Eemil Määttä

TEKOÄLY KYBERPUOLUSTUKSESSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Määttä, Eemil
Tekoäly kyberpuolustuksessa
Jyväskylä: Jyväskylän yliopisto, 2023, 36 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja(t): Riekkinen, Janne

Tekoäly on kehittynyt todella monella alalla, ja sen luomat mahdollisuudet kyberpuolustuksessa ovat jatkuvassa kasvussa. Tässä tutkielmassa käsiteltiin tekoälyä ja sen hyödyntämistä kyberpuolustuksen näkökulmasta. Tutkielmassa perehdyttiin mahdollisuuksiin, joita tekoäly tarjoaa kyberpuolustukseen. Tutkielma toteutettiin kirjallisuuskatsauksena. Kirjallisuuskatsauksen tiedonkeruussa hyödynnettiin erilaisia tietokantoja, joista löydettiin tutkimusartikkeleita ja muuta tutkimuskirjallisuutta. Tutkielma pyrki vastaamaan tutkimuksen kahteen pääkysymykseen: ”Mikä on tekoälyn rooli kyberpuolustuksessa?” ja ”Miten tekoälyä voidaan hyödyntää tulevaisuuden kyberpuolustuksessa?” Tutkielmassa esitettiin ensin tekoälyn ja kyberpuolustuksen määritelmät, joiden jälkeen pureuduttiin niiden yhteensovittamiseen. Kirjallisuuskatsauksen johtopäätöksenä voidaan todeta, että tekoälyn hyödyntäminen kyberpuolustuksessa on erittäin merkityksellistä ja sen potentiaali puolustuksen vahvistajana on huomattava. Tutkielman perusteella tekoälyä hyödynnetään puolustuksessa jo jossain määrin, mutta tulevaisuudessa sen merkitys kasvaa entisestään hyökkäysten kehittyessä tekoälyn myötä yhä edistyksellisemmiksi. Tutkielmassa esitettiin sekä tekoälyn rooli nykyajan kyberpuolustuksessa että tekoälyn mahdollisuuksia tulevaisuuden kyberpuolustuksessa.

Asiasanat: tekoäly, kyberpuolustus, puolustus, kyberuhka, kyberpuolustusmenetelmä

ABSTRACT

Määttä, Eemil
Artificial intelligence in cyber defense
Jyväskylä: University of Jyväskylä, 2023, 36 pp.
Information Systems Science, Bachelor's thesis
Supervisor(s): Riekkinen, Janne

Artificial intelligence has advanced in numerous fields, and the opportunities it creates in cyber defense are continuously increasing. This Bachelor's thesis discussed artificial intelligence and its utilization from the perspective of cyber defense. The thesis examined the possibilities that artificial intelligence offers for cyber defense. The study was conducted as a literature review, utilizing various databases to find research articles and other relevant literature. The thesis aimed to answer two main research questions: "What is the role of artificial intelligence in cyber defense?" and "How can artificial intelligence be utilized in future cyber defense?" First, definitions of AI and cyber defense were presented, followed by a discussion of their compatibility. As a conclusion of the literature review, it can be stated that the utilization of artificial intelligence in cyber defense is highly significant and its potential as a defense enhancer is considerable. Based on the thesis, artificial intelligence is already being used to some extent in defense, but its importance will grow even further in the future as attacks become increasingly advanced with the help of artificial intelligence. The thesis presented both the role of artificial intelligence in current cyber defense and its possibilities in future cyber defense.

Keywords: artificial intelligence, cyber defense, defense, cyber threat, cyber defense methods

KUVIOT

SISÄLLYS

1 JOHDANTO

Tässä kandidaatin tutkielmassa tutkitaan, kuinka tekoälyä voidaan käyttää kyberpuolustuksen tukena ja apuna. Tutkimuksen tavoitteena on selvittää, miten tekoälyä voidaan hyödyntää kyberpuolustuksessa ja kuinka se voi parantaa puolustusta. Tutkielmassa keskitytään erityisesti siihen, millaisia mahdollisuuksia tekoäly pystyy tällä hetkellä tarjoamaan kyberpuolustukseen, mutta sivutaan myös mahdollisia tulevaisuuden kehityssuuntia ja käyttökohteita.

Kyberhyökkäykset ovat lisääntyneet ja edistyneet huomattavasti viime vuosikymmenten aikana, ja ne ovat yhä monimutkaisempia ja haastavampia torjua. Tekoäly tarjoaa uusia mahdollisuuksia kyberpuolustuksen kehittämiseen, sillä sen avulla pystytään havaitsemaan ja torjumaan kyberhyökkäyksiä huomattavasti entistä nopeammin ja tarkemmin.

Tekoälyn käsite itsessään on haastava määriteltävä, minkä vuoksi sille ei ole vieläkään yleisesti vakiintunutta määritelmää. Suuri syy määrittämisen vaativuudelle lienee tekoälyn monitahoisuus ja monitieteisyys. Tekoäly käsittää niin monta eri asiaa mukaan lukien koneoppimisen, neuroverkot, luonnollisen kielen käsittelyn, robotiikan ja automaation, tietokoneet sekä ohjelmistot, joilla on tiettyjä älykkyyden piirteitä. Lisäksi tekoälyn monitulkintaisuus ja ihmisten erilaiset odotukset tekoälyn potentiaalista ja siitä, miten sen tulisi toimia vaikuttavat käsitteen määrittämisen haastavuuteen. Myös tekoälyn jatkuva edistyksellisyys ja kehitys tuovat uusia tekniikoita ja sovelluksia, joiden vuoksi määritelmä voi laajentua ja muuttua ajan kuluessa. Edellä mainittujen syiden vuoksi tekoälystä on esitetty useita erilaisia määritelmiä ja yleisesti hyväksyttävää määritelmää on vaikea muodostaa. Tässä tutkielmassa sivutaan joitain esitettyjä tekoälyn määritelmiä.

Kyberpuolustus on kehittynyt rinta rinnan yhdessä tietokoneiden kanssa. Tietokoneiden alkuajoista lähtien ihmisten riesana ovat olleet tietoturvaongelmat, joiden vuoksi syntyi tarve kehittää menetelmiä tietojen suojaamiseksi ja turvallisuuden ylläpitämiseksi. Modernista kyberpuolustuksesta puhuttaessa voidaan sanoa kyberpuolustuksen historian ulottuvan ainoastaan joidenkin vuosikymmenten päähän. Internetin yleistyminen ja levittäytyminen ovat lisänneet

kyberpuolustuksen merkitystä ja tärkeyttä huomattavasti, sillä jokainen internetissä toimiva tietokone voi altistua hyökkäykselle.

Tekoäly ei ole uusi keksintö, vaan tekoälytutkimus alkaa jo 1950-luvulta. Myös kyberpuolustuksen tutkimuksen alkuaika sijoittuu suunnilleen samaan aikaan. Sen sijaan tekoälyä kyberpuolustuksessa – etenkään tulevaisuuden kyberpuolustuksessa – ei ole tutkittu kovin paljon, minkä vuoksi aihe kaipaa lisätutkimusta. Aihepiiriä on syytä tutkia enemmän, sillä tekoälyn avulla kyberpuolustusta saadaan kehitettyä valtavasti eteenpäin. Tutkimuksen tarvetta lisää myös se, että myös kyberhyökkäyksissä hyödynnetään tekoälyä – ja hyökkäykset ovat jopa puolustusta edistyksellisempiä. Tekoälyllä on kyberpuolustuksessa niin valtava potentiaali, että sen avulla voitaneen saavuttaa kyberhyökkäysten edistyksellisyys.

