Matti Mänttäri

VESIHUOLTOON KOHDISTUVAT KYBERUHAT 2020-LUVULLA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Mänttäri, Matti
Vesihuoltoon kohdistuvat kyberuhat 2020-luvulla
Jyväskylä: Jyväskylän yliopisto, 2024, 62 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Frantti, Tapio

Tämä tutkielma vastaa kysymykseen, mitä kyberuhkia vesihuoltoon on kohdistunut aikavälillä 1/2020–2/2024. Tutkimuskysymyksinä selvitettiin, mitä kyberuhkia vesihuoltoon kohdistui aikavälillä 1/2020–2/2024 ja miten niihin reagoitiin vesihuollosta vastaavien tahojen toimesta. Tutkimuksen aineistona käytettiin viranomaistahojen ja yksityisten toimijoiden raportteja, uutisia ja tiedotteita tapahtuneista kyberhyökkäyksistä 2020-luvulla. Aineisto analysoitiin teoriaohjaavasti teemoittelemalla.

Tutkielman teoriaosuudessa tarkasteltiin kyberuhkia sekä niiden uhkataksonomiaa ja uhkamallinnusta. Lisäksi tarkasteltiin Suomen vesihuollon kokonaisuutta sekä aiempia tutkimuksia vesihuollosta ja vesihuoltoon kohdistuneista kyberhyökkäyksistä. Aiemmat tutkimukset toivat esiin vesihuoltoon kohdistuvia uhkia, vesihuollon haavoittuvuuksia ja mitä vaikutuksia vesihuoltoon kohdistuneilla kyberhyökkäyksillä oli ollut. Vesihuolto on osa kriittistä infrastruktuuria. Vesihuollon järjestelmät ovat merkittävissä määrin kyberfyysisiä eli niissä tietokoneet ohjaavat toimilaitteita toteuttamaan jonkin fyysisen toimen, esimerkiksi veden pumppaamisen. Tämä altistaa vesihuollon järjestelmät erilaisille kyberuhille, jotka voivat onnistuessaan vaikuttaa merkittävästi vesihuollon toimintaan.

Tässä tutkielmassa selvisi, että vesihuoltoon kohdistuneita kyberuhkia aikavälillä 1/2020–2/2024 ovat olleet kiristysohjelmat, tietomurrot ja haittaohjelmat. Ne ovat kohdistuneet miltei jokaiseen vesihuollon osaan, mutta erityisesti vesihuoltolaitoksiin, vedenjakelujärjestelmiin sekä tietokantoihin. Ne eivät kuitenkaan pitkäaikaisesti kyenneet vaikuttamaan itse veden puhdistamisen ja jakelun toteutumiseen, mutta tietokantoihin kohdistuneet kyberuhat pahimmillaan lamauttivat niiden toiminnan jopa kuukausiksi.

Vesihuollosta vastaavien tahojen reaktio kyberhyökkäyksiin havaittiin koostuvan viidestä vaiheesta. Ensireaktiossa kyberhyökkäys yritettiin pysäyttää, vahinkoja pyrittiin välttämään ja toimintoja jatkamaan. Vahinkojen korjaaminen aloitettiin pikimmiten. Viranomaisia sekä mahdollisia asianomaisia tiedotettiin. Yhteistoiminta aloitettiin eri viranomais- sekä yksityisten tahojen kanssa tilanteen ratkaisemiseksi. Lopulta järjestelmiä ja kyberturvallisuustoimia pyrittiin parantamaan vesihuollosta vastaavissa organisaatioissa. Nämä vaiheet saattoivat kestää kuukausia tai jopa vuosia.

Asiasanat: vesihuolto, kyberuhka, kyberhyökkäys, kyberturvallisuus, uhka, vesi

ABSTRACT

Mänttäri, Matti
Cyber threats to the water supply in the 2020s
Jyväskylä: University of Jyväskylä, 2024, 62 pp.
Cyber Security, Master's Thesis
Supervisor: Frantti, Tapio

This master's thesis answers the question of what cyber threats were there to the water supply in the span of 1/2020 to 2/2024. The research questions answered as to what cyber threats were there to the water supply in the span of 1/2020 to 2/2024 and how did the parties responsible for the water supply respond to these threats. The material for this thesis utilized reports from authorities and private parties, news and publications about cyber attacks that had taken place in the 2020s. The material was analyzed by using theory guided thematic analysis.

The theoretical part of the thesis reviewed cyber threats as well as their threat taxonomy and threat modeling. In addition, the whole Finnish water supply was examined as well as previous studies about the water supply and cyber-attacks that had targeted the water supply. Previous studies presented threats against the water supply, vulnerabilities in the water supply and what effect the attacks against the water supply had. The water supply is a part of the critical infrastructure. The systems of the water supply are in significant amounts, cyber physical meaning that in them a computer guides an actuator to accomplish a physical task, for example the pumping of water. This predisposes the systems of the water supply to be vulnerable to different cyber threats that can, if successful, considerably affect the function of the water supply.

This thesis found that cyber threats that targeted the water supply in the span of 1/2020 to 2/2024 were ransomware, data breaches and malware. They targeted almost every section of the water supply but especially water treatment plants, water distribution systems and databases. However, they were not able to affect the water treatment nor distribution long term, but the cyber threats that targeted databases could at worst cripple their function for months.

The reaction to a cyber-attack from the parties responsible for the water supply was found to comprise of five phases. In the first reaction they tried to stop the cyber-attack, attempt to minimize damages caused, and continue their operations. Mending of damages begun as quickly as possible. Authorities and other relevant parties were informed. Co-operation began with different authorities and private parties to solve the issue at hand. Finally, attempts were made to improve the systems and cyber security measures in the organizations responsible for the water supply. These phases could last for months, even years.

Keywords: water supply, cyber threat, cyber-attack, cyber safety, threat, water

KUVIOT

TAULUKOT

SISÄLLYS

1 Johdanto

Kriittinen infrastruktuuri on yhteiskunnan selkäranka, sillä sen toimivuudelle rakentuu kaikki muu yhteiskunnan toiminta ja nykyaikana eri valtioiden ollessa riippuvaisia toistensa kriittisestä infrastruktuurista, myös kansanyhteisöjen toiminta (Hagelstam, 2005, s. 19). Kriittisen infrastruktuurin toimivuus itsessään ei ole kriittinen asia, vaan kriittistä on se toiminta, mitä yhteiskunnallista toimintoa kriittiseksi infrastruktuuriksi luetut alat mahdollistavat (Hagelstam, 2005, s. 17). Myös kriittisen infrastruktuurin eri alojen sisällä voi olla kriittisyydeltään eriarvioisia osakokonaisuuksia, tehden kriittisyyden arvioimisen varsin haastavaksi kokonaisuudeksi (Hagelstam, 2005, s. 17). Osa voi olla symbolisesti merkittäviä eli niillä voi olla roolistaan tai funktiostaan johtuen suuri tärkeys yhteiskunnalle, osa voi taas olla keskeisiä tai muiden järjestelmien yhtymäkohdissa sijaitsevia, tehden niistä teknisesti merkittäviä (Hagelstam, 2005, s. 17–18). Kriittisen infrastruktuurin järjestelmät myös ovat pitkälti riippuvaisia toisistaan, jolloin niiden suojaamisen suunnittelu eri osa-alueiden arvottamisen suhteen voi myös olla ongelmallista (Hagelstam, 2005, s. 18).

Kriittiseen infrastruktuuriin lasketaan kuuluvaksi eri kokonaisuuksia riippuen valtiosta tai yhteisöstä. Euroopan unioni on määritellyt kriittisen infrastruktuurin koostuvan yhdestätoista alasta. Nämä alat ovat: ”Energia, liikenne, pankkitoiminta, rahoitusmarkkinainfrastruktuuri, digitaalinen infrastruktuuri, juomavesi ja jätevesi, elintarvikkeet (tuotanto, jalostus ja jakelu mukaan lukien), terveydenhuolto, julkishallinto ja avaruus” (Euroopan parlamentti, 2022). Nimetyt alat on velvoitettu ilmoittamaan tapahtuneista vaaratilanteista ja häiriöistä viranomaisille, jotka taas ovat velvoitettu niistä julkisesti tiedottamaan (Euroopan parlamentti, 2022). Näihin häiriötekijöihin sisältyvät myös alojen kohtaamat kyberhäiriötilanteet.

Tutkielman rajaus on tehty sen kritiikin perusteella, jota kokonaisvaltaista riskienhallinnan lähestymistapa kyberturvallisuuteen on saanut. Kokonaisvaltainen riskienhallinta arvottaa kaikki toimijat saman arvoisiksi ja sen on koettu täten korostavan liian vähän kybertuvallisuuden tavoitetilaan kohdistuvia uhkia. (Muckin & Fitch, 2019; Walls ym., 2023) Riskienhallinta myös usein sisältää riskien siedettävyyden arvioinnin, joka ei kriittisen infrastruktuuriin kuuluvan

vesihuollon kanssa ole yksinkertaisesti mahdollista, sen toimimattomuuden ollessa sietämätön olotila kansalliselle turvallisuudelle ja hyvinvoinnille (Raggad, 2010, s.294–295; DHS, 2015, s. 6). Tutkielma rajautuu tarkastelemaan uhkia, sillä uhkien tunnistaminen ja tarkastelu ovat lähtökohta onnistuneeseen kyberturvallisuuteen, huolimatta niiden painoarvosta.

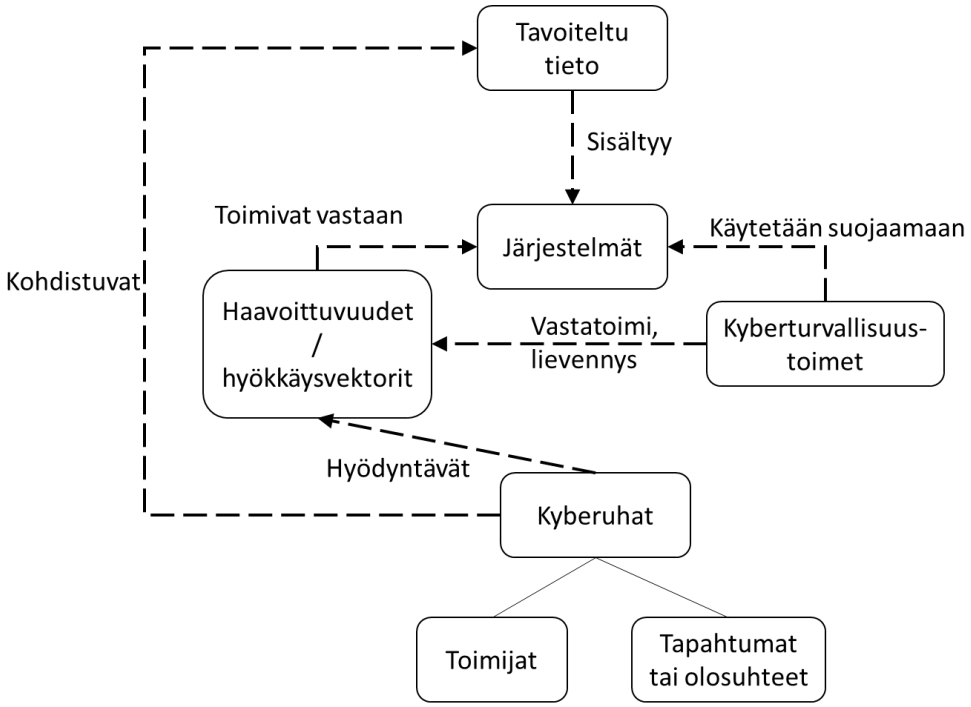
Tämä tutkielma keskittyy kahteen kriittisen infrastruktuurin osa-alueista: juomaveteen ja talousveteen, eli vesihuoltoon. Tutkielmassa tarkastellaan kyberuhkia, suomalaista vesihuoltoa ja sen kyberuhille alttiita osia sekä esitellään aikavälillä vuoden 2020 tammikuun alusta vuoden 2024 helmikuun loppuun (1/2020–2/2024) tapahtuneita vesihuoltoon kohdistuneita kyberhyökkäyksiä ja -uhkia. Lopuksi pohditaan, miten vesihuoltoon kohdistuviin kyberuhkiin on reagoitu ja miten niistä on toivuttu.

2 Kyberuhka

Kyberturvallisuus on ”tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan” (Turvallisuuskomitea, 2018, s. 22). Siihen kuuluvat erinäiset toimenpiteet, joilla ennakoivasti pyritään hallitsemaan sekä myös sietämään kyberuhkia ja niiden vaikutuksia (Turvallisuuskomitea, 2018, s. 22). Yksi yleinen toimenpide on riskienhallinta, jolla pyritään riskiympäristö määrittelemällä, riski tunnistamalla ja arvioimalla, siihen vastaamalla ja sitä tarkkailemalla hallitsemaan tietoturvaan kohdistuvia riskejä (NIST, 2012, s. 4–5). Kyberturvallisuudessa on keskitytty tarkastelemaan ja ratkaisemaan kyberuhkien muodostamat riskit seuraamalla esimerkiksi asetettuja standardeja, jotka toimeenpannaan käyttäen merkittävät määrät resursseja, mutta ilman uhkamallinnusta tai kunnollista operoinnin sekä analytiikan yhteensovittamista itse järjestelmien kanssa (Muckin & Fitch, 2019, s. 3). Tämä on johtanut siihen, että organisaatioihin voi syntyä valheellinen turvallisuuden tunne, kun turvatoimet on näennäisesti toteutettu ja niiden toimivuus on tarkastettu standardin toimeenpanon, eikä tehokkuuden avulla (Muckin & Fitch, 2019, s. 3). Resursseja on myös hukattu kyberuhilta suojautumiseen sellaisia uhkia vastaan, jotka eivät välttämättä kohdistu suojattuun organisaatioon (Muckin & Fitch, 2019, s. 3). Mainittujen ongelmien löytämiseksi ei myöskään ole tehty tarvittavia analyysejä tai tarkasteluja, joiden puute itsessään, yhdessä muiden ongelmien kanssa, nostaa organisaation riskiä joutua alttiiksi uhalle (Muckin & Fitch, 2019, s. 3). Hyvi n usein myös keskitytään yksittäisten haavoittuvuuksien paikkaamiseen ja etsintään, jolloin jätetään havainnoimatta suurempia uhkakokonaisuuksia, jotka saattavat kohdata organisaatiota (Muckin & Fitch, 2019, s. 3). Muckin & Fitch Lockheed Martinin vuonna 2019 (s. 3) julkaistussa tekstissään tuovat esiin heidän uhkalähtöisen tapansa hallita kyberturvallisuutta, joka nimensä mukaisesti arvottaa uhat tärkeimmäksi huomioitavaksi teemaksi kyberturvallisuuden suunnittelussa, toimeenpanossa ja käytössä.

Uhkalähtöinen kyberturvallisuus näkyy kyberturvallisuuden toimintavoissa ja ajattelutavassa, uhka ensin, jonka lopputuotteena on järjestelmä, joka täyttää asetetut standardit ja vaatimukset, mutta joka on lisäksi myös turvallinen järjestelmä (Muckin & Fitch, 2019, s. 4). Malli, joka toimii pohjana tälle lä-

hestymistavalle, korostaa uhkan merkitystä, sillä sen laatu ja käyttämät haavoittuvuudet tai hyökkäystavat ovat pohja sille minkälaisia kyberturvallisuustoimia on syytä käyttää järjestelmien ja tiedon suojana (Muckin & Fitch, 2019, s. 5–6; kuvio 1). Muckin & Fitch (2019, s. 6) esittävät täten, että kyberturvallisuustoimien on vastattava ensisijaisesti tunnistettuihin uhkiin, hyökkäysvektoreihin ja haavoittuvuuksiin, eikä sokeina vain suojata tietoa tai järjestelmää.

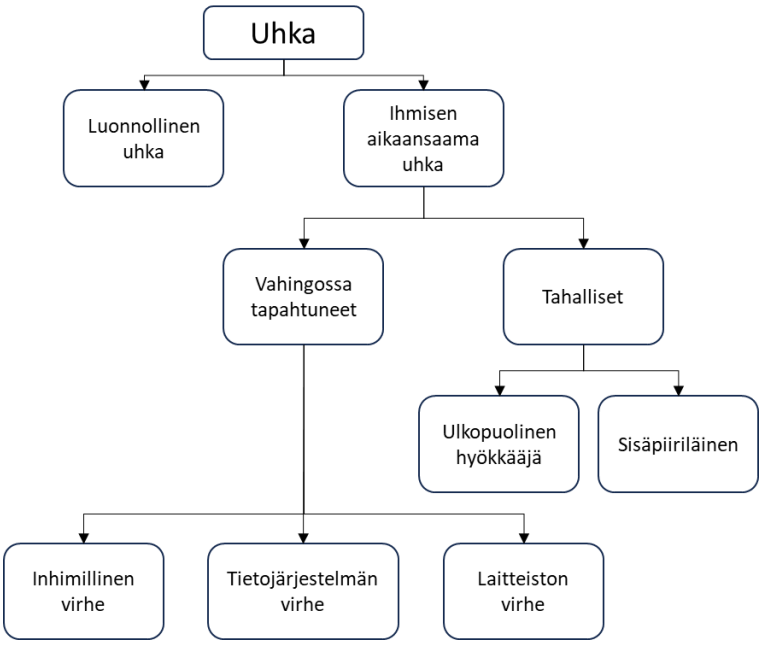


KUVIO 1 Uhkalähtöinen malli (Muckin & Fitch, 2019, s. 6)

2.1 Uhkataksonomia

Raggad esittää vuonna 2010 julkaistussa kirjassaan uhkataksonomian (kuvio 2; Raggad, 2010, s. 84) Hän jakaa uhat aluksi kahteen kategoriaan: luonnollisiin ja ihmisen aikaansaamiin (Raggad, 2010, s. 84). Luonnolliset uhat ovat esimerkiksi salamaniskut tai tulvat ja ihmisten aikaansaamat, nimensä mukaisesti, ihmisen joko tahallaan tai tahtomattaan aiheuttamia uhkia (Raggad, 2010, s. 84). Tutkimus keskittyy ihmisten aiheuttamiin uhkiin. Ihmisten tahattomasti aiheuttamat uhat voivat olla ihmisen virheestä tapahtuvia uhkia, kuten vahingossa tehty datan poistaminen tai järjestelmien ja pääsynhallinnan väärinkäyttö (Raggad, 2010, s. 84–85). Myös tietojärjestelmissä tai laitteistoissa voi olla vahingossa uhkia aiheuttavia virheitä, jotka voivat johtaa järjestelmien vaurioitumiseen tai tiedon katoamiseen (Raggad, 2010, s. 84–85). Ihmisen aikaansaamat tahallisesti aiheuttamat uhat voivat taas olla joko ulkopuolisten hyökkääjien esimerkiksi hakkereiden tai sisäpiiriläisten tekemiä (Raggad, 2010, s. 84–85). Ihmisen tahallisesti aiheutetut uhat ovat vaikutuksiltaan moninaisia ja voivat johtaa tiedon tai järjestelmien hetkelliseen lamautumiseen tai jopa järjestelmien tuhoutumi-

seen (Raggad, 2010, s. 83–85). Uhkia ei voi kuitenkaan tarkastella vain yksittäisenä tapahtumana, vaan ne hyvin voivat toteutuessaan aiheuttaa uhkien tapahtumisen jatkumon. Tästä esimerkkinä Raggad (2010, s. 84) kuvailee ukkosmyrskyn juuriuhaksi, josta johtuu sekundaarisena uhkana tulipalo, joka voi johtaa sähkön katkeamiseen, joka voi johtaa pakastimen toiminnan lakkaamiseen. Esitetty esimerkki koski luonnollisia uhkia, mutta voi hyvin tapahtua myös kybertoimintaympäristössä.



KUVIO 2 Uhkataksonomia (Raggad, 2010, s. 84)

Kyberhäiriötilanne on ”toteutunut kyberuhka, joka haittaa organisaation tai järjestelmän toimintaa” (Turvallisuuskomitea, 2018, s. 25). Kyberuhka taas on kybertoimintaympäristöön, eli yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuvaan toimintaympäristöön, kohdistuva haitallinen tapahtuma tai kehityskulku, joka toteutuessaan vaarantaa siitä riippuvaisen toiminnon (Turvallisuuskomitea, 2018, s. 21, 25). Kyberhyökkäykset ovat taas vihamielisten toimijoiden muodostamia uhkia, jotka pyrkivät hyväksikäyttämään eri haavoittuvuuksia, kuten kuviossa 1 on esitetty (NIST, ei pvm.). Toimijat voivat olla valtiollisia, rikollisia tai yksityisiä tahoja, joista yksityiset voivat olla tehtäväänsä palkattuja tai ideologisia haktivisteja (ENISA, 2023, s. 20). Haavoittuvuuden löydettyään vihamielinen toimija hyväksikäyttää sitä ja pyrkii vaikuttamaan järjestelmiin tai niissä oleviin tietoihin. Vihamieliset toimijoiden päämäärät tai tavoitteet voivat olla rahallisia, tiedustelua, häirintää, tuhoamista tai aatteellisia (ENISA, 2023, s. 17).

Pääasiallisesti Euroopan unionin alueelle kohdistuneet kyberuhat ovat olleet vuoden 2020 huhtikuusta vuoden 2023 kesään saakka kiristysohjelmia, haittaohjelmia, sosiaalinen manipulointia, tietomurtoja ja -vuotoja, palvelunestohyökkäyksiä, yhteyksien katkaisemista, tiedon manipulointia, toimitusketjuun kohdistuvia hyökkäyksiä, kryptokaappauksia ja ei-haitallisia uhkia (ENISA, 2021, s. 8–9; ENISA, 2022, s. 7–10; ENISA, 2023, s. 6–8). Kiristysohjelmilla on

estetty eri järjestelmien käyttö ja vaadittu lunnaita hallinnan palauttamisesta, kun taas haittaohjelmilla, jotka ovat luvattomia toimia tekeviä ohjelmia, on vaikutettu järjestelmien tai tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen (ENISA, 2023, s. 6). Hyödyntäen ihmisten inhimillisiä ominaisuuksia ja virheitä on manipuloinnilla myös päästy käsiksi rajoitettuun tietoon tai järjestelmiin (ENISA, 2023, s. 7). Tietomurrot ja -vuodot eroavat toisistaan käytännössä tapahtumatavan perusteella. Tietomurrot ovat vihamielisen toimijan tarkoituksen mukaisia toimia, kun taas tietovuodot ovat vahinkoja tai tuntemattomia haavoittuvuuksia, jotka johtavat tiedon joutumisen vääriin käsiin. (ENISA, 2023, s. 6) Palvelunestohyökkäykset ja yhteyksien katkaiseminen vaikuttavat molemmat tiedon saatavuuteen. Palvelunestohyökkäykset toimivat ylikuormittamalla halutun resurssin tai osan verkosta, kun taas yhteyksien katkaiseminen voi olla fyysistä kaapelien katkaisemista tai verkkojen osien sulkemista muusta internetistä. (ENISA, 2023, s. 6) Tiedon manipulointi on tarkoituksenmukaista väärän tiedon levittämistä, jolla pyritään vaikuttamaan arvoihin, toimintatapoihin ja poliittiseen toimintaan (ENISA, 2023, s. 6). Tiedon manipulointia voidaan kuvailla myös misinformaationa, joka on tahallisesti tai tahattomasti levitettyä levittäjän oikeaksi luulemaa väärää tai virheellistä tietoa, sekä disinformaationa, joka on taas nimenomaisesti tahallisesti levitettyä väärää tai virheellistä tietoa (ENISA, 2022, s. 9). Toimitusketjuun kohdistuvat hyökkäykset kohdistuvat organisaation ja tuottajan väliseen suhteeseen kohdistamalla hyökkäyksen molempiin osapuoliin (ENISA, 2023, s. 6). Kryptokaappaukset taas käyttävät hyödyksi haltuun saatua järjestelmää ja sen resursseja kryptovaluuttojen generoimiseen tai ”louhimiseen” (ENISA, 2021, s. 8). Lopuksi ovat ei-haitalliset uhat, jotka ovat pääasiassa vahinkoja tai virheitä, mutta joilla voi olla merkittäviä seuraamuksia järjestelmien toiminnalle (ENISA, 2021, s. 8). Kriittiseen infrastruktuuriin kuuluvan alan on oltava tietoinen ja varauduttava torjumaan siihen kohdistuvat kyberuhat, jos se haluaa pysyä toimintakykyisenä 2020-luvun kybertoimintaympäristön uhkien keskellä.

2.2 Uhkamallinnus

Uhkamallinnuksen tarkoitus on löytää järjestelmiin kohdistuvia uhkia, jotta niihin voidaan vastata ja ne torjua (Shostack, 2014, s. 3). Se mahdollistaa systemaattisen tavan tunnistaa ja raportoida järjestelmään kohdistuvia uhkia ja sen järjestelmän vahvuuksista (Xiong el al., 2021, s 158). Se myös mahdollistaa ongelmien havaitsemisen ajoissa, turvallisuusvaatimusten ymmärtämisen, parempien järjestelmien suunnittelemisen ja sellaisten ongelmien havaitsemisen, joita muilla tavoin ei välttämättä olisi voinut edes löytää (Shostack, 2014, s. xxiii–xxiv). Uhkamallinnus voi olla manuaalista tai automaattisoitua sekä se voi perustua matemaattisiin kaavoihin tai esimerkiksi graafisiin hyökkäyspuihin ja taulukoihin (Xiong el al., 2021, s 158). Valmiita malleja on erilaisia, kuitenkin niistä jokainen pyrkii tekemään järjestelmästä turvallisemman (Shostack, 2014; Khan ym., 2018; Fernandez, 2016). Rakennettaessa turvallista järjes-

telmää on ymmärrettävä nimenomaisesti siihen kohdistuvia uhkia, joita vastaan puolustautua, sillä yleisesti sopivat ja käytetyt tietoturvatoimet eivät välttämättä kata jokaiseen järjestelmään kohdistuvia uhkia (Fernandez, 2016, s. 1). Lisäksi on ymmärrettävä oman järjestelmän toimintaperiaatteet ja miten mahdollinen hyökkääjä voi hyödyntää niitä omien tavoitteidensa saavuttamiseksi (Fernandez, 2016, s. 1).

Oman järjestelmän ymmärtäminen onkin Shostackin (2014, s. xxviii) uhkamallinnusta käsittelevässä kirjassaan esittelemän neliportaisen prosessin ensimmäinen askel. On ymmärrettävä suojattavan järjestelmän kokonaisuus, sen osien vaikutus toisiinsa ja miten sen eri osista vaikutetaan toisiin sekä miten tieto näiden välillä liikkuu (Shostack, 2014, s. 5–7). Järjestelmät ovat erilaisia, saattaen pitää sisällään vain muutaman osan, kun taas muut järjestelmät saattavat olla merkittävästi monimutkaisempia (Shostack, 2014, s. 6; Khan ym., 2018, s. 5). Monimutkaisten järjestelmien tarkastelu ja niiden toimintojen kartoittaminen voi viedä tästä syystä merkittävästi kauemmin.

Seuraavalla Shostackin prosessin portaalla pohditaan ja etsitään asioita, jotka voivat mennä pieleen aiemmalla portaalla kartoitetussa järjestelmässä (2014, s. xxviii). Uhkia voi kartoittaa useilla eri tavoin ja hyödyntäen erilaisia valmiita uhkakirjastoja. Shostack (2014, s. 7–11) omassa prosessissaan esittelee korttipelin, jonka avulla järjestelmän eri osa-alueisiin kohdistuvia uhkia voidaan tarkastella ja analysoida. Hän myös hyödyntää uhkien tunnistamisessa STRIDE-menetelmää, joka pitää sisällään kuusi tietojärjestelmiin kohdistuvaa mahdollista huonosti menevää asiaa (Shostack, 2014, s. 9–11). STRIDE:n lisäksi on myös muita menetelmiä, kuten MITRE ATT&CK Enterpris Matrix, joka yksityiskohtaisena sisältää 12 eri hyökkäystaktiikkaa ja 266 hyökkäystekniikkaa, jotka voivat mahdollisesti kohdistua suojattavaan järjestelmään (Xiong el al., 2021, s 159–161). Oli valittu menetelmä mikä tahansa, sitä hyödyntäen ja tarkastellen joko järjestelmällisesti kohta kohdalta tai menetelmän mukaisesti kohta kohdalta, kyetään löytämään järjestelmään kohdistuvia erilaisia uhkia (Shostack, 2014, s. 11–12). On oleellista myös keskittyä realistisiin uhkiin sekä ottamaan kaikki mahdolliset uhat huomioon, olivatpa ne valitun menetelmän mukaisia tai eivät (Shostack, 2014, s. 12).

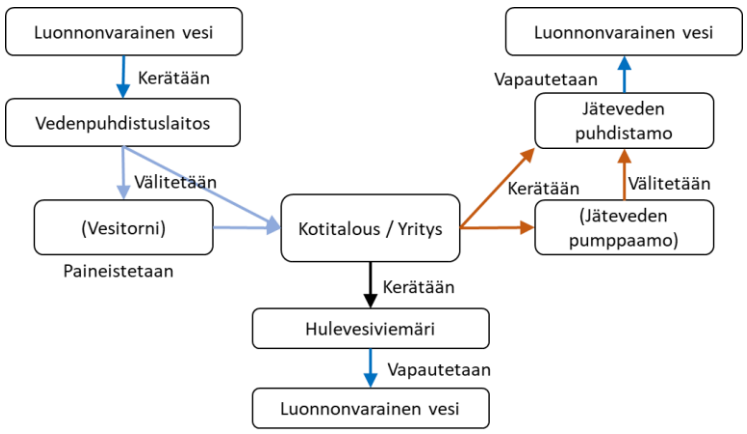
Prosessin aikana löytyneille uhille on tehtävä jotain, jotta järjestelmästä saadaan turvallisempi. Uhkia voidaan minimoida eli niiden hyödyntämistä voidaan vaikeuttaa. Esimerkiksi salasanan pituuteen liittyvää uhkaa voidaan minimoida vaatimalla vähintään kahdeksan merkkiä pitkä salasana. (Shostack, 2014, s. 12) Uhat voidaan mahdollisesti poistaa kokonaan, jos on esimerkiksi mahdollista päivittää järjestelmän osia turvallisempiin versioihin tai luopumalla jostain riskialttiista järjestelmän osasta (Shostack, 2014, s. 12–13). Uhat voidaan myös siirtää muiden vastuulle, kuten hankkimalla eri tietoturvaohjelmia estämään uhkia tapahtumasta tai vaatimalla käyttäjiä ymmärtämään heihin kohdistuvan uhkan mahdollisuuden, jos he eivät toimi turvallisella tavalla (Shostack, 2014, s. 13). Tietysti uhat voidaan yksinkertaisesti hyväksyä ja jättää huomioimatta esimerkiksi niiden torjumisen kalleuden vuoksi (Shostack, 2014, s. 13).

