteisiin ja muita kyseisen toimintakentän erityispiirteitä. Jälkikäteen tarkasteltuna tämän työn kaltainen tutkimus olisi saattanut olla hyödyllisempi Hossain et al. (2024) esittämien asioiden jatkotutkimuksena, jolloin olisi tarkasteltu Hossain et al. (2024) havaitsemia asioita Suomen kuntien kontekstissa.

Ruotsin, Norjan ja Yhdysvaltojen kuntien tarkastelun rajautuessa Suomen kanssa suhteellisen samankaltaisiin maihin, niistä saatuja johtopäätöksiä voidaan pitää mielekkäinä. Osaltaan näiden tulosten hyödyntäminen oli tarpeellista johtuen muuten liian vähäisestä aineistomäärästä, jos tarkastelu olisi rajoittunut ainoastaan Suomeen. Työstä voisivat hyötyä aihetta työssään tai tutkimuksessaan käsittelevät henkilöt. Työstä löytyy listaus tapahtuneista kyberhyökkäyksistä yhdestä paikkaa, mitä ei aikaisemmin ollut, mikä puolestaan vähentää kyseisten henkilöiden työmäärää tapauksia ja niiden lähteitä etsittäessä.

6.3 Tarve jatkotutkimukselle

Jatkotutkimuksen tarpeiksi havaitaan empiirisen kyselytutkimuksen tekeminen Suomen julkisella ja kuntasektorilla toimivien IT- ja kyberturvallisuusammattilaisia koskien kyberturvallisuutta. Jatkotutkimuksen voisi myös toteuttaa erilaisista kyberturvallisuuden ennakointi- ja kehittämisstrategioista, koska niistä vaikutta olevan saatavilla ainoastaan vähän tietoa. Osaltaan tutkimusta voisi toteuttaa myös hyvinvointialueiden suhteen, koska ne ovat olleet olemassa vasta vähän aikaa ja verrata niiden kyberturvallisuuden tasoa esimerkiksi kuntiin tai valtionhallintoon.

Aihetta voitaisiin tarkastella myös kuntien hallinnassa olevaa kriittistä infrastruktuuria spesifisti koskien. Kriittisen infrastruktuurin tarkastelussa voitaisiin mahdollisesti verrata eroavaisuuksia kunnan ja yksityisessä omistuksessa olevien kohteiden välillä. Jatkotutkimuksena voisi myös selvittää kappaleessa 4.1 havaituilta kyberhyökkäyksen kohteeksi joutuneilta kunnilta kyberhyökkäyksen vaikutuksista kyselytutkimuksen avulla. Hyödyllistä olisi myös kyselytutkimuksen avulla selvittää, kuinka paljon tapahtuneita kyberhyökkäyksiä torjutaan ja jätetään ilmoittamatta eri kuntien kohdalta. Osassa ulkomaisessa aineistoissa aihetta oli tarkasteltu laajojen data-aineistojen ja regressiomallin avulla. Tällainen tarkastelu voisi olla myös hyödyllistä, jos kyseisen kaltainen laaja data-aineisto olisi tehty Suomen kuntien kyberturvallisuuden suhteen. Osaltaan myös tällaisen aineiston kerääminen olisi hyödyllistä tulevan tutkimuksen kannalta.

LÄHTEET

Andreasson, A., Artman, H., Brynielsson, J. & Franke, U. (2021). A Census of Swedish Public Sector Employee Communication on Cybersecurity during the COVID-19 Pandemic. 2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), pp. 727–733.

Andreasson, A., Artman, H., Brynielsson, J. & Franke, U. (2024). Cybersecurity work at Swedish administrative authorities: taking action or waiting for approval. *Cognition, Technology & Work*, Vol.26(4), pp. 709–731.

Caldarulo, M., Olsen, J. & Feeney, M.K. (2024). Oversharing: The downside of data sharing in local government. *Public Administration*, Vol.102(4), pp. 1647–1664.