Tutkielman tavoitteena on selvittää, miten tekoälyä käytetään kyberpuolustuksessa ja toisaalta, miten sitä voidaan hyödyntää tulevaisuudessa puolustuksen tukena. Tutkielman keskeiset tutkimuskysymykset ovat:

- Mikä on tekoälyn rooli kyberpuolustuksessa?
- Miten tekoälyä voidaan hyödyntää tulevaisuuden kyberpuolustuksessa?

Tutkielma on toteutettu kirjallisuuskatsauksena. Tutkimuskirjallisuuden etsinnässä on hyödynnetty useita tietokantoja kuten JYKDOK, Google Scholar, ACM Digital Library, Web of Science ja IEEE-kirjasto. Lähdekirjallisuuden hakusanoina ja -lauseina on käytetty seuraavia hakusanoja ja niiden yhdistelmiä: *artificial intelligence, intelligence, AI, tekoäly, machine learning, deep learning, natural language processing, neural networks, cyber defence, cyber defense, cyber*, kyber* ja kyberpuolustus.*

Tutkielman merkittävimmät rajoitteet liittyvät saatavilla olevaan avoimeen tutkimuskirjallisuuteen. Etenkin kyberpuolustus aiheena on erittäin sensitiivinen ja siksi tietojen saatavuus on hyvin rajoitettua. Suuri osa aiemmasta aiheen tutkimuksesta ja kirjallisuudesta ei ole avoimesti saatavilla, mikä vaikeuttaa aiheen tutkimista ja sen myötä myös tämän tutkielman tekemistä. Tutkielmaan käytettävää aiempaa tutkimusmateriaalia joudutaan rajaamaan käyttöoikeuksien vuoksi. Tämä ei kuitenkaan vaikuta merkittävästi tutkielman validiteettiin tai merkityksellisyyteen, vaan rajoitukset vaikeuttavat ja rajoittavat tutkimuksen mahdollisuuksia syventyä aiheeseen ja käsitellä sitä laajemmin.

Tutkielma koostuu viidestä pääluvusta: johdanto, kolme sisältölukua ja yhteenveto. Johdannossa esitellään tutkimuksen tausta, ongelmat, tarkoitus, tarve, tavoitteet, tutkimusmenetelmät sekä saavutetut tulokset merkityksineen. Ensimmäisessä sisältöluvussa määritellään tekoäly, käydään läpi sen historiaa ja erilaisia teknologioita. Toinen sisältöluku käsittelee kyberpuolustusta – sen määritelmää, kyberuhkien tunnistamista ja puolustamista sekä kyberpuolustusmenetelmiä. Viimeisessä sisältöluvussa käsitellään tekoälyä kyberpuolustuksessa ja se vastaa myös tutkimuskysymyksiin. Yhteenvedossa tiivistetään tutkielma. Se sisältää tutkielman tärkeimmät tutkimustulokset, keskeiset johtopäätökset sekä tutkielman tavoitteiden ja tutkimuskysymysten pääpiirteet. Yhteenvedossa

esitetään tutkimustulokset vastaamalla tutkimuskysymyksiin. Lopuksi esitetään potentiaalisia jatkotutkimusaiheita. Tutkielman päättää lähdeluettelo, johon on listattu kaikki kirjallisuuskatsauksessa käytetyt lähteet.

Saavutetuista tuloksista voidaan päätellä, että hyödynnettäessä tekoälyä kyberpuolustuksen tukena voidaan tulevaisuudessa kehittää mitä kehittyneempiä autonomisia ja ennakoivia puolustusmenetelmiä. Tekoälyn käyttö puolustuksessa tarjoaa valtavasti potentiaalia etenkin aktiiviseen ja ennakoivaan puolustukseen perinteisten reaktiivisten puolustusmenetelmien rinnalle. Tutkimuksessa saavutettujen tulosten merkitystä ei voi väheksyä, sillä tekoälyn tutkiminen kyberpuolustuksen kontekstissa on vielä melko lapsenkengissä, joten se vaatii runsaasti lisää tutkimusta. Tutkielman tuloksista hyötyvät niin tekoälyn kuin kyberpuolustuksenkin tutkijat. Tulokset voivat toimia pohjana aiheen jatkotutkimuksille. Tässä tutkielmassa esitetään tekoälylle kyberpuolustuksessa myös joitain tulevaisuuden potentiaalisia käyttökohteita, jotka vaativat lisätutkimusta. Lisätutkimuksen myötä ne saattavat olla valtava harppaus tulevaisuuden kyberpuolustukselle.

2 TEKOÄLY

Tässä luvussa määritellään tekoäly käsitteenä, käydään läpi sen historiaa, käyttötapoja ja sovelluksia. Ensimmäisessä alaluvussa määritellään tekoälyn käsite, toisessa alaluvussa keskitytään tekoälyn historiaan ja kolmannessa alaluvussa pureudutaan tekoälyn käyttötapoihin ja sovelluksiin.

Tekoäly on tärkeä osa informaatioteknologiaa ja nykypäivänä se esiintyy hyvin monella eri alalla. Yksi esimerkki tästä on kyberpuolustus, johon tutkielmassa keskitytään. Tekoäly on ollut viime vuosina entistä enemmän pinnalla, ja sen kehitys on jatkuvaa. Tekoäly luo uusia menetelmiä, joissa yhdistyvät uudet ja perinteiset teknologiat (Li ym., 2018). Täten sen hyödyntäminen kyberpuolustuksessa saattaa mahdollistaa uusia, tehokkaampia keinoja ja ratkaisuja suojella kyberhyökkäyksiltä.

Tekoäly ei ole kuitenkaan ainoastaan hyvä asia ja pelastus yhteiskunnalle; Elon Musk sanoo tekoälyn olevan jopa ydinaseita vaarallisempi ja Stephen Hawkingin varoituksen mukaan tekoäly voi olla kaikista pahin ja vaarallisin ilmiö ihmiskunnalle koko historian saatossa (Koetsier 2017; Clifford 2018). Jääskeläinen (2019) lisää tähän maailmanlopun ja ihmiskunnan alistamisesta puhuneiden listaan myös Bill Gatesin. Koetsier (2017) kirjoittaa artikkelissaan Hawkingin sanoneen, että tekoäly voi kehittää oman tahtonsa. Hawking lisää, että tekoäly saattaa ohittaa ihmisen älykkyydessä nopeammin kuin uskomme (Koetsier, 2017).

Hopgoodin (2021) mukaan lopullinen saavutus tekoälyn alalla olisi rakentaa ihmisen henkiset kyvyt ylittävä kone. Henkisiä kykyjä ovat muun muassa päättely, mielikuvitus, luovuus, tunteet, tunnistaminen ja ymmärrys. (Hopgood, 2021.) Toistaiseksi edellä mainittua tavoitetta ei ole saavutettu.

2.1 Tekoälyn määritelmä

Tekoälyn määritelmästä ei olla päästy sopuun vielä tänäkään päivänä runsaasta tutkimuksesta huolimatta, vaan sille on edelleen useita erilaisia määritelmiä.