Shostackin (2014) prosessin lopussa tarkastellaan tehtyä uhkamallinnusta. Ensin tarkastellaan järjestelmästä tehtyä mallia tai kaavioita. Halutaan varmistua siitä, että malli tai kaavio on kattava, tarkka, päivitetty tehdyillä turvatoimilla ja että se varmasti kelpaa tulevaisuudessakin (Shostack, 2014, s. 24–25). Tämän jälkeen tarkastellaan havaittuja uhkia ja varmistutaan, että kaikki mahdolliset uhat on löydetty ja että löydetyille uhille on tehty oikea tai haluttu toimi niitä vastaan (Shostack, 2014, s. 25–26). Lopulta varmistetaan, että järjestelmän turvallisuutta varten tehdyt testit koettelevat järjestelmää oikeita uhkia vastaan ja oikeilla tavoin olivat sitten automaattisesti tai manuaalisesti toteutettavia (Shostack, 2014, s. 26).

Shostackin (2014) uhkamallinnuksen prosessi on yksi monista mahdollisista uhkamallinnuksen prosesseista, joita voidaan hyödyntää uhkien löytämiseen ja torjumiseen (Khan ym., 2018; Fernandez, 2016). Shostackin (2014) esittelemä uhkamallinnuksen prosessi keskittyy löytämään uhkia järjestelmän rakenteen kautta järjestelmäkeskeisesti. Järjestelmän rakenteeseen keskittymisen lisäksi uhkamallinnusta voi tehdä puolustettavan omaisuuden tai hyökkääjän näkökulmista (Shostack, 2014, s. 56–57). Omaisuuskeskeisessä uhkamallinnuksessa pohditaan sitä, mihin hyökkääjä haluaisi päästä järjestelmässä käsiksi, mitä me haluamme suojata järjestelmässä ja mitä muita asioita hyödyntäen hyökkääjä voi päästä käsiksi haluamaansa tai siihen, mitä me haluamme suojella (Shostack, 2014, s. 36–37). Hyökkääjäkeskeinen uhkamallinnus taas pyrkii luomaan profiileja mahdollisista hyökkääjistä ja heidän käyttämistään keinoista, joita vastaan puolustautua (Shostack, 2014, s. 40–41). Tätä lähestymiskulmaa Yeboah-Ofori ja Islam (2019) hyödynsivät tehdessään uhkamallinnusta toimitusketjun osana olevaan organisaatioon. Kaikkia näitä Shostackin (2014) mainitsemia lähestymistapoja voidaan onnistuneesti hyödyntää uhkamallintamisessa, vaikka hän itse kannustaakin lähestymään uhkamallinnusta järjestelmäkeskeisesti (Shostack, 2014, s. 41–42).

3 Suomen vesihuolto

Vesihuolto ottaa ympäristöstä veden, jonka vedenpuhdistuslaitokset puhdistavat, joka välitetään asiakkaille, joiden jätevesi lähetetään jätevedenpuhdistuslaitoksille, joka puhdistetaan ja vapautetaan takaisin ympäristöön (Ikäheimo & Metsävuo, 2020, s. 8; kuvio 3). Vesihuoltoon kuuluu lisäksi hulevesiverkosto, jonka tarkoituksena on poistaa sadevesi ja lumesta sulanut vesi pois asutulta alueelta (Myllylä, 2012, s. 5; kuvio 3). Tämä verkosto on elintärkeä miljoonille suomalaisille. Sen toiminta takaa elintärkeän juomaveden puhdistamisen ja toimittamisen asiakkaille, mutta myös jäteveden toimittamisen asiakkailta sekä sen puhdistamisen. Oikein puhdistettu ja jaettu juomavesi sekä oikein puhdistettu jätevesi mahdollistavat yhteiskunnallisen terveyden, asumisen, palveluiden ja yritystoiminnan sekä ympäristön varjelun (Tuorila & Saastamoinen, 2022). Kyseessä ovat Euroopan unioninkin vuonna 2022 määrittämät kriittisen infrastruktuurin kaksi osa-aluetta, joiden toiminta yhteiskunnan kannalta on elintärkeää (Euroopan parlamentti, 2022). Vesihuollon toimivuus on myös yhteydessä muihin kriittisen infrastruktuurin alojen toimintaan, kuten terveydenhuoltoon (Maa- ja metsätalousministeriö, 2021, s. 8).



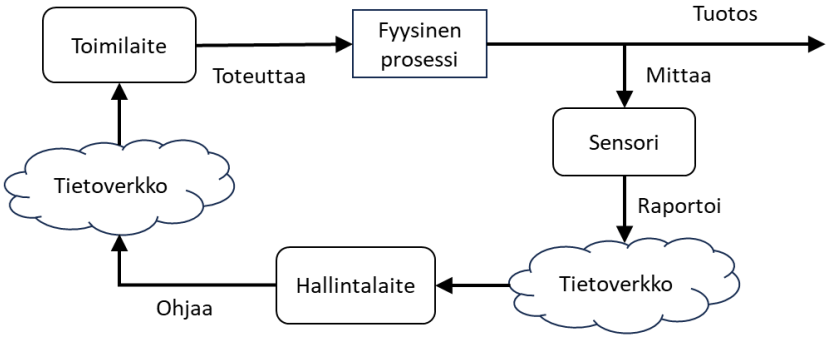
KUVIO 3 Vesihuollon yksinkertaistettu rakenne (Ikäheimo & Metsävuo, 2020, s. 8; Myllylä, 2012, s. 11)

Suomen vesihuoltoverkoston yhtenäinen pituus oli 2020-luvulle saavuttaessa miltei 160 000 kilometriä, sen koostuessa noin 107 000 kilometristä vesijohtoverkostoa ja noin 50 000 kilometristä viemäri- ja hulevesiverkostoa (Kuulas, Renko & Kuivamäki, 2017, s 11). Vesijohtoverkon putket ovat muovisia tai metallisia ja viemäriverkoston lisäksi myös betonisia (Myllylä, 2012, s. 12–13). Näiden putkien sisällä tapahtuvaa virtaamista ja painetta hallitaan erinäisillä venttiileillä, kuten sulku-, paineenalennus- ja ilmanpoistoventtiileillä, joita voidaan käyttää myös hätätilanteissa vedenkulun pysäyttämiseen (Myllylä, 2012, s. 13). Vesihuoltoverkoston toimintaa mitataan valvontalaitteilla, jotka mittaavat esimerkiksi painetta ja virtausta järjestelmässä sekä kuuntelulaitteilla, jotka kuulostelevat esimerkiksi putkirikkojen varalta (Myllylä, 2012, s. 13). Vesijohtoverkoston paine luodaan paineistettuja putkia käyttämällä koneellisesti pumppaamalla tai vesitorneja eli ylävesisäiliöitä hyödyntämällä (Myllylä, 2012, s. 11). Myös jätevettä joudutaan joskus pumppaamaan eteenpäin putkistossa jätevedenpumppaamoilla, jotka sisältävät myös erinäisiä puhdistus-, ilmanvaihto-, käynnistys- ja hälytinlaitteita (Myllylä, 2012, s. 16).

Vesihuolto ei kuitenkaan koostu vain metallisista ja muovisista putkista ja niiden valvontalaitteista, vaan myös vesihuoltolaitoksista eli vedenpuhdistuslaitoksista ja jätevedenpuhdistuslaitoksista, joita on eri kokoisina Suomessa yhteensä noin 1100 kappaletta. Näistä noin 80 suurinta, vastaavat lähes 80 prosentista kaikesta tuotetusta vesihuollosta. (Maa- ja metsätalousministeriö, 2021, s. 8) Vesihuollon toimivuus on siis osin keskittynyt suurimpiin toimijoihin, joiden mahdolliset toimintavaikeudet varmasti heijastuisivat koko yhteiskuntaan. Vedenpuhdistuslaitokset puhdistavat kerätyn raakaveden useiden eri prosessien avulla ja pumppaavat puhdistetun veden kuluttajille (kuvio 3). Prosessin aikana raakavesi puhdistetaan erinäisin keinoin esimerkiksi välppäämällä, saostamalla, flotaatiolla, siivilöimällä, suodattamalla, kemiallisesti puhdistamalla ja alkaloimalla muuttaen veden pH-arvoa (Huhtakangas, 2017, s. 44–46). Jätevedenpuhdistuslaitokset taas puhdistavat jäteveden ja vapauttavat sen luontoon puhdistamisen jälkeen (kuvio 3). Jäteveden puhdistamoissa puhdistusprosessi tehdään esimerkiksi aktiivilietelaitoksissa Suomenojalla ja Viikinmäessä mekaanisesti, biologisesti ja kemiallisesti, jotta vedestä saadaan kaikki haitalliset aineet ja yhdisteet poistettua (HSY, 2019, s. 10–12). Prosessissa syntynyttä lietettä käytetään myös biokaasun, lämmön ja sähkön valmistamisessa, kunnes se jatkojalostetaan multatuotteiksi (HSY, 2019, s. 10–12).

Vesihuolto koostuu fyysisten osien lisäksi eri tietojärjestelmistä, kuten vesihuoltolaitosten hallintajärjestelmistä ja vesihuollon valvontalaitteista, jotka ylläpitävät sekä valvovat vesihuollon toimintaa (Hassanzadeh ym., 2020, s. 3). Vedenpuhdistuslaitoksissa on erilaisia tuotannonohjausjärjestelmiä, jotka ovat automatisoineet puhdistusprosessin. Kurkelanrannan vedenpuhdistuslaitoksessa on esimerkiksi käytössä Honeywell Total Plant-automaatiojärjestelmä ja Hintan vedenpuhdistuslaitoksessa Valmet DNA-automaatiojärjestelmä (Huhtakangas, 2017, s. 44, 46). Ne ovat niin sanotusti kyberfyysisiä järjestelmiä, jotka määritellään toiminnallisiksi kokonaisuuksiksi, jotka muodostuvat ”kybertoiminnallisuuksista, fyysisistä toiminnallisuuksista ja nämä läheisesti yhdistäväs-

tä rajapinnasta" (Viljanen, 2021, s. 13). Käytännössä ne ovat järjestelmiä, joissa tietokoneet ja tietoverkot ohjaavat sekä valvovat fyysisiä prosesseja, usein muodostaen takaisinkytkennän (Lee, 2006, s. 1–2). Hallintalaitteena oleva tietokone pyrkii toteuttamaan sille määrätyn prosessin. Se toteuttaa prosessin ohjaamalla toimilaitetta, esimerkiksi pumppua, toimimaan ja tuottamaan fyysisen työn. Työtä, esimerkiksi veden pumppaamista, seuraa sensori, joka lähettää tiedon verkkoa pitkin hallintalaitteelle, jotta hallintalaite voi mahdollisesti muokata toimilaitteen toimintaa. (Tuptuk ym., 2021, s. 6; kuvio 4.) Kyberfyysinen järjestelmä tarvitsee myös energiaa ylläpitoonsa, joka vesihuoltolaitosten osalta saadaan esimerkiksi sähköverkosta tai generaattoreista (Viljanen, 2021, s. 56).



KUVIO 4 Kyberfyysinen järjestelmä, yksinkertaistettu (Tuptuk ym., 2021, s. 6)

Kyberfyysisten järjestelmien lisäksi on vesihuollon toimintaa sekä kuntoa valvovia ja niistä tietoa kokoavia tietojärjestelmiä, kuten Suomessa Veeti ja Venla, joilla pyritään pitämään yllä vesihuollon tilannekuvaa valtakunnallisesti (Tuorila & Saastamoinen, 2022, s. 47–48). Veeti on Suomen ympäristökeskuksen ylläpitämä tietojärjestelmä, jonne lain määräämänä vesihuoltolaitokset ilmoittavat perus- ja tunnuslukuja, kuten verkoston määrän, liittyjämäärät ja välitetyn veden määrän. (Tuorila & Saastamoinen, 2022, s. 47). Venla-tietojärjestelmä on Vesilaitosyhdistyksen ylläpitämä vesihuoltolaitosten vertaisarviointiin tarkoitettu vanhempi ja osin päällekkäinen Veeti-tietojärjestelmän kanssa (Tuorila & Saastamoinen, 2022, s. 47). Venla on myös vapaaehtoinen, mutta Veeti-tietojärjestelmän kanssa yhteisen rajapinnan avulla se on kahdesta tietojärjestelmästä kattavampi (Tuorila & Saastamoinen, 2022, s. 47).

Näiden vesihuollossa hyödynnettävien tietojärjestelmien kyberturvallisuutta voidaan tarkastella CIA-kolminaisuuden (luottamuksellisuus, eheys, käytettävyys) osa-alueita hyödyntäen, kuten Huoltovarmuuskeskuksen vuonna 2021 (s.42) julkaisemassa Turvallisuusjohtaminen vesihuoltolaitoksilla-julkaisussa. CIA-kolminaisuus on myös yleisesti käytössä oleva turvallisuustavoitteita kuvaava käytäntö, jota pääosa yrityksistä ja kirjallisuudesta tunnustaa (Raggad, 2010, s. 20). Luottamuksellisuutta tarkoittaa tiedon jakamista vain sitä tarvitseville, näin pitäen tiedon saatavissa vain sellaisille henkilöille, joilla on oikeus sitä tarkastella (Raggad, 2010, s. 20). Eheys on taas pitää järjestelmiin tallennetun tiedon oikeanlaisena ja pyrkii estämään sen korruptoitumisen tai muuttumisen vääränlaiseksi (Raggad, 2010, s. 20). Lopulta käytettävyys tarkoit-

taa sitä, että tarvittava tieto on saatavissa, kun sitä tarvitaan (Raggad, 2010, s. 20).

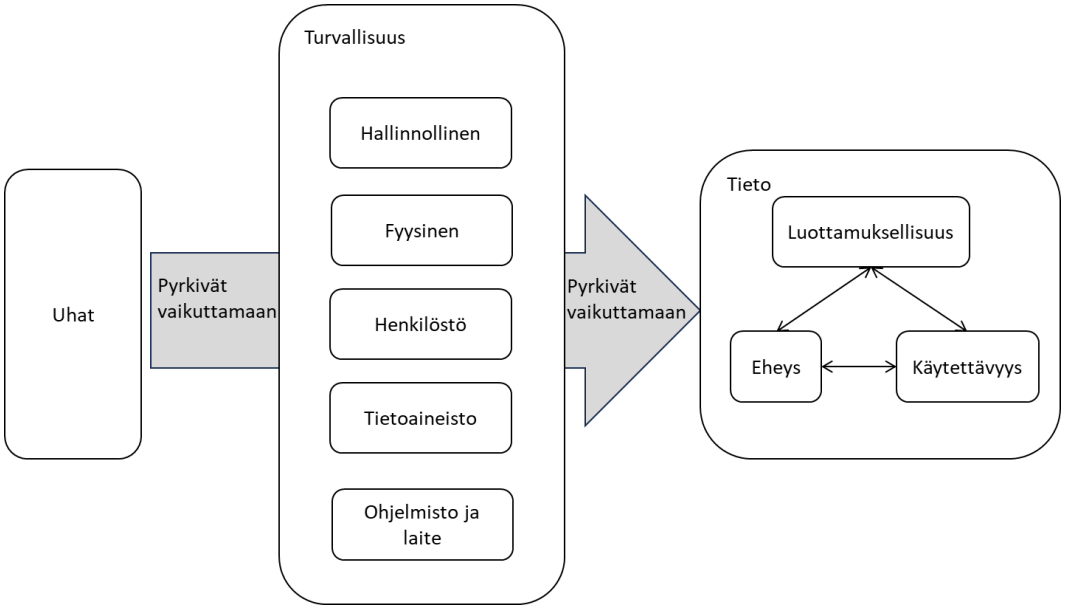
Huoltovarmuuskeskus (2021, s. 42) kuvailee luottamuksellisuuden tärkeyttä seuraavasti:

> Luottamuksellisuus suojaa esimerkiksi vesihuoltolaitoksen omistusoikeutta omaan tietoonsa tai vesihuoltolaitoksen asiakkaan yksityisyyttä. Vesihuollon turvallisuuden kannalta herkkiä tietoja ovat muun muassa vedenottokaivojen, vesijohtoverkoston ja muiden vesihuollon kohteiden tarkat sijaintitiedot, laitosten tarkat prosessitiedot, valvonta- ja ohjausjärjestelmien tiedot, erilaiset turvallisuusjärjestelyitä koskevat tiedot, vesihuoltolaitosten riskiarvioita koskevat tiedot sekä vesihuollon varautumissuunnitelmat.

Edellä mainittuja tietoja on varmasti tallennettuina niin vesihuoltolaitosten tietokantoihin, mutta myös Venla ja Veeti-tietojärjestelmiin. Tiedon eheys taas korostuu esimerkiksi tiedottamisessa, jossa väärä tiedote vesihuollon toimintakyvystä tai veden turvallisuudesta voi aiheuttaa laajaa vahinkoa kohdealueelle tai väärien päätösten tekoa itse vesihuoltolaitoksissa (Huoltovarmuuskeskus, 2021, s. 42). Käytettävyys mahdollistaa sen, että tarvittava tieto on oltava käytettävissä niillä henkilöillä, jotka sitä tarvitsevat, jotta vesihuolto voi jatkaa normaalia toimintaansa (Huoltovarmuuskeskus, 2021, s. 42).

Huoltovarmuuskeskus (2021, s. 43–44) hyödyntää valtionhallinnon tietoturvallisuuden johtoryhmän viittä tieto- ja kyberturvallisuuden osa-aluetta silloin, kun se tarkastelee vesihuollon tietojärjestelmiin kohdistuvia uhkia. Hallinnollisen turvallisuuden osalta koettiin oleelliseksi varata resurssit kouluttamaan työntekijät ymmärtämään tietoturvallisuuden merkityksen, sillä kaikki hyvätkin tietoturvajärjestelyt romuttuvat, jos työntekijä vain päästää hyökkääjän järjestelmään (Huoltovarmuuskeskus, 2021, s. 43). Fyysinen turvallisuus keskittyy taas estämään tietojärjestelmien luo murtautumisen ja tietojärjestelmissä oleviin tietoihin käsiksi pääsyn, vaikka asettamalla muistitikun tietokoneeseen tai varastamalla osan koko palvelimesta (Huoltovarmuuskeskus, 2021, s. 43–44). Henkilöstöturvallisuus keskittyy pääosin saatavuuden hallitsemiseen ja valvontaan, jotta väärät henkilöt eivät pääse käsiksi luottamukselliseen tietoon tai järjestelmiin (Huoltovarmuuskeskus, 2021, s. 44). Tietoaineistoturvallisuus taas käsittää vesihuollon tietojärjestelmissä olevien tietojen luokittelun ja itse järjestelmien tärkeyden tunnistamista sekä niihin oikein reagointia koko niiden elinkaaren ajan (Huoltovarmuuskeskus, 2021, s. 44). Vesihuollon tietojärjestelmien ohjelmisto- ja laiteturvallisuus keskittyy järjestelmien pitämiseen ajan tasalla erilaisine elinkaaripäivityksineen, erityisesti erilaisten automaatiojärjestelmien, kuten kaukovalvontajärjestelmien, osalta (Huoltovarmuuskeskus, 2021, s. 44).

Kuviossa 5 on mallinnettu vesihuoltoon kohdistuvien kyberuhkien hallintaa ja pyritty esittämään edellä mainittujen käsitteiden yhteisvaikutusta selkeämmin. Uhkien vaikutus on moninainen ja niiden kohdistuminen vesihuoltoon voidaan tarkastella uhkalähtöisesti (kuvio 1) ja samalla vastata uhkataksonomian (kuvio 2) mukaisiin uhkiin omin turvallisuustoimenpitein (Huoltovarmuuskeskus, 2021, s. 43–44).



KUVIO 5 Vesihuollon tieto- ja hallintajärjestelmiin kohdistuvien kyberuhkien hallinta

Vesihuollon tieto- ja hallintajärjestelmiin on mahdollista vaikuttaa monin eri tavoin. Vesihuollon eri tieto- ja hallintajärjestelmät pitävät sisällään vihamieliselle hyökkääjälle yllä mainittua arvokasta tietoa ja mahdollisuuksia päästä vaikuttamaan suureen joukkoon ihmisiä. Tiedustelutiedon saaminen vesihuollon eri osa-alueiden sijainneista ja toimintaperiaatteista edesauttaa verkostoon kohdistuvia kyberhyökkäyksiä. Kyberturvallisuus on siis tärkeä osa vesihuollon turvallisuutta, jonka onnistunut toiminta on entistä kriittisempää nyt ja tulevaisuudessa, kun verkottuminen, digitalisaatio ja sähköinen asiointi lisääntyvät (Huoltovarmuuskeskus, 2021, s. 43). Täten vesihuollon on panostettava aktiivisemmin kyberturvallisuuteen, sillä se on toimialana jäänyt vertailussa hyvän perustason alapuolelle (Huoltovarmuuskeskus, 2022, s. 34). Toimiala on kuitenkin kehittynyt kyberturvallisuudessa henkilöstön johtamisessa ja kehittämisessä, kehitystyötä ohjaavissa toimissa sekä omaa sovelluskehitystä tekevien toimijoiden kypsyystason nousussa tietoturvallisessa kehitystyössä (Huoltovarmuuskeskus, 2022, s. 34). Erityisinä haasteina vesihuollon kyberturvallisuudelle ovat vuoden 2022 Toimialojen kypsyysselvityksen mukaan ”kyberturvallisuuden kokonaishallinnan puutteet, erityisesti IT-toimittajien suuntaan, heikko näkyvyys kumppanien toimintaan kehitystyössä ja korkea riippuvuussuhde IT-palveluntoimittajiin” (Huoltovarmuuskeskus, 2022, s. 34). Edellä mainitut haasteet on syytä ratkaista, sillä erilaiset hyökkäykset, myös vesihuoltoa kohtaan, ovat kasvussa (Huoltovarmuuskeskus, 2022, s. 11).

4 Tutkimuksia vesihuollon kyberturvallisuudesta

Vesihuoltoon kohdistuneista kyberhyökkäyksistä, mahdollisista uhista sekä haavoittuvuuksista ja näiden vaikutuksesta on tehty tutkimuksia ympäri maailmaa jo vuosikymmeniä. Näistä uusimmat kuitenkin sijoittuvat 2020-luvun alkuun tai ovat sitä vanhempia. Pääosa tutkimuksista nostaa esiin vesihuoltoon kohdistuneita kyberhyökkäyksiä sivuhuomioina, mutta ei keskity suoraan tarkastelemaan kyberhyökkäyksiä itsessään. Pääosa tällaisista artikkeleista keskittyy eri riskimallien, toimintatapojen tai käytäntöjen vertailuun. Tapahtuneet kyberhyökkäykset ovat sivuseikkoja tai esimerkkejä. Tarkasteluun on valittu vuonna 2016 tai myöhemmin julkaistuja artikkeleita ja tekstejä, jotka käsittelivät vesihuoltoon kohdistuvia uhkia, vesihuollon haavoittuvuuksia tai onnistuneiden hyökkäysten vaikutusta vesihuoltoon (taulukko 1). Tarkoitus oli valita mahdollisimman tuoreita tutkimuksia nopeasti muuttuvan ja kehittyvän kyberuhan ajantasaiseen tarkasteluun.

TAULUKKO 1 Valitut tutkimukset ja niiden aiheet

Artikkeli	Aihe
Adepu ym. (2020)	Tapaustutkimus kyberhyökkäyksen vaikutuksista vesihuoltoon.
Aslam ym. (2023)	Vesihuollon haavoittuvuuksia ja tapahtuneiden hyökkäyksien tarkastelu ja kehitysehdotukset.
Addeen ym. (2021)	Vesihuoltoon kohdistuvat hyökkäykset ja niiden havaitseminen.
Bello ym. (2022)	Australian vesihuollon kyberturvallisuustoimien ja riskienhallinnan haasteiden kriittinen tarkastelu.
Berglund ym. (2020)	Vesihuollon suojautumisen kirjallisuuden tarkastelu.
Clark, ym. (2016)	Yhdysvaltojen vesihuollon tarkastelu kyberturvallisuuden näkökulmasta.
Hassanzadeh ym. (2020)	Vesihuoltoon kohdistuneiden kyberhyökkäysten tarkastelu.
Mishra ym. (2019)	Malli vesihuollon tietoturvan testaamiseen.
Moraitis ym. (2020)	Tapaustutkimus vesihuoltoon kohdistuvien kyberfyysisten hyökkäysten vaikutuksista.
Nikolopoulos ym. (2018)	Malli vesihuollon tietoturvan testaamiseen.
Palleti ym. (2021)	Vesihuoltoon kohdistuvien kyberhyökkäysten mallintaminen.
Taormina ym. (2017)	Vesihuoltoon kohdistuvien kyberhyökkäysten mallintaminen.
Tuptuk ym. (2021)	Kirjallisuuskatsaus vesihuollon kyberturvallisuudesta tehdystä kirjallisuudesta.

Vesihuollon kokonaisturvallisuuden näkökulmasta tehtyjä tutkimuksia, jotka tarkastelivat tehtyä kirjallisuutta ja eri toimenpiteitä, oli esimerkiksi Berglund ym. (2020) julkaisu, jossa kyberturvallisuus nostettiin yhdeksi tärkeydessään kasvavaksi osa-alueeksi vesihuollon turvallisuuden osalta (s. 28). Myös Bello ym. (2022) tarkastelivat vesihuoltoon kohdistuneita kyberturvallisuustoimia, mutta rajaten tarkastelun Australiaan. Tarkastelussa oli myös vesihuoltoon kohdistuva uhkaympäristö, haavoittuvuudet ja miten eri toimijat olivat valmistautuneet mahdollisiin riskeihin (Bello ym, 2022, s. 2). Yhdysvaltojen osalta Clark ym. (2016, s. 2, 15–16) tarkastelivat vesihuoltoon kohdistuvien kyberuhkia ja niiden torjuntaa eri keinoja hyödyntäen. Tutkimukset painottivat vesihuoltoon kohdistuvien kyberhyökkäysten ja uhkien määrän olevan korkea ja myös kasvavan tulevaisuudessa järjestelmien automatisoituessa entisestään, ei pelkästään valtiollisten toimijoiden vuoksi, vaan myös rahaa tavoittelevien rikollisjärjestöjen toimesta (Berglund, 2020, s. 28; Bello ym, 2022, s.15–17; Clark, ym., 2016, s. 13). Kirjallisuuskatsauksen aiheesta tekivät myös Tuptuk ym. (2021), jossa he havaitsivat pääosan kirjallisuudesta keskittyvän vesihuollon juomaveden puoleiseen toimintaan (Tuptuk ym., 2021, s. 24). Vesihuoltoon kohdistuviin uhkiin on tutkimuksissa suhtauduttu vakavasti, joka on johtanut erinäisten mallien rakentamiseen, joilla voidaan koetella vesihuollon eri osa-alueiden kestävyyttä hyökkäyksiä vastaan (Nikolopoulos ym., 2018, s. 11; Mishra ym., 2019, s. 1).

Itse uhkia ja hyökkäyksiä tarkastelivat eri artikkelit, kuten Hassanzadeh ym. vuonna 2020 julkaistu vesihuoltoon kohdistuneiden hyökkäyksien katsaus. Tutkimukseen on valittu viisitoista eri kyberhyökkäystä, joiden vaikutuksia tarkastellaan ja pohditaan, mitä niistä on opittu kyberturvallisuuden paranta-

misen näkökulmasta (Hassanzadeh ym., 2020, s. 5–11). Tuptuk ym. sekä Aslam ym. myös tarkastelivat vesihuoltoon tapahtuneita hyökkäyksiä yhdessä eri tutkimuksissa mallinnettujen hyökkäysten kanssa (Tuptuk ym., 2021, s. 4, 17; Aslam ym., 2023, s. 15–16). Myös Addeen ym. (2021) tarkastelivat vesihuoltoon mahdollisesti tapahtuvia yleisimpiä kyberhyökkäyksen kohteita, niihin kohdistuneiden hyökkäysten vaikutusta ja hyökkäysten eri havaitsemiskeinoja (s. 1).

Tutkimuksissa esitetyt 2000-luvulla tapahtuneet hyökkäykset ovat kohdistuneet vesihuollon joka osa-alueeseen, vesihuoltolaitoksista aina pumppuihin ja vedenjakeluverkostoihin (Hassanzadeh ym., 2020, s. 5–11; Tuptuk ym., 2021, s. 4; Aslam ym., 2023, s. 13–16). Addeen ym. (2021, s. 4) jakavat nämä vesihuoltoon kohdistuvat hyökkäykset sensoreihin, toimilaitteisiin, hallintalaitteisiin, ohjelmoitaviin logiikkaohjaimiin ja tietoverkkoihin kohdistuviksi hyökkäyksiksi. Hyökkäykset ovat myös tapahtuneet erilaisten vihamielisten toimijoiden, kuten sisäpiiriläisten, eli nykyisten tai entisten työntekijöiden, mutta myös ulkopuolisten, eli esimerkiksi haktivistien ja kyberrikollisten toimesta (Hassanzadeh ym., 2020, s. 5–11; Tuptuk ym., 2021, s. 4; Aslam ym., 2023, s. 13–16). Tapahtuneet hyökkäykset ovat tapahtuneet eri tavoin, eri kohteisiin ja erilaisten toimijoiden tekeminä. Tehdyistä tutkimuksista voidaan todeta vesihuollon olevan monin tavoin kohde mahdollisille vaikuttajille, jolloin sen suojaaminen sekä hyökkäysten paljastaminen on elintärkeää, jotta vaikutukset pystytään minimoimaan.