CSIS. (2025). Significant Cyber Incidents. Saatavissa (29.4.2025): https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-02/250210_Cyber_Events.pdf?VersionId=mVS9NdLoTU7PuRE.O7eiNhj0INtYm8gQ

DVV. (2021). Kuntien digitaalisen turvallisuuden selvitys. Saatavissa (29.4.2025): <https://cdn.verkkopalvelu.suomi.fi/files/Raportti%20-%20Kuntien%20digitaalisen%20turvallisuuden%20selvitys-cad4e83611d047ae44f8f9d8a8b9b402.pdf>

DVV. (2023). Organisaation digiturvakysely. Saatavissa (29.4.2025): <https://dvv.fi/documents/16079645/110183105/Organisaation+digiturvakysely,+raportti+kev%C3%A4t+2023.pdf/f8bededb-4702-85d3-2623-fadd5096458d/Organisaation+digiturvakysely,+raportti+kev%C3%A4t+2023.pdf?t=1691566149881>

Euroopan unioni. (2016). Asetus EU 2016/679. Saatavissa (29.4.2025): <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A32016R0679>

Euroopan unioni. (2019). Asetus EU 2019/881. Saatavissa (29.4.2025): <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A02019R0881-20190607>

Euroopan unioni. (2022). Yleinen tietosuoja-asetus (GDPR). Saatavissa (29.4.2025): <https://eur-lex.europa.eu/FI/legal-content/summary/general-data-protection-regulation-gdpr.html>

Euroopan komissio. (n.d.) EU-lainsäädännön tyypit. Saatavissa (29.4.2025): https://commission.europa.eu/law/law-making-process/types-eu-law_fi

ENISA. (2024). ENISA threat landscape 2024: July 2023 to June 2024. Publications Office. Saatavissa (29.4.2025): <https://op.europa.eu/publication-detail/-/publication/e71394ea-85f0-11ef-a67d-01aa75ed71a1>

Halminen, L. (2024). Martti J. Kari: Käsikirjoitukset eivät pala. Jyväskylä. Docendo.

Hanhinen, H., Bogdanov, J. & Heikkilä, M. (2024). Venäläishakkerien palvelunestohyökkäykset sulkiivat usean kaupungin verkkosivut torstaina. Yle. Saatavissa (29.4.2025): <https://yle.fi/a/74-20072492>

Hannula, P. (2020). Vuosi sitten Lahdessa tapahtui jotain merkillistä ja koko kaupunki pysähtyi – näin taisteltiin miljoonavahingot aiheuttanutta tuntematonta hyökkääjää vas-