Kaplanin (2016) mukaan kullakin määritelmällä on omat näkökulmansa ja useimmat määritelmistä viittaavat tietokoneohjelmiin tai koneisiin, jotka kykenevät käyttäytymään älykkäästi ihmisten tavoin. Tämän kanssa linjassa on myös kyberturvallisuuskeskuksen määritelmä, jonka mukaan tekoäly on ihmisen tai muun eläimen älykkäältä käytökseltä näyttävää koneen toimintaa (Vähä-Sipilä ym., 2021). Merilehto (2018) määrittelee tekoälyn olevan sellaista koneen suorittamaa toimintaa, joka olisi älykästä, mikäli tekijänä olisi ihminen. Myös Boden (2016) summaa, että tekoälyn avulla pyritään saamaan koneet tekemään sellaisia asioita, joita myös mieli kykenee tekemään. Jääskeläinen (2019) lisää aiempiin tietokoneiden kyvyn mukauttaa toimintaansa syötetyn datan perusteella. Edellä esitetyt määritelmät tekoälylle ovat yhtä mieltä siitä, että tekoäly on ihmisen, sen mielen tai muun eläimen käytöstä jäljittelevää.

Tekoälyn määrittelemisen haastavuutta lisää sen nopean kehityksen lisäksi se, että älykkyyttä itsessään on vaikea määritellä. Jotta voimme määritellä tekoälyn, tulee meidän ensin määritellä mitä älykkyys tarkoittaa. Älykkyys on moninainen käsite, ja sitä on määritelty useista eri näkökulmista. AllWords Dictionaryn (2006) mukaan älykkyys on ”kykyä käyttää muistia, tietoa, kokemusta, ymmärrystä, päättelyä, mielikuvitusta ja arvostelukykyä ongelmien ratkaisemiseksi ja sopeutumiseksi.” Älykkyys on kuitenkin laaja ja monipuolinen käsite, ja sille on olemassa yhtä monia määritelmiä kuin on määritelmän esittäjiäkin. Legg ja Hutter (2007) kokosivat yhteen useiden eri alojen asiantuntijoiden älykkyyden määritelmiä. Niiden keskeisistä piirteistä älykkyyden voidaan tiivistää tarkoittavan kykyä oppia, käsitellä uutta ympäristöä ja ennakoimattomia tilanteita sekä niihin sopeutumista. Myös Fletcher ja Hattie (2011) ovat samoilla linjoilla älykkyyden määritelmässä. Heidän mukaansa älykkyyteen kuuluu kyky ajatella, oppia kokemuksista, ympäristöstä ja uusista tilanteista sekä sopeutua niihin. Edellä mainittujen määritelmien pohjalta tämä tutkielma määrittelee älykkyyden olevan kyky oppia, ajatella ja sopeutua.

Tekoäly on yleisesti jaettu kahteen eri alaluokkaan: heikkoon eli kapeaan tekoälyyn ja vahvaan eli yleiseen tekoälyyn. Kapean tekoälyn kone kykenee toimimaan järkevästi tai älykkäästi, kun taas vahvan tekoälyn kone ajattelee ihmisen kaltaisesti ja sillä on jonkinlaista tietoisuutta (Ailisto ym., 2018). Seuraavissa kappaleissa tarkastellaan näitä hieman tarkemmin.

Merilehdon (2018) mukaan heikko eli kapea tekoäly tarkoittaa sitä, että se on kyvykäs ratkaisemaan vain yhden tietyn, sille opetetun tehtävän, eikä kykene mukautumaan uuteen tilanteeseen. Hän esittää syöpäkasvaimen tunnistamisen kuvasta konenäön avulla olevan käytännön esimerkki heikosta tekoälystä. Lisäksi hän toteaa sen sisältävän kaiken nykypäivän tekoälyn. (Merilehto, 2018.) Myös Siau ja Yang (2017) määrittelevät heikon tekoälyn keskittyvän tiettyihin kapeisiin tehtäviin. Näiden määritelmien pohjalta voidaan sanoa, että heikko tekoäly kykenee suorittamaan tietyn, sille asetetun spesifin tehtävän, mutta se ei osaa sopeutua uuteen tilanteeseen soveltamalla aiemmin oppimaansa.

Vahva eli yleinen tekoäly kykenee ratkomaan hyvin laajalla skaalalla erilaisia ongelmia – se osaa esimerkiksi kokata ja ajaa autoa (Merilehto, 2018). Siau ja Yang (2017) määrittelevät vahvan tekoälyn koneeksi, jonka älykkyys kattaa

useamman kuin yhden alueen. Heidän mukaansa vahvalla tekoälyllä on aistimuksia, tietoisuutta ja mieli. Merilehdon (2018) mukaan tätä ei ole vielä pystytty kehittämään. Vahva tekoäly pystyisi ratkaisemaan laajalti erilaisia ongelmia ja mukautumaan tilanteeseen. Se sijoittuu ominaisuuksiltaan huomattavasti lähemmäs ihmistä tai muuta eläintä sen aistimusten, mielen ja tietoisuuden vuoksi. Edelleen on epäselvää, pystytäänkö vahvaa tekoälyä koskaan kehittämään.

Merilehto (2018) toteaa, että ennen kuin koneet kykenisivät ihmisten kaltaiseen älykkyyteen tekoälyn avulla, tulee ratkaista ainakin itsenäinen oppiminen ja siirto-oppiminen. Itsenäinen oppiminen tarkoittaa sitä, että kone kykenee itsenäiseen oppimiseen ilman ihmistä. Siirto-oppimisen myötä tekoäly kykenisi oppimaan aiemmin opitusta tehtävästä tai tilanteesta ja hyödyntämään sitä toimiessaan uudessa ympäristössä. (Merilehto, 2018.)

Merilehdon (2018) mukaan itseajava auto lukeutuu vahvaan tekoälyyn, kun taas Siau ja Yang (2017) puolestaan luokittelevat sen heikkoon tekoälyyn, joten määritelmät ovat tältä osin ristiriidassa keskenään. Todennäköisesti eroavaisuus syntyy itseajavan auton määritelmästä, sillä heikkoon tekoälyyn lukeutuvia autopilotteja on jo keksitty, mutta vahvaan tekoälyyn lukeutuvaa täysin itseohjautuvaa autoa ei ole vielä pystytty kehittämään.

Anyoha (2017) kertoo artikkelissaan, että tekoälyn matemaattisia mahdollisuuksia tutkiva Alan Turing esitti loogisen kehyksen, jonka mukaan koneet voisivat käyttää tietoa ja järkeä ongelmanratkaisussa ihmisten tavoin. Alan Turing käsitteli älykkäiden koneiden rakentamista ja niiden älykkyyden testaamista. Tietokoneilta puuttui kuitenkin vielä ennen vuotta 1949 kyky tallentaa käskyjä, mitä pidetään keskeisenä edellytyksenä älykkyydelle. Tietokoneet tekivät mitä käskettiin, mutta ne eivät muistaneet tekemäänsä. (Anyoha, 2017.) Vuonna 1950 Turing esitteli idean, jonka mukaan älykkäitä koneita voidaan luoda ja niiden älykkyyttä voidaan testata. Testiä kutsutaan Turingin testiksi ja se on yhä tärkeä tekoälyn älykkyyden tunnistamisessa. (Haenlein & Kaplan, 2019.) Turingin testissä keskustellaan ihmisen ja tekoälyn kanssa luonnollisella kielellä ja mikäli ei kyetä luotettavasti erottamaan konetta ihmisestä, koneen katsotaan läpäisseen testin (Bogue, 2014). Koneen tavoitteena on siis saada testaaja uskomaan, että hän on tekemisessä ihmisen kanssa. Testin läpäisseen koneen katsotaan olevan älykäs.