Tutkimuksissa tarkasteltiin simuloitujen hyökkäysten vaikutusta vesihuollon eri osa-alueisiin. Adepu ym. (2020) tutkivat vesihuoltoon kohdistuneiden kyberhyökkäyksien vaikutuksia vesihuollon toimintaan. He havaitsivat simuloituun vedenjakelukeskukseen tapahtuneiden hyökkäysten aiheuttaneen ongelmia vedenjakelussa, mutta sen lisäksi fyysiset järjestelmät saattoivat tuhoutua hyökkäyksien vuoksi. Vedenjakelun ongelmia olivat veden tuleminen ja sen paine. Hyökkäykset mahdollistaisivat myös toisenlaisten hyökkäysten, esimerkiksi veden saastuttamisen onnistumisen, koska sensorit eivät toimisi niiden oletetulla tavalla. (Adepu ym., 2020, s. 18) Kyberhyökkäysten seuraamukset vesihuollon eri osa-alueisiin vaihtelevat aina toiminnan vaikeuttamisesta järjestelmän tuhoamiseen (Addeen ym., 2021, s. 6). Moraitis ym. (2020, s. 11–13) tapaustutkimuksessa vesihuoltoon kohdistuvien kyberfyysisten hyökkäysten vaikutuksista havaittiin onnistuneiden hyökkäysten aiheuttavan laajamittaista häiriötä vesihuollon toimintaan. Väärän tiedon välittäminen hallintalaitteille aiheutti venttiilien sulkeutumisen, joka muutamien tuntien päästä johti vedenjakelun vaikeutumiseen tietyillä alueilla (Moraitis ym., 2020, s. 11–13). Samankaltaisiin vaikutuksiin pääsivät myös Taormina ym. heidän hyökkäysmallinnuksellaan, jossa seitsemällä eri hyökkäystavalla vaikutettiin vesihuoltoon tulvittamalla tai tyhjentämällä säiliöitä sekä antamalla väärää tietoa hallintalaitteille (Taormina ym, 2017, s. 6–8). Eri vesihuollon osa-alueiden joutuessa kyberhyökkäyksen kohteeksi vaikuttaa se myös koko vesihuollon toimintaan sekä muuhun vesihuollosta riippuvaiseen kriittiseen infrastruktuuriin (Paletti ym, 2021, s. 1; 7–15).

2000-luvulla tapahtuneiden hyökkäysten vaikutukset ovat simuloitujen hyökkäysten mukaisia, kuitenkin vaihdellen tietomurrosta aina katastrofaaliseen vesihuollon eri järjestelmien vääriin toimintoihin (Hassanzadeh ym., 2020, s. 5–11; Tuptuk ym., 2021, s. 4; Aslam ym., 2023, s. 13–16). Hyökkäyksistä palautuminen voi myös kestää hyvin pitkään, jos niistä on edes mahdollista palautua. Tietojärjestelmiin tallennettuja tietoja on joutunut vääriin käsiin tai tuhoutunut hyökkäyksissä, joiden vaikutusten rahallista arvoa on vaikea arvioida. (Hassanzadeh ym., 2020, s.13; Tuptuk ym., 2021, s. 4; Aslam ym., 2023, s. 16) Rahallinen arvo tuhoutuneelle tai vaurioituneelle järjestelmälle voidaan antaa, oli se sitten vedenjakelun keskeytyminen tai ympäristön siivoamiskustannukset satojen tuhansien jätevesilitrojen karkaamisesta puhdistamattomana luontoon (Hassanzadeh ym., 2020, s.13; Tuptuk ym., 2021, s. 4; Aslam ym., 2023, s. 16).

Tehtyjen tutkimusten (taulukko 1) perusteella vesihuolto on täynnä monenlaisia haavoittuvuuksia, joita vihamieliset hyökkääjät hyväksikäyttävät, mikäli he saavat siihen mahdollisuuden. Hyökkäykset ovat moninaisia ja kohdistuvat eri vesihuollon osa-alueisiin. Nämä hyökkäykset toteutuessaan aiheuttavat myös merkittävää taloudellista ja maineellista haittaa vesihuollosta vastuussa olevalle taholle. Niistä ei olla varmasti pääsemässä eroon 2020-luvun edetessä, kun vesihuolto jatkaa verkostoitumista ja digitalisoitumista 2030-luvun lähestyessä (Ikäheimo & Metsävuo, 2020, s. 8).

5 Tutkimusmetodi

Tutkimusongelmaksi on valittu selvittää mitä kyberuhkia vesihuoltoon on kohdistunut aikavälillä 1/2020–2/2024. Tämä ongelma jalostuu kahdeksi tutkimuskysymykseksi, joista ensimmäinen kysyy mitä on tapahtunut ja toinen, miten näihin hyökkäyksiin on reagoitu. Tutkimuskysymykset ovat:

1. Mitä kyberturvallisuusuusuhkia on kohdistunut vesihuoltoon aikavälillä 1/2020–2/2024?
2. Miten vesihuollosta vastaavat tahot ovat reagoineet kyberhyökkäyksiin aineiston perusteella?

5.1 Tutkimuskysymykset

Tutkimuskysymyksiin pyritään vastaamaan tarkastelemalla aineistona käytettäviä 2020-luvulla julkaistuja raportteja, uutisia ja tiedotteita tapahtuneista kyberhyökkäyksistä eri kyberturvallisuusjärjestöiltä, vesihuollosta vastaavilta tahoilta sekä muilta toimijoilta. Eskola ja Suoranta (2008, s. 117) tuovatkin esiin, että erityisesti laadullisessa tutkimuksessa tutkijalla on käytössä valmiita aineistoja, joita voi ja on järkevä hyödyntää. Kysymyksiin saadaan vastaus jo valmiiksi kerätystä aineistosta eri maiden kyberturvallisuudesta sekä vesihuollosta vastaavien tahojen raporteista. Kuten Eskola ja Suoranta (2008, s. 64) toteavat, laadullista aineistoa on käytännössä loputtomasti, jonka vuoksi oli keskeistä tehdä rajaus tässä tutkimuksessa nimenomaisesti 2020-luvulla tapahtuneisiin vesihuoltoon kohdistuneisiin kyberuhkiin. Esitetyt tapaukset analysoidaan teemoittelemalla etsien niistä yhteneväisiä piirteitä tai toimintatapoja. Tutkimus on tarkentunut koko kriittistä infrastruktuuria koskevasta tarkastelusta nimenomaisesti 2020-luvulla vesihuoltoon kohdistuneiden kyberhyökkäyksien tarkasteluun.

Kyberturvallisuudesta vastaavien viranomaisten vuosiraporteista tai muilta vesihuoltoon sekä kyberturvallisuuteen erikoistuneilta tahoilta saadun viit-

teen jälkeen, kyberhyökkäyksistä haettiin lisää tietoa ja näkökulmia eri hakukoneita käyttäen. Tutkielman aineistossa esitettyjen tapahtuneiden kyberhyökkäysten kartoittamiseen käytettiin DuckDuckGo-hakukonetta ja Google-hakukonetta. Näistä hakukoneista haettiin tapahtuneista kyberhyökkäyksistä lisätietoa esimerkiksi tapahtumavuoden, paikan tai vesihuollosta vastaavan tahon nimen mukaan. Näin löydettiin pienempien paikallisjulkaisujen tai vesihuollosta paikallisella tasolla vastaavien toimijoiden tiedotteita sekä lausuntoja. Löydetyistä lähteistä itsessään löytyi tarkempia hakutermejä sekä täysin uusia tapahtuneita vesihuoltoon kohdistuneita kyberhyökkäyksiä, jotka lisättiin aineistoon. Osa käytetyistä lähteistä paljastui aluelukituksi kohdemaahan tai maanosaan, jolloin Suomesta niiden tarkastelu tavanomaisesti ei ollut mahdollista. Uutiset ja artikkelit saatiin tutkimuksen aineistoksi käyttämällä virtuaalista erillisverkkoa (VPN) jolla kyettiin ohittamaan sivuille asetettu rajoitus. Valittu virtuaalinen erillisverkko oli Freedome, jolla oli mahdollista asettaa erillisverkko artikkelin tai uutisen lukuoikeuden piirin kuuluvaan maahan. Tällöin artikkeli tai uutinen kyettiin lisäämään osaksi aineistoa.

5.2 Teemoittelu

Tutkimus on luonteeltaan laadullinen ja tutkimusmenetelmäksi on valittu teemoittelun. Se on suositeltava analysointitapa, kun yritetään ratkaista käytännöllistä ongelmaa (Eskola & Suoranta, 2008, s. 178). Teemoittelu eroaa luokittelusta siinä, että vaikka se luokittelee aineistosta tutkimusongelmaa koskevia aiheita, teemoittelussa kiinnostaa nimenomaisesti mitä teemoista on sanottu, eikä niiden määrälliset luvut (Tuomi & Sarajärvi, 2009, s. 93). Teemoittelu sisällönanalyysin keinona pyrkii etsimään kerätystä aineistosta tutkimustehtävään liittyviä asiakokonaisuuksia ja piirteitä, joita voidaan sitten tarkastella sekä analysoida tarkemmin (Eskola & Suoranta, 2008, s. 178; Juhila, ei pvm.). Teemoittelu ei kuitenkaan ole pelkkien lainauksien tai piirteiden listaamista, vaan myös aineiston analysointia teemoja vertailemalla, selittämällä ja tulkitsemalla (Eskola & Suoranta, 2008, s. 179–180). Aineistosta teemoittelemalla löytyneet teemat ovat tärkeää luoda itse analyysin aikana eikä siten, että aineistoa jaetaan jo valmiiksi suunniteltuihin kategorioihin (Juhila, ei pvm.).

Tutkimuksessa kerättyä aineistoa analysoidaan teoriaohjaavasti teemoittelun aikana. Teoriaohjaavassa analyysissä on kytkentöjä teoriaan, mutta analyysi ei pohjaudu suoraan teoriaan tai ei ole teoriaa testaava (Tuomi & Sarajärvi, 2009, s. 96–97). Tässä tutkimuksessa kytkennät teoriaan tapahtuvat uhkien määrittelyn osalta, niiden pohjautuessa Raggadin (2010) uhkataksonomiaan (kuvio 2) sekä Muckin & Fitch (2019) uhkalähtöiseen malliin (kuvio 1). Aineiston hankinta on vapaata, mutta sen analysoinnissa siihen liitetään teoriaohjaava ote (Tuomi & Sarajärvi, 2009, s. 99).

Teemoittelua hyödynnettiin Braun & Clarke (2006, s. 15–23) antaman ohjeistuksen mukaisesti kuusiportaisella toimintatavalla. Braun & Clarken (2006) mukaan ensimmäinen askel aineiston keräämisen jälkeen on tutkijan tutustu-

minen aineistoon. Tutkija lukee läpi aineistonsa useita kertoja, jonka aikana hän pyrkii tunnistamaan esiin nousevia teemoja (Braun & Clarke, 2006, s. 16–18). Toinen vaihe on niin sanottujen koodien löytäminen aineistosta. Koodit ovat tutkijalle kiinnostavia seikkoja tai toistuvia yksityiskohtia käytettävässä aineistossa, joista myöhemmin muodostetaan teemoja (Braun & Clarke, 2006, s. 18–19). Kolmannessa vaiheessa aloitetaan teemojen muodostaminen tehtyjä aineiston koodeja hyödyntämällä. Teemojen muodostamisessa voi auttaa visuaalisten asettelujen tekeminen koodeista, joista lopulta muodostuvat merkittävimmät pääteemat, alateemat ja tutkimukselle tarpeettomat teemat. (Braun & Clarke, 2006, s. 19–20) Luonnostellut teemat arvioidaan vaiheessa neljä, jossa teeman varteenotettavuutta arvioidaan tarkastelemalla siihen liitettyjä koodeja sekä teeman suhdetta kaikkeen muuhun aineistoon (Braun & Clarke, 2006, s. 20–21). Mikäli teema hyväksytään, siirrytään vaiheeseen viisi, jossa teemaa analyysin perusteella edelleen jatkojalostetaan ja se nimetään tarkemmin. Teemoista kirjoitetaan analyysi, jossa hyödynnetään alateemoja tarkentamaan ja selventämään valittua pääteemaa. (Braun & Clarke, 2006, s. 22–23) Viimeinen vaihe on kirjoittaa aineiston analyysin perusteella ”tarina”, joka luotuja teemoja sekä aineistoa hyödyntäen kertoo tehdyn analyysin pätevyyden, joka on oltava lähempänä argumenttia kuin tiivistelmää aineistosta (Braun & Clarke, 2006, s. 23).

Braunin ja Clarken (2006) esittämän teemoittelun tavoin toimi Rautiainen (2023) väitöskirjassaan tutkiessaan kokemusten kertomista oppimispäiväkirjoissa. Hän luki aineistonaan olleet oppimispäiväkirjat useasti ja koodasi aineiston kolmesta eri näkökulmasta, joista muodostettiin ryhmiä ja lopulta teemoja, jotka lopullisesti määriteltiin niiden tekstilukuja kirjoittaessa (Rautiainen, 2023, s. 25–27). Nämä näkökulmat kumpusivat hänen tutkimuskysymyksistään (Rautiainen, 2023, s. 15). Rautiainen (2023, s. 43–120) kirjoitti teemoittelulla tehdyn analyysin tutkimuskysymysten mukaisiin omiin lukuihinsa samalla tukien niitä alateemoilla, jotka olivat selvinneet ryhmittelyn aikana. Johtopäätösluvussa kirjoitetut analyysiluvut esitettiin vastauksena tutkimuskysymyksiin (Rautiainen, 2023, s. 124–125).

6 Aineisto ja analyysi

Vesihuoltoon aikavälillä 1/2020–2/2024 kohdistuneet kyberuhat on esitetty tässä kappaleessa. Aineisto koottiin lukemalla valtiollisten kyberturvallisuudesta vastaavien tahojen vuosiraportteja, uutisia, tiedotteita ja muita eri julkaisuja, joista pyrittiin keräämään sekä esittelemään vesihuoltoon kohdistuneita kyberuhkia. Jo hyvin varhaisessa vaiheessa aineistonkeruuprosessia ilmeni, että raportit keskittyvän laajaan kyberturvallisuusuhkakenttään kokonaisvaltaisesti. Esimerkiksi Euroopan unionin kyberturvallisuudesta vastaavan viraston (ENISA) vuosittaiset uhkaympäristöraportit keskittyivät nimenomaisesti Euroopan unioniin tai sen lähialueelle kohdistuviin kyberuhkiin kokonaisuutena (ENISA, 2021, s. 10). Tällöin ne saattoivat mainita vesihuoltoon kohdistuvia kyberuhkia määrällisesti, mutta jättäen mainitsematta mihin, miten tai kenen toimesta kyberuhka oli vesihuoltoon kohdistunut (ENISA, 2020a; ENISA, 2020b; ENISA, 2021, s 12; National Cyber Security Centre, 2022). Osassa valtiollisten toimijoiden julkaisuja saattoi olla esimerkkejä tapahtuneista vesihuoltoon kohdistuneista kyberhyökkäyksistä, mutta ne eivät kokonaisuudessaan kattaneet kaikkia merkittävimpiäkään kansainvälisiä vesihuoltoon kohdistuneita hyökkäyksiä, vaan pysyivät yleisesti kansallisella tasolla (CISA, 2021a; NJCCIC, 2023).

Koska virallisten tahojen raportit ja julkaisut keskittyivät kybertoimintaympäristön uhkaympäristöön pääosin kokonaisuutena, aineistona käytettiin yksityiskohtien löytämiseen lisäksi paljon paikallisia uutisjulkaisuja sekä yksityisiä kyberuhkia tai kyberturvallisuutta yleisesti käsitteleviä tahoja. Lähteet vaihtelevat paikallisuutisista aina kyberturvallisuutta yleisesti käsittelevien julkaisujen analyyseihin tapahtuneesta, myös hyökkääjän näkökulmasta. Uutislähteissä usein haastatellaan hyökkäyksen kohteeksi joutunutta vesihuollosta vastaavaa tahoa, joka on voinut haastatteluissa antaa enemmän tietoa kuin virallisessa julkaisussa on ollut. Vaillinaisesti viitteistettyjä uutisia tai julkaisuja hyödynnettäessä on syytä kuitenkin muistaa, että tarinaa on voitu liioitella tai joitain yksityiskohtia vähätellä sekä peitellä. Erityisesti hyökkääjä haluaa korostaa onnistumistaan, kun taas mahdollisesti uhriksi joutunut vesihuollon vastaava toimija haluaa mahdollisesti julkaisuissaan rauhoitella asiakas- tai omistajakuntaansa.

On syytä huomioida, että tutkimuksessa esitellyt vesihuoltoon kohdistuneet kyberhyökkäykset eivät edusta absoluuttista määrää hyökkäyksistä, vaan ovat julkisuuteen esiteltyjä, vuotaneita tai paljastettuja kyberhyökkäyksiä. Osa uhriksi joutuneista vesihuollosta vastaavista tahoista on julkaissut tapahtuneesta kyberhyökkäyksestä tiedotteen, osa tapahtumista on taas tullut esiin kyberhyökkäyksen vaikutuksista kärsineiden ulostulojen takia ja osa on hyökkääjien itsensä julkaisemia tapahtumia. On siis täysin mahdollista, että 2020-luvulla on tapahtunut lukuisia kyberhyökkäyksiä, joiden vaikutusta ei ole kyetty edes havaitsemaan, jotka kyettiin torjumaan tai joita ei ole vain ilmoitettu vesihuollosta vastaavien tahojen toimesta viranomaiselle tai asianomaisille. Aineiston keruu on myös rajoittunut tutkielman tekijän kielitaidon vuoksi englannin kielellä raportoiviin ja uutisoiviin tahoihin, joka rajaa aineiston keruusta ulos suurimman osan maailman väestöstä ja osan merkittävistä toimijoista vesihuollon kuin myös kyberturvallisuuden saralla. Joissain tapauksissa englanninkielisistä lähteistä on siirrytty paikallisiin muun kielisiin lähteisiin, joiden tarkastelussa on hyödynnetty automaattisia kääntäjiä. Tällöin varsinkin pienempiä tapahtuneita kyberhyökkäyksiä, joilla ei ole ollut merkittävää uutisarvoa, on voinut jäädä aineiston ulkopuolelle.

6.1 Tapahtuneet kyberhyökkäykset

2020-luvun ensimmäisiä vesihuoltoon kohdistuvia hyökkäyksiä oli Israelissa huhtikuussa vuonna 2020 tapahtunut vedenpuhdistuslaitoksiin kohdistunut hyökkäys, josta Israelin valtiollinen The National Cyber Array (2020) julkaisi tiedotteen kannustaen vaihtamaan vesi- ja energiasektoreilla toimivien järjestelmien salasanat (Staff, 2020a). Hyökkääjät pääsivät vaikuttamaan vedenpuhdistuslaitoksien ja jätevedenpuhdistuslaitoksien järjestelmiin alueellisesti (Staff, 2020a). Hyökkäys kohdistui hallintalaitteisiin, joilla ohjattiin vedenjakelujärjestelmän venttiileitä (DHS, 2021, s. 1). Hyökkäys kyettiin havaitsemaan ajoissa, jolloin hyökkäyksellä ei ollut vaikutusta pitkäaikaista vaikutusta vesihuollon toimintaan (DHS, 2021, s. 1). Mikään taho ei ottanut vastuuta hyökkäyksestä, mutta hyökkäystä epäiltiin valtiollisen tahon toteuttamaksi (Wall, 2022).

Muutama kuukausi myöhemmin israelilaisiin maataloudessa käytettäviin vesipumppuihin kohdistui kyberhyökkäys (Staff, 2020b). Hyökkäys vaikutti maataloudessa käytettävän veden pumppuihin ja yleisesti vesihuollon järjestelmiin alueellisesti Ylä-Galileassa ja Matte Yehudassa (Ahya, 2020; Staff, 2020b). Hyökkäyksen kohteeksi joutuneet pumput kyettiin pikaisesti korjaamaan, eikä hyökkäyksellä ollut merkittävää vaikutusta kastelun jatkumiselle tai vesihuollon toiminnalle (Ahya, 2020; Staff, 2020b). Mikään taho ei jälleen ottanut vastuuta hyökkäyksestä, mutta sen uskottiin olevan osa Iranin ja Israelin välistä kyberkamppailua (Staff, 2020b).

Yhdysvalloissa Kalifornian osavaltiossa Camrosa vesipiirin asiakkailleen lähettämän tiedotteen mukaan heidän palvelimensa olivat tulleet kiristysohjelman salaamiksi vuoden 2020 elokuussa (Stafford, 2020, s.1). Asiakkaiden ja

työntekijöiden henkilökohtaisia tietoja, kuten tilitietoja ja henkilötunnuksia oli saattanut vuotaa hyökkääjien käsiin, mutta tästä ei ollut täyttä varmuutta (Stafford, 2020, s.1). Tiedotteessa ei tullut esiin hyökkäykseen syyllistynyttä tahoa, mutta Camrosa vakuutti parantaneensa järjestelmiensä kyberturvallisuutta hyökkäyksen jälkeen (Stafford, 2020, s.1). Hyökkäyksestä vastuullista tahoa ei raportissa nimetty.

Syyskuun lopussa vuonna 2020 New Jerseyssä Yhdysvalloissa tapahtunut kyberhyökkäys esti pääsyn vesihuollon toiminnan kannalta oleellisiin tietoihin, kuten vesi- ja viemäriverkon tietoihin (D'Auria, 2021). Hyökkääjät hyödynsivät mahdollisesti Makop-kiristysohjelman uutta versiota, joka esti pääsyn vesihuollon tietoihin salaten ne ja vaatien tietojen vapauttamisesta lunnaita (NJCCIC, 2022; CISA, 2021a). Tarkalleen sitä, mitä tietoja salattiin ei ollut tiedossa, mutta hyökkäys oli silti vaarantanut vesihuollon asiakkaiden terveyden, turvallisuuden ja hyvinvoinnin (D'Auria, 2020). Palautuminen hyökkäyksestä ei ollut nopeaa, vaan kesti paikallisen uutisjulkaisun mukaan kuukausia (D'Auria, 2021). Hyökkäyksen jälkeen vesihuollosta vastuussa ollut valtuusto solmi kyberturvallisuusyrityksen kanssa satojen tuhansien arvoisen sopimuksen tarkoituksena parantaa järjestelmien kyberturvallisuutta ja palauttaa menetetyt tiedot (D'Auria, 2021). Hyökkäyksestä vastuullista tahoa ei uutisoinnissa nimetty.

Vuoden 2020 joulukuussa Israelissa kohdistui kyberhyökkäys vesivarantoon (Even, 2020). Hyökkääjät pääsivät käsiksi vesivarannon HMI-järjestelmään (Human Machine Interface) eli käyttöliittymään, joka oli suojaamattomassa yhteydessä internetiin (Even, 2020). Altistunut järjestelmä mahdollisti hyökkääjille esimerkiksi vedenpaineen tai lämpötilan muokkaamisen, mutta vaikutusta vesihuollon toimintaan ei kuitenkaan ilmoitettu viranomaisten toimesta ja pääsy järjestelmään oli seuraavana päivänä salasanasuojattu (Even, 2020). Vastuun hyökkäyksestä otti sen julkaissut iranilainen Unidentified TEAM, joka on tehnyt muitakin kyberhyökkäyksiä eri maihin ja kohteisiin (Even, 2020).

Vuosi 2020 jakautui ENISA:n raporteissa kahteen osuuteen. Vuoden 2020 (a, 2020b) raportti koski aikaa vuonna 2020 tammikuusta huhtikuuhun ja vuoden 2021 raportti jatkui siitä vuoden 2021 heinäkuuhun saakka. ENISA:n vuoden 2020 (a, 2020b) raportti ei yksilöinyt vesihuoltoon kohdistuneita kyberhyökkäyksiä eikä erotellut vesihuoltoa omaksi osa-alueekseen tarkastellessaan tapahtuneita hyökkäyksiä. ENISA:n (2021, s 12) raportin mukaan vuonna 2020 huhtikuusta heinäkuuhun on tapahtunut yksi vesihuoltoon kohdistunut hyökkäys joka kuukausi heidän tekemänsä avoimien lähteiden tiedustelun perusteella, eli yhteensä neljä kappaletta. Kuitenkaan raportissa ei ole eritelty sitä, mihin vesihuollon osa-alueisiin nämä hyökkäykset ovat kohdistuneet, missä maissa tai miten ne on toteutettu. On täten haastavaa sijoittaa esimerkiksi Israelin huhtikuun ja kesän kyberhyökkäyksiä ENISA:n (2021) raporttiin, sillä ei voida olla varmoja, tarkoitetaanko raportin merkinnöillä nimenomaisesti näitä kyberhyökkäyksiä vai muita kyberhyökkäyksiä. Sen lisäksi raportissa ilmenneistä (ENISA, 2021, s. 12) toukokuun tai kesän tapauksista ei löytynyt muualta ilmoituksia tai raportteja.

Vuoden 2021 ensimmäinen vesihuoltoon kohdistunut kyberhyökkäys osui kalifornialaiseen San Franciscon kaupungin vesihuoltolaitokseen, jossa hyökkääjä onnistui poistamaan veden puhdistuksen hallinnassa käytetyt tietokoneohjelmat (Collier, 2021). Hyökkäys toteutettiin NBC-uutisten näkemän Northern California Regional Intelligence Center:n raportin mukaan yhden laitoksen työntekijän TeamViewer-etähallintaohjelman tunnuksia ja salasanaa käyttäen (Collier, 2021). Hyökkäys havaittiin vasta seuraavana päivänä, jolloin ohjelmat asennettiin uudestaan ja tilanne palautui normaaliksi (Collier, 2021). Hyökkäys ei tuottanut vahinkoa veden laadulle (Collier, 2021). Paria vuotta myöhemmin syylliseksi epäiltyä entistä vesihuoltolaitoksen työntekijää vastaan nostettiin syyte ohjelmien poistamisesta ja palvelimien sammuttamisesta, josta hänet voitaisiin tuomita jopa kymmeneksi vuodeksi vankilaan ja satojen tuhansien dollarien sakkoihin (DOJ, 2023).

Heti seuraavana kuukautena floridalaiseen Oldsmarin kaupungissa sijaitsevaan vesihuoltolaitokseen uskotaan kohdistuneen hyvin samanlainen kyberhyökkäys kuin San Franciscon kaupungin vesihuoltolaitokseen, jonka seurauksena hyökkääjä sai hallintaansa laitoksen SCADA-järjestelmän eli valvomoohjelmiston (CISA, 2021b, s. 1). Hyökkääjä yritti nostaa vedenpuhdistusprosessissa käytetyn emäksisen lipeän määrää vedessä, mutta laitoksen henkilöstö havaitsi poikkeaman ennen kuin sillä oli vaikutusta veden laatuun (CISA, 2021b, s. 1). Yhdysvaltalainen kyberturvallisuudesta ja infrastruktuurista vastaava turvallisuusviraston (CISA) (2021b, s. 1) julkaisemassa eri virastojen yhteisraportissa hyökkäyksen uskotaan käyttäneen hyödyksi kohdejärjestelmässä käytettyjen salasanojen vaillinaisuutta ja kohteen vanhentunutta käyttöjärjestelmää sekä mahdollisesti järjestelmän hallinnan etäkäyttöön asennettua TeamViewer-ohjelmaa. Käytetty käyttöjärjestelmä, Windows 7, oli elinkaarensa päässä eikä se ollut saanut turvallisuuteenkaan liittyviä järjestelmäpäivityksiä kokonaiseen vuoteen johtuen sen elinkaarituen loppumisesta (CISA, 2021b, s. 2). Kaksi vuotta myöhemmin Oldsmarin kaupungin virkamiehenä tapahtuman aikaan ollut henkilö toi julkishallinnon järjestön seminaarissa esiin, että kyberhyökkäystä ei välttämättä ollut tapahtunutkaan, vaan kyse oli käyttäjävirheestä (Axelbank, 2023; Chawaga, 2023).

Yhdysvaltojen Kaliforniassa oleva Metropolitan Water District of Southern California joutui Pulse Connect Secure-ohjelmassa olevien haavoittuvuuksien vuoksi hakkeroiduksi yhdessä useiden muiden kriittisten infrastruktuurin sekä muiden toimijoiden kanssa (Suderman, 2021). Haavoittuvuudet mahdollistivat sen, että hyökkääjät pystyivät asentamaan järjestelmiin lisää takaportteja, joilla he edelleen pääsivät entistä syvemmälle altistuneisiin järjestelmiin mahdollistaen niiden etäkäytön (CISA, 2021c). Vesihuollon tiedottajan mukaan sisäisiä tietoja ei olisi tiedettävästi joutunut hyökkääjien käsiin (Suderman, 2021). Mikään taho ei ole ilmoittautunut tietomurron tekijäksi, mutta kyseessä saattoi olla valtiollinen toimija (Suderman, 2021).

Myös Pennsylvanian osavaltion kahteen vesihuoltolaitokseen uskotaan samana vuonna kohdistuneen tietomurtoja, joiden seurauksena hyökkääjät saivat asennettua etäkäyttöohjelman järjestelmiin (Van Osdol, 2021). Uutisoinnin

mukaan hyökkäys kuitenkin havaittiin ja torjuttiin ilman suurempaa vaikutusta vesihuoltolaitoksen toiminnalle (Van Osdol, 2021). Hyökkäyksestä vastuullista tahoa ei uutisoinnissa nimetty.