- taan. MTV Uutiset. Saatavissa (29.4.2025): <https://www.mtvuutiset.fi/artikkeli/vuosi-sitten-lahdessa-tapahtui-jotain-merkillista-ja-koko-kaupunki-pysahtyi-nain-taisteltiin-miljoonavahingot-aiheuttanutta-tuntematonta-hyokkaajaa-vastan/7839558>
- Hillamo, T. & Pesonen, J. (2022). Kuntien tietohallinnon roolit. Kuntaliitto. Saatavissa (29.4.2025): <https://www.kuntaliitto.fi/julkaisut/2022/2216-kuntien-tietohallinnon-roolit>
- Hiltunen, E. (2014). Supo: Ulkoministeriö joutui kaksi kertaa vakoilun kohteeksi. Yle. Saatavissa (29.4.2025): <https://yle.fi/a/3-7332824>
- Hossain, S.T., Yigitcanlar, T., Nguyen, K. & Xu, Y. (2024). Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework. Applied Sciences, Vol.14(13), pp. 5501-.
- Hyvärinen, S. & Parviainen, J. (2018). Kuntien tietotekniikkakartoitus 2018. Kuntaliitto. Saatavissa (29.4.2025): <https://www.kuntaliitto.fi/julkaisut/2018/1966-kuntien-tietotekniikkakartoitus-2018>
- Kesan, J.P. & Zhang, L. (2021). An Empirical Investigation of the Relationship between Local Government Budgets, IT Expenditures, and Cyber Losses. IEEE Transactions on Emerging Topics in Computing, Vol.9(2), pp. 582–596.
- Joensuu, J. (2019). Porin kaupunkiin kohdistunut tietomurto onkin odotettua vakavampi. Yle. Saatavissa (29.4.2025): <https://yle.fi/a/3-10916012>
- Lampinen, J. (2023). Verkkohyökkäyksen seurauksena puhelimet ovat pirisseet tavanomaista enemmän Vesannon kunnassa. Kuntalehti. Saatavissa (29.4.2025): <https://kuntalehti.fi/uutiset/tekniikka/verkkohyokkayksen-seurauksena-puhelimet-ovat-pirisseet-tavanomaista-enemman-vesannon-kunnassa/>
- Lehtilä, O., Nyström, P., Ronikonmäki, N.-M. & Sirviö, T.-H. (2021). Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla: Työryhmän loppuraportti. Liikenne- ja viestintäministeriön julkaisuja 2021:1. Saatavissa (29.4.2025): <https://julkaisut.valtioneuvosto.fi/handle/10024/162783>
- Limnell, J. & Lehto, M. (2019). The Importance of Strategic Leadership in Cyber Security: Case of Finland. Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019, Academic Conferences and Publishing International, pp. 288–296.
- Linnake, T. (2009). Hyökkäys kaatoi kuusi kuntaa verkosta. Taloussanomat. Saatavissa (29.4.2025): <https://www.is.fi/taloussanomat/art-2000001659031.html>
- Lyly, L., Kettunen, E., Salminen, A. & Lappalainen, A. (2021). Kuntien digitalisaatiokartoitus 2021. Kuntaliitto. Saatavissa (29.4.2025): <https://www.kuntaliitto.fi/julkaisut/kuntien-digitalisaatiokartoitus-2021>
- Kuntaliitto. (2023). Luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi. Saatavissa (29.4.2025): <https://www.kuntaliitto.fi/lau-sunnot/2023/luonnos-hallituksen-esitykseksi-kyberturvallisuusdirektiivin-nis2-direktiivi>
- Kyberturvallisuuskeskus. (n.d.a). Tietojenkalastelu ja identiteettivarkaudet verkossa. Saatavissa (29.4.2025): <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tietojenkalastelu%20ja%20identiteettivarkaudet.pdf>

Kyberturvallisuuskeskus. (n.d.b). NIS2 - Euroopan unionin kyberturvallisuusdirektiivi. Saatavissa (29.4.2025): <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi>

Kyberturvallisuuskeskus. (2025). ISAC-tiedonvaihtoryhmät. Saatavissa (29.4.2025): <https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/isac-tiedonvaihtoryhmat?toggle=Kunnat>

Kärkölen kunta. (2023). Tietomurto verkkosivujen palvelutuottajan palvelimelle. Saatavissa (29.4.2025): <https://karkola.fi/2023/12/22/tietomurto-verkkosivujen-palvelutuottajan-palvelimelle/>

Magnusson, L., Dalipi, F. & Elm, P. (2023). Cybersecurity Compliance in the Public Sector: Are the Best Security Practices Properly Addressed? HCI International 2023 Posters, vol. 1835, Springer, 2023, pp. 219–226.

Moliis, P. (2023). Rautavaaralla korjataan kyberhyökkäyksen jälkiä – hallinnon tiedostoja kryptattu, hyökkääjä vaati rahaa purkamisesta. Kuntalehti. Saatavissa (29.4.2025): <https://kuntalehti.fi/uutiset/tekniikka/rautavaaralla-korjataan-kyberhyokkayksen-jalkia-hallinnon-tiedostoja-kryptattu/>

Muuramen kunta. (2022). Kunnan palvelimelle tehtiin tietomurto. Saatavissa (29.4.2025): <https://www.muurame.fi/kunnan-palvelimille-tehtiin-tietomurto/>

NIST. (n.d.). Glossary - cybersecurity. Saatavissa (29.4.2025): <https://csrc.nist.gov/glossary/term/cybersecurity>

Norris, D.F., Mateczun, L., Joshi, A. & Finin, T. (2021). Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity. *Journal of Urban Affairs*, Vol.43(8), pp. 1173–1195.