Haenlein ja Kaplan (2019) toteavat tekoälyn olevan järjestelmän kykyä tulkita tietoa, oppia siitä ja käyttää oppimaansa sopeutumalla tiettyihin tehtäviin ja tavoitteisiin. Jääskeläisen (2019) määritelmä on siltä osin samaa mieltä, että hänen mukaansa tekoäly kykenee itsenäisesti muuttamaan omaa toimintaansa saamansa datan perusteella. Molemmat määritelmät sisältävät tekoälyn kyvyn sopeutua ja muuttaa omaa toimintaansa vastaanottamansa tiedon tai datan perusteella. Myös Ailisto ym. (2018) ovat sitä mieltä, että tekoälyn avulla koneet, laitteet, järjestelmät ja palvelut sopeutuvat tehtävän ja tilanteen mukaan. Yllä esitetyissä määritelmissä ei oteta huomioon lainkaan sitä, että tekoälyn tulisi olla, toimia tai ajatella kuten ihminen, mikä esiintyy useissa tekoälyn määritelmissä. Tästä esimerkkinä Hopgoodin (2021) määritelmä tekoälylle: ”Tekoäly on tiede, jossa jäljitellään tai ylitetään ihmisen henkisiä kykyjä tietokoneessa.”

Hänninen (2022) esittää, että tekoälyltä vaaditaan autonomisuutta ja adaptiivisuutta. Tekoälyn autonomisuus tarkoittaa sitä, että sen täytyy kyetä suorittamaan itsenäisesti sille annettuja monimutkaisia tehtäviä. Adaptiivisuuden mukaan tekoälyn tulee kyetä oppimaan ja kehittymään kokemustensa perusteella.

Yhteenvetona voidaan todeta, että tekoälylle ei ole sen laajasta tutkimuksesta huolimatta vakiinnutettu yhtenäistä määritelmää, vaan sille on ehdotettu useita erilaisia määritelmiä. Useiden määritelmien pohjalta voidaan summata tekoälyn olevan sellaista älykästä toimintaa, jolla on kyky oppia ja jäljitellä vähintäänkin jollain tasolla elävän olennon kykyä suoriutua tehtävistä.

2.2 Tekoälyn historia

Modernin tekoälyn historian katsotaan alkaneen 1900-luvun alusta, jolloin kehitettiin ensimmäisiä laskemiseen käytettäviä sähköisiä laskukoneita (Russell ym., 2010). Tekoälyn historian alkuajan voidaan katsoa sijoittuvan myös myöhemmäksi, sillä Haenleinin ja Kaplanin (2019) mukaan tekoälyn alkuaikaa ei voida tarkkaan määritellä. Heidän mukaansa tekoälyn juuret juontuvat todennäköisesti yhdysvaltalaisen tieteiskirjailija Isaac Asimovin vuonna 1942 julkaistusta teoksesta *Runaround*, joka innoitti robotiikan, tekoälyn ja tietojenkäsittelytieteen tutkijoita.

1950-luvulla tekoäly sai suurta huomiota vuonna 1956 pidetyssä Dartmouth Collegen konferenssissa, jossa julkisesti esiteltiin ensimmäisen kerran käsite tekoäly (Koski, 2018). Konferenssissa käsitettä käytti John McCarthy, jota pidetään tekoäly-termin isänä (Bogue, 2014). Konferenssia voidaan pitää merkittävänä tapahtumana tekoälyn historiassa, sillä sen jälkeinen aika oli tekoälyn kultaaikaa. Lähes kahden konferenssia seuraavan vuosikymmenen aikana tekoälyn alalla saavutettiin merkittävää menestystä (Haenlein & Kaplan, 2019). Myös Anyohan (2017) mukaan konferenssin merkitystä ei voi väheksyä, sillä sen ansiosta käynnistyi tekoälytutkimuksen seuraavat kaksi vuosikymmentä. Tämän vuoksi konferenssi mielletään yleisesti modernin tekoälyn synnyksi. Tekoäly pysyi melko tuntemattomana yli puolen vuosisadan ajan, mutta nykyään se on laskentatehon kehittymisen myötä noussut jälleen julkiseen keskusteluun (Haenlein & Kaplan, 2019).

Kaplan (2016) esittää, että todennäköisesti ensimmäinen tekoälyn virstanpylväs oli Deep Blue -ohjelma, joka päihitti hallitsevan maailmanmestarin shakissa vuonna 1997. Kuitenkin tekoälyn julkisista voitoista tunnetuin ja vaikuttavin lienee televisiotietokilpailun *Jeopardy* voitto. (Kaplan, 2016.)

Kosken (2018) mukaan 2000-luvulla tekoälyn kehitys- ja tutkimustyö muuttui merkittävästi, kun tutkimuksissa alettiin painottaa neuroverkkoihin perustuvaa syväoppimista. Syväoppimisen mahdollistivat tietokoneiden laskentatehon nousu sekä tarjolla olevan datan määrän kasvaminen. (Koski, 2018.) Myös Ventre (2020) linjaa, että 2010-luku on ollut maailmanlaajuisen kiinnostuksen ajanjakso tekoälyn saralla. Hänkin on samaa mieltä siitä, että ajanjakson mahdollistajina ovat muun muassa big data ja tietokoneiden tehojen kasvu.

Yhteenvetona voidaan todeta, että tekoälyn historia ei ole erityisen pitkä – mutta se on lyhyessäkin ajassa edistynyt huimaa vauhtia. Laskentatehon kasvun ja datan määrän kasvamisen myötä tekoäly edistynee ja kehittynee koko ajan kiihtyvään tahtiin. Tekoälyn lopullinen tulevaisuus on kuitenkin vielä epävarmaa.

2.3 Tekoälyn tekniikoita

Tekoäly koostuu useista erilaisista tekniikoista, jotka ovat yleisesti käytettyjä tekoälyn suunnittelussa, toteutuksessa ja käytössä. Tekoälyjärjestelmissä voidaan yhdistellä useita erilaisia tekniikoita saavuttaakseen parhaan mahdollisen suorituskyvyn. Tässä alaluvussa käsitellään joitain tekoälyn yleisimpiä tekniikoita.

Koneoppimisella (engl. *Machine Learning, ML*) tarkoitetaan tapoja, joiden avulla koneet tai järjestelmät voivat oppia ja tehdä päätöksiä niille syötetyn datan perusteella ilman, että niitä on ohjelmoitu tiettyyn tehtävään. Termin keksi tekoälytutkija Arthur Lee Samuel vuonna 1995 käyttäessään termiä tieteestä, jossa tietokoneet saadaan toimimaan halutulla tavalla ilman tarkkaa ohjelmointia (Syam & Sharma, 2018). Arkinen esimerkki koneoppimisen sovelluksista ovat suoratoistopalveluiden suositusalgoritmit. Akerkarin (2019) mukaan koneoppiminen on laskennallinen menetelmä, jonka avulla voidaan tehdä tarkkoja ennusteita ja parantaa suorituskykyä. Koneoppiminen jäljittelee ihmisille ominaista oppimisen prosessia käyttämällä samankaltaisia periaatteita oppimiseen. Tällaisia periaatteita ovat esimerkiksi kokemus ja havainnoista oppiminen. Merilehdon (2018) mukaan koneoppiminen kattaa suurimman osan tekoälyn sovelluksista.