Yhdysvaltojen eri osavaltioiden vesihuoltolaitoksiin kohdistui vuonna 2021 tietomurtojen lisäksi kyberhyökkäyksiä kiristysohjelmien muodossa. Maaliskuussa Nevadassa olevan laitoksen SCADA-järjestelmä ja varajärjestelmät joutuivat tuntemattoman kiristysohjelman uhriksi (CISA, 2021a). Tarkempaa tietoa hyökkääjästä tai hyökkäyksen kattavuudesta ei ole julkaistu.

Toukokuussa Marylandin osavaltiossa vesihuollosta vastaavan yrityksen WSSC Waterin yritystoiminnasta vastaavat tietojärjestelmät joutuivat kiristysohjelman uhriksi (Brown, 2021). Kesäkuussa julkaistussa tiedotteessa yritys ilmoitti, että kiristysohjelma poistettiin tunneissa havaitsemisesta, eikä käytännön vesihuollon toiminnalle kohdistunut mitään vaaraa (Brown, 2021). Kuitenkin joitakin asiakastietoja sekä henkilötietoja oli saattanut joutua hyökkäyksen myötä rikollisten käsiin (Brown, 2021). WSSC Water ei tuonut esille hyökkääjiä sen tarkemmin, vaan mainitsi heidät yleisesti rikollisina (Brown, 2021).

Heinäkuussa kaksi Mainen osavaltiossa sijaitsevaa haja-asutusalueiden jätevesihuoltolaitoksien SCADA-järjestelmää saastui ZuCaNo-kiristysohjelmasta, joka pakotti laitokset hoitamaan vedenpuhdistuksen paikallisesti ja manuaalisesti lisämiehityksellä (CISA, 2021a). Viranomaisten mukaan asiakkaiden tietoja ei vuotanut hyökkääjille eikä hyökkäyksestä aiheutunut yleistä turvallisuusuhkaa (Wood, 2021). Kuitenkin Mainen osavaltion veden laadusta vastaava taho julkaisi tiedotteen, joka painotti vesihuoltoon kohdistuvien kyberhyökkäysten kykenevän mahdollisesti merkittäviin fyysisiin ja rahallisiin tuhoihin (Kavanah, 2021). Hyökkäyksestä vastuullista tahoa ei uutisoinnissa nimetty.

Kuukauden kuluttua edellisestä kiristysohjelmahyökkäyksestä, kalifornialaisen vesihuoltolaitoksen havaittiin joutuneen Ghost-kiristysohjelman uhriksi elokuussa (CISA, 2021a). Ghost-kiristysohjelman epäiltiin olleen SCADA-järjestelmässä noin kuukauden ajan ennen havaitsemista (CISA, 2021a). Tarkempaa tietoa hyökkääjästä tai hyökkäyksen kattavuudesta ei ole julkaistu.

ENISA (2021, s. 12) esittää vuosiraportissaan, että vuoden 2021 alkupuolella, tammikuusta heinäkuuhun, ei tapahtunut Euroopan unionin alueella tai sen lähialueella yhtään vesihuoltoon kohdistunutta kyberhyökkäystä. Kuitenkin vuoden 2021 jälkipuoliskolla ja vuoden 2022 ensimmäisellä puolikkaalla ENISA:n (2022, s. 14–18) raportista selviää, että vesihuoltoon on kohdistunut yksi tai muutamia kyberhyökkäyksiä. Näiden hyökkäysten merkitys on kuitenkin monilta osin jäänyt vähäiseksi tai tuntemattomaksi, eikä niitä on sen tarkemmin raportissa yksilöity tai tarkasteltu (ENISA, 2022, 14–18). Vuoden 2022 jälkipuoliskoa ja vuoden 2023 alkupuolta käsittelevä ENISA:n (2023, s. 14–15) raportti tuo esiin sen, että Euroopan ja sen lähialueiden vesihuolto on joutunut kiristysohjelmien, palvelunestohyökkäyksien, tietomurtojen, haittaohjelmien ja sosiaalisen manipuloinnin kohteeksi kyseisellä ajanjaksolla. Hyökkäyksiä ei kuitenkaan käsitellä yksityiskohtaisesti ja ne ovat määrällisesti muihin sektoreihin nähden hyvin vähäisiä (ENISA, 2023, 14–15).

Yhdistyneiden kuningaskuntien vesihuollon osa South Staffordshire PLC, South Staffs Water- ja Cambridge Water-vesihuoltoyhtiöiden isäntäyhtiö, joutui kyberhyökkäyksen kohteeksi elokuussa vuonna 2022 julkaistun tiedotteen mukaan (South Staffs Water, 2022). Hyökkääjät pääsivät käsiksi yhtiön asiakkaiden henkilökohtaisiin tietoihin, mukaan lukien asiakkaiden nimiin, osoitteisiin ja pankkikorttitietoihin (WaterISAC, 2022). Hyökkääjiksi ilmoittautui Cl0p-kiristysohjelmaryhmä, joka väitti päässeensä asiakastietojen lisäksi vesihuoltolaitoksen SCADA-järjestelmään (WaterISAC, 2022). Itse uhriksi joutunut yhtiö on tuonut esiin vain sen, että asiakastietoja on joutunut hakkereiden käsiin ja niitä on osin myös vuotanut julkisuuteen (WaterISAC, 2022). Uhriksi joutuneen yhtiön tytäryhtiön julkaisun mukaan hyökkäys ei vaikuttanut vesihuollon toimintaan tai puhdistetun veden laatuun (South Staffs Water, 2022).

Vuoden 2023 helmikuussa Italiassa Rooman kaupungin vedenjakelusta vastaava yritys joutui kyberhyökkäyksen kohteeksi, joka ei kuitenkaan päässyt vaikuttamaan käytännön vedenjakeluun (Kaspersky, 2023, s. 21). Hyökkäyksen tehnyt kiristysohjelmaryhmä Black Basta ei yrityksen tiedotuksen mukaan päässyt käsiksi henkilökohtaisiin tietoihin, sillä yrityksen oma kyberturvallisuusryhmä yhteistyössä Italian kansallisen kyberturvallisuusviraston kanssa onnistui torjumaan ja palautumaan hyökkäyksestä alle viikossa. (Agenzia Nova, 2023).

Vuoden 2023 helmikuussa portugalilainen vesihuolto- ja energiayritys ilmoitti joutuneensa kyberhyökkäyksen kohteeksi, mutta samalla rauhoitellen, että vesihuollon käytännön toimintaan tai turvallisuuteen ei ollut kohdistunut häiriöitä (Porto, 2023). Hyökkäyksestä vastuun otti LockBit-kiristysohjelmaryhmä, joka väitetysti sai salattua osan yrityksen tiedoista, kuitenkin vain hidastaen asiakaspalveluaikoja (Greig, 2021c).

Vuoden 2023 maaliskuussa Puerto Ricon vesihuollosta vastaava taho joutui kyberhyökkäyksen kohteeksi, jossa kiristysohjelmaryhmä Vice Society sai haltuunsa asiakkaiden henkilötietoja sisältäviä asiakirjoja, kuten passien ja ajokorttien kuvia (Greig, 2023d). Kyberhyökkäys ei kuitenkaan vaikuttanut vesihuollon käytännön toimintaan, johtuen viranomaisten mukaan verkon jakautumisesta eri osiin, joka suojasi koko järjestelmää vaarantumasta (Greig, 2023d).

Vuoden 2023 huhtikuussa noin kymmenen eri maanviljelijän israelilaista maatalouden kastelujärjestelmää joutui kyberhyökkäyksen kohteeksi, joka väliaikaisesti keskeytti kastelun alueella (JNS, 2023). Vedenohjauslaitteiden näytöillä oli viesti, joka ilmoitti järjestelmän joutuneen hakkeroinnin kohteeksi sekä julistus ”DOWN WITH ISRAEL” (JNS, 2023). Hyökkäyksestä saatiin ennakkovaroitus, jonka vuoksi merkittävää vahinkoa ei tapahtunut ja kastelua jatkettiin manuaalisesti (JNS, 2023). Vastuullista tahoa hyökkäykselle ei ole tiedossa, mutta hakkerien jättämä viesti on luonteeltaan poliittinen ja hyvin samankaltainen kuin iranilaisen CyberAv3ngers-ryhmän jättämä sen tekemän hakkeroinnin jälkeen (CISA, 2023).

Euroopassa italialainen vesihuollon yritys Alto Calore Servizi SpA joutui kyberhyökkäyksen kohteeksi, jossa yrityksen tietokantojen sisältö altistui hyökkääjien kiristykselle (CERT-EU, 2023, s. 3). Iskun takana oli Medusa-

kiristysohjelmaryhmä, jonka hyökkäys ei vaikuttanut itse vesihuollon käytännön toimintaan, mutta asiakkaiden henkilötietoja, vesihuoltoverkoston tietoja ja muita tietoja joutui hyökkääjien salaamaksi (Greig, 2023a). Hyökkäys esti yritystä pääsemästä käsiksi tietokannassa olevaan tietoon ennen sen palautumista (Greig, 2023a).

Vuoden 2023 marraskuussa Yhdysvalloissa Pennsylvanian osavaltiossa kyberhyökkäyksen toteuttanut CyberAv3ngers-ryhmä pääsi murtautumaan kahteen veden paineistusasemaan (WaterISAC, 2023). Hyökkäys ei päässyt vaikuttamaan vedenpaineeseen, sillä järjestelmä antoi hyökkäyksen tapahtuessa hälytyksen, jonka vuoksi paineistukseen käytettäviä laitteita käytettiin manuaalisesti (WaterISAC, 2023). Hyökkääjät kohdistivat hyökkäyksensä tarkoituksella israelilaisiin ohjelmoitaviin logiikkoihin (PLC), joita käytetään yleisesti vesihuollon eri automatisoiduissa järjestelmissä, mutta myös muilla sektoreilla (CISA, 2023, s. 1). Hyökkääjät hyväksikäyttivät käytetyn ohjelmoitavan logiikan internetiin vuotaneita oletussalasanoja ja oletusportin numeroa (CISA, 2023, s. 2). Yhdysvaltalainen kyberturvallisuudesta ja infrastruktuurista vastaava turvallisuusvirasto julkaisi joulukuussa 2023 tiedotteen, jossa nimesi CyberAv3ngers-ryhmän ja paljasti sen nimissä tehdyn useita yksilöimättömiä hyökkäyksiä yhdysvaltalaisiin vesihuollon järjestelmiin, jotka ovat hyödyntäneet israelilaisia ohjelmoitavia logiikoita toiminnassaan (CISA, 2023).

Samalla viikolla edellisestä Yhdysvalloissa Texasin pohjoinen vesihuoltopiiri, joka vastaa kahden miljoonan ihmisen vesihuollon toimivuudesta, joutui kyberhyökkäyksen kohteeksi (Greig, 2023b). Vesihuoltopiirin tiedottajan mukaan tutkimukset olivat edelleen käynnissä, mutta tiedossa oli, että hyökkäys kohdistui yrityksen tietoverkkoon eikä vaikuttanut vesihuollon käytännön toimintaan (Greig, 2023b). Kuitenkin vastuun hyökkäyksestä ottanut Daixin–kyberrikollisryhmä väitti varastaneensa ja vuotaneensa vesihuoltopiirin asiakkaiden henkilökohtaisia tietoja, kuten henkilötunnuksia ja osoitteita (Paganini, 2023). Yrityksen puhelinjärjestelmä oli myös muutamia päiviä poissa käytöstä (Greig, 2023b).

Marraskuussa Pariisin vesihuollosta vastaava SIAAP julkaisi tiedotteen, jossa se kertoi joutuneensa kyberhyökkäyksen kohteeksi (SIAAP, 2023). Tarkempaa tietoa hyökkäyksen laadusta tai vaikutuksesta ei kuitenkaan ole kerrottu tai tuotu esiin viranomaisten toimesta, eikä mikään ryhmä ole ottanut vastuuta hyökkäyksestä (Greig, 2023e).

Vuoden 2023 joulukuussa Western People-lehti uutisoi irlantilaisen hajaasutusseudun yksityisen vesihuollon joutuneen kyberhyökkäyksen kohteeksi, joka pysäytti vedenjakelun kahdeksi päiväksi (Quinn, 2023). Hyökkäys pysäytti vesihuoltoverkoston pumppausaseman, joka onnistuttiin käynnistämään manuaalisesti kaksi päivää hyökkäyksen havaitsemisesta (Quinn, 2023). Hyökkäyksen epäiltiin olleen poliittisesti kohdistettu nimenomaisesti Israelista hankittuja järjestelmiä kohtaan, mahdollisen valtiollisen toimijan toimesta (Quinn, 2023).

Floridassa samoihin aikoihin vesihuollosta alueellisesti vastaava St. Johns River Water Management District ilmoitti tulleensa hyökkäyksen kohteeksi,

mutta onnistuneesti eristäneensä hyökkäyksen (Greig, 2023f). Kiristysohjelmaryhmä ilmoittautui iskun tekijäksi, mutta tarkalleen ei ole tiedossa, kuinka paljon vahinkoa hyökkäys sai aikaan tai kuinka paljon tietoa päätyi hyökkääjien käsiin (Greig, 2023f).

Vuosi 2024 on tämän tutkielman kirjoittamisen aikaan vasta alkanut, eikä sen aikana tapahtuneista vesihuoltoon kohdistuneista kyberhyökkäyksistä ole täten vielä vuosiraportteja. Kuitenkin yksittäisiä tapahtumia voidaan nostaa esille. Kansainvälinen vesihuolto- ja energiayritys Veolia ilmoitti tiedotteessaan osan heidän Pohjois-Amerikan vesihuollon ohjelmistoista joutuneen kiristysohjelman kohteeksi (Veolia, 2024). Hyökkäys ei Veolian tiedotteen mukaan vaikuttanut itse vesihuollon käytännön toimintaan. Kuitenkin yrityksen laskutuspalvelut olivat viivästyneet sekä osan asiakkaiden henkilökohtaisista tiedoista oli saattanut vuotaa hyökkääjille. (Veolia, 2024) Laskutusjärjestelmät olivat poissa käytöstä, kunnes ne saatiin palautettua (Veolia, 2024). Hyökkäyksestä vastuullista tahoa ei uutisoinnissa tai tiedotteessa nimetty.

Yhdistyneiden kuningaskuntien Englannin eteläosien vedestä vastaava Southern Water ilmoitti tutkivansa tammikuun 2024 tiedotteessaan mahdollista tietomurtoa, jossa asiakkaiden tietoja olisi joutunut vääriin käsiin (Southern Water, 2024a). Southern Water (2024b) ilmoitti helmikuussa julkaistussa tiedotteessa, että 5–10 prosenttia asiakaskunnan ja osan työntekijöiden tiedoista oli vuotanut kyberhyökkääjille. Vastuun hyökkäyksestä otti Venäjään yhdistetty Black Basta-kiristysohjelmaryhmä, joka väitti saaneensa haltuunsa yli 750 gigatavua Southern Waterin asiakastietoja sekä sisäisiä dokumentteja (Page, 2024).

Alla olevassa taulukossa 2 on tiivistetty tutkimuksessa esitellyt vesihuollon eri osa-alueisiin kohdistuneet kyberhyökkäykset. Taulukko 2 esittää vuoden tarkkuudella sen, milloin kyberhyökkäys on kohdistunut, mihin maahan se on kohdistunut, millä tavoin ja mikä on ollut sen lopullinen kohde. Kohteet on jaoteltu tietokantoihin, vedenpuhdistuslaitoksiin, vesihuoltoverkostoon ja loppukäyttäjän järjestelmiin, kuten kastelujärjestelmiin.

TAULUKKO 2 Vesihuoltoon kohdistuneet kyberhyökkäykset

Vuosi	Tapahtumapaikka	Uhka	Kohde
2020	Israel	Tietomurto	Vedenpuhdistuslaitos
2020	Israel	Tietomurto	Loppukäyttäjän järjestelmä, vedenpuhdistuslaitos
2020	Yhdysvallat, Kalifornia	Kiristysohjelma	Tietokannat
2020	Yhdysvallat, New Jersey	Kiristysohjelma	Tietokannat
2020	Israel	Tietomurto	Vedenpuhdistuslaitos
2021	Yhdysvallat, Kalifornia	Tietomurto	Vedenpuhdistuslaitos
2021	Yhdysvallat, Florida	Tietomurto	Vedenpuhdistuslaitos
2021	Yhdysvallat, Kalifornia	Tietomurto	Tietokannat, vedenpuhdistuslaitos
2021	Yhdysvallat, Pennsylvania	Tietomurto	Tietokannat, vedenpuhdistuslaitos
2021	Yhdysvallat, Nevada	Kiristysohjelma	Vedenpuhdistuslaitos
2021	Yhdysvallat, Maryland	Kiristysohjelma	Tietokannat
2021	Yhdysvallat, Maine	Kiristysohjelma	Vedenpuhdistuslaitos
2021	Yhdysvallat, Kalifornia	Kiristysohjelma	Vedenpuhdistuslaitos
2022	Yhdistynyt kuningaskunta	Kiristysohjelma	Tietokannat
2023	Italia, Rooma	Kiristysohjelma	Tietokannat
2023	Portugali	Kiristysohjelma	Tietokannat
2023	Yhdysvallat, Puerto Rico	Kiristysohjelma	Tietokannat
2023	Israel	Haittaohjelma	Loppukäyttäjän järjestelmä
2023	Italia	Kiristysohjelma	Tietokannat
2023	Yhdysvallat, Pennsylvania	Tietomurto	Vedenpuhdistuslaitos
2023	Yhdysvallat, Texas	Tietomurto	Tietokannat
2023	Ranska, Pariisi	Ei tietoa	Ei tietoa
2023	Irlanti, Erris	Haittaohjelma	Vesihuoltoverkosto
2023	Yhdysvallat, Florida	Tietomurto	Ei tietoa
2024	Pohjois-Amerikka	Kiristysohjelma	Tietokannat
2024	Yhdistynyt kuningaskunta	Kiristysohjelma	Tietokannat

6.2 Tapahtuneiden kyberhyökkäyksien analyysi

Aineisto analysoitiin teoriaohjaavasti teemoittelemalla vesihuoltoon kohdistuvan kyberuhan näkökulmasta. Aineiston analyysi suoritettiin kuusiportaisesti, aloittaen vaiheessa yksi lukemalla kerätty aineisto useaan kertaan. Lukemisen aikana aineistoa pohdittiin kyberuhan näkökulmasta, etsien siitä tutkimukselle kiinnostavia seikkoja sekä yksityiskohtia lainauksien muodossa. Vaiheessa kaksi aineistosta esiin nousseet kiinnostavat sekä toistuvat seikat nimettiin koodisanoilla, jotta analyysin jatkuessa näistä kyettiin muodostamaan edelleen teemoja. Koodit pyrkivät kuvailemaan lainauksen suhdetta tapahtuneeseen kyberhyökkäykseen. Aineiston analyysiä kirjattiin tapahtuneiden kyberhyökkäysten mukaisesti tapahtumajärjestyksessä Excel-pöytäkirjaan, jossa jokaisesta lainauksesta kävi ilmi, mihin kyberhyökkäykseen se liittyi, mistä lähteestä lainaus oli ja vaiheessa kaksi, mikä koodaus lainaukselle annettiin. Kuviossa 6 on esitelty esimerkki aineiston analyysissä käytetystä taulukosta.

Vuosi	Maa	Kohde	Lähde	Lainaus	Koodaus	Alateema	Teema
2021	Yhdysvallat, Kalifornia	Vedenpuhdistuslaitos	Collier, 2021	After logging in, the hacker, whose name and motive are unknown and who hasn't been identified by law enforcement, deleted programs that the water plant used to treat drinking water.	Hyökkäystapa	Tapa	Hyökkäys
2021	Yhdysvallat, Kalifornia	Vedenpuhdistuslaitos	Collier, 2021	The hack wasn't discovered until the following day, and the facility changed its passwords and reinstalled the programs.	Ensivaste	Ensireaktio	Seuraamus

KUVIO 6 Esimerkki tehdystä koodauksesta ja teemoittelusta

Vaiheessa kolme tarkasteltiin muodostettuja koodeja kokonaisuutena, pyrkien etsimään muodostuvia teemoja. Tähän apuna hyödynnettiin visuaalisia kaavioita, joilla pystyi tarkastelemaan, oliko joitain koodisanoja enemmän kuin toisia ja mitkä koodisanat nousivat esiin määrällisesti analyysistä. Tämän perusteella tultiin siihen johtopäätökseen, että osa koodeista oli merkittävyydeltään niin vähäisiä, että ne eivät analyysissä kiinnostaneet ja että osa niistä voitaisiin yhdistää merkityksellisempiin koodeihin. Koodeja vertailtiin toisiinsa ja poimit-

tuihin lainauksiin, jotta ne olisivat yhdenmukaisia ilman, että saman koodin aihealuetta kuvasti useita eri koodinimiä. Tarkastelun aikana aineistosta nousi esiin kolme vahvaa teemaa, joihin koodit luontaisesti jakautuivat. Teemat kuvasivat kyberhyökkäystä, kyberhyökkäyksen aiheuttamaa vahinkoa ja mitä seuraamuksia tapahtuneella kyberhyökkäyksellä oli. Muodostettuja teemoja tarkasteltiin muuhun aineistoon nähden vaiheessa neljä, jossa teemat vakiinnuttivat paikkansa, mutta myös jakautuivat osiin alateemoiksi selittämään kyberhyökkäyksiä, niiden aiheuttamia vahinkoja ja kyberhyökkäyksien seuraamuksia yksityiskohtaisemmin. Aineistosta nousseet teemat ja niiden alateemat on esitetty kuviossa 7.

Alateemat	Teemat
Tekijä	Hyökkäys
Tapa	
Kohde	
Ei vahinkoa	Vahinko
Mahdollinen vahinko	
Aiheutettu vahinko	
Ensireaktio	Seuraamus
Vahingon korjaaminen	
Tiedottaminen	
Yhteistoiminta	
Toimintojen päivittäminen	

KUVIO 7 Aineistosta havaitut teemat ja niiden alateemat

Seuraavassa vaiheessa kirjoitettiin aineiston analyysi, jossa aineiston analyysiä esiteltiin luotujen teemojen sekä aliteemojen avulla. Tehdyn analyysin perusteella tuotiin esiin vastaukset tutkielman esitettyihin tutkimuskysymyksiin.

6.2.1 Hyökkäys

Kerätyn aineiston analysoinnissa kyberuhkan näkökulmasta nousi ensimmäisenä teemana esiin itse kyberhyökkäys. Kyberhyökkäys terminä rajaa tapahtuneen kyberuhan olevan nimenomaisesti tahallinen, joko ulkopuolisen tai sisäpiiriläisen tekemänä (Raggad, 2010, s. 84). Käytännössä kaikki aineistossa olleet 26 tapausta olivat hyökkäyksiä. Yhdessä tapauksista oli mahdollista, että sisäpiiriläinen oli vahingossa aiheuttanut hyökkäyksen kaltaisen tilanteen. Ilman virallista tiedotetta sitä tapausta kohdellaan aineistossa kuten muitakin kyberhyökkäyksiä. (Axelbank, 2023; Chawaga, 2023)

Tapahtuneita kyberhyökkäyksiä tarkasteltaessa oli syytä analyysin helpottamiseksi jakaa tapahtunut hyökkäys edelleen alateemoihin, joista kukin piti

sisällään olennaisen osan itse hyökkäyksestä. Analyysissä havaittu ensimmäinen hyökkäyksen alateema oli hyökkäyksen tekijä. Hyökkäyksen tekijä nousi esiin aineistosta, sillä hyökkäyksillä oli useita tekijöitä, eri tarkoitusperiä sekä ne olivat ulkoisia sekä sisäisiä. Kun on tarkasteltu kyberhyökkäyksen tekijää, kuten Muckin & Fitch (2019, s. 6) uhkamallissa, luonnollinen jatkumo sille on, mitä haavoittuvuutta tai hyökkäysvektoria tekijä on hyödyntänyt eli, mikä on ollut hyökkäyksen tekotapa. Aineistosta selvisi useita tapoja, joilla hyökkäyksien tekijät pääsivät vaikuttamaan vesihuollon eri osa-alueisiin. Näitä osa-alueita tarkastellaan jälleen Muckin & Fitch (2019, s. 6) uhkamallissakin järjestelminä, jotka ovat kohteina tekijöille sekä heidän kyberhyökkäystensä tekotavoille.

Kyberhyökkäyksien tekijät olivat monitahoisia pysyen joskus tuntemattomina, ottaen joskus kunnian hyökkäyksestä itse tai vastuun ottajan puuttuessa tekijäksi saatettiin epäillä syystä tai toisesta jotain tahoa. Tekijät voivat jäädä tuntemattomiksi, jos hyökkäyksiä ei kyetä jäljittämään ja hyökkääjä ei tule esiin ottamaan vastuuta teoistaan:

> It’s unclear who was responsible for the attack or if JCMUA officials paid a ransom (D’Auria, 2020).

> On February 5, 2021, unidentified cyber actors obtained unauthorized access to the supervisory control and data acquisition (SCADA) system at a U.S. drinking water treatment facility. – – Through the course of the investigation, the FBI was not able to confirm that this incident was initiated by a targeted cyber intrusion. (CISA, 2021b)

> No hacking group has taken credit for the attack, but water authorities have been a prime target for ransomware gangs eager to target critical services in possession of sensitive customer information (Greig, 2023e).

Kun hyökkäyksen tekijästä ei ole tietoa tai sitä ei haluta viranomaisten toimesta kertoa, on vaikeaa syyttää yksittäistä tahoa hyökkäyksestä tai arvioida sen yleisiä kyvykkyyksiä hyökkäysten toteuttamiselle jatkossa. Kyberhyökkäyksen tekijän henkilöttömyys avaa myös oven spekulaatioille tekijän alkuperästä ja motiivista, kuten Ranskassa vuonna 2023 (Greig, 2023e) tapahtuneessa kyberhyökkäyksessä ja muissakin tapauksissa:

> A cyberespionage campaign blamed on China was more sweeping than previously known, with suspected state-backed hackers exploiting a device meant to boost internet security to penetrate the computers of critical US entities (Suderman, 2021).

> Though the attacker is unknown, it is alleged that Iran was behind the intrusions (Wall, 2022).

Hyökkäyksen tekijän ilmoittauduttua, voidaan syylliseksi silti myös maalata tekijän lisäksi jokin tukeva taho tai valtiollinen tekijä, jonka on ennen todettu tukevan tai komentavan hyökkäyksiä. Se onko tämän kaltainen toimija valtiollinen toimija, valtiollisen toimijan tukema tai suojelema vai pelkästään astinkivi, jolla syyttää toista poliittista tahoa väärästä toiminnasta, ei aineistosta sel-

vinnyt. Ideologian ajama yksittäinen tekijähän voi olla vain valtiollisen toimijan tavoitteet jakava toimija, ilman sen kummempaa kytköstä isompaan tahoon. Black Basta-kiristysohjelmaryhmä on esimerkki valtiolliseen toimijaan liitetystä tahosta, joka on tässä tapauksessa Venäjä:

> The January cyberattack on Southern Water, which the company first disclosed on January 23, was claimed by the Black Basta ransomware group, a Russia-linked gang that last year took responsibility for a hack on U.K. outsourcing giant Capita (Page, 2024).

Venäjä ei ole kuitenkaan ainoa taho, johon liitettyjä ryhmittymiä mainitaan aineistossa. Toinen aineistossa mainittu maa on Kiina (Suderman, 2021). Iran on myös ollut nimettynä useissa Israeliin tai sen valmistamiin teollisuuden välineisiin kohdistuneissa hyökkäyksissä. Rikollisryhmän tai muun tekijän taustalla oleva vaikuttaja voidaan raportoinnissa ja uutisoinnissa nimetä, vaikka tarkkoja todisteita syyllisyyden osoittamiseksi ei välttämättä ole:

> Possible Iran-linked cyber actors in April 2020 attempted to disrupt operations at two Israeli water facilities by targeting ICS controllers that operated valves in water distribution systems (DHS, 2021).

> While few details are currently known, according to open-source reporting, on Saturday the Municipal Water Authority of Aliquippa in western Pennsylvania was attacked by an Iranian-backed cyber group known as CyberAv3ngers (Water-ISAC, 2023).

> The breach was initially published over the Telegram channel of an Iran-based hacker group, named "Unidentified TEAM" (Even, 2020).

Tekijä ei aina välttämättä ollut poliittisen tahon ohjaama tai ideologian ajama, vaan mahdollisesti rahan motivoima. Tämän kaltaisia tekijöitä olivat esimerkiksi rikollisryhmät, jotka ilmoittautuivat itse tekijöiksi. Syy ilmoittautumiselle voi olla uhrin painostaminen lunnaiden maksamiseen, kunnian hakeminen tai mikä tahansa tekijän itsellensä motivoima syy:

> Multiple news outlets reported yesterday that the Cl0p ransomware group was claiming responsibility for a ransomware attack at a UK water utility (WaterISAC, 2022).

> The Daixin Team group claims to have hacked the North Texas Municipal Water District (US) and threatened to leak the stolen data (Paganini, 2023).

> On Tuesday, the Medusa ransomware group took credit for the attack and said they were giving the water company seven days to pay a ransom (Greig, 2023a).

Kuka tahansa voisi ottaa vastuun mistä tahansa tapahtuneesta hyökkäyksestä sen tultua tavalla tai toisella julkisuuteen. Täten hyökkäyksien tekijät saattoivat myös julkaista varastamiaan tietoja todisteina hyökkäyksistään, jolloin vastuu voitiin kohdistaa heihin:

> On Friday, the Vice Society ransomware group added the authority to its list of victims, sharing samples of stolen documents that included passports, driver's licenses and more (Greig, 2023d).