Norris, D.F., Mateczun, L., Hatcher, W., Meares, W.L. & Heslen, J. (2024). Local government cyber insecurity: Causes and recommendations for improvement. *Public Administration Review*, Vol.84(4), pp. 651–659.

Ollila, K. (2021). Näin Lahti selvisi uhkaavasta kyberhyökkäyksestä – ”Juttu oli jo aika lailla housuissa”. *Tivi*. Saatavissa (29.4.2025): <https://www.tivi.fi/uutiset/nain-lahti-selvisi-uhkaavasta-kyberhyokkayksesta-juttu-oli-jo-aika-lailla-housuissa/bd987413-f328-469d-bf24-2320be92b778>

Onnettomuustutkintakeskus. (n.d.) Poikkeukselliset tapahtumat. Saatavissa (29.4.2025): <https://www.turvallisuustutkinta.fi/fi/index/tutkintaselostukset/poikkeukselliset-tapahtumat.html>

Onnettomuustutkintakeskus. (2024). Helsingin kaupungin tietomurto poikkeuksellisen laaja: riskien rajaamiseksi omien tietojen suojaaminen tärkeää. Saatavissa (29.4.2025): <https://turvallisuustutkinta.fi/fi/index/ajankohtaista/tiedotteet/2024/helsinginkaupungin-tietomurtopoikkeuksellisenlaajariskienrajaamiseksiomientietojensuojaaminenarkeaa.html>

Paananen, R. (2021). Kyberturvallisuuden kehittämisohjelma. Liikenne- ja viestintämisteriön julkaisuja 2021:7. Saatavissa (29.4.2025): <http://urn.fi/URN:ISBN:978-952-243-599-6>

- Paananen, R., Soikkeli M., Starck, M., Aro, M., Kuusisto, T., Rusila, T. ja Tuulensuu T. (2024). Suomen kyberturvallisuusstrategia 2024–2035. Valtionneuvoston kanslian julkaisuja 2024:11. Saatavissa (29.4.2025): <https://urn.fi/URN:ISBN:978-952-383-376-0>
- Poliisi. (2016). Kolmea epäillään palvelunestohyökkäyksistä viranomaisten verkkosivuille. Saatavissa (29.4.2025): <https://poliisi.fi/-/kolmea-epaillaan-palvelunestohyokkayksista-viranomaisten-verkkosivuille>
- Poliisi. (2018). Keskusrikospoliisi on saanut selvitettyä julkiseen hallintoon kohdistuneiden isojen palvelunestohyökkäysten epäillyn tekijän. Saatavissa (29.4.2025): <https://poliisi.fi/-/keskusrikospoliisi-on-saanut-selvitettya-julkiseen-hallintoon-kohdistuneiden-isojen-palvelunestohyokkaysten-epaillyn-tekijan>
- Poliisi. (2019). Edistyneet kiristysyökkäykset jatkuvat. Saatavissa (29.4.2025): <https://poliisi.fi/-/edistyneet-kiristysyokkaykset-jatkuvat>
- Poliisi. (2021). Poliisi jatkanut eduskunnan tietojärjestelmiin kohdistuneen tietomurron tutkintaa. Saatavissa (29.4.2025): <https://poliisi.fi/-/poliisi-jatkanut-eduskunnan-tietojarjestelmiin-kohdistuneen-tietomurron-tutkintaa>
- Poliisi. (2023). Vastaamo-tietomurron esitutkinta on valmistunut. Saatavissa (29.4.2025): <https://poliisi.fi/-/vastaamo-tietomurron-esitutkinta-on-valmistunut>
- Poliisi. (2024). Poliisi tutkii Helsingin kaupungin tietoverkon laajaa tietomurtoa. Saatavissa (29.4.2025): <https://poliisi.fi/-/poliisi-tutkii-helsingin-kaupungin-tietoverkon-laajaa-tietomurtoa>
- Preis, B. & Susskind, L. (2022). Municipal Cybersecurity: More Work Needs to be Done. *Urban affairs review*, Vol.58(2), pp. 614–629.
- Raivio, P. (2013). Ulkoministeriön tietomurto sai vauhtia valtion suojautumishankkeisiin. Yle. Saatavissa (29.4.2025): <https://yle.fi/a/3-6913949>
- Rajamäki, T. (2013). Tuomioja: Vakoilua on kestänyt neljä vuotta. *Helsingin Sanomat*. Saatavissa (29.4.2025): <https://www.hs.fi/politiikka/art-2000002686439.html>
- Rantala, K. (2023). Säkylän kyberhyökkäyksen takana jonkin valtion läheinen ammattiryhmä, kunnanjohtaja vaitonaisena: ”Me emme tee ulkopoliitiikkaa”. Yle. Saatavissa (29.4.2025): <https://yle.fi/a/74-20055949>
- Rantanen, A., Enlund, T., Korpelainen, L., Siltanen, M., Amonoo, H. and Degerman, R. (2024). Useiden kaupunkien verkkosivut kaatuivat tänäänkin – ainakin osassa taustalla venäläiset hakkerit. Yle. Saatavissa (29.4.2025): <https://yle.fi/a/74-20072640>
- Ring, T. 2014. Threat intelligence: why people don't share. *Computer fraud & security*, Vol.2014(3) pp. 5–9.
- Rita, M. (2025). KRP epäilee rikosta Helsingin kaupungin toiminnassa – poliisin arvio tietomurron uhrimäärästä ”laajassa haarukassa”. Yle. Saatavissa (29.4.2025): <https://yle.fi/a/74-20149294>
- Romanosky, S. & Acquisti, A. (2009). Privacy Costs and Personal Data Protection: Economic and Legal Perspectives. *Berkeley technology law journal*, Vol.24(3), pp. 1061–1101.