Vahvistusoppiminen (*Reinforcement Learning, RL*) on koneoppimisen alalaji, jossa kone oppii tekemään päätöksiä havainnoimalla ympäristöä ja saamaansa palautetta. Koneelle annetaan palautetta eri tilanteissa sen toiminnan ja onnistumisen mukaan (Merilehto, 2018). Vahvistusoppimisen ansiosta kone kykenee oppimaan tehokkaita toimintatapoja, joiden avulla voidaan ylläpitää järjestelmän suorituskykyä kertomatta sille toimintatavoista (Applebaum ym., 2022). Sisällyttämällä vahvistusoppimismenetelmiä perinteisten menetelmien rinnalle voidaan ratkaista monimutkaisia tietoturvaongelmia omista kokemuksistaan oppimalla (Kaloudi & Li, 2020). Akerkarin (2019) mukaan vahvistusoppimisessa koneelle ei kerrota toimia, joita sen tulee tehdä, vaan sen on löydettävä sellainen tekeminen, joka tuottaa mahdollisimman suuren hyödyn.

Neuroverkot (*Artificial Neural Networks, ANN*) jäljittelevät ihmisten aivojen toimintaa. Neuroverkot ovat kokoelma havainnoimalla oppimaan kykeneviä yksiköitä (Merilehto, 2018). Syamin ja Sharman (2018) mukaan neuroverkkojen tapa ratkaista ongelmia eroaa perinteisistä tietokonealgoritmeista, sillä neuroverkkojen tapa ratkaista ongelmia ei riipu loogisista ja vaiheittaisista ohjeista – toisin kuin perinteisten tietokonealgoritmien. Neuroverkot ovat tehokkaimpia sellaisissa tilanteissa, joissa data on monimutkaista ja sotkuista. Neuroverkot käsittelevät tietoa ja ratkaisevat ongelmia ihmisten tavoin. (Syam & Sharma, 2018.)

Schmidhuber (2015) kertoo tutkimusartikkelissaan jokaisen neuronin tuottavan lukuarvon, joka auttaa verkon tiedonkäsittelyssä.

Syväoppiminen (*Deep Learning, DL)* on keino toteuttaa koneellista oppimista koneelle tai järjestelmälle. Syväoppiminen on koneoppimisen alalaji, jossa käytetään neuroverkkoja oppimiseen ja tietojen analysointiin. Tietokone voi ratkaista ja rakentaa monimutkaisia käsitteitä ja sovelluksia syväoppimisen avulla (Goodfellow ym., 2016; Li ym. (2018)). Li ym. (2018) kirjoittavat tutkimusartikkelissaan, että syväoppimisessa pyritään neuroverkkojen avulla löytämään mallit, säännöt ja piilotetut suhteet suurista tietomassoista. LeCun ym. (2015) uskovat syväoppimisen suureen menestykseen lähitulevaisuudessa, sillä se kykenee hyödyntämään saatavilla olevan datan määrän kasvua. Samoin Hänninen (2022) kertoo syväoppimisen herättävän eniten odotuksia kaikista koneoppimisen osa-alueista. Akerkar (2019) kertoo syväoppimisen koostuvan useista hierarkkisista arkkitehtuurikerroksista, minkä vuoksi se tarjoaa ihmisen kaltaista usean kerroksen käsittelyä. Koneoppimisen parhaat tulokset on saatu syväoppivia neuroverkkoja hyödyntämällä (Li ym., 2018; Schmidhuber, 2015). Hänninen (2022) ja LeCun ym. (2015) osoittavat, että syväoppimisella on edessään valoisa tulevaisuus. Heidän mukaansa syväoppiminen tullee menestymään jopa muita koneoppimismenetelmiä paremmin. Syväoppiminen on erityisesti käytössä monimutkaisten ja suurten tietojoukkojen käsittelyssä, sillä niissä sen on havaittu olevan erityisen tehokasta.

Luonnollisen kielen käsittelyllä (*Natural Language Processing, NLP*) tarkoitetaan ihmisen tuottaman – puhutun tai kirjoitetun – kielen ymmärtämistä ja käsittelyä. Eisenstein (2018) kertoo luonnollisen kielen käsittelyn keskittyvän laskennallisten algoritmien analysointiin. Luonnollisen kielen prosessointi pyrkii tarjoamaan tietokoneille kyvyn ymmärtää ja käsitellä ihmiskieltä. Tämä voi sisältää useita eri toimia, kuten kielten välisen kääntämisen, kysymyksiin vastaamisen, tiedon poimimisen teksteistä, keskustelun käymisen ja ohjeiden vastaanottamisen. Luonnollisen kielen prosessoinnin tavoitteena on kehittää laskennallisia menetelmiä ja tekniikoita, joiden avulla voidaan toteuttaa edellä mainittuja toimia.

Yhteenvetona voidaan todeta edellä esitettyjen tekoälytekniikoiden voivan tarjota useita mahdollisuuksia tietojen ennustamiseen ja analysoimiseen. Nämä tekniikat mahdollistavat koneiden ja järjestelmien oppimisen ja soveltamisen uusilla tavoilla, mikä tarjoaa runsaasti mahdollisuuksia kyberpuolustukseen. Tekoälytekniikoilla on merkittävä rooli monissa sovelluksissa, kuten kuvan- ja puheentunnistuksessa sekä automaattisessa päätöksenteossa. On tärkeää jatkaa tekoälytekniikoiden tutkimista ja kehittämistä voidaksemme hyödyntää niiden valtavaa potentiaalia entistä tehokkaammin tulevaisuuden kyberpuolustuksessa.

3 KYBERPUOLUSTUS

Kyberpuolustus on viime vuosikymmeninä noussut entistä enemmän ihmisten huulille. Teknologian ja digitalisaation kehittyessä kyberrikollisuus ja -hyökkäykset ovat kehittyneet ja lisääntyneet entisestään, minkä vuoksi myös kyberpuolustuksen on kehityttävä. Jokainen ihminen voi tehdä oman osansa estääkseen ja välttääkseen kyberhyökkäyksiä. Tässä tutkielmassa keskitytään kyberhyökkäyksiin pääasiassa kyberpuolustuksen näkökulmasta, mutta ymmärtääksemme kyberpuolustusta tulee myös ymmärtää mitä kyberhyökkäykset ovat.

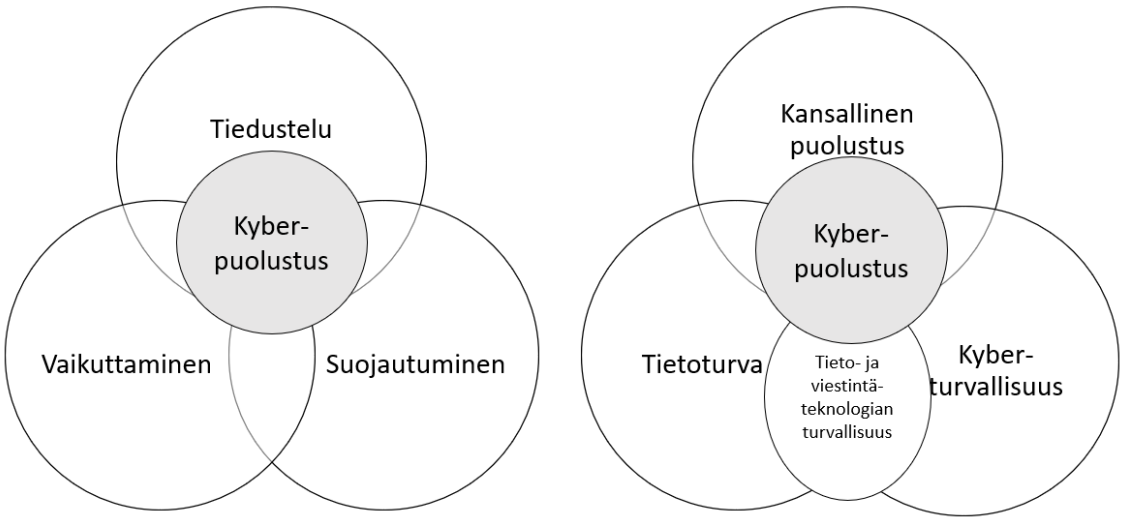
Kyberhyökkäykset ovat lisääntyneet, koska ne voidaan suorittaa anonyymisti ja suhteellisen edullisesti verrattuna muihin hyökkäysalueisiin (Seker & Ozbenli, 2018). Varsovassa vuonna 2016 pidetyssä huippukokouksessa todettiin, että verkkohyökkäykset ja -uhkat ovat yleistyneet ja kehittyneet ja niillä on entistä vahingollisempia seurauksia (NATO Summit Guide, 2016). Edellä mainittujen syiden takia on äärimmäisen tärkeää, että kyberpuolustus toimii moitteettomasti ja ettei se jää kehityksessä kyberhyökkäyksen jalkoihin – vaan päinvastoin ottaisi sen kehittyneisyydessä kiinni ja menisi ohi.