Edellä mainitut tekijät ovat olleet Raggadin (2010, s. 84) uhkataksonomian kuvailemia ulkopuolisia hyökkääjiä. Kuitenkin uhka voi kohdistua myös sisäpuolelta, sisäisen tekijän toimesta, kuten vuonna 2021 Kaliforniassa, jossa työntekijän syytetään poistaneen vesihuoltolaitoksen toiminnan kannalta oleellisia tietokoneohjelmia laitoksen järjestelmistä:

> The indictment alleges that while Gallo was employed with Company A, he installed software on his own personal computer and on Company A's private internal network that allowed him to gain remote access to Discovery Bay's Water Treatment facility computer network. Then, in January of 2021, after Gallo had resigned from Company A, he allegedly accessed the facility's computer system remotely and transmitted a command to uninstall software that was the main hub of the facility's computer network and that protected the entire water treatment system, including water pressure, filtration, and chemical levels. (DOJ, 2021)

Edellisen kaltaisia tekijöitä on vaikea torjua, koska heillä saattaa usein olla täysi pääsy vesihuollon eri järjestelmiin. Sisäisen tekijän aikomus vahingoittaa vesihuoltoa tekee uhasta vaarallisen hänen tietojensa ja mahdollisten tekijän rakentamien takaovien vuoksi. Kuitenkin vahingossa tehdyt sisäisen tekijän toimet voivat olla yhtä turmiollisia, kuten vuonna 2021 Floridassa, jossa tapahtuneesta kyberhyökkäyksestä ei voi olla varmoja, oliko kyseessä hyökkäys vai työntekijän vahinko:

> According to a local official with direct knowledge, an alarming drinking water contamination event thought to be the result of cyberattack was actually just an operations flub (Chawaga, 2023).

Vesihuoltoon kohdistuvien kyberhyökkäysten tekijöitä on monenlaisia eikä yhtä kantavaa tyypillistä syyllistä tai tahoa esiinny aineistossa. Osassa hyökkäyksistä voi tekijöinä olla merkittävät resurssit omaava valtiollinen taho, kun taas toisessa voi olla yksittäinen, henkilökohtaisen motiivin omaava hyökkääjä, jolla on erityisosaamista tai sisäpiiritietoa suorittaa hyökkäys. Myöskään tekijöiden käyttämät hyökkäystavat eivät ole rajoitettu vain resurssirikkaiden tahojen käyttöön.

Hyökkäyksien tapoja aineistossa olivat erityisesti kiristysohjelmat ja vesihuollon tietojärjestelmiin murtautuminen. Nimeltä mainittuja vesihuoltoa vastaan käytettyjä kiristysohjelmia olivat Makop (NJCCIC, 2023), ZuCaNo (CISA, 2021a) ja Ghost (CISA, 2021a) sekä näiden lisäksi vesihuoltoon kohdistui lukuisia nimeämättä jääneitä kiristysohjelmia. Merkittävä osa kiristysohjelmista ei kohdistunut itse vesihuoltoon keskittyviin järjestelmiin, vaan vesihuollosta vastaavien yritysten tietokantoihin:

> The ransomware attack, which occurred "on or about" Sept. 30, caused the agency to "lose access to vital information and documentation related to the provision of water and sewerage services to the citizens of the City of Jersey City," according to a resolution approved in October (D'Auria, 2020).

> According to the BBC, South Staffordshire PLC, the parent company of South Staffs Water and Cambridge Water, said it discovered its ransomware attackers (Cl0p/Clop) may have exfiltrated and potentially leaked bank details of its customers, although how many customers is currently unknown (WaterISAC, 2022).

Vesihuollon tietokannat saattavat olla kiristysohjelmia hyödyntävien tahojen mielestä parempia kohteita kuin itse vesihuollosta vastaavat järjestelmät, johtuen niiden sisältävän tiedon määrästä ja arkaluontoisuudesta. Asiakkaiden ja vesihuollon työntekijöiden henkilötiedot ovat arkaluonteisia eikä niiden varmasti haluta vuotavan ulkopuolisten käsiin. Kuitenkin vesihuollosta vastaavat järjestelmätkin voivat olla kiristysohjelmien kohteita ja niiden toiminnalle voidaan tehdä merkittävää vahinkoa:

> The ransomware variant had been in the system for about a month and was discovered when three supervisory control and data acquisition (SCADA) servers displayed a ransomware message (CISA, 2021a).

> In July 2021, cyber actors used remote access to introduce ZuCaNo ransomware onto a Maine-based WWS facility's wastewater SCADA computer (CISA, 2021a).

Kiristysohjelmat voivat kohdistua vesihuollon eri alueisiin, mikäli niille löydetään pääsy järjestelmiin, oli se sitten sosiaalisen manipuloinnin tai vaikka hakkeroinnin kautta. Aineistossa ei tarkalleen käsitelty sitä, miten kiristysohjelmat olivat järjestelmiin päässeet tai mitä haavoittuvuutta ne saattoivat hyödyntää. Osa saattoi liittyä ohjelmoitavien logiikoiden (Wall, 2022), muiden ohjelmien tai järjestelmien haavoittuvuuksiin (CISA, 2021c). Kiristysohjelmien läsnäolo järjestelmissä tuli uhrien tietoon käytännössä niiden aktivoiduttua (CISA, 2021a, WaterISAC, 2022).

Kiristysohjelmien lisäksi vesihuollon eri järjestelmät olivat uhattuina eri keinoja käyttävien hakkereiden toimesta. Tietojärjestelmiin murtautuminen ja järjestelmien asetusten muokkaaminen tai käytön estäminen nousivat aineistossa esiin useissa vesihuollosta vastaaviin järjestelmiin kohdistuneissa hyökkäyksissä:

> According to reports in Israeli and Western media outlets, Iran tried to hack into Israel's water system in April and poison the water by increasing chlorine levels in water flowing to residential areas (Staff 2020b).

> These PLC and related controllers are often exposed to outside internet connectivity due to the remote nature of their control and monitoring functionalities. The compromise is centered around defacing the controller's user interface and may render the PLC inoperative. (CISA, 2023)

> The unidentified actors used the SCADA system's software to increase the amount of sodium hydroxide, also known as lye, a caustic chemical, as part of the water treatment process (CISA, 2021b).

Vesihuollon järjestelmien asetusten muokkaaminen, erityisesti veden puhdistuksen osalta, osoittautui yhdeksi merkittäväksi kohteeksi hyökkääjille. Hyökkääjien tapa päästä järjestelmiin sisälle vaihteli riippuen kohteessa käytössä olleista järjestelmistä sekä niiden suojauksen tasosta. Esiin nousseita tapoja, joilla järjestelmiin päästiin käsiksi, oli erilaisten etäkäyttöohjelmien turvattomuus, esimerkiksi salasanojen osalta tai yleisesti niiden toimintojen osalta:

> The hacker had the username and password for a former employee's TeamViewer account, a popular program that lets users remotely control their computers... (Collier, 2021).

> The cyber actors likely accessed the system by exploiting cybersecurity weaknesses, including poor password security, and an outdated operating system. Early information indicates it is possible that a desktop sharing software, such as TeamViewer, may have been used to gain unauthorized access to the system, although this cannot be confirmed at present date. (CISA, 2021b)

Etäkäyttöohjelmilla kyetään hallinnoimaan laajalle levitettyä vesihuoltoa ja sen osia tehokkaasti, mutta niiden tuomat haavoittuvuudet saattavat olla niiden tuomia hyötyjä pahempia. Aineistossa nousi esiin myös hyökkääjien tapa hyödyntää vesihuollon järjestelmien turvattomuutta ja haavoittuvuuksia itse järjestelmissä:

> From experience gained in multiple attacks researched by the OTORIO team, we can assume that the main reason the reservoir was targeted is that it provided easy, unprotected access (Even, 2020).

> Cyber threat actors likely compromised these PLCs since the PLCs were internet-facing and used Unitronics' default password (CISA, 2023).

Vesihuollon eri järjestelmät voivat aineiston perusteella joutua erilaisten hyökkäysten kohteiksi. Hyökkääjä hyödyntää havaitsemiaan haavoittuvuuksia ja pyrkii eri tavoin vaikuttamaan vesihuollon toimintaan. Hyökkäyksiin käytetyt tavat eivät ole myöskään vaatineet niin suuria resursseja, etteikö valtiollisen toimijan lisäksi myös yksityinen ja yksittäinen toimija olisi voinut toteuttaa eri hyökkäystapoja. Haavoittuvuuksien ilmetessä kyse onkin enemmän siitä, ennättääkö hyökkääjä hyödyntää niitä, ennen kuin vesihuollon kyberturvallisuudesta vastaavat tahot ennättävät suojautua haavoittuvuuksia vastaan, joka voi olla hyvinkin hidas ja haastava prosessi:

> "It has several challenges: limited cybersecurity budget and staff, significant third-party dependencies, and one of the most direct vectors for causing wide-spread effects on life, safety, and health," he said (Greig, 2023b).

Kohteina tekijöiden hyökkäyksille olivat käytännössä koko vesihuollon eri osat, tietokannoista aina vesihuollosta vastaaviin järjestelmiin sekä loppukäyttäjän järjestelmiin. Vesihuoltolaitoksen järjestelmistä joutuivat kohteiksi SCADA-järjestelmät sekä huoltolaitosten ohjainjärjestelmät:

> Possible Iran-linked cyber actors in April 2020 attempted to disrupt operations at two Israeli water facilities by targeting ICS controllers that operated valves in water distribution systems (DHS, 2021).

> On Jan. 15, a hacker tried to poison a water treatment plant that served parts of the San Francisco Bay Area. (Collier, 2021).

Veden siirtämisestä vedenpuhdistuslaitoksiin ja sieltä kuluttajille vastaavat järjestelmät eivät myöskään säästyneet kohteiksi joutumiselta. Vesihuollon vesivarantoihin sekä paineistusjärjestelmiin kohdistui hyökkäyksiä:

> Possible Iran-linked cyber actors in April 2020 attempted to disrupt operations at two Israeli water facilities by targeting ICS controllers that operated valves in water distribution systems (DHS, 2021).

> A local Pittsburgh news channel (KDKA) reported that CyberAv3ngers took control of the booster station that monitors and regulates pressure for Raccoon and Potter Townships (Water-ISAC, 2023).

Merkittävä määrä hyökkäyksistä ei kohdistunut itse vesihuollon veden tai jäteveden puhdistamiseen tai siirtämiseen lainkaan, vaan näitä hallinnoineiden yritysten tietokantoihin. Näissä tietokannoissa oli vesihuollon ylläpitämiseen liittyviä tietoja, mutta myös asiakkaiden ja henkilöstön tietoja, joihin hyökkääjät pääsivät murtautumaan ja salaamaan:

> On September 28, 2020, we determined that the file servers accessed included the names and Social Security numbers of Camrosa's current (and in some cases former) employees and current and former customers who currently or formerly paid invoices from Camrosa authorizing Camrosa to debit the customers checking or savings accounts (via ACH). The information in the accessed file servers may have included your Social Security number and your checking or savings account number. (Stafford, 2020)

> The investigation into the attack on the Puerto Rico Aqueduct and Sewer Authority (PRASA), which was announced on March 19, found that customer and employee information was compromised in the incident (Greig, 2023d).

> WSSC Water is investigating a ransomware attack on May 24 that impacted a portion of our network that operates non-essential business systems (Brown, 2021).

Itse vesihuollon eri osien järjestelmien lisäksi myös loppukäyttäjän järjestelmät olivat hyökkäyksen kohteina pääosin maataloudessa:

> One attack targeted agricultural water pumps in the upper Galilee, while the other struck infrastructure in the center of the country (Staff 2020b).
>
> A cyber attack shut down some 10 water controllers in agricultural areas in Israel, temporarily stopping irrigation systems on affected farms on Sunday (JNS, 2023).

Mitään tarkkaa tai tiettyä kohdetta vesihuoltoon kohdistuneille hyökkäyksille aineistosta ei löytynyt. Myöskään mikään osa-alue ei vaikuta olevan erityisessä hyökkääjien suosiossa, vaan kaikki kohteet ovat otollisia, jos niihin vain päästiin murtautumaan. Joskus kohde voi myös jäädä epäselväksi, vaikka vaikutukseen olisikin päästy (D'Auria, 2021).

Vesihuoltoon kohdistuva hyökkäys teemana toi esiin sen, kuinka moninaisesta uhasta on kyse. Hyökkäykset eivät rajoitu vain suurien valtiollisten tekijöiden tekemiksi, vaan voivat myös olla yksittäisten henkilöiden tai rikollisryhmien aikaansaamia (Greig, 2023a; DOJ, 2021). Myöskään tavat eivät ole aina monimutkaisia resursseja vaativia hakkerointeja, vaan tekijät voivat hyödyntää tapana yksinkertaisia vesihuollon järjestelmissä olevia haavoittuvuuksia (Even, 2020; CISA, 2023). Kohteina ei myöskään ole vain vesihuoltolaitokset ja niiden järjestelmät, vaan vesihuollon kyberturvallisuutta on tarkasteltava koko vesihuoltoa kattavasti, myös niiden järjestelmien osalta, jotka eivät suoraan ole vesihuollon kanssa suoraan tekemisissä (CISA, 2023; Greig, 2023d; DHS, 2021). Täten voidaan nähdä vesihuollon olevan kohde joka tasolla, joka tavalla ja aina jollain tavoin motivoituneen hyökkääjän toimesta. Tämä on oltava vesihuollossa työskentelevien henkilöiden ja sen kyberturvallisuudesta vastaavien mielessä sen toimintoja suunnitellessa, mutta myös arkipäiväisessä työssä.

6.2.2 Vahinko

Kyberhyökkäys pyrkii eri tekijöiden toimesta ja eri tavoin vaikuttamaan eri kohteisiin ja vesihuoltoon kohdistuessaan sillä voi olla merkittäviä vaikutuksia:

> Cyberattacks on wastewater infrastructure can cause significant harm, such as interrupting treatment processes by accessing the system remotely to open and close valves, overriding alarms, disabling pumps or other equipment, or overriding SCADA systems. Customers' personal or credit card data can be stolen from the utility's billing system. Criminals often demand millions of dollars of ransom to unlock the data or restore functionality to the system. (Kavanah, 2021)

Aineistoa analysoidessa esiin nouseva seuraava kiinnostava teema oli se, mitä vahinkoa kyberhyökkäys kohteessa aiheuttaa käytännössä. Kuten kuviossa 5 on esitetty, kyberhyökkäykset eli uhat pyrkivät vaikuttamaan tiedon käytettävyyteen, luottamuksellisuuteen sekä eheyteen vahingoittaen kohdetta, sen toimintaa tai tietoa. Aina kuviossa 1 esitetyn uhkalähtöisen mallin kyberturvallisuustoimet eivät ole riittäviä, jolloin hyökkääjä pääsee vaikuttamaan vesihuollon eri järjestelmiin. (Muckin & Fitch, 2019, s. 6)

Luonnollisesti hyökkäys saattoi olla myös aiheuttamatta vahinkoa, koska se esimerkiksi ehdittiin estää tai hyökkäys ei itse ollut onnistunut. Jokaisella hyökkäyksellä olisi myös ollut usein merkittävä potentiaalinen vahinko, jos se olisi onnistunut tekijän haluamalla tavalla. Hyökkäykset myös toisinaan onnistuivat osittain, aiheuttaen vahinkoa osaan vesihuollon järjestelmistä, mutta epäonnistuen vaikuttamaan toisiin osiin. Aineistoa analysoitaessa nämä kolme alateemaa, aiheutettu vahinko, ei vahinkoa ja mahdollinen vahinko, nousivat tutkielmaa kiinnostavina vahingon alateemoina joka tapauksen kohdalla esiin (kuvio 7).

Kyberhyökkäyksien aiheuttamaa vahinkoa voidaan tarkastella CIA-kolminaisuuden osa-alueita (luottamuksellisuus, eheys, käytettävyys) hyödyntäen. Aineistosta kuitenkin nousee vain luottamuksellisuuteen tai käytettävyyteen vaikuttaneita hyökkäyksiä. Tämä ei kuitenkaan tarkoita, etteikö vesihuollon tiedon eheyskin olisi voinut vaarantua onnistuneiden kyberhyökkäysten vuoksi, mutta sitä ei ole vain raportoitu aineistossa. Myöskään kyberhyökkäys ei vaikuta pelkästään luottamuksellisuuteen tai käytettävyyteen, vaan ne usein kärsivät yhdenaikaisesti.

Luottamuksellisuus kärsi aineiston tapauksissa merkittävästi erityisesti erilaisten tietomurtojen vuoksi. Useissa tapauksissa asiakkaiden ja vesihuollosta vastaavien yritysten sisäisiä tietoja oli päätynyt ulkopuolisten käsiin:

> South Staffs updated its website disclosing that "names and addresses of account holders, together with the sort codes and account numbers used for Direct Debit payments all could have been accessed by hackers" (WaterISAC, 2022).

> The investigation into the attack on the Puerto Rico Aqueduct and Sewer Authority (PRASA), which was announced on March 19, found that customer and employee information was compromised in the incident (Greig, 2023d).

> U.K.-based water utility Southern Water has confirmed that hackers stole the personal data of as many as 470,000 customers in a recent data breach (Page, 2024).

Tietomurtojen aiheuttamat vahingot eivät pelkästään vaikuta tiedon luottamuksellisuuteen. On valitettavaa, että ihmisten henkilökohtaisia tai yrityksen salaisia tietoja joutuu vääriin käsiin, mutta todellinen vaara on se, mitä murretuilla tiedoilla voidaan saada aikaiseksi. Tämä nousi tietomurtojen osalta esiin aineistossakin:

> The ransomware gang claims the theft of board meeting minutes, internal project documentation, personnel details, audit reports, and more. The leak of the data puts the company at risk of frauds in the next months. (Paganini, 2023)

Hyökkääjä voi tehdä yksityishenkilön tai yrityksen tiedoilla merkittävästi vahinkoa, josta voi koitua esimerkiksi rahallista- tai mainehaittaa eri tahoille. Tämän vuoksi rikollisryhmät voivat alkaa kiristää uhriksi joutuneita yksityishenkilöitä ja vesihuollosta vastaavia yrityksiä:

> The gang claims to have stolen a huge amount of sensitive data from the company and threatens to publish it (Paganini, 2023).

Tällä tavoin rikolliset pyrkivät kiristämään merkittäviä rahasummia uhreiksi joutuneilta tahoilta. Rikolliset pyrkivät hyödyntävät tietomurrosta aiheutunutta mainehaittaa rahallisesti. Tietomurroissa vuodettu tieto ei pelkästään ole hyökkääjien käsissä, vaan murtajat jakavat tietoa eteenpäin tai julkaisevat sitä kaikkien nähtäville:

> Since then, a limited amount of data has been published (Southern Water, 2024a).

> On Friday, a ransomware gang said it attacked the organization, providing samples of what it stole. The cybercriminals did not say how much total data was taken in the attack. (Greig, 2023f)

Hyökkääjät eivät kuitenkaan aina onnistu täysin murtamaan kaikkea tietokannoista tai he eivät pääse käsiksi kuin osaan tiedoista. Tilanne on hyvin valitettava uhriksi joutuneelle vesihuollosta vastaavalle taholle ja sen asiakkaille, mutta tilanne olisi voinut kuitenkin olla pahempi:

> Simon Fluendy, a spokesperson for Southern Water, told TechCrunch that the company has approximately 4.7 million customers, and did not dispute that between 235,000 and 470,000 customers had data stolen (Page, 2024).

> Based on our forensic investigations so far, which are ongoing, we are notifying in the order of 5 to 10 percent of our customer base to let them know that their personal data has been impacted. We are also notifying all of our current employees and some former employees. (Southern Water, 2024b)

Luottamuksellisuus ja käytettävyys kärsivät yhdenaikaisesti kyberhyökkäyksissä, joissa hyödynnetään kiristysohjelmia. Kiristysohjelmat salaavat uhrin tiedot ja samanaikaisesti hyökkääjä siirtää tietoa itselleen. Ne voivat myös aiheuttaa haasteita vesihuollon järjestelmien toiminnassa (Greig, 2023c). Kiristysohjelmaryhmät toimivat mahdollisesti näin saadakseen kiristettyä korvauksen tiedon julkaisemattomuudesta ja tiedon vapauttamisesta:

> Officials from Jersey City and the autonomous utilities agency have said little about the Sept. 30 ransomware attack, which MUA documents said blocked access to “vital” water and sewer information (D'Auria, 2021).

> “Due to the incident, some customer services suffered constraints," the utility said, urging people to find other ways to get information, "since the company's response capacity is limited (Greig, 2023c)."

Tiedon käytettävyys kärsii, kun hyökkäys estää järjestelmää toimimasta tai tahoja pääsemästä käsiksi tarvittavaan tietoon (D'Auria, 2021). Ne voivat myös aiheuttaa haasteita vesihuollon järjestelmien toiminnassa (Greig, 2023c). Pahimmillaan hyökkäykset voivat täysin estää tiedon ja järjestelmien käytettävyyden, esimerkiksi estämällä pääsyn tietoon tai hallintalaitteeseen:

> The ransomware affected the victim's SCADA system and backup systems (CISA, 2021a).
>
> "It will not be possible to carry out any operations or provide information that requires querying the database," the company said (Greig, 2023a).

Hyökkäyksen aiheuttama vahinko voi olla mahdollisesti täysin lamautettu vesihuollon järjestelmien toiminta, esimerkiksi poistamalla tarvittavia ohjelmia tai tuhoamalla tietokannat:

> But the MUA spent nearly half a million dollars to address the attack, and the agency's computer systems were still not fully functional even three months after the cyber incursion, an MUA resolution passed last month shows (D'Auria, 2021).
>
> The company manages 58 million cubic meters of water a year. But on Friday, the company said a recent hack rendered all of their IT systems unusable. (Greig, 2023a)

Vesihuoltoon kohdistuva vahinko itsessään on merkittävä tapahtuma, mutta se, mitä viivästys tai toimimattomuus vesihuollon eri osa-alueilla aiheuttaa, on se todellinen siitä aiheutuva vahinko. Kerätyssä aineistossa tämä vaihteli niinkin vähäisestä asiasta kuin pidemmistä jonotusajoista asiakaspalveluun (Greig, 2023c) tai laskutusjärjestelmien hitauteen (Veolia, 2024), aina täydelliseen vedenjakelun katkeamiseen:

> Residents on the Binghamstown/Drum scheme were without their water supply on Thursday and Friday after the extraordinary incident as crews worked to repair the Eurotronics Israeli-made water pumping system (Quinn, 2023).
>
> A cyber attack shut down some 10 water controllers in agricultural areas in Israel, temporarily stopping irrigation systems on affected farms on Sunday (JNS, 2023).

Tietomurrot ja muutaman päivän vedenjakelun seisahtuminen pienellä paikkakunnalla tai kastelujärjestelmien pysähtyminen voivat vaikuttaa merkittäviltä vahingoilta, ja sitä ne todellisesti yksilölle ovatkin. Kuitenkin pahempaa olisi voinut tapahtua, jota aineistossa kuvailtiin, mikäli hyökkääjät olivat saaneet tehdä järjestelmissä mitä tahansa:

> The head of Israel's National Cyber Directorate hinted that the attack might have aimed to mix chlorine or other chemicals into the water supply (Staff 2020b).
>
> Additionally there was a chance that the attack would have triggered a fail-safe, shutting down the pumps and leaving thousands without water during a severe heatwave (Staff 2020b).
>
> But they acknowledged that cyberattacks against the towns — which occurred during a holiday in April in Mount Desert Island and on the Fourth of July in Limestone — could have overridden the plants' alarms or disabled critical pumps and other equipment (Wood, 2021).

Hyökkäyksien aiheuttamaa vahinkoa voi myös olla vaikea arvioida, jolloin se on voinut olla mahdollisesti merkittävä tai vähäinen. Tähän voi olla syynä esimerkiksi hyökkäyksen tekijän julkaisemat väärennetyt tiedot hyökkäyksestä, murrettujen tietojen määrä on epäselvä tai uhri itsessään ei julkaise ulkopuolisille tietoa hyökkäyksestä:

> It’s unclear exactly what data the hackers targeted or how long JCMUA officials lost access to that data (D'Auria, 2020).

> While Cl0p claims to have access to SCADA systems and SecurityWeek posted a screenshot of an HMI supposedly captured by the attackers, at the time of this writing the claims remain unsubstantiated (WaterISAC, 2022).

> It's unclear what sensitive information, if any, was accessed. Some of the targets said they did not see any evidence of data being stolen. (Suderman, 2021)

Aineistossa nousee vahinkojen raportointiin ja uutisointiin liittyen usein esiin myös se, mitä vahinkoa ei kyberhyökkäys päässyt aiheuttamaan. Erityisesti haluttiin korostaa sitä, että vedenjakelu- ja puhdistusprosessit eivät vaarantuneet hyökkäyksissä:

> As a result, the water treatment process remained unaffected and continued to operate as normal (CISA, 2021b).

> Public water supply and sanitation were not affected by the attack (Greig, 2023c).

> It is important to highlight that all essential public water supply and sanitation services are perfectly assured (Porto, 2023).

Syy tähän voi luonnollisesti olla se, että vesihuollon asiakkaiden ensisijainen huolenaihe on, toimiiko vedenjakelu ja onko vesi turvallista. Tietysti vesihuollosta vastaava yritys voi haluta myös korostaa heidän palvelunsa luotettavuutta, vaikka kyberhyökkäys olisikin onnistunut. Aineistosta selviää, että yksikään tähän tutkimukseen löydetyistä 2020-luvulla tapahtuneista vesihuoltoon kohdistuneista kyberhyökkäyksistä ei kyennyt vaikuttamaan itse vesihuollon tai vedenjakelun toimintaan muutamaa päivää kauemmin (Quinn, 2023). Eri hyökkäyksissä kyettiin palautumaan nopeasti:

> The authority reported the actors were able to gain control of a remote booster station serving two townships, but stressed there is no known risk to the drinking water or water supply. (Water-ISAC, 2023).

> "These are two point and small sewage facilities in the agricultural sector that were repaired immediately and independently by the local person in charge of the kibbutz and the facility, without damage to the service or actual effect," the water authority said (Ahya, 2020).

Vaikka hyökkäys pääsikin vaikuttamaan vesihuollon eri järjestelmiin, kyettiin ne paikallisesti ja omin toimin korjaamaan, jotta veden puhtaus ja jakelu eivät kärsineet pitkästi. Syitä, miksi vesihuollon toiminta ei vaarantunut, vaikka kyberhyökkäys pääsikin vaikuttamaan toisinaan veden puhdistamisesta vastaaviin voimaloihin, oli useita hyökkäyksen havaitsemista ajoissa aina järjestelmien segmentointiin:

> The intrusions were caught before they could impact the water supply… (DHS, 2021).

> In Mount Desert Island, officials said the attack took computers offline for three days, but treatment plants were not affected because they are controlled manually (Wood, 2021).

> But officials noted that the authority's critical infrastructure was not affected by the incident due to network segmentation (Greig, 2023d).

Tietokantoihin kohdistuneet iskut eivät itsessään kykene vaikuttamaan vesihuoltojärjestelmien toimintaan, mutta niistä voi koitua merkittävää vahinkoa vesihuoltoa ylläpitäville tahoille. Aina ne eivät kuitenkin pääse vaikuttamaan tietojärjestelmiin, kuten osassa aineistonkin tapauksista:

> She said there was "no known data exfiltration" (Suderman, 2021).

> The network said the hacks were detected and thwarted and the FBI is now investigating (Van Osdol, 2021).

Joskus kyberhyökkäykset kuitenkin murtautuvat tietokantoihin ja aiheuttavat vahinkoa salaten ja tuhoten niissä olevaa tietoa. Kuitenkaan tietokantoihin kohdistuneissa kyberhyökkäyksissäkään ei aina aiheutunut pysyviä vahinkoja, vaan niistä kyettiin palautumaan uutisoinnin mukaan hyvinkin nopeasti, jolloin aiheutettu vahinko jäi lopulta vähäiseksi:

> Officials said they paid no ransom and no data was compromised in the attacks on Maine's water infrastructure (Wood, 2021).

> Acea: "After the hacker attack, the operations of the IT systems have been restored" (Agenzia Nova, 2023).

> WSSC Water restored files from back-ups and there was no significant impact on business operations. (Brown, 2021).

Kriittiseen infrastruktuuriin kohdistuvan uhan konkretisoituessa esimerkiksi onnistuneena kyberhyökkäyksenä, voidaan ajatella sen aiheuttavan merkittävää fyysistä vahinkoa sen varassa oleville ihmisille (Hagelstam, 2005, s. 19). Kuitenkin aineistoa tarkasteltaessa voidaan nähdä, että vaikka potentiaalinen vahinko olisi onnistuneella vesihuoltoon kohdistuneella kyberhyökkäyksellä merkittävä, eivät hyökkäykset onnistu konkretisoimaan pelkoa todelliseksi (Staff 2020b; Wood, 2021). Vesihuoltoon vaikuttavien järjestelmien jouduttua

kyberhyökkäyksen kohteeksi, huolimatta aiheutuneesta vahingosta, vesihuolto kykeni pääsääntöisesti toteuttamaan veden puhdistamisen ja vedenjakelun (Wood, 2021; DHS, 2021). Mikäli kyberhyökkäys oli lamauttanut järjestelmät kokonaan, kyettiin tilanteesta palautumaan ja jatkamaan toimintaa, vaikka joskus resursseja kuluttavammin keinoin (Ahya, 2020; Wood, 2021).

Tietokantoihin kohdistuneet kyberhyökkäykset aiheuttivatkin sinänsä enemmän vahinkoa, sillä tietomurrossa vuotanutta tietoa on käytännössä mahdotonta saada enää takaisin. Vahinko oli tapahtunut, eikä tiedon luottamuksellisuutta voinut enää täydelliseksi palauttaa. Kuitenkin tietokantoihin kohdistuneista kyberhyökkäyksistä kyettiin myös tietokantojen toiminnallisuuden osalta nopeasti palautumaan (Agenzia Nova, 2023; Brown, 2021), mutta poikkeuksiakin oli, joissa vahinkojen korjaamiseen meni kuukausia (D'Auria, 2021). Tuhansien ja jopa miljoonien ihmisten henkilökohtaisten tietojen joutuminen rikollisten käsiin voidaan kokea merkittävänä vahinkona. Mutta onko tämä kuitenkaan se pahin uhkakuva, jota ajatellaan, kun pohditaan kriittiseen infrastruktuuriin kuuluvan vesihuollon joutumista onnistuneen kyberhyökkäyksen kohteeksi? Eri vesihuollosta vastaavien tahojen ja viranomaisten raporteissakin korostetaan useasti veden turvallisuutta ja vedenjakelun varmuutta, koska ne ovat varmasti niitä asioita, joita ihmiset pelkäävät menettävänsä (CISA, 2021b; Porto, 2023). Arkaluontoisten tietojen vuotamisen jälkeen voidaan jatkaa elämää, mutta ilman vettä elämän jatkaminen ei ole mahdollista (Biswas, 2004).