- Salminen, A. (2011). Mikä kirjallisuuskatsaus? johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasa. Vaasan yliopisto.
- Sanastokeskus TSK. (2018). Kyberturvallisuuden sanasto. Saatavissa (29.4.2025): https://sanastokeskus.fi/tsk/fi/kyberturvallisuuden_sanasto_tsk_52-1125.html
- Savonen, S. (2019). Hakkerit iskivät Suomessa, Siuntio varoittaa kalasteluviesteistä. Mikrobitti. Saatavissa (29.4.2025): <https://www.mikrobitti.fi/uutiset/hakkerit-iskivat-suomessa-siuntio-varoittaa-kalasteluviesteista/f34d558a-6486-4ce3-b44b-95ec3de26c4b>
- SFS Suomen Standardit. (n.d.). ISO/IEC 27000 Tietoturvallisuuden standardisarja. Saatavissa (29.4.2025): <https://sfs.fi/standardeista/tutustu-standardeihin/suosittut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/>
- Skjelvik, A. & Vestad, A. (2023). Digital safety alarms – Exploring the understandings of the cybersecurity practice in Norwegian municipalities. In Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference (EICC '23), pp. 129–133.
- Sosiaali- ja terveysministeriö. (2023). Hyvinvointialueet vastaavat sote-palvelujen ja pelastustoimen järjestämisestä. Saatavissa (29.4.2025): <https://stm.fi/hyvinvointialueet>
- STT. (2019a). KRP vahvistaa: Lahden tietojärjestelmän saastuttanut ohjelma on troijalainen, tekijä vielä epäselvä. Yle. Saatavissa (29.4.2025): <https://yle.fi/a/3-10833458>
- STT. (2019b). Lahden troijalaishyökkäys ei tullut yllätyksenä, sillä kuntien tietoturvassa on puutteita – "Joissain kunnissa piilee vakava peiliin katsomisen paikka". Yle. Saatavissa (29.3.2025): <https://yle.fi/a/3-10834466>
- STT. (2022). Tietoturva-asiantuntija: Suomalaisia diplomaatteja vakoiltu toisen valtion toimesta. Yle. Saatavissa (29.4.2025): <https://yle.fi/a/3-12293637>
- STT. (2025). Krp tutkii törkeää tietomurtoa ulkoministeriössä. Helsingin Sanomat. Saatavissa (29.4.2025): <https://www.hs.fi/suomi/art-2000011131252.html>
- Tammelin, J. (2021). Tietoturvastrategian ja -politiikan merkitys kyberhyökkäyksen torjunnassa kunnissa. Jyväskylän yliopisto.
- Tietosuoja laki. (2018). L 1050/2018. Saatavissa (29.3.2025): <https://finlex.fi/eli?uri=http://data.finlex.fi/eli/sd/2018/1050/ajantasa/2024-01-12/fin>
- TEPA Termipankki. (n.d). Tietomurto. Sanastokeskus. Saatavissa (29.3.2025): <https://termipankki.fi/tepa/fi/haku/tietomurto>
- Turvallisuuskomitean sihteeristö. (2019). Suomen kyberturvallisuusstrategia 2019. Turvallisuuskomitea. Saatavissa (29.4.2025): https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf
- Turvallisuus- ja puolustusasiain komitean sihteeristö. (2013). Suomen kyberturvallisuusstrategia 2013. Saatavissa (29.4.2025): <https://puolustusvoimat.fi/documents/2182700/0/Kyberturvallisuusstrategia/bb56d179-9b3a-4816-806d-84c84b04da30>
- Ulkoministeriö. (2022). Ulkoministeriö on saanut selvitettyä siihen kohdistuneen vakoilutapauksen. Saatavissa (29.4.2025): https://um.fi/tiedotteet/-/asset_publisher/ued5t2wDmr1C/content/ulkoministerio-on-saanut-selvitettya-siihen-kohdistuneen-vakoilutapauksen