Tämän luvun alaluvuissa ensin määritellään kyberpuolustus, sitten tutustutaan kyberuhkien tunnistamiseen ja torjumiseen sekä lopuksi käydään läpi kyberpuolustusmenetelmiä.

3.1 Kyberpuolustuksen määritelmä

Kyberavaruus on tunnustettu yhdeksi taistelukentäksi muiden taistelukenttien joukkoon maan, meren, ilman ja avaruuden lisäksi, minkä vuoksi kyberpuolustuksella on suuri merkitys etenkin kansallisen turvallisuuden kannalta (Seker & Ozbenli, 2018). Laari ym. (2019) määrittelevät kyberpuolustuksen olevan maanpuolustuksellinen osa-alue, joka muodostuu tiedustelusta, vaikuttamisesta ja suojautumisesta. Kyberpuolustuksen tavoitteena on suojata kriittinen tieto, tietojärjestelmät sekä tietoliikennejärjestelyt. Myös Galinec ym. (2017) ovat samoilla linjoilla, sillä heidän mukaansa kyberpuolustus on välttämätöntä omaisuuden

turvaamiseksi ja tietojen suojaamiseksi. Kyberpuolustus ei tarkoita vain sitä, mitä tapahtuu kyberhyökkäyksen aikana, vaan kyberpuolustusta tapahtuu jatkuvasti. Kyberpuolustus analysoi ympäristöä ja mahdollisia uhkia. Tiedustelulla kerätään tietoa tietojärjestelmistä ja laitteista ja suojautumisella ennaltaehkäistään, estetään ja torjutaan toisen valtion suorittamaa vaikuttamista tai tiedustelua (Candolin, 2022). Lee ja Kim (2021) huomauttavat, että kyberpuolustus ei rajoitu ainoastaan sotilaalliseen kontekstiin, vaan se liittyy myös kansalliseen turvallisuuteen. He määrittelevät kyberpuolustuksen muodostuvan kansallisesta puolustuksesta, kyberturvallisuudesta, tietoturvasta sekä tieto- ja viestintäteknologian turvallisuudesta. Tätä määritelmää on havainnollistettu kuvion 1 oikeanpuoleisessa Venn-diagrammissa. Kuvio 1 kokonaisuudessaan kuvaa kyberpuolustuksen määritelmän aiemmin esitetyn perusteella.

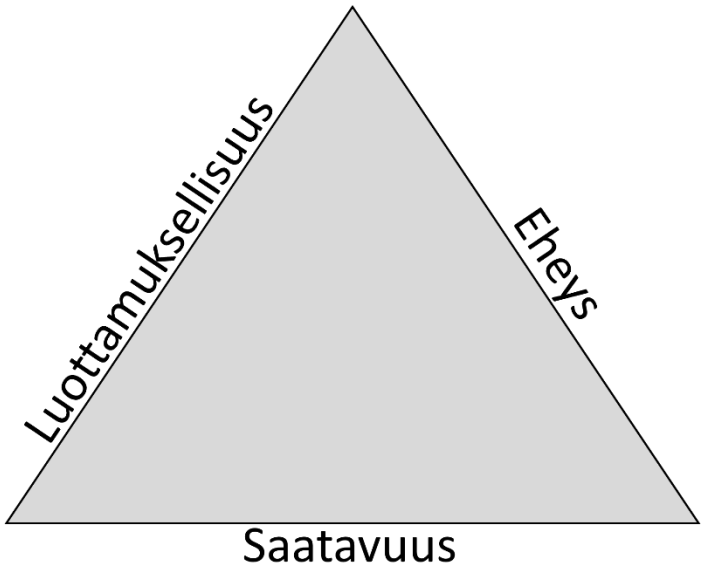


KUVIO 1: Kyberpuolustuksen määritelmä (osittain mukaillen Lee & Kim, 2021).

Lu ym. (2013) esittävät epäsymmetrian kasvavan kyberhyökkäyksen ja -puolustuksen välillä kyberhyökkäysten kehittyessä ja niiden tehon lisääntyessä. Kyberpuolustus ei pysy hyökkäyksen kehityksen mukana, sillä puolustus on usein reaktiivista, eli puolustustoimiin ryhdytään vasta hyökkäyksen havaittua. (Lu ym., 2013.)

Tähän tarkoitukseen on kehitetty aktiivinen kyberpuolustus. Broeders (2021) määrittelee aktiivisen kyberpuolustuksen ”ennakoivien kyberturvallisuustoimenpiteiden kirjoksi, joka sijoittuu perinteisen passiivisen puolustuksen ja hyökkäyksen väliin”. Hammondin ja Gummerin (2016) mukaan aktiivisessa kyberpuolustuksessa järjestelmää tai verkkoa vahvistetaan kestämään hyökkäyksiä paremmin. Aktiivisen kyberpuolustuksen avulla pyritään lisäämään ennakoivaa puolustusta ja uhkien torjumista. Aktiivinen kyberpuolustus poikkeaa perinteisistä puolustusmenetelmistä – kuten palomuurista tai haittaohjelmien torjuntatyökaluista – siten, että se perustuu ”hyvälaatuisten matojen” levittämiseen, millä pyritään torjumaan kyberhyökkäyksen haittaohjelmia (Lu ym., 2013).

Kokonaisvaltainen puolustusratkaisu edellyttää optimaalista reaktiivisen, aktiivisen ja ennakoivan kyberpuolustuksen yhdistelmää (Lu ym., 2013). Tällä tavoin kyberhyökkäysten havainnointi, niihin valmistautuminen ja vastaaminen onnistuisivat huomattavasti paremmin, mikä saattaisi tuoda merkittävää etua kyberpuolustukselle nykyiseen nähden. Kyberpuolustukseen liittyy laajasti suojelevia ja nopeaa reagointia lisääviä erilaisia toimintoja, jotka voivat vähentää ympäristön houkuttelevuutta hyökkäyksen kohteeksi joutumiseksi, tunnistaa kriittisiä paikkoja ja tietoja, havaita hyökkäyksiä sekä lisätä reagointi- ja vastauskykyä hyökkäyksiä vastaan (Galinec ym., 2017).



KUVIO 2: CIA-kolmio

Kuten tietoturva ja tietojärjestelmien suojaaminen, myös kyberpuolustus perustuu kuviossa 2 esitettyyn CIA-kolmioon (*CIA triad*) ja sen periaatteiden säilyttämiseen. CIA-kolmion nimi tulee sanoista luottamuksellisuus (*confidentiality*), eheys (*integrity*) ja saatavuus (*availability*). Se auttaa tunnistamaan vaatimukset ja varmistamaan tietojärjestelmän suojaamisen kaikilta kolmelta osin.