6.2.3 Seuraamus

Hyökkäyksen ja sitä seuranneen mahdollisen vahingon jälkeen aineiston analyysissä nousi esiin kiinnostava teema siitä, mitä tapahtunut hyökkäys sai aikaan vesihuollosta vastaavissa tahoissa ja muissa yhteistyökumppaneissa. Seuraamushan alkaa välittömästi kyberhyökkäyksen tai sen aikaansaaman vahingon paljastumisen jälkeen ja jatkuu kauas tulevaisuuteen, riippuen esimerkiksi hyökkäyksen tavasta tai onnistumisesta. Aineistosta havaittiin yhteensä viisi alateema, jotka pitivät sisällään analyysissä havaittujen seuraamusten eri ulottuvuudet.

Kyberhyökkäyksen seuraamus alkoi havaitsemisen jälkeen usein ensireaktiolla, jossa erinäiset tahot pyrkivät rajoittamaan hyökkäyksen etenemistä ja aiheutunutta vahinkoa. Tämän jälkeen alkoi välitön vahinkojen korjaaminen, joka jatkui tarpeen vaatiessa hyvinkin pitkään. Vahinkojen korjaamisen yhteydessä tiedotettiin tapahtuneesta mahdollisille asianomaisille, mutta myös muille vesihuollosta vastaaville tahoille, jotta he voisivat ennaltaehkäistä saman tapahtuman omilla vastuualueillaan. Tiedottaminen jatkui myös erilaisten raporttien ja koosteiden muodossa jopa vuosia hyökkäyksen jälkeen. Yhteistoiminta alateemana nousi seuraamuksien aikana esiin hyvin nopeasti hyökkäykseen reagoimisen jälkeen ja jatkui siitä parhaimmillaan vuosia eteenpäin. Hyökkäyksestä palautumisen jälkeen usein seuraamuksen osana oli toimintojen päivittäminen tulevaisuuden varalle.

Kyberhyökkäyksen paljastuessa voi vahinko olla jo tapahtunut tai hyökkäys olla edennyt hyvinkin pitkälle. Hyökkäykseen on reagoitava välittömästi, jotta vahinkoja saadaan vähennettyä tai hyökkäys jopa torjuttua. Aineiston raportit ja uutisoinnit toivat esiin sen, miten kyberhyökkäysten jälkeiset toimet vaikuttivat merkittävästi vesihuollon toiminnan jatkuvuuteen:

> The ransomware virus was successfully removed within hours and WSSC Water is fully operational (Brown, 2021).

> This is thanks to the robust systems and controls over water supply and quality we have in place at all times as well as the quick work of our teams to respond to this incident and implement the additional measures we have put in place on a precautionary basis (South Staffs Water, 2022).

> An alarm reportedly went off as soon as the attack occurred. The system has been disabled and is being operated manually (Water-ISAC, 2023).

Valmiit toimintatavat ja suunnitelmat kyberhyökkäyksien varalla nopeuttavat reaktioaikaa, jos hyökkäys tapahtuu. Myös automaattisten järjestelmien asentaminen valvomaan vesihuollon toimintaa voi hälyttää epäilyttäviin muutoksiin järjestelmissä. Nämä molemmat seikat nostettiin esiin uhreiksi joutuneiden vesihuollon tahojen tiedotteissa, jotka korostivat valmiina olevien toimintatapojen ja omien kyberturvallisuustoimijoiden sekä järjestelmien automaattisten valvontajärjestelmien nopeaa reagointia hyökkäysten pysäyttämisessä:

> Water treatment plant personnel immediately noticed the change in dosing amounts and corrected the issue before the SCADA system's software detected the manipulation and alarmed due to the unauthorized change (CISA, 2021b).

> Existing cybersecurity safeguards and swift action taken by WSSC Water's IT department helped minimize the impact of this attack (Brown, 2021).

> This is thanks to the robust systems and controls over water supply and quality we have in place at all times as well as the quick work of our teams to respond to this incident and implement the additional measures we have put in place on a precautionary basis (South Staffs Water, 2022).

Nopea reagointi eri järjestelmien toiminnan osalta, asiakkaiden tiedottaminen, selvitysten aloittaminen ja muiden yhteistyökumppaneiden tuominen tietoisiksi tapahtuneesta mahdollistaa vahingon minimoimisen sillä hetkellä, mutta myös pitkällä aikavälillä. Hyökkäys saadaan pysäytettyä, korjaavat toimenpiteet aloitettua ja selvitys sekä yhteistyö voivat ennaltaehkäistä muita joutumasta samankaltaisen hyökkäyksen uhreiksi. Tapahtuneiden kyberhyökkäysten jälkitoimissakin kuvailtiin näitä asioita:

> We had previously detected suspicious activity, and had launched an investigation, led by independent cyber security specialists (Southern Water, 2024a).

> Our IT and Security Incident Response Teams were quickly mobilized, and we are actively cooperating with law enforcement and other third parties to investigate and address this incident (Veolia, 2024).

> Employees at the water facility detected a change in water chlorine levels and swiftly alerted Israel's cybersecurity agency, who took it from there (Wall, 2022).

> "The government offices instructed the farmers to carry out basic and immediate actions to secure the systems and to carry out the irrigation manually. "(JNS, 2023)

On tietysti mahdollista, että vesihuollosta vastaavat tahot haluavat tuoda itsestään tällaisella viestinnällä esiin mahdollisimman valmiin ja vastuullisen kuvan kertomalla, kuinka he olivat valmiita toimimaan ja näin luoden luottamusta siihen, että he kykenevät ratkaisemaan jatkossakin tämän kaltaiset haasteet. Jos suunnitelmia ja vastatoimia kyberhyökkäysten varalle ei aiemmin ollut, tapahtuneet kyberhyökkäykset saavat mahdollisesti vesihuollosta vastaavat tahot oppimaan ja asettamaan ne toimintaan.

Ensireaktion jälkeen on aloitettava tapahtuneen vahingon korjaaminen. Oli aiheutunut vahinko sitten vesihuoltoon, vedenjakeluun tai tietokantoihin kohdistunut, voi sen korjaaminen olla pitkä ja kallis prosessi. Vesihuollon ja jakelun vahingot aiheuttivat aineistossa esiintyneissä hyökkäyksissä poikkeusjärjestelyitä sekä lisäresurssien kohdentamista järjestelmien valvontaan:

> The treatment system was run manually until the SCADA computer was restored using local control and more frequent operator rounds (CISA, 2021a).

> IT teams have worked since Wednesday to secure industrial systems and close off all external connections in order to prevent the attack from spreading (Greig, 2023e).

Tietokantoihin kohdistuva vahingon korjaaminen näyttäytyi kahtena toimena; vahingon korjaaminen asiakkaille ja itse tietokantojen korjaaminen. Mikäli asiakkaiden tietoja oli vuotanut rikollisille, ei niitä voinut saada enää takaisin. On kuitenkin olemassa asiakkaille tarjottavia palveluita, joita hyödyntämällä voidaan välttyä esimerkiksi identiteettivarkauden tai maksuvälinepetoksen uhriksi joutumiselta:

> As an added precaution, we are offering you a complimentary one-year membership with Experian's® IdentityWorksSM. This product helps detect possible misuse of your personal information and provides you with identity protection support. (Stafford, 2020)

> As the investigation continues, WSSC Water will notify in writing any individuals whose personal identifying information was exposed. Those individuals will be offered five years of credit monitoring with $1,000,000 in identity theft insurance at no cost to them. (Brown, 2021)

Vakuutusmaksut ja eri palvelut voivat kuitenkin olla varsin kalliita, joten hyökkääjä voi tarjoutua avuksi (Brown, 2021). Vahingon ”korjaamiseksi” nostettiin

aineistossa kiristysohjelmien ja tietomurtojen aikana varastettujen tietojen osalta myös lunnaiden maksaminen, mutta yksikään uhri ei tiettävästi ollut tähän taipunut tai ainakaan myöntänyt sitä:

> It's unclear who was responsible for the attack or if JCMUA officials paid a ransom (D'Auria, 2020).
>
> It's unclear whether or not the MUA paid a ransom, and whether any data is still being blocked (D'Auria, 2021).
>
> WSSC Water has not and will not pay or support the criminals behind this cyberattack (Brown, 2021).
>
> At the time of writing, Southern Water is no longer listed on Black Basta's website. It's not uncommon for victim companies who pay a ransom to the hackers to have their public listings removed. Southern Water declined to say whether it had paid a ransom demand. (Page, 2024)

Tietokantojen ja eri järjestelmien palauttaminen toimintakuntoisiksi oli aineiston mukaan yhtä raskas tai jopa raskaampi prosessi kuin vesihuollosta ja vedenjakelusta vastaavien järjestelmien korjaaminen. Merkittäviä rahallisia sekä ihmisresursseja oli hyödynnettävä, jotta vahingot saataisiin korjattua:

> The contract comes on the heels of an $18,675 contract with a different information technology firm, as well as a $25,000 contract with Pennsylvania law firm Mullen Coughlin to investigate the incident — putting known expenditures related to the incident at $434,675 (D'Auria, 2021).
>
> The SIAAP crisis unit remains mobilized to manage the aftermath of this attack and to support the continuity of the work of all of its agents from this week in a context and a working environment largely degraded by the current situation (SIAAP, 2023).
>
> Since the incident, our IT security teams have worked with independent incident response experts, using enhanced monitoring and protection tools to check actively for any suspicious activity on our IT estate (Southern Water, 2024b).

Kyberhyökkäyksen vahinkojen korjaaminen ja niistä palautuminen voi myös olla helppoa, jos hyökkäys ei ole oikeastaan aiheuttanut mitään vahinkoa tai jos aiheutettu vahinko on ollut yksinkertaisesti korjattavissa. Nämä tapaukset jäivät kuitenkin selväksi vähemmistöksi ja niissä yleensä korjaustoimi tai haavoittuvuus oli varsin yksinkertainen:

> The hack wasn't discovered until the following day, and the facility changed its passwords and reinstalled the programs (Collier, 2021).
>
> As of the morning of December 2, 2020, the HMI web application already requires authentication to access the system (Even, 2020).

Kyberhyökkäyksestä tiedottaminen ilmeni aineistosta useiden eri toimijoiden tekeminä, joskus vuosiakin itse tapahtuman jälkeen, lyhyinä tiedotteina, raportteina tai lausuntoina medialle. Aineistoa ei olisi voitu kerätä, jos tiedot olisi pidetty salaisina viranomaisten ja vesihuollosta vastaavien tahojen kesken. Vesihuoltoon kohdistuneista hyökkäyksistä tiedotettiin tavalla tai toisella ainakin tutkielman löytämänä 26 kertana, jotka mahdollistivat tutkielman aineiston keruun ja analyysin tekemisen:

> We are writing to inform you about an incident that may have involved some of your information (Stafford, 2020).
>
> WSSC Water is investigating a ransomware attack on May 24 that impacted a portion of our network that operates non-essential business systems (Brown, 2021).
>
> Last week, a ransomware incident affected some software applications and systems in a portion of Veolia North America's Municipal Water division (Veolia, 2024).

Vesihuollosta vastanneet tahot pääasiassa tiedottivat asiakkailleen hyökkäyksestä ja pyrkivät rauhoittelemaan sekä korostamaan omaa toimintaansa hyökkäykseen reagoimisessa sekä vaurioiden korjaamisessa (South Staffs Water, 2022; Porto, 2023; Stafford, 2020). Myös toimintaohjeita sekä varoituksia jaettiin:

> Although the investigation did not determine that the cyber attacker viewed or exfiltrated your personal information, we are providing this notice out of an abundance of caution (Stafford, 2020).
>
> All individuals are encouraged to remain vigilant and closely examine their financial statements and report anything suspicious to their bank or card issuer (Brown, 2021).
>
> The company was still able to process customer requests at in-person service desks, and it urged people to get virtual service tickets that could be obtained instead of standing in line (Greig, 2023c).

Kuitenkin joissakin tapauksissa uhriksi joutuneet tahot eivät julkaisseet tiedotteita, vaan tapaukset tulivat esiin osana viranomaisten raportteja tai yleisiä varoituksia (CISA, 2021a; Water-ISAC, 2023). Viranomaiset myös julkaisivat yleisiä toimintaohjeita useiden kyberhyökkäysten jälkeen tai yksittäisten merkittävien haavoittuvuuksien havaitsemisen jälkeen. Näissä tiedotuksissa annettiin yleispäteviä sekä yksityiskohtaisia ohjeita, miten kyberhyökkäykset ovat kohdistuneet vesihuollon eri osa-alueisiin ja miten niiltä voi suojautua:

> Refrain from connecting (all) PLCs to the internet. If remote access is not necessary, a PLC connected to the internet represents an unnecessary risk to safety, availability, and control of your SCADA environment (Water-ISAC, 2023).
>
> Upgrade devices to 9.9.00 VisiLogic software, which requires users to change the default passwords on PLCs and HMIs. Use a strong password (CISA, 2023).

> CISA strongly encourages organizations using Ivanti Pulse Connect Secure appliances to immediately run the Pulse Secure Connect Integrity Tool, update to the latest software version, and investigate for malicious activity (CISA, 2021c).

Kyberhyökkäyksen uhriksi joutuminen voi olla mainehaitta vesihuollosta vastaavalle taholle ja voi kertoa sen huonosta valmistautumisesta tai sen kyberturvallisuustoimien puuttumisesta. Kuitenkin avoimuus voidaan nähdä myös vastuun kantamisena, kun vastuussa ollut taho ei peittele epäonnistumisiaan. Tiedottamisella voidaan myös korostaa onnistumisia kyberhyökkäyksen torjunnassa tai siitä toipumisessa:

> Águas e Energia do Porto was the target of a computer attack, and security protocols were immediately activated (Porto, 2023).

Kyberhyökkäyksen jälkeen esiin nousi miltei joka tapauksen osalta jonkinlainen yhteystoiminta kyberhyökkäyksestä palautumisen yhteydessä. Se saattoi olla viranomaisiin tukeutumista, kyberturvallisuusyritysten tai muiden asiantuntijoiden palkkaamista sekä eri tahojen pitäminen tietoisena tapahtuneesta. Kansalliset eri tasojen viranomaiset pidettiin tietoisina tapahtuneesta, johtuen määräyksistä esimerkiksi Euroopan unionin alueella (Euroopan parlamentti, 2022), mutta myös varmasti niiden resurssien ja asiantuntijuuden vuoksi:

> A comprehensive investigation is underway. WSSC Water has notified the FBI, Maryland Attorney General and state and local homeland security officials and will cooperate with any investigation (Brown, 2021).

> Águas e Energia do Porto said it contacted both the Portuguese National Cybersecurity Center and the Judiciary Police for assistance with the situation (Greig, 2023c).

> Throughout this process we have been working with Government, our regulators and the National Cyber Security Centre (Southern Water, 2024b).

Kyberhyökkäysten uhrit tukeutuivat myös yksityisten kyberturvallisuustoimijoiden palveluihin. Yksityiset kyberturvallisuusyritykset voivat tarjota osaamista, jota vesihuollosta vastaavien tahojen kyberturvallisuussektoreilla tai vastaavilla ei ole. Voi myös olla, että vesihuollosta vastaavilla tahoilla ei ole osaamista kyberturvallisuudesta lainkaan. Kyberturvallisuusyritysten palveluihin tarttuminen voi olla myös nopea ratkaisu, jolla korostetaan vesihuollosta vastaavan tahon halua ja pontevuutta ratkaista ongelma:

> In response to the attack on their water systems, Israel hired cybersecurity company SIGA OT Solutions to aid in protecting against future cyberattacks on critical infrastructure (Wall, 2022).

> At a Dec. 17 meeting, the MUA Board of Commissioners voted to approve a new $391,000 emergency contract with cyber security firm Digital Team Six for “technical restoration services,” according to a resolution obtained through an Open Public Records request (D'Auria, 2021).

> We have engaged leading independent cybersecurity experts to monitor the "dark web" (Southern Water, 2024b).

Kyberturvallisuus ei ole kuitenkaan ainoa asia, jossa yhteistyö tulee esiin. Kyberhyökkäyksestä palautuminen voi vaatii useiden eri alojen osaamista, jotta hyökkäyksestä voidaan palautua, vahingot korjata ja jatkaa toimintaa turvallisemmin:

> As the need arises, technological experts on behalf of the system manufacturer will work in coordination with the farmers… (JNS, 2023).

> The Jersey City Municipal Utilities Authority has hired a law firm to investigate a cyberattack that blocked access to "vital" water and sewer service information and led to an "emergency condition" (D'Auria, 2020).

Aineistossa nousi esiin tärkeys ja perustoimintatapa pitää eri tahot tietoisina tilanteen kehittymisestä (South Staffs Water, 2022; Southern Water, 2024b). Yhteistyö voi myös mahdollistaa muiden tahojen oman valmistautumisen mahdollisiin muihin tuleviin tai jo käynnissä oleviin kyberhyökkäyksiin. Yhdessä on mahdollista jakaa resursseja yli yksittäisen vesivoimalan tai vesihuollosta vastaavan tahon oman kapasiteetin.

Hyökkäyksen ja siitä palautumisen jälkeen oli eri vesihuollosta vastaavien tahojen toiminta yleisesti selvä; estää tapahtunut toistumasta tulevaisuudessa. Tästä nostettiin käytännön esimerkkejä aineistossa:

> The Israeli facilities updated all firmware on the ICSs and replaced outdated equipment with newer systems. All employees of the facilities were required to change their login passwords as a precaution. (Wall, 2022)

> We have already implemented additional security measures to enhance the security of our network, including deploying an endpoint threat detection and response tool, implementing multi-factor authentication for employee access into the Camrosa network, and implementing firewall Intrusion Prevention and Intrusion Detection Systems (IPS and IDS) (Stafford, 2020).

> The statement was accompanied by an emergency order from Thursday authorizing officials at the organization to hire outside cybersecurity firms and purchase any equipment necessary to recover or restore systems needed for them to continue their work (Greig, 2023e).

Toiminnan kehittäminen eri tapauksissa keskittyi vain järjestelmien turvallisuuden parantamiseen uusien tietoturvaohjelmistojen ja järjestelmien päivittämisen muodossa (Wall, 2022; Stafford, 2020; Axelbank, 2023; Brown, 2021; Wood, 2021; SIAAP, 2023; Greig, 2023e; Quinn, 2023). Uutisissa tai tiedotteissa ei mainittu kyberturvallisuuskulttuurin parantamisesta vesihuollosta vastaavissa tahoissa eikä myöskään koulutuksen lisäämisestä työntekijöille. Hyvin usein työntekijät kuitenkin ovat kyberturvallisuuden heikoin lenkki tutkimuksen perusteella (Siponen, Mahmood & Pahnila, 2014, s. 218). Tietysti voi olla, että hen-

kilöstön koulutukseen on panostettu enemmän hyökkäyksen jälkeen, mutta sitä ei ole vain mainittu. On valitettavaa, että vasta hyökkäyksen jälkeen kyberturvallisuuteen panostetaan, koska on täysin mahdollista, että uhkaan perustuvan kyberturvallisuusanalyysin avulla nämä parannukset olisi voitu toimeenpanna ennen vahingon tapahtumista.

Vaikka tässä luvussa onkin esitelty seuraamuksen alateemat jokseenkin kronologisessa järjestyksessä, ei tämä kuitenkaan tarkoita sitä, että järjestys olisi aina täysin sama tai näin jäykkä eri tapauksissa. Todennäköisesti jo ensireaktion aikana aloitetaan yhteistoiminta viranomaisten kanssa ja tiedottaja aloittaa laatimaan tiedotetta asiakkaille tapahtuneesta, jota päivitetään myöhemmin (Southern Water, 2024a). Myös ensireaktion aikana toimintoja suorittavat henkilöt havaitsevat varmasti keinoja korjata aiheutettu vahinko tai päivittää järjestelmiä turvallisemmiksi. Ajatukset ja havainnot kuitenkin toimeenpannaan vasta myöhäisempänä ajankohtana tai raportoidaan, kun siihen on aikaa.

Kokonaisuutena voidaan tarkastella miten vesihuollosta vastaavat tahot ovat toimineet kyberhyökkäyksen jälkeen alateemojen kautta. On ollut kyky reagoida mahdollisimman nopeasti tapahtuneeseen hyökkäykseen vahinkojen minimoimiseksi ja hyökkäyksen pysäyttämiseksi, vaikka vahinko olisikin jo merkittävän laaja (D'Auria, 2021; Brown, 2021). Vahinkoa on aloitettu korjaamaan omin resurssein tai tuomalla ulkopuolisia asiantuntijoita mukaan avuksi, oli vahinko sitten järjestelmiin aiheutettua tai murrettujen tietojen aiheuttamien vahinkojen lievittämistä (SIAAP, 2023; Stafford, 2020). Yhteistoiminta aloitettiin pian viranomaisten ja muiden tahojen kanssa tilanteen ratkaisemiseksi (Brown, 2021; Greig, 2023c). Tiedottaminen hoidettiin joko omin toimin, median kautta tai viranomaisten toimesta (Greig, 2023c; Veolia, 2024; CISA, 2021b). Lopuksi järjestelmiä kehitettiin siten, että uhkaan pyrittiin vastaamaan paremmin (Wall, 2022; Greig, 2023e).

7 Johtopäätökset

7.1 Vesihuoltoon kohdistuneet kyberturvallisuusuhat

Vastauksena ensimmäiseen tutkimuskysymykseen, *mitä kyberturvallisuusuusuhkia on kohdistunut vesihuoltoon aikavälillä 1/2020–2/2024*, tässä tutkimuksessa löydettiin 26 eri vesihuollon osa-alueisiin kohdistunutta kyberturvallisuusuhkaa (taulukko 2). Niistä kaikki paitsi yksi kyettiin kategorisoimaan uhkansa perusteella, koska yhdestä ei ollut käytännössä löytynyt muuta tietoa kuin, että kyberhyökkäys oli tapahtunut (SIAAP, 2023). Kohdistuneista uhista kyettiin myös aineiston ja siitä tehdyn analyysin perusteella tarkastelemaan kyberhyökkäyksen tekijää, tekotapaa ja mihin hyökkäys oli kohdistunut. Tämän lisäksi aineiston ja analyysin perusteella kyettiin arvioimaan hyökkäyksen aiheuttamaa vahinkoa vesihuollon eri järjestelmille.

Haittaohjelmat jäivät aineistossa kokonaisuudessaan määrällisesti vähäiseksi vesihuoltoon kohdistuneeksi uhaksi (taulukko 2). Haittaohjelmien hyödyntämisen vähyydestä huolimatta niillä kyettiin aiheuttamaan myös merkittävin vesihuoltoon liittyvä vahinko, joka kuitenkin kohdistui vain irlantilaiseen haja-asutusalueella olevaan pumppausasemaan eikä esimerkiksi miljoonakaupungin vesihuollon pumppausasemaan (Quinn, 2023). Haittaohjelmaa hyödynnettiin onnistuneesti myös israelilaisia maatalouden kastelujärjestelmiä vastaan, joka aiheutti myös väliaikaisen toiminnan keskeytymisen (JNS, 2023). Molemmat haittaohjelmia hyödyntäneet hyökkäykset ovat mahdollisesti olleet poliittisesti motivoituja niiden kohdistuessa nimenomaisesti israelilaisia tai Israelista hankittuja järjestelmiä vastaan siten, että haittaohjelma on estänyt laitteen käytön ja tuonut hyökkääjän sanoman samanaikaisesti esille (Quinn, 2023; CISA, 2023).

Näin pienellä otannalla on vaikea yleistää haittaohjelmien uhan merkittävyyttä vesihuollon toimivuudelle ja turvallisuudelle, mutta nämä kaksi edellä mainittua hyökkäystä ovat kyenneet pysäyttämään ainakin osittain vesihuollon eri osa-alueiden toiminnan. Yksittäisen pumppausaseman tai loppukäyttäjän järjestelmän toiminnan pysäyttäminen haittaohjelmalla ei edellä mainituissa

tapauksissa kuitenkaan johtanut merkittäviin henkilö- tai materiaalitappioihin. Haittaohjelmissa piilee kuitenkin merkittävä uhka, sillä on täysin mahdollista, että se kyetään asentamaan huomattavasti kriittisempäänkin järjestelmään esimerkiksi sellaiselle alueelle, joka on riippuvainen jatkuvasta vedensaannista. Tällöin parinkin päivän tai hetken vedenjakelun keskeytyminen voi aiheuttaa katastrofaalista tuhoa maataloudelle tai ihmisille esimerkiksi alueilla, joissa vedestä on yleisesti pulaa.

Haittaohjelmia merkittävämpi uhka vesihuollon järjestelmille aikavälillä 1/2020–2/2024 oli kerätyn aineiston perusteella eri kiristysohjelmat (taulukko 2). Ne kohdistuivat pääosin vesihuollosta vastaavien tahojen tietokantoihin eivätkä itse vesihuollosta ja sen jakelusta vastaaviin järjestelmiin, mutta muutamissa tapauksissa nekin joutuivat kiristysohjelman uhreiksi (taulukko 2). Nämä vesihuoltolaitoksiin iskeneet kiristysohjelmat havaittiin vuoden 2021 aikana niiden vaikutettua vesihuoltolaitoksien SCADA-järjestelmiin eri Yhdysvaltojen osavaltioissa (CISA, 2021a). Vesihuoltolaitoksiin kohdistuneet kiristysohjelmat eivät kuitenkaan tiedettävästi saaneet aikaan merkittävää vahinkoa, mutta potentiaalinen vahinko olisi voinut olla merkittävämpää (CISA, 2021a; Wood, 2021; Kavanah, 2021).

Kiristysohjelmat olivat uhkana vesihuollosta vastaavien tahojen tietokannoille koko aikavälin 1/2020–2/2024 ajan ympäri maailmaa (taulukko 2). Niitä hyödynsivät rikollisryhmät rahallisessa tarkoituksessa, mutta jotka saattoivat olla myös valtiollisen toimijan tukemia (Page, 2024; Water-ISAC, 2023; Greig, 2023a). Vaikka ne eivät suoraan vaikuttaneet vesihuollon ja sen jakelun toimintaan, aiheuttivat ne merkittävää vahinkoa tietokannoissa olleiden tietojen luottamuksellisuudelle ja saatavuudelle (WaterISAC, 2022; Porto, 2023; Southern Water, 2024a). Hyökkäyksissä, joissa on aineiston perusteella hyödynnetty kiristysohjelmia, ei pelkästään vaikuteta tiedon saatavuuteen salaamalla tietokantoja vaan myös varastetaan tietoa myytäväksi tai levitettäväksi eteenpäin (Brown, 2021; WaterISAC, 2022; Greig, 2023a; Greig, 2023d). Tietokannoissa säilytetään niin vesihuollosta ylläpitävän tahojen sisäisiä tietoja työntekijöiden tiedoista aina vesihuollon eri osien sijaintiin, mutta myös asiakkaiden henkilötietoja (D'Auria, 2020; WaterISAC, 2022). Uhriksi joutuneet tahot ovat kuitenkin kyenneet rajoittamaan vahinkojen laajuutta omalla toiminnallaan hyökkäyksen tapahduttua ja jo ennen sitä tarpeellisilla kyberturvallisuustoimilla (Agenzia Nova, 2023; Page, 2024). Vaikka vesihuollon tai vedenjakelun toiminta ei tietokantoihin kohdistuneissa kiristysohjelmahyökkäyksissä vaarantunutkaan, aiheutettiin niillä silti merkittäviä rahallisia sekä mahdollisia imagollisia tappioita uhreille (Paganini, 2023; Greig, 2023d).

Haittaohjelmien tavoin kiristysohjelmat ovat kykeneviä lamauttamaan sen järjestelmän, johon ne kyetään asentamaan (D'Auria, 2020; CISA, 2021a). Tällöin on täysin mahdollista, että oikeaan järjestelmään ja oikealla hetkellä asennettu kiristysohjelma on kykenevä aiheuttamaan merkittävää tuhoa myös veden puhdistuksen ja jakelun osalta. Aineiston perusteella kuitenkin merkittävä vahinko saadaan aikaan kiristysohjelmilla, kun ne nimenomaisesti kohdistetaan vesihuollon tietokantoihin. Kiristysohjelman nimen mukainen kiristäminen voi-

si kuitenkin olla merkittävästi tehokkaampaakin tietokantojen sijaan, jos kiristykseen alistumisen vaihtoehtona olisi vedenjakelun katkeaminen juuri pahimpaan helleaaltoon tai, kun vettä tarvittaisiin muissa kriittisen infrastruktuurin toimialoilla. Vaikka tietokannat ovat olleet määrällisesti lukuisampi kohde kiristysohjelmille, ei vesihuoltolaitoksia tai muita veden puhdistamisen ja jakelun järjestelmiin kohdistuvaa kiristysohjelmien aiheuttamaa uhkaa saa unohtaa.