Valio. (2025). Tietomurron kohteena aiempaa arviota suurempi määrä Valion Eläkekassan vakuutettuja. Saatavissa (29.4.2025): <https://www.valio.fi/uutiset/tietomurron-kohteena-aiempaa-arviota-suurempi-maara-valion-elakekassan-vakuutettuja/>

Valtioneuvosto. (2023). Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa. Valtioneuvoston julkaisuja 2023:31. Saatavissa (29.4.2025): <http://urn.fi/URN:ISBN:978-952-383-542-9>

Valtioneuvosto. (2024a). Kyberturvallisuudirektiivin kansallinen täytäntöönpano etenee: Hallitus esittää uutta kyberturvallisuuslakia. Saatavissa (29.4.2025): <https://valtioneuvosto.fi/-/1410829/kyberturvallisuudirektiivin-kansallinen-taytantonpano-etenee-hallitus-esittaa-uutta-kyberturvallisuuslakia>

Valtioneuvosto. (2024b). Kyberturvallisuusstrategian toimeenpanosuunnitelma. Saatavissa (29.4.2025): https://api.hankeikkuna.fi/asiakirjat/b9b35c4c-2719-4cfb-89fa-4388c855e2f0/c4785613-4037-43b5-b1cc-22d9b82c0d69/KIRJE_20241204070347.PDF

Valtiovarainministeriö. (n.d.). Kuntien tehtävät ja toiminta. Saatavissa (29.3.2025): <https://vm.fi/kuntien-tehtavat-ja-toiminta>

Yle. (2010). Tietomurto Espoon kaupungin palvelimella. Saatavissa (29.4.2025): <https://yle.fi/a/3-5514981>

Ylä-Tuuhonen, M. (2023). Säskylän kyberhyökkäys johtui ulkoisen palveluntuottajan vakavasta virheestä. Kuntalehti. Saatavissa (29.4.2025): <https://kuntalehti.fi/uutiset/teknikka/sakylan-kyberhyokkays-johtui-ulkoisen-palveluntuottajan-vakavasta-virheesta/>