3.2 Kyberuhkien tunnistaminen ja puolustaminen

Digitalisaation kasvu ja tekoälyn kehittyminen tuovat myös tietoturvallisia haasteita. Kyberhyökkäykset ja -uhkat muuttuvat monimutkaisemmiksi ja yleisemmiksi, ja ne voivat aiheuttaa merkittäviä vahinkoja yhteiskunnasta yksilöön. Tämän vuoksi kyberuhkien tunnistaminen ja puolustaminen ovat nousseet tärkeäksi osaksi tietoturvallista kokonaisuutta ja kyberpuolustusta. Tunnistamalla ja puolustamalla kyberuhkia voidaan ehkäistä hyökkäyksiä ja niiden aiheuttamaa vahinkoa sekä suojata tietoja ja järjestelmiä. Tässä kappaleessa käsitellään

kyberuhkia sekä niiden tunnistamista ja puolustamista. Tässä kappaleessa tarkastella myös erilaisia työkaluja, joita voidaan käyttää tavoitteiden saavuttamiseksi. Kyberuhkia voidaan tunnistaa ja puolustaa usein eri tavoin. Tunnistus voi tapahtua esimerkiksi haittaohjelmien havaitsemisen, verkkoliikenteen valvonnan ja haavoittuvuuksien skannauksen avulla. Puolustus voi tapahtua esimerkiksi tietoturvaohjelmistojen avulla, pitämällä järjestelmät ja sovellukset ajantasaisina sekä salaamalla verkkoliikenne.

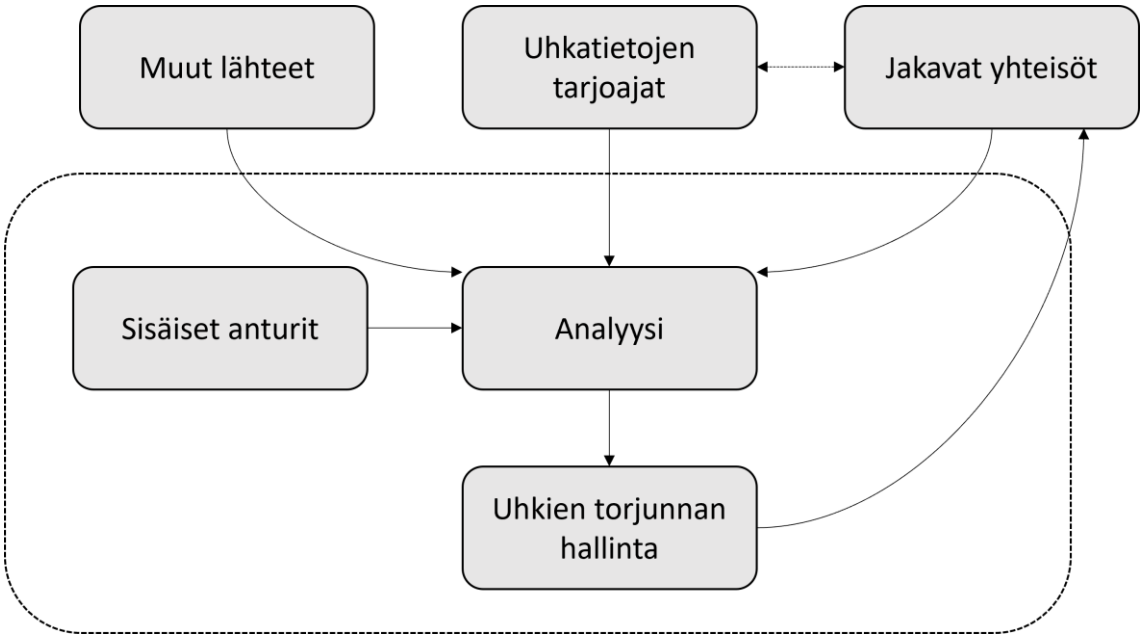
Turvallisuuskomitea (2018) määrittelee kyberuhan olevan kybertoimintaympäristöön kohdistuva haitallinen tapahtuma tai kehityskulku, joka mahdollisesti toteutuu ja joka toteutuessaan vaarantaa ympäristöstä riippuvaisen toiminnon. Kyberuhka voi aiheutua joko toteutuneesta tietoturvauhasta tai sellaisista teoista, jotka vaarantavat yhteiskunnallista turvallisuutta. (Turvallisuuskomitea, 2018.) Uhka on kybermaailman haitallinen tapahtuma, jolla on mahdollisuus tapahtua. Singer ja Friedman (2014) korostavat, että on tärkeää erottaa uhka ja haavoittuvuus toisistaan: Lukitsematon ovi on haavoittuvuus, mutta se muuttuu uhaksi vasta, kun joku haluaa mennä ovesta sisään. Kyberuhkat voidaan jakaa toimijan motiiveihin perustuvaan kuusiportaiseen malliin (Lehto, 2021). Kyberuhkien kuusiportainen rakennemalli on esitetty kuviossa 3. Sen portaat ylhäältä alas ovat kybersodankäynti, -sabotaasi, -terrorismi, -tiedustelu, -rikollisuus ja -vandalismi.

KUVIO 3: Kyberuhkien rakennemalli (Lehto, 2021).

Kohteena kyberuhkille voivat olla kriittinen infrastruktuuri, yhteiskunnan elintärkeät toiminnot tai yksittäinen kansalainen (Turvallisuuskomitea, 2018). Myös Lehdon (2021) mukaan tärkein kohde on kriittinen infrastruktuuri, eli

yhteiskunnan jatkuvalle toiminnalle välttämättömät toiminnot ja rakenteet. Kyberuhkien tunnistus ja jäljitys on todella haastavaa, sillä ne saattavat tulla valtion sisä- tai ulkopuolelta. Kyberuhkille – kuten muillekin uhkille – asetetaan numeerinen arvo sen todennäköisyyden mukaan. (Lehto, 2021.)

Tärkeimpiä kyberuhkien tunnistamiseen ja puolustukseen liittyvistä toimia ovat kybertiedustelu ja uhkatiedustelu. Kybertiedustelu tarkoittaa tiedonhankintaa, jolla kartoitetaan ja lisätään ymmärrystä riskeistä, uhkista ja muutoksista sekä mahdollistetaan näihin varautuminen (Lehto, 2021). Uhkatiedustelulta puuttuu edelleen laajasti hyväksytty määritelmä, mutta Amthor ym. (2019) määrittelevät sen olevan näyttöön perustuvaa tietoa, informaatiota tai dataa uhkista, joita voidaan käyttää uhkien lieventämiseen tai estämiseen. Koska hyökkäykset kehittyvät ja nopeutuvat jatkuvasti, myös puolustus muuttuu vaikeammaksi ja monimutkaisemmaksi. Tämän vuoksi eri sidosryhmät ovat aloittaneet koordinoidun yhteistyön tekemisen kyberuhkien torjumiseksi (Zibak & Simpson, 2019). Alla kuvio uhkatiedustelun hallintajärjestelmän mallista. Mallin mukaisesti voidaan saada tietoverkkouhkiin liittyvää tietoa useista eri lähteistä, kuten jakavien yhteisöjen, avoimen lähdekoodin, organisaation sisäisten tietolähteiden ja kaupallisten syötteiden kautta. Malli voi auttaa hallitsemaan uhkatiedustelua ja hyödyntämään sitä kyberpuolustuksen ja tietoturvan parantamisessa.