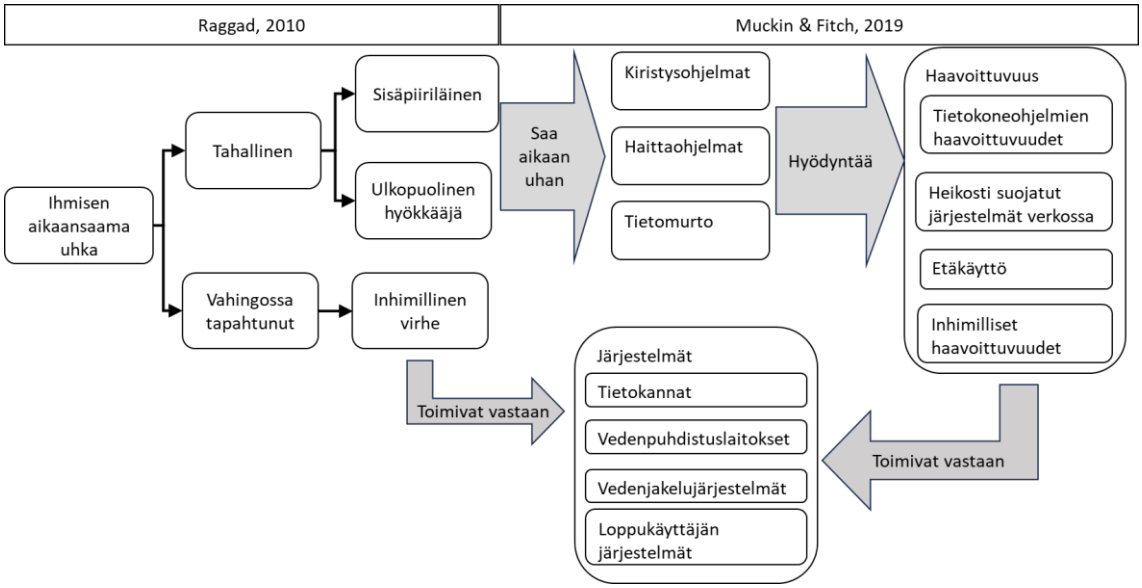
Toinen määrällisesti merkittävä vesihuoltoon kohdistuva uhka kiristysohjelmien lisäksi oli erilaiset tietomurrot (taulukko 2). Vaikka kiristysohjelmat uhkana tarvitsevat toteutuakseen tietomurron, jotta kiristysohjelma saadaan asennettua, on aineistosta eritelty tarkasteluun sellaiset tietomurrot, joiden ei raportoitu hyödyntäneen kiristysohjelmien tai haittaohjelmien käyttöä. Tietomurtoihin on saattanut osin liittyä kiristysohjelmien tai haittaohjelmien käyttö ilman, että niistä on tarkemmin raportoitu tai uutisoitu. Tietomurrot kohdistuivat vesihuollon eri järjestelmiin tasapuolisemmin kuin kiristysohjelmat, jakautuen kohteissaan vedenpuhdistuslaitosten, tietokantojen ja loppukäyttäjän järjestelmien välille (taulukko 2).

Vedenpuhdistuslaitoksiin kohdistuneet tietomurrot kohdistuivat eri järjestelmiin ja niiden hallintalaitteisiin. Uhreiksi joutuneita järjestelmiä olivat esimerkiksi venttiileitä hallinnoiva järjestelmä (DHS, 2021, s. 1), vesivarantoa hallinnoiva järjestelmä (Even, 2020) ja jopa koko vedenpuhdistusprosessia hallinoiva järjestelmä (Collier, 2021). Osassa tietomurtojen kohteista ei ollut yksilöity järjestelmiä, joihin hyökkäys oli kohdistunut, mutta osassa tapahtuneet tietomurrot olisivat voineet mahdollistaa eri järjestelmien etäkäytön (CISA, 2021c; Van Osdol, 2021; Collier, 2021; CISA, 2021b, s. 1). Osassa tietomurroista etäkäytön mahdollisti haavoittuvuus käytetyssä tietokoneohjelmassa (Suderman, 2021) ja osassa etäkäyttöön soveltuvia ohjelmia oli väärinkäytetty eikä niihin ollut mahdollisesti asetettu tarpeeksi turvallisia salasanoja (CISA, 2021b, s. 1; Collier, 2021). Yhdessä tapauksessa vesihuollon järjestelmä oli yhteydessä suojaamattomana internetiin (Even, 2020). Haavoittuvuus ohjelmoitavissa logiikoissa (PLC) aiheutti myös tietomurtoja veden puhdistuksesta ja veden siirrosta vastaaviin järjestelmiin (CISA, 2023, s. 2). Pääosa tietomurroista tapahtui ulkopuolisen hyökkääjän toimesta, mutta kahdessa tapauksessa kyse oli vesihuollosta vastaavan sisäpiiriläisen tekemistä tietomurroista, joista ainakin toisessa teko oli todistetusti tahallinen (CISA, 2021b, s. 1). Siinä vaikutettiin jokaiseen CIA-kolminaisuuden osa-alueeseen poistamalla vedenpuhdistuslaitoksen veden puhdistamisesta vastaavat tietokoneohjelmat ja sammuttamalla palvelimet. (DOJ, 2023) Toinen sisäpiiriläisen tekemistä tietomurroista saattoi olla mahdollisesti vain käyttäjävirhe, joka voi tosin myös koitua kalliiksi vesihuollon toiminnalle (Chawaga, 2023).

Tietokantoihin kohdistuneet tietomurrot mahdollistivat tiedon luottamuksellisuuden vaarantumisen, kuitenkaan aiheutettu vahinko ei ollut niin merkittävää kuin kiristysohjelmien tekemät vahingot (Suderman, 2021; Greig, 2023b). On jälleen syytä huomioida, että tietokantoihin murtauduttaessa on käytetty usein lisäksi kiristysohjelmaa, jolloin tietokantoihin kohdistuneet tietomurrot on jo esitetty, kun on tarkasteltu kiristysohjelmia uhkana (taulukko 2). Tapah-

tuneet aineistossa esitetyt tietomurrot ovat aiheuttaneet lähtökohtaisesti pelkästään vahinkoa järjestelmissä olevan tiedon luottamuksellisuuteen, eikä merkittävää vahinkoa ole aiheutettu vesihuollon järjestelmille tai vedenjakelulle pitkäksi aikaa (DHS, 2021, s. 1; Even, 2020). Hyökkääjien pääsy merkittäviin vesihuollon järjestelmiin mahdollistaa kuitenkin veden myrkyttämisen puhdistusaineilla, veden puhdistuksen tai jakelun pysäyttämisen ja jopa kyberfyysisten järjestelmien pysyvän tuhoamisen (Staff 2020b; Wood, 2021).

Vesihuoltoon kohdistuneita kyberturvallisuusuhkia aikavälillä 1/2020–2/2024 ovat olleet kiristysohjelmat, tietomurrot ja haittaohjelmat (taulukko 2). Kyberuhat kohdistuivat käytännössä vesihuollon jokaiseen osa-alueeseen (taulukko 2). Kyberhyökkäykset toteutettiin ulkoisten hyökkääjien, mutta myös sisäpiiriläisten toimesta (CISA, 2021b, s. 1; DOJ, 2023). Ulkoiset uhat ovat olleet rikollisten, mutta myös mahdollisesti valtiollisten toimijoiden toteuttamia, osan jäädessä tuntemattomiksi (Suderman, 2021; Wall, 2022; Greig, 2023e). Kerätyssä aineistossa ei saatu selville jokaisen yksittäisen kyberuhan toteuttamiseen käytettyä tapaa, mutta osaan on liittynyt järjestelmissä olleet haavoittuvuudet, joiden avulla hyökkääjä on päässyt järjestelmään sisälle asentamaan esimerkiksi kiristysohjelmia, haittaohjelmia tai hallinnoimaan itse järjestelmää etäkäytöllä (CISA, 2023; CISA, 2021b; Even, 2020). Haavoittuvuudet eivät kuitenkaan ole vain teknisiä vaan vesihuollon työntekijöiden aikaansaamia haavoittuvuuksia esimerkiksi vajavaisten salasanojen asettamista tai järjestelmien jättämistä täysin suojatta (CISA, 2021b; Even, 2020). Kuviossa 8 on esitetty Muckin ja Fitch (2019, s. 6) uhkalähtöistä mallia sekä Raggadin (2010, s. 84) uhkataksonomiaa mukaillen aikavälillä 1/2020–2/2024 vesihuoltoon kohdistuneita kyberuhkia.



KUVIO 8 Vesihuoltoon kohdistuneet kyberuhat aikavälillä 1/2020–2/2024

Kirjallisuuskatsauksessa esitetyt ennen 2020-lukua tapahtuneet vesihuoltoon kohdistuneet kyberhyökkäykset ovat kohdistuneet, kuten tässäkin tutkielmassa on havaittu, vesihuollon joka osa-alueeseen (taulukko 2; Hassanzadeh ym., 2020,

s. 5–11; Tuptuk ym., 2021, s. 4; Aslam ym., 2023, s. 13–16). Kuitenkin aiemmissa tutkimuksissa ei ole puhuttu vesihuollosta vastaavien tahojen tietokantoihin kohdistuneista hyökkäyksistä juurikaan, joka kuitenkin paljastui määrällisesti merkittäväksi kohteeksi aikavälillä 1/2020–2/2024 tapahtuneissa kyberhyökkäyksissä (taulukko 2). On kuitenkin mahdollista, että kirjallisuuskatsauksessa olleet artikkelit ovat tarkoituksellisesti rajanneet tarkastelunsa koskemaan pääosin vain veden puhdistamiseen ja vedenjakeluun liittyviin järjestelmiin kohdistuneita hyökkäyksiä vesihuollon kaikkien järjestelmien, myös tietokantojen, sijaan. Täten ei voida varmasti sanoa ovatko kyberuhat vesihuollon tietokantoihin kasvaneet 2020-luvulla aiempiin vuosikymmeniin verrattuna suuremmiksi. Aiemmat tutkimukset kuitenkin tunnistivat tietokantojen sisältämän tiedon rahallisen merkittävyyden ja rahallisen arvioinnin haasteen (Hassanzadeh ym., 2020, s.13; Tuptuk ym., 2021, s. 4; Aslam ym., 2023, s. 16).

Kuviossa 8 esitettyjen aineistosta havaittujen uhkien aikaansaajat ovat myös ennen 2020-lukua tapahtuneissa kyberhyökkäyksissä samankaltaiset. Niitä on kohdistunut sisäpiiriläisten ja ulkopuolisten tekeminä, kuten 2020-luvullakin (taulukko 2; Hassanzadeh ym., 2020, s. 5–11; Tuptuk ym., 2021, s. 4; Aslam ym., 2023, s. 13–16). Vesihuoltoon uhkia kohdistaneet tahot ovat pysyneet siis myös monipuolisina viime vuosikymmenistä 2020-luvun alkuun saakka, pitäen sisällään yksittäiset rikolliset sekä valtiollisiin toimijat. Aiemmat tutkimukset ovat olleet siis ennustuksissaan oikeassa ja vesihuolto on pysynyt monipuolisten toimijoiden kohteena myös 2020-luvulla, kuten kuvio 8 esittää. (Berglund, 2020, s. 28; Bello ym, 2022, s. 15–17; Clark, ym., 2016, s. 13) Tulevaisuuteen on vaikea nähdä, mutta erityistä muutosta parempaan tuskin on vesihuoltoon kohdistuvissa kyberuhkissa nähtävillä. Sillä kuten Ikäheimo ja Metsävuo (2020, s. 8) tuovat esiin, vesihuolto jatkaa verkostoitumista ja digitalisoitumista 2030-luvun lähestyessä, joka varmasti tuo tullessaan uusia haavoittuvuuksia ja väyliä vihamielisten toimijoiden hyödynnettäviksi.

Tämän tutkielman vastausta ensimmäiseen tutkimuskysymykseen voidaan hyödyntää käytännössä sekä jatkotutkimuksissa. Vesihuoltolaitoksien kyberturvallisuudesta vastaavat henkilöt voivat hyödyntää havaittuja kyberuhkia omissa uhka-arvioissaan sekä tarkastella, mihin sekä kuinka paljon vahinkoa nämä hyökkäykset ovat saaneet aikaan. Hyökkääjäkeskeisen uhkamallinnuksen aineistoina voidaan myös hyödyntää tämän tutkielman havaintoja tapahtuneista kyberhyökkäyksistä. Omaisuuskeskeistä hyökkäysmallintamista tekevät voivat taas hyötyä tutkielmassa esiin nousseista kyberhyökkäyksien kohteista. Tämä mahdollistaa uhkaan varautumisen ennen kyberhyökkäyksen tapahtumista sekä toimimisen hyvänä perusteluna sille, miksi vesihuollon kyberturvallisuus on merkittävä ja panostamisen arvoinen asia vesihuollosta vastaavissa organisaatioissa. Tutkimuskysymyksen vastauksen merkitys tulevalle kirjallisuudelle on toimia alustana, jolle voidaan rakentaa lopun 2020-luvun ja 2030-luvun vesihuoltoon kohdistuvien kyberuhkien tarkastelu. Vesihuoltoon kohdistuneet kyberuhat voidaan myös ottaa huomioon muiden kriittisen infrastruktuurin ja niihin kohdistuvien kyberuhkien tutkimisessa. Tutkielma myös tarjoaa esimerkin Raggadin (2010, s. 84) uhkataksonomian sekä Muckin ja Fitch (2019, s.

6) uhkalähtöisen mallin yhdistämisestä ja hyödyntämisestä selittämään kyberuhkien kohdistumista teoreettisessa mallissa (kuvio 8).

7.2 Tehdyt toimet kyberhyökkäyksen tapahduttua

Vesihuollon tahojen reaktioita niihin kohdistuneiden hyökkäysten jälkeen tarkasteltiin aineiston analyysissä seuraamuksena. Seuraamus teemana jakautui viiteen eri alateemaan, jotka kuvasivat niitä viittä eri kokonaisuutta kyberhyökkäyksen jälkeen, joita aineistosta kyettiin erottelemaan. Alateemat on esitetty jokseenkin aikajärjestyksessä kyberhyökkäyksen havaitsemisesta alkaen, mutta ne käytännössä tapahtuvat limittäin ja osin myös aikajärjestyksessä (kuvio 7). Kaikista tapahtumista ei ole raportoitu tarkasti sitä, miten kyberhyökkäykseen oli kokonaisuutena reagoitu, joten analyysi on yhteenveto koko aineistosta, huolimatta uhan laadusta tai mihin se on kohdistunut.

Kyberhyökkäyksen havaitsemisen jälkeen tapahtui vesihuollosta vastaavien tahojen ensireaktio, jonka avulla hyökkäys saatiin ehkä pysäytettyä, mahdollisia vahinkoja saatiin vältettyä tai ainakin jatkettua vesihuollon järjestelmien toimintaa (Water-ISAC, 2023; Brown, 2021). Ensireaktion onnistumisessa tukivat jo valmiina olevat kyberturvallisuusjärjestelmät, jotka ensinnäkin kykenivät havaitsemaan hyökkäyksen, mutta myös hälyttämään vesihuollon henkilöstöä tapahtuneesta (CISA, 2021b; Water-ISAC, 2023; Brown, 2021; South Staffs Water, 2022). Itse hyökkäyksen pysäyttämisen ja lisävahinkojen ehkäisyn lisäksi vesihuollosta vastaavat tahot tiedottivat ja toivat mukaan ulkopuolisia kyberturvallisuusammattilaisia tai viranomaistahoja, jotka kykenivät avustamaan kykyjensä mukaan (Southern Water, 2024a; Veolia, 2024; Wall, 2022). Viranomaistahot saattoivat myös ottaa tilanteen johtoon kokonaan, joka saattaa olla hyväkin toimintapa silloin, kun vesihuollosta vastaavalla taholla ei itsellään ole kykyä torjua kyberhyökkäystä (JNS, 2023).

Luonnollisesti kyberhyökkäyksessä tapahtunut vahinko oli korjattava, jotta vesihuollon järjestelmät kyettiin palauttamaan takaisin normaaliin toimintaan. Tosin aineistosta nousi esiin tapauksia, joissa vaadittavat korjaukset olivat minimaalisia eikä vahinkoakaan juuri päässyt tapahtumaan, joko esimerkiksi hyökkäyksen epäonnistumisen tai hyvällä tasolla olevien kyberturvallisuustoimien vuoksi (Collier, 2021; Even, 2020). Tämä ei kuitenkaan suoraan aina onnistunut, vaan järjestelmiä oli ylläpidettävä väliaikaisesti jopa manuaalisesti (CISA, 2021a). Myös henkilöresursseja oli hyödynnettävä tehokkaammin, jotta korjaustoimenpiteet kyettiin saattamaan pikaisesti alkuun tai järjestelmät palauttamaan toimintaan edes osin (Greig, 2023e). Tietokantoihin kohdistuneiden kyberhyökkäysten vahingot näyttäytyivät aineistossa merkittävästi haastavammiksi korjata verrattuna vesihuoltolaitoksiin kohdistuneisiin hyökkäyksiin, vieden merkittäviä rahallisia ja henkilöstöresursseja sekä mahdollisesti jopa kuukausia aikaa (D'Auria, 2021; SIAAP, 2023; Southern Water, 2024b). Käytännössähän tämä saattoi johtua siitä, että vesihuoltolaitoksia ja vedenjakelusta vastaavia kyberfyysisiä järjestelmiä oli mahdollista käyttää manuaalisesti edes rajallisesti, kun

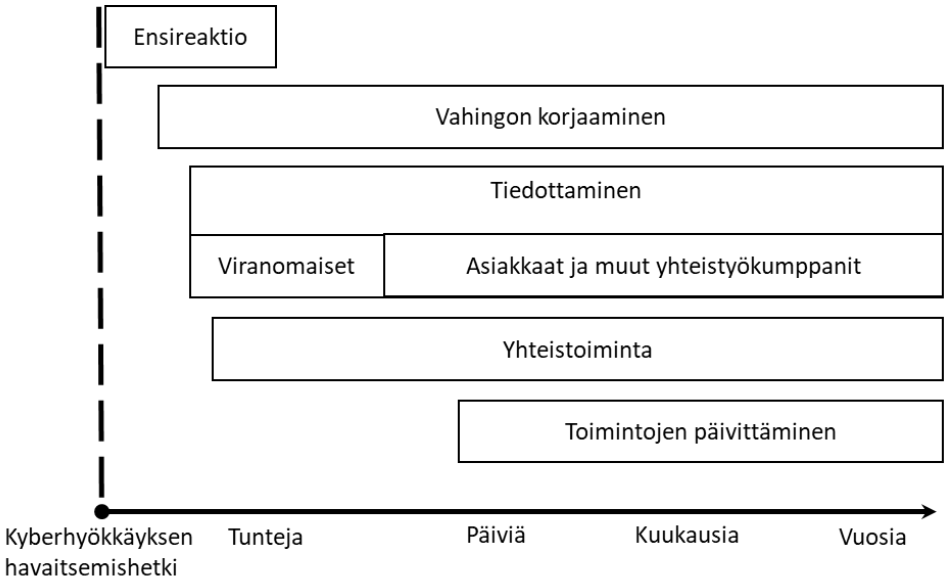
taas tietokantoja ei välttämättä ollut varmuuskopioina missään. Kiristysohjelmien ja niihin liittyvien tietomurtojen osana vuodetut asiakastiedot aiheuttivat myös korvausvastuun vesihuollosta vastaaville tahoille. Tähän reagoitiin esimerkiksi tarjoamalla erilaisia yksityisyyttä suojaavia tai identiteettivarkaudelta suojaavia palveluita, kuten vakuutusta (Stafford, 2020; Brown, 2021). Tämä kaikki tarjottiin tietysti vesihuollosta vastaavan tahon laskuun. Aineistossa nousi esiin myös mahdollisuus alistua kiristysohjelmia hyödyntäville tai tietomurrossa saaduilla tiedoilla kiristäville rikoksille, mutta missään tapauksessa ei ainakaan julkisesti tähän vaihtoehtoon tartuttu (D'Auria, 2020; Brown, 2021; Page, 2024).

Hyvin pian ensireaktion jälkeen aloitettiin tiedottaminen tapahtuneesta kyberhyökkäyksestä. Kuitenkin osassa tapauksista tiedottamista saatettiin lykätä kuukausia tai tiedottaa vain viranomaisia, jolloin vesihuoltoon kohdistuneet kyberhyökkäykset tulivat esiin vasta viranomaisten tekemissä raporteissa tai vuosikertomuksissa (CISA, 2021a; Water-ISAC, 2023). Osa vesihuollosta vastaavista tahoista toi omatoimisesti kuitenkin tiedotteissaan esiin kyberhyökkäykset, sillä tällöin he kykenivät mahdollisesti osoittamaan luotettavuutensa asiakkailleen. Tahot pääsivät myös korostamaan omien kyberturvallisuustoimiensa onnistumista tai edes, että hyökkäys oli havaittu. Vesihuollosta vastaavat tahot toivat osassa tapahtumista esiin hyvinkin pian tapahtuneen kyberhyökkäyksen julkisella tiedotuksella (Brown, 2021; Veolia, 2024; Stafford, 2020). Näissä tiedotteissa pyrittiin usein rauhoittelemaan asiakaskuntaa ja korostamaan, että tilanne oli hallinnassa (Stafford, 2020; Brown, 2021; South Staffs Water, 2022; Porto, 2023). Viranomaiset julkaisivat omia raporttejaan hyödyntäen vesihuollosta vastaavien tahojen ilmoituksia ja raportteja, joilla annettiin ohjeita ja hyviä toimintatapoja muille vesihuollosta vastaaville tahoille (Water-ISAC, 2023; CISA, 2023; CISA, 2021c). Osa ohjeista oli varsin yksityiskohtaisia koskien tiettyjä ohjelmia tai järjestelmiä, kun taas osa oli enemmän yleispäteviä ohjeistuksia (Water-ISAC, 2023; CISA, 2023; CISA, 2021b).

Yhteistoiminta aloitettiin eri viranomaisten ja muiden tahojen kanssa mahdollisimman pian kyberhyökkäyksen paljastuttua (Brown, 2021; Greig, 2023c; Southern Water, 2024b). Ne pidettiin tietoisina tapahtuneesta sekä tilanteen kehittymisestä (South Staffs Water, 2022; Southern Water, 2024b). Viranomaisissa oli kyse luonnollisesti eri kyberturvallisuuspuolen viranomaisista, mutta myös poliisi ja oikeuslaitos voitiin kutsua avuksi selvittämään tapahtunutta (Brown, 2021; Greig, 2023c; Southern Water, 2024b). Valtiollisten tahojen lisäksi turvauduttiin erilaisiin kyberturvallisuusyrityksiin, jotka tukivat kyberhyökkäyksen torjumisessa, siitä palautumisessa ja toiminnan kehittämisessä tulevaisuudessa (Wall, 2022; D'Auria, 2021; Southern Water, 2024b). Yksityisen puolen osaamisessa hyödynnettiin kyberturvallisuuden lisäksi laitevalmistajien sekä lakimiesten apua (JNS, 2023; D'Auria, 2020).

Hyökkäyksestä palautumisen jälkeen toimintoja päivitettiin, jotta mahdollisesti vastaavanlaisia kyberhyökkäyksiä ei tulevaisuudessa enää tapahtuisi. Toimintojen päivittämiseen kuuluivat itse järjestelmien ja ohjelmistojen päivittämiset, mutta myös kyberturvallisuuteen liittyvien ohjelmistojen toimeenpa-

neminen vesihuollon eri järjestelmiin sekä laitoksiin (Wall, 2022; Stafford, 2020). Uudet hankinnat ja niihin mahdollisesti tarvittavat konsultit luonnollisesti olivat osin merkittävä rahallinen investointi (Greig, 2023e). Vähemmälle huomiolle aineistossa jäivät kuitenkin ihmiset ja heidän toimintatapojen eli kybertuvallisuuskulttuurin parantaminen vesihuoltojärjestelmistä vastaavissa organisaatioissa.



KUVIO 9 Kyberhyökkäykseen reagointi vesihuollossa

Kuvio 9 on aineistosta analysoitu yksinkertaistettu aikaan sidottu kuvio, jossa on esitetty vesihuollosta vastaavien tahojen reaktio kyberhyökkäykseen sen tapahtumisesta aina jopa vuosiksi eteenpäin. Ensireaktio pitää sisällään vesihuollosta vastaavien toimijoiden sisäisen tilanteenarvion siitä, mitä oikein on tapahtunut. Tilanteenarvioissa tarkastellaan, mikä uhka vesihuollon järjestelmään on kohdistunut ja mitä vahinkoa se on saanut aikaan. Tämän jälkeen aloitetaan nopeat toimet tapahtuneen vahingon korjaamiseksi sekä otetaan yhteyttä asiaan kuuluviin viranomaisiin. Vahingon korjaamista ja tiedonvaihtoa viranomaisten kanssa jatketaan, jonka yhteydessä ensimmäiset yhteistoimintatahot tuodaan mukaan ongelman ratkaisemiseksi. Nämä voivat olla julkisia tai yksityisiä kyberturvallisuuden sekä muiden alojen asiantuntijoita. Ensireaktiosta tilanne vakiinnutetaan ja korjaamista sekä tiedottamista ja yhteistoimintaa jatketaan. Kun on saatu tarvittava ymmärrys siitä mitä on tapahtunut, voidaan julkaista julkinen tiedote asiakkaille. Asian julkiseksi tuominen voi kestää kauankin, mikäli esimerkiksi kyberhyökkäyksen vahingot ovat epäselviä tai, jos asian tuo esiin viranomaistaho omassa raportissaan. Toimintojen päivittäminen aloitetaan heti, kun siihen on mahdollisuus sillä, vaikka muut toimet ovatkin vielä käynnissä, on hyökkäyksen tapahtuminen osoittanut, että kaikki ei ole kyberturvallisuuden osalta kunnossa kyseisessä vesihuollon järjestelmässä tai sitä ylläpitävässä organisaatiossa. Kaikki aineistosta havaitut merkittävät reaktiot ovat nyt käynnissä tai tapahtuneet ja ne voivat pahimmillaan jatkua kuvion 9 mukaisesti vuosia, jos vahinkoa ei saada esimerkiksi korjattua tai toimintoja

päivitettyä (D'Auria, 2020). Tietysti on myös täysin mahdollista, että hyökkäys saadaan torjuttua miltei täysin ja kuvion 9 aikaikkuna kestää vain muutamia päiviä tai kuukausia (Van Osdol, 2021; Brown, 2021).

Aineiston analyysin perusteella luotu kuvio 9 pitää sisällään samoja toimintatapoja kuin Traficomin toimintaohjeissa kiristysohjelmien (2022a) ja tietomurtojen (2022b) osalta, vaikkakin Traficomin toimintaohjeet eivät yritä luoda aikautusta eri toimintojen kestolle. Traficomin (2022a; 2022b) ohjeistus on kuitenkin huomattavasti yksityiskohtaisempi ja huomio ensireaktion teknisen puolen tarkemmin. Kuitenkin myös Traficomin (2022a, s. 9–11; 2022b, s. 8–9) ensireaktio tai ”välittömät toimenpiteet” (Traficom, 2022a, s. 9; 2022b, s. 8) pitää sisällään ensimmäiset korjaustoimenpiteet, joissa saastuneet järjestelmät eristetään, tiedotetaan tekemällä ilmoitus viranomaisille sekä yhteistyökumppaneille ja aloitetaan ulkopuolisen avun tarpeen kartoittaminen eli yhteistoiminta. Traficomin (2022a; 2022b) ohjeistus erittelee vielä tietoturvaloukkauksen selvityksen omaksi alueekseen, jota ei tämän tutkielman aineiston analyysin perusteella voinut eritellä omaksi alateemakseen, koska se ei tullut aineistossa merkittävästi esiin, mutta joka kuitenkin sisältyi ensireaktioon. Kuviossa 9 esitetty vahinkojen korjaaminen jatkuu Traficomin (2022a; 2022b) palautuminen -osiossa, jossa järjestelmät palautetaan toimintakuntoisiksi ja viimeistään informoidaan henkilöitä, joiden tiedot ovat saattaneet joutua hyökkääjien käsiin (Traficom, 2022b, s. 13). Traficomin (2022a; 2022b) toimintaohjeet eivät ota huomioon toimintojen päivittämistä teknisellä tasolla vaiheena, mutta pitävät sisällään viimeisenä toimena itsearvioin siitä, miten organisaatio on selvinnyt kyberhyökkäyksestä ja minkä asioiden osalta toimintaa voitaisiin lähteä itsearvion perusteella kehittämään. Tämä osa-alue ei tullut aineiston analyysissä esiin, mutta sen perusteellahan toimintoja lähdetään kuitenkin päivittämään. Muutenhan voitaisiin turhaan päivittää järjestelmiä, jotka eivät edes edesauttaneet kyberhyökkäyksen tapahtumista. Kyberturvallisuuskeskus haluaa myös saada tietoonsa tehdyn itsearvon, sillä heidän mukaansa ”palautumisesta saadut opit auttavat kehittämään kaikkien organisaatioiden varautumista” (Traficom, 2022b, s. 14). Tämä lainauksen sisältämä viesti koskee myös vesihuollosta vastaavia tahoja.

Tutkielman toisen tutkimuskysymyksen, *miten vesihuollosta vastaavat tahot ovat reagoineet kyberhyökkäyksiin aineiston perusteella*, vastauksia voidaan hyödyntää käytännössä tukemaan vesihuollosta vastaavien organisaatioiden kyberturvallisuustoimenpiteitä tarkastelemalla muiden vastaavien tahojen reagointia eri kyberhyökkäyksiin. Kyberturvallisuudesta vastaavat henkilöt voivat tarkastella, miten reaktiot eri kyberhyökkäyksiin ovat vaikuttaneet esimerkiksi tilanteesta palautumiseen. Vaikka tarkkaa tietoa ei ole siitä, mitä vaikutusta reaktiolla on ollut, he voivat arvioida reaktion vaikutusta kyberturvallisuuden, mutta esimerkiksi myös viestinnän onnistumisen kannalta. Teorian osalta tutkimuskysymyksen vastaus tuo esiin, millä keinoin vesihuollosta vastaavat tahot ovat reagoineet kyberuhkiin sekä miten reaktiot ovat ilmenneet eri virallisten tahojen raporteissa sekä mediassa. Tuloksia voidaan mahdollisesti hyödyntää koko kriittistä infrastruktuurin koskevien uhkien hallinnan ja niiden aikaansaaman reaktion tarkasteluun eri infrastruktuurin tahojen organisaatioissa.