KUVIO 4: Uhkatiedustelun hallintajärjestelmän malli (Zibak & Simpson, 2019).

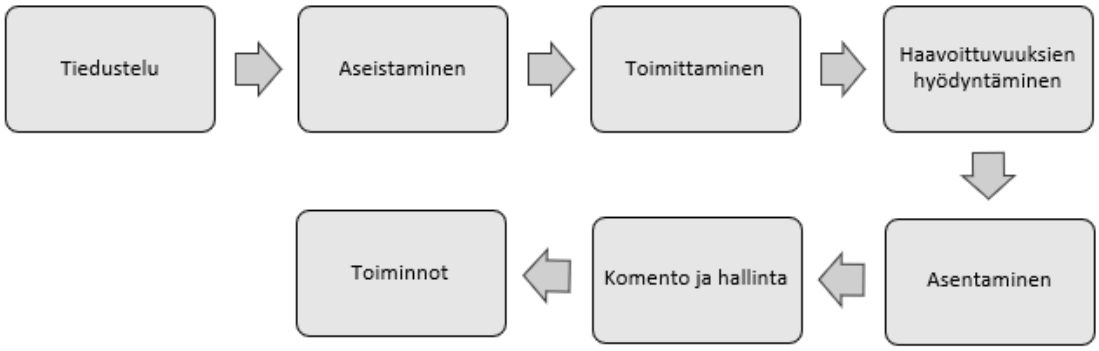
Suuria kyberuhkia ovat myös nollapäivähaavoittuvuudet. Niitä ilmaantuu tieto- ja viestintäjärjestelmiin, ne vaikeuttavat kyberpuolustusta ja ovat järjestelmille hyvin vaarallisia (Hu ym., 2017). Nollapäivähaavoittuvuus tarkoittaa aukkoa tietoturvassa, joka löydetään hyökkääjien toimesta ennen kuin sitä keretään paikata. Liikkuvan kohteen puolustus (*Moving Target Defense, MTD*) on yksi lupaavista keinoista puolustautua nollapäivähyökkäyksiltä (Hu ym., 2017).

Kyberuhkien torjuminen edellyttää entistä nopeampaa, läpinäkyvämpää ja paremmin koordinoitua yhteistoimintaa kaikilta osapuolilta (Lehto, 2021). Viime vuosina syntyneiden uusien uhkien taustalla ovat uudet, entistä kehittyneemmät tekniikat ja menetelmät. Tällaisten uhkien torjuminen on vaikeutunut useista syistä kuten esineiden internetin (*Internet of Things, IoT*) ja kyberfyysisten järjestelmien (*Cyber Physical Systems, CPS*) protokollien jatkuvasta kasvusta, hyökkääjien ammattimaistumisesta, rahoituksien lisääntymisestä ja kehittyneiden Crime-as-a-Service-palveluiden yleistymisestä (Wendzel ym., 2022). Uusiin uhkiin pyritään vastaamaan kehittämällä uusia vastatoimia.

3.3 Kyberpuolustusmenetelmät

Kyberhyökkäykset ovat muuttuneet entistä vakavimmiksi, nopeammiksi ja edistyksellisemmiksi, minkä vuoksi myös kyberpuolustusmenetelmien merkitys kasvaa jatkuvasti. Tässä luvussa käsitellään joitakin yleisiä kyberpuolustusmenetelmiä.

On tärkeää tietää kuinka hyökkääjät toimivat, jotta voidaan selvittää, miten heidät voidaan pysäyttää (Kaloudi & Li, 2020). Kun kyberhyökkäysten tyypilliset tekniikat ja toimintatavat ovat tiedossa, on huomattavasti helpompaa hyödyntää kyberpuolustuksessa käytettyjä menetelmiä oikeassa paikassa ja oikea-aikaisesti. Hyökkääjien toimia ja käyttäytymistä pyritään havainnoimaan ja esittämään erilaisten kyberhyökkäysten viitekehysten avulla (Kaloudi & Li, 2020). Galinec ym. (2017) esittävät yhdeksi tunnetuimmista malleista kuviossa 6 esitetyn tunkeutumisen tappoketjun (*Intrusion Kill Chain, IKC*). Mallin vaiheet ovat tiedustelu, aseistaminen, toimittaminen, haavoittuvuuksien hyödyntäminen, asentaminen, komento ja hallinta sekä toiminnot. Malli kuvaa hyökkääjän toimintaa tunkeutumisen suunnittelussa ja toteutuksessa. Nämä seitsemän vaihetta ovat välttämättömiä hyökkääjän kannalta suunnitellessaan ja toteuttaessaan tunkeutumisen. (Galinec ym., 2017.)



KUVIO 5: Tunkeutumisen tappoketju (Galinec ym., 2017).

Perinteiset puolustustoimenpiteet – kuten palomuuri ja tunkeutumisen havaitsemisjärjestelmät – ovat alttiita hyökkäyksille, koska ne jäävät usein passiiviseen tilaan reagoidessaan entistä koordinoidumpiin ja älykkäämpiin hyökkäyksiin (Zheng ym., 2022). Seuraavissa kappaleissa käydään läpi perinteisiä puolustusmenetelmiä.

Kolme tunnetuinta perinteistä puolustusmenetelmää ovat salasanasuojaus, virustentorjuntaohjelmisto sekä palomuuri. Salasanasuojaus on perinteinen tietoturvan keino, joka on ensiaskel kaikelle kyberpuolustukselle. Sen avulla suojataan käyttäjätunnukset ja muu henkilökohtainen tieto luvattomalta käytöltä. Virustentorjuntaohjelmisto tarkkailee tietokoneen toimintaa ja havaitsee ja poistaa mahdolliset haittaohjelmat, kuten virukset ja troijalaiset. Palomuuri on ohjelmisto- tai laitteistopohjaisesti toteutettu järjestelmä (Lehto, 2021). Palomuuri toimii suodattimena verkkojen välillä valvoen liikennettä ja estäen haitallisen pääsyn verkossa olevaan järjestelmään. Palomuuri suojelee verkkoa haitalliselta liikenteeltä, kuten palvelunestohyökkäyksiltä, haittaohjelmilta ja tietomurroilta.

Perinteisiin puolustusmenetelmiin kuuluvat myös tunkeilijan havaitsemisjärjestelmä ja turvallisuuden tapahtumien hallinta. Tunkeilijan havaitsemisjärjestelmä (*Intrusion Detection System, IDS*) on verkkoon suuntautuvien hyökkäysyritysten tunnistamiseen ohjelmoitu järjestelmä (Lehto, 2021). Järjestelmä pyrkii löytämään potentiaalisia hyökkäyksiä tarkkailemalla dataa, joka liikkuu järjestelmään ja sieltä ulos. Turvallisuuden tapahtumien hallinta eli SIEM (*Security Information and Event Management*) puolestaan vahtii tietoverkoissa ja -järjestelmissä tapahtuvaa normaalista poikkeavaa toimintaa ja hälyttää niistä (Lehto, 2021). SIEMin avulla organisaatiot havaitsevat mahdolliset normaalista poikkeavat toiminnat ja pystyvät reagoimaan hyökkäyksiin nopeammin ja tehokkaammin.

Kyberpuolustukseen liittyvät keinot ja menetelmät kehittyvät samaan tahtiin yleisen teknologiakehityksen kanssa (Candolin, 2022). Tämä tarkoittaa sitä, että uhkakuvat ja hyökkäykset muuttuvat ja kehittyvät jatkuvasti, mikä vaatii