7.3 Jatkotutkimusmahdollisuudet

Tämän tutkielman tavoite oli vastata tutkimusongelmaan siitä, *mitä kyberhyökkäyksiä vesihuoltoon on kohdistunut aikavälillä 1/2020–2/2024*. Tutkielman kirjoittamisajankohdan vuoksi 2020-luvusta on tarkasteltu kuitenkin vain ensimmäiset vuodet, joista vain ensimmäiset neljä vuotta ovat olleet kokonaisia. Tämän haasteen vuoksi tulevaisuuteen jää tutkittavaksi, pysyvätkö tutkielman havaitsemat vesihuoltoon kohdistuneet kyberturvallisuusuhat samoina vai korvaantuvatko ne mahdollisesti toisilla uhilla 2030-lukua lähestyttäessä. Tässä tutkielmassa ei myöskään pyritty ennustamaan, miten vesihuoltoon kohdistuvat kyberuhat tulisivat kehittymään 2020-luvun edetessä. Esimerkiksi, jos näin olisi tehty, niiden aikaansaamaa vahinkoa, nimettyä tekijää tai tekotapaa olisi voitu tarkastella 2020-luvun päättyessä ja pohtia syitä siihen, miksi vesihuoltoon kohdistuneet uhat olivat kehittyneet arvioista poikkeaviksi tai sen mukaisiksi. Jatkotutkimuksissa voitaisiin myös vertailla, mitä kyberuhkia muihin kriittisen infrastruktuurin osa-alueisiin on kohdistunut sekä mitä yhdenmukaisuuksia tai eriäväisyyksiä niillä on ollut vesihuoltoon kohdistuviin kyberuhkiin verrattuna.

Tässä tutkielmassa ollut aineisto oli koottu eri toimijoilta ja erilaisista lähteistä uutisista raportteihin, jolloin niiden luotettavuus niin sisällön kuin tarkoitusperienkin osalta voi olla johtanut harhaan tämän tutkimuksen johtopäätöksiä ja analyysiä. Mikäli on mahdollista saada tukeutua tulevissa tutkimuksissa viranomaisten omiin aineistoihin tapahtuneista kyberhyökkäyksistä, voi se olla merkittävästi neutraalimpaa ja syvällisempää kuin uutiset tai uhriksi joutuneiden tahojen julkaistut tiedotteet. Aineistossa voitaisiin tuoda mahdollisesti esille myös ne tapahtuneet kyberhyökkäykset, joita ei ole tuotu julkisuuteen, mutta jotka on raportoitu viranomaisille. Tämä voisi tosin rajoittaa tutkimuksien julkaisumahdollisuuksia, ainakin jos kohteiksi joutuneet vesihuollosta vastaavat tahot olisivat tunnistettavissa.

Tarkempi ja täydellisempi aineisto myös mahdollistaisi luotettavamman tarkastelun eikä pelkästään mitä kyberuhkia on kohdistunut vesihuoltoon vaan miten, kenen toimesta tai miksi ne ovat kohdistuneet. Nyt kerätyssä aineistossa oli mahdollista yksittäisten tapausten osalta arvioida miten, kenen toimesta tai miksi hyökkäys oli tehty, mutta täysin varmaa syytä ei uutisjulkaisuista voi saada. Aineistoon tulisi saada tarkkoja ja objektiivisia raportteja, joista voitaisiin koota luotettavampi kokonaiskuva.

Uhkalähtöisen lähestymistavan vertaamista riskien hallintaan perustuvaan lähestymistapaan voisi tuoda myös merkittäviä käytännön kyberturvallisuutta tukevia havaintoja. Tässä tutkielmassa hyödynnettiin Raggadin (2010, s. 84) uhkataksonomiaa sekä Muckin ja Fitch (2019, s. 6) uhkalähtöistä mallia selittämään vesihuoltoon kohdistuvia kyberuhkia, mutta uhkalähtöistä mallia ei kuitenkaan tarkasteltu kriittisesti eikä sille esitetty vaihtoehtoja lähtökohtana vesihuollon kyberturvallisuuden suunnittelulle ja toteuttamiselle. Jatkotutkimus erilaisten mallien hyödyntämisestä vesihuollon turvaamiseksi kyberuhilta

toisi merkittävää sekä käytännön että teoreettista hyötyä myös muille kriittisen infrastruktuurin osa-alueille.

Vesihuollosta vastaavien tahojen reaktiota kyberhyökkäyksiin voitaisiin tutkia yksityiskohtaisemmin myös tulevaisuudessa. Erityisesti, jos on mahdollista päästä tarkastelemaan uhriksi joutuneen tahon sisäisiä prosesseja ja vertaamaan niiden toimeenpanemista kyberturvallisuusohjeistuksiin (Traficom, 2022a; 2022b). Tämä mahdollistaisi selvittämisen siitä, miksi kaikissa tai tietyissä tapauksissa kyberhyökkäyksiin on reagoitu ja miten mahdollisesti vesihuollosta vastaavat tahot voisivat toimintaansa kehittää tai kyberturvallisuusohjeistuksia päivittää. Vesihuollosta vastaavien tahojen sisäpiiriläisille toteutetut haastattelut ja kyselyt tutkimuksen johtopäätöksistä voisivat tuoda myös lisää näkökulmia, joilla tuotaisiin tutkimukseen lisää yksityiskohtaista ja ammatillista näkemystä varsinkin, jos haastateltava oli ollut osallisena selvittämässä tapahtunutta kyberhyökkäystä. Heitä haastattelemalla olisi myös mahdollista saada kokonaisempi ja ehkä rehellisempi kuva vesihuollon kyberturvallisuudesta kuin viestinnän ammattilaisten kirjoittamista tiedotteista. Tässä tutkimuksessa tarkasteltiin myös vesihuollosta vastaavien tahojen reaktioita kyberhyökkäyksiin kokonaisuutena, eikä uhkien mukaan eriteltynä. Jatkossa olisi mahdollista tutkia, mitä eroja eri kyberuhkiin oli havaittavissa ja seurasivatko ne annettuja julkisia, mutta myös organisaation sisäisiä kyberturvallisuusohjeistuksia.

LÄHTEET

Addeen, H., Xiao, Y., Li, J. & Guizani M. (2021). A Survey of Cyber-Physical Attacks and Detection Methods in Smart Water Distribution Systems. *IEEE Access, vol. 9*, pp. 99905-99921. 2021. doi: 10.1109/ACCESS.2021.3095713.

Adepu, S., Palleti, V.R., Mishra, G., Mathur, A. (2020). Investigation of Cyber Attacks on a Water Distribution System. In: Zhou, J., ym. Applied Cryptography and Network Security Workshops. *ACNS 2020. Lecture Notes in Computer Science(), vol 12418. Springer*, 274-291, Cham. https://doi.org/10.1007/978-3-030-61638-0_16

Agenzia Nova. (2023, 6. helmikuuta). Acea: "*After the hacker attack, the operations of the IT systems have been restored*". https://www.agenzianova.com/en/news/acea-after-the-hacker-attack-the-operation-of-the-computer-systems-was-restored/

Ahya, R. (2020, 17. heinäkuuta). *Again: a cyber attack on water facilities in Israel*. Ynet. Käännetty Google-kääntäjällä lähteestä englanniksi. https://www.ynet.co.il/article/rJrCqmAkw

Aslam, M. M., Tufail, A., Kim, K. H., Apong, R. A. A. H. M., & Raza, M. T. (2023). A Comprehensive Study on Cyber Attacks in Communication Networks in Water Purification and Distribution Plants: Challenges, Vulnerabilities, and Future Prospects. *Sensors* 2023, 23(18), 7999. https://doi.org/10.3390/s23187999

Axelbank, E. (2023, 11. huhtikuuta). '*Hack*' *of Oldsmar water plant reported two years ago could have been employee error*. FOX13 Tampa. https://www.fox13news.com/news/hack-of-oldsmar-water-plant-reported-two-years-ago-could-have-been-employee-error

Bello, A., Jahan, S., Farid, F., & Ahamed, F. (2022). A Systemic Review of the Cybersecurity Challenges in Australian Water Infrastructure Management. *Water*, 15(1), 168. https://doi.org/10.3390/w15010168

Berglund, E. Z., Pesantez, J. E., Rasekh, A., Shafiee, M. E., Sela, L., & Haxton, T. (2020). Review of Modeling Methodologies for Managing Water Distribution Security. *Journal of water resources planning and management*, 146(8), 1–23. https://doi.org/10.1061/(ASCE)WR.1943-5452.0001265

Berninger, K., Laakso, T., Paatela, H., Virta, S., Rautiainen, J., Virtanen, R., Vahala, R. (2018). *Tulevaisuuden kestävä vesihuolto – ennakointi, ohjaus ja järjestäminen* (julkaisusarja 56/2018). Valtioneuvoston kanslia. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161028/56-

2018-Tulevaisuuden%20kestava%20vesihuolto.pdf?sequence=1&isAllowed=y

Biswas, A. K. (2004). Integrated water resources management: a reassessment: a water forum contribution. *Water international*, 29(2), 248-256. https://doi.org/10.1080/02508060408691775

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2), 77-101. https://doi.org/10.1191/1478088706qp063oa

Brown, C. (2021, 25. kesäkuuta). *WSSC Water Investigating Ransomware Cyberattack.* WSSC Water. https://www.wsscwater.com/news/2021/june/wssc-water-investigating-ransomware-cyberattack

CERT-EU. (2023). *Cyber Security Brief (May 2023).* CERT-EU. https://cert.europa.eu/static/threat-intelligence/TLP-CLEAR-CB-23-06.pdf

Chawaga, P. (2023, 29. maaliskuuta). *Former Official Claims Oldsmar Drinking Water Hack Was Really Operator Error*. Water Online. https://www.wateronline.com/doc/former-official-claims-oldsmar-drinking-water-hack-was-really-operator-error-0001

Cybersecurity & Infrastructure Security Agency (CISA). (2021a, 25. lokakuuta). *Ongoing Cyber Threats to U.S. Water and Wastewater Systems*. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-287a

Cybersecurity & Infrastructure Security Agency (CISA). (2021b). *Compromise of U.S. Water Treatment Facility*. Joint Cybersecurity Advisory. https://www.cisa.gov/sites/default/files/2023-04/AA21-042A_Joint_Cybersecurity_Advisory_Cyber_Actors_Compromise_U.S._Water_Treatment_Facility.pdf

Cybersecurity & Infrastructure Security Agency (CISA). (2021c, 24. elokuuta). *Exploitation of Pulse Connect Secure Vulnerabilities*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-110a

Cybersecurity & Infrastructure Security Agency (CISA). (2023). *IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities*. https://www.cisa.gov/sites/default/files/2023-12/aa23-335a-irgc-affiliated-cyber-actors-exploit-plcs-in-multiple-sectors-1.pdf

Clark, R. M., Panguluri, S., Nelson, T. D., & Wyman, R. P. (2017). Protecting drinking water utilities from cyberthreats. *Journal (American Water Works Association)*, 109(2), 50-58. https://www.osti.gov/pages/servlets/purl/1372266

Collier, K. (2021, 17. kesäkuuta). *50,000 security disasters waiting to happen: The problem of America's water supplies*. NBC News. https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password-rcna1206

D'Auria, P. (2021, 12. tammikuuta). *3 months after cyberattack that threatened 'public health crisis,' Jersey City MUA computer systems still not fully restored*. The Jersey Journal. https://www.nj.com/hudson/2021/01/3-months-after-cyberattack-that-threatened-public-health-crisis-jersey-city-mua-computer-systems-still-not-fully-restored.html

D'Auria, P. (2020, 11. joulukuuta). *Jersey City utilities agency investigating ransomware attack that blocked access to 'vital' data*. The Jersey Journal. https://www.nj.com/hudson/2020/12/jersey-city-utilities-agency-investigating-ransomware-attack-that-blocked-access-to-vital-data.html

Department of Homeland Security (DHS). (2015). *Water and Wastewater Systems Sector-Specific Plan*. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf

Department of Homeland Security (DHS). (2021). *Malicious Cyber Actors Likely to Continue Exploiting Vulnerabilities in Water and Wastewater Systems Networks*. https://mwua.org/wp-content/uploads/2021/05/Malicious-Cyber-Actors-Likely-to-Continue-Exploiting-Vulnerabilities-05202021.pdf

Department of Justice (DOJ). (2023, 7. heinäkuuta). *Tracy Resident Charged With Computer Attack On Discovery Bay Water Treatment Facility*. United States Attorney's office; Northern District of California. https://www.justice.gov/usao-ndca/pr/tracy-resident-charged-computer-attack-discovery-bay-water-treatment-facility

The European Union Agency for Cybersecurity (ENISA). (2020a). *ENISA Threat Landscape 2020*. The European Union Agency for Cybersecurity. https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/enisa-threat-landscape-2020?v2=1&tab=details

The European Union Agency for Cybersecurity (ENISA). (2020b). *ENISA Threat Landscape 2020: Main incidents in the EU and worldwide*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents

The European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape 2023*. The European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

The European Union Agency for Cybersecurity (ENISA). (2022). *ENISA Threat Landscape 2022*. The European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

The European Union Agency for Cybersecurity (ENISA). (2021). *ENISA Threat Landscape 2021*. The European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Eskola, J. & Suoranta, J. (2008). *Johdatus laadulliseen tutkimukseen*. Vastapaino. Gummerrus Jyväskylä.

Euroopan parlamentti. (2022, 22. marraskuuta). *Mepit hyväksyivät uudet säännöt EU:n kriittisen infrastruktuurin suojaamiseksi.* [Lehdistötiedote]. Mepit hyväksyivät uudet säännöt EU:n kriittisen infrastruktuurin suojaamiseksi | Ajankohtaista | Euroopan parlamentti (europa.eu)

Even, N. (2020, 3. joulukuuta). *What We've Learned From The Israeli Reservoir Attack on Dec 1st*. Otorio. https://www.otorio.com/blog/what-we-ve-learned-from-the-december-1st-attack-on-an-israeli-water-reservoir/

Fernandez, E. B. (2016). Threat modeling in cyber-physical systems. *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)* (pp. 448-453). IEEE. DOI: 10.1109/DASC-PICom-DataCom-CyberSciTec.2016.89

Greig, J. (2023a, 3. toukokuuta). *North Italian water supplier serving 500,000 people hit with ransomware attack.* The Record. https://therecord.media/italian-water-supplier-ransomware-attack-disruptions-medusa

Greig, J. (2023b, 28. marraskuuta). *North Texas water utility serving 2 million hit with cyberattack*. The Record. https://therecord.media/north-texas-water-utility-cyberattack

Greig, J. (2023c, 21. helmikuuta). *LockBit gang takes credit for attack on water utility in Portugal. The Record*. https://therecord.media/porto-portugal-water-utility-cyberattack-lockbit

Greig, J. (2023d, 24. maaliskuuta). *FBI, CISA investigating cyberattack on Puerto Rico's water authority*. The Record. https://therecord.media/fbi-investigating-cyberattack-on-puerto-rico

Greig, J. (2023e, 21. marraskuuta). *Greater Paris wastewater agency dealing with cyberattack*. The Record. https://therecord.media/paris-wastewater-agency-hit-cyberattack

Greig, J. (2023f, 4. joulukuuta). *Florida water agency latest to confirm cyber incident as feds warn of nation-state attacks.* The Record. https://therecord.media/florida-water-agency-ransomware-cisa-warning-utilities

Hagelstam, A. (2005). *CIP – kriittisen infrastruktuurin turvaaminen, käsiteanalyysi ja kansainvälinen vertailu* (Julkaisuja 1/2005). Huoltovarmuuskeskus. https://www.huoltovarmuuskeskus.fi/files/019d67575f48fdb84212fd8bd9164b8ac8829ccd/cip-raportti_final.pdf

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. K. (2020). A review of cybersecurity incidents in the water sector. *Journal of Environmental Engineering, 146(5),* 03120003. https://arxiv.org/pdf/2001.11144.pdf

Helsingin seudun ympäristöpalvelut (HSY). (2019*). Jätevedenpuhdistus pääkaupunkiseudulla 2019 - Viikinmäen ja Suomenojan jätevedenpuhdistamot* (Julkaisuja 3/2020). https://julkaisu.hsy.fi/jatevedenpuhdistus-paakaupunkiseudulla-2019.html

Huhtakangas, S. (2017). *Vedenpuhdistuslaitosten kokonaistehokkuuden parantaminen tuotannon tasapainottamisen avulla* [opinnäytetyö, Oulun ammattikorkeakoulu]. Theseus-julkaisuarkisto. https://urn.fi/URN:NBN:fi:amk-2017060111818

Huoltovarmuuskeskus. (2021). *Turvallisuusjohtaminen vesihuoltolaitoksilla* (monistesarja nro 68). https://www.vvy.fi/site/assets/files/5826/vesihuoltolaitosten_turvallisuusjohtaminen_raportti_painos2.pdf

Huoltovarmuuskeskus. (2022). *Toimialojen kyberkypsyyden selvitys 2022* (kansallinen koosteraportti). https://www.huoltovarmuuskeskus.fi/files/29b11d0af56a115126ad490af444f1c4fd7885af/hvk-toimialojen-kyberkypsyyden-selvitys-2022.pdf

Ikäheimo, A. & Metsävuo, J. (2020). *Vesihuoltolaitosten digistrategia – portaat digitalisaation hyödyntämiseen* (monistesarja nro 59). Vesilaitosyhdistys. https://www.vvy.fi/site/assets/files/3211/vvy_digitalisaatiostrategia_loppuraportti.pdf

Jewish News Syndicate (JNS). (2023, 10. huhtikuuta). *Cyber attack shutters Galilee farm water controllers.* https://www.jns.org/cyberattack-shutters-galilee-farm-water-controllers/

Juhila, K. (ei pvm.) Teemoittelu. Haettu 21.11.2023 osoitteesta https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/analyysitavan-valinta-ja-yleiset-analyysitavat/teemoittelu/

Kaspersky. (2023). *H1 2023 –a brief overview of main incidents in industrial cybersecurity*. Kaspersky ICS CERT. https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-H1-2023-a-brief-overview-of-main-incidents-in-industrial-cybersecurity-En.pdf

Kavanah, B. (2021, 8. heinäkuuta). *Cybersecurity Threats to Water and Wastewater Infrastructure in Maine*. State of Maine, Department of environmental protection. https://mwua.org/wp-content/uploads/2021/07/DEP-Cybersecurity-memo-7-8-21.pdf

Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2018). STRIDE-based Threat Modeling for Cyber-Physical Systems. *2017 IEEE PES: Innovative Smart Grid Technologies Conference Europe (ISGT-Europe): Proceedings IEEE*. https://doi.org/10.1109/ISGTEurope.2017.8260283

Kuulas, A., Renko, T., Kuivamäki, R. (2017). *Vesihuollon investointitarpeet vuoteen 2040* (monistesarja nro 63). Vesilaitosyhdistys. https://www.vvy.fi/site/assets/files/5239/vesihuollon_investointitarpeet_vvy_10092020_final.pdf

Laakso, T., Hell, K., Malmlund, J., Sivonen, K., Laukkanen, J. (2021). *Vesihuoltoverkoston mittaus ja dokumentointi*. Suomen Vesilaitosyhdistys ry. ISBN 978- 952-6697-63-5 https://www.vvy.fi/site/assets/files/5659/vesihuoltoverkosto_004_19022021.pdf

Lee, E. A. (2006). Cyber-physical systems-are computing foundations adequate. *NSF workshop on cyber-physical systems: research motivation, techniques and roadmap* (Vol. 2, pp. 1-9). https://ptolemy.berkeley.edu/publications/papers/06/CPSPositionPaper/Lee_CPS_PositionPaper.pdf

Maa- ja metsätalousministeriö. (2021). *Kansallisen vesihuoltouudistuksen ohjelma* (julkaisuja 2021:7). https://mmm.fi/documents/1410837/6164691/KansallisenVesihuoltouudistuksenOhjelma.pdf/c0e480ef-cbd0-c63e-6f37-fb61621421a0/KansallisenVesihuoltouudistuksenOhjelma.pdf?t=1623735510993

Mishra, V. K., Palleti, V. R. & Mathur, A. (2019). A modeling framework for critical infrastructure and its application in detecting cyber-attacks on a water distribution system. *International Journal of Critical Infrastructure Protection. Volume 26*, 100298. https://doi.org/10.1016/j.ijcip.2019.05.001

Muckin, M., & Fitch, S. C. (2019*). A Threat-Driven Approach to Cyber Security*. Lockheed Martin-yhtiö. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf

Myllylä, H. (2012). *Vesihuollon suunnitteluohje, Suunnittelukäytännöt pääkaupunkiseudulla* [insinöörityö, Metropolian ammattikorkeakoulu]. Theseus-julkaisuarkisto. https://www.theseus.fi/bitstream/handle/10024/42439/Vesihuol.pdf?se-quence=1

Moraitis G., Nikolopoulos, D., Bouziotas, D., Lykou, A., Karavokiros, G. & Makropoulos, C. (2020). Quantifying Failure for Critical Water Infrastructuresunder Cyber-Physical Threats. *Journal of Environmental Engineering*, Vol. 146, No. 9. 04020108. https://doi.org/10.1061/(ASCE)EE.1943-7870.000176

National cyber security centre. (2022). *Cyber Threat Report 2021/2022*. Government Communications Security Bureau.

https://www.ncsc.govt.nz/assets/NCSC-Documents/2021-2022-Cyber-Threat-Report.pdf

Nikolopoulos, D., Makropoulos, C., Kalogeras, D., Monokrousou, K. & Tsoukalas, I. (2018). Developing a stress-testing platform for cyber-physical water infrastructure, *2018 International Workshop on Cyber-Physical Systems for Smart Water Networks (CySWater)*, 9–11. doi:10.1109/CySWater.2018.00009

National Institute of Standards and Technology (NIST). (2012). *Guide for Conducting Risk Assessments*. NIST SP 800-30 Rev. 1. https://doi.org/10.6028/NIST.SP.800-30r1

National Institute of Standards and Technology (NIST). (ei pvm.). Cyber Attack. Glossary. Haettu 2.5.2024 osoitteesta https://csrc.nist.gov/glossary/term/Cyber_Attack

Paganini, P. (2023, 28. marraskuuta). *Daixin team group claimed the hack of north Texas municipal water district*. Security affairs. https://securityaffairs.com/154881/cyber-crime/daixin-team-north-texas-municipal-water-district.html

Page, C. (2024, 14. helmikuuta). *UK utility giant Southern Water says hackers stole personal data of hundreds of thousands of customers*. Techcrunch. https://tcrn.ch/3wlfEiw

Palleti, V., Adepu, S., Mishra, V. & Mathur, A. (2021). Cascading effects of cyber-attacks on interconnected critical infrastructure. *Cybersecur 4*, 1-19. https://doi.org/10.1186/s42400-021-00071-z

Panguluri, S., Phillips, W. & Cusimano, J. (2011). Protecting water and wastewater infrastructure from cyber attacks. *Front. Earth Sci. 5*, 406–413. https://doi.org/10.1007/s11707-011-0199-5

Porto. (2023, 8. helmikuuta). *Comunicado: Águas e Energia do Porto alvo de ataque informático*. Porto. Käännetty Google-kääntäjällä lähteestä englanniksi. https://www.aguasdoporto.pt/noticias/comunicado-aedp-ataqueinformatico

Quinn, T. (2023, 7. joulukuuta). *Hackers hit Erris water in stance over Israel*. Western People. https://westernpeople.ie/news/hackers-hit-erris-water-in-stance-over-israel_arid-4982.html

Raggad, B. G. (2010). *Information security management: Concepts and practice*. CRC Press.

Rautiainen, A, M. (2023). *"Ne totuudet on jotenkin sisäisiä silloin" : kokemusten kertominen kirjoittamisen perusopintojen oppimispäiväkirjoissa* [väitöskirja, Jyväskylän yliopisto]. JYX-julkaisuarkisto. http://urn.fi/URN:ISBN:978-951-39-9722-9

Shostack, A. (2014). *Threat modeling, designing for security.* John Wiley & Sons, Inc.

Silfverberg, P. (2017). *Vesihuollon suuntaviivat 2020-luvulle* (monistesarja nro 44). Vesilaitosyhdistys. https://valtioneuvosto.fi/documents/1410837/1516651/Vesihuollon+suuntaviivat+2020-luvulle_final_20170622.pdf/cb687a80-dd57-4733-88c7-f3962e4bf9f4

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management, 51(2)*, 217-224. https://doi.org/10.1016/j.im.2013.08.006

South Staffs Water. (2022, 15. elokuuta). *Important statement*. https://www.south-staffs-water.co.uk/news/important-statement

Southern water. (2024a, 23. tammikuuta). *Cyber investigation*. https://www.southernwater.co.uk/the-news-room/the-media-centre/2024/january/cyber-investigation

Southern water. (2024b, 12. helmikuuta). *Cyber attack – update for customers*. https://www.southernwater.co.uk/the-news-room/the-media-centre/2024/february/cyber-attack-update-for-customers

Staff, T. (2020b, 17. kesäkuuta) *Cyber attacks again hit Israel's water system, shutting agricultural pumps*. The Times of Israel. https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/

Staff, T. (2020a, 19. maaliskuuta) *6 facilities said hit in Iran's cyberattack on Israel's water system in April*. The Times of Israel. https://www.timesofisrael.com/6-facilities-said-hit-in-irans-cyberattack-on-israels-water-system-in-april/

Stafford, T. (2020). *Notice of data breach*. Camrosa water district. https://oag.ca.gov/system/files/Camrosa%20-%20California%20Notification.pdf

Suderman, A. (2021, 15. kesäkuuta). *China hacked an internet security tool to target Verizon and Southern California's water supplier, among others*. Business Insider. https://www.businessinsider.com/chinese-breach-pulse-secure-network-targeted-verizon-water-supplier-2021-6?op=1&r=US&IR=T

Syndicat interdépartemental pour l'assainissement de l'agglomération parisienne (SIAAP). (2023, 18. marraskuuta). *Bulletin-cyberattaque*. Käännetty Google-kääntäjällä lähteestä englanniksi. https://www.siaap.fr/presse-publications/publications/detail/actualites/bulletin-cyberattaque/

The National Cyber Array. (2020, 24. huhtikuuta). *Attack attempts on control and control systems in the water sector*. Käännetty Google-kääntäjällä lähteestä englanniksi. https://www.gov.il/he/departments/publications/reports/scadaalert

The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC). (2023, 6. maaliskuuta). *Water Sector Threat Analysis Report*. https://www.cyber.nj.gov/threat-analysis-reports/water-sector-threat-analysis-report

The New Jersey Cybersecurity and Communications Integration Cell (NJCCIC). (2022, 20. lokakuuta). *Threat of Ransomware Continues; Garden State Cyber Threat Highligh*. https://www.cyber.nj.gov/Home/Components/News/News/192/

Traficom. (2022a). *Toimintaohje – Kiristyshaittaohjelma* (julkaisuja 23/2022). Liikenne- ja viestintävirasto, kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/KiristyshaittaohjelmaToimintaohje.pdf

Traficom. (2022b). *Toimintaohje – Tietomurto* (julkaisuja 24/2022). Liikenne- ja viestintävirasto, kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/TietomurtoToimintaohje.pdf

Tuorila, H. & Saastamoinen, A. (2022). *Uudistuva vesihuolto* (tutkimusraportteja 3/2022). Kilpailu- ja kuluttajavirasto. https://www.kkv.fi/uploads/sites/2/2022/04/2022-03-tutkimusraportteja-uudistuva-vesihuolto.pdf

Tuptuk, N., Hazell, P., Watson, J., & Hailes, S. (2021). A Systematic Review of the State of Cyber-Security in Water Systems. *Water*, 2021 13(1), 81. https://doi.org/10.3390/w13010081

Turvallisuuskomitea. (2018). *Kyberturvallisuuden sanasto*. Huoltovarmuuskeskus. https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Tuomi, J. & Sarajärvi, A. (2009). *Laadullinen tutkimus ja sisällönanalyysi*. Tammi. Hansaprint Oy, Vantaa.

Van Osdol, Paul. (2021, 10. huhtikuuta). *FBI investigating hacking threats at Pennsylvania water systems.* 4ABC WTAE. https://www.wtae.com/article/fbi-investigating-hacking-threats-at-pennsylvania-water-systems/36386504#

Veolia. (2024, 19. tammikuuta). Veolia Responds to Cyber Incident. Veolia. https://mywater.veolia.us/veolia-responds-cyber-incident

Viljanen, V. (2021). *Kyberfyysisten järjestelmien mallintaminen* [opinnäytetyö, Metropolia Ammattikorkeakoulu]. Theseus-julkaisuarkisto. https://urn.fi/URN:NBN:fi:amk-202105199558

Walls, A., McMullen, L., Heiser, J. & Gopal, D. (2023). Risk Management Produces Bad Cybersecurity. Maverick research. Gartner.

Water Information Sharing and Analysis Center (WaterISAC). (2022, 1. joulukuuta). *Investigation Update to UK's South Staffs Water Cyber Incident*. https://www.waterisac.org/portal/UK-south-staffs-water-ransomware

Water Information Sharing and Analysis Center (WaterISAC). (2023, 30. marraskuuta). *Water Utility Control System Cyber Incident Advisory: ICS/SCADA Incident at Municipal Water Authority of Aliquippa*. https://www.waterisac.org/portal/tlpclear-water-utility-control-system-cyber-incident-advisory-icsscada-incident-municipal

Wall, T. (2022, 26. toukokuuta). *Throwback Attack: Hackers attempt to flood Israeli water supply with chlorine*. Industrial cybersecurity pulse. https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-hackers-attempt-to-flood-israeli-water-supply-with-chlorine/

Wood, C. (2021, 18. elokuuta). *Ransomware hit two Maine water facilities earlier this year.* Statescoop. https://statescoop.com/ransomware-maine-water-facilities/

Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2022). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling, 21*(1), 157-177. https://doi.org/10.1007/s10270-021-00898-7

Yeboah-Ofori, A., & Islam, S. (2019). Cyber security threat modeling for supply chain organizational environments. *Future internet, 11*(3), 63. https://doi.org/10.3390/fi11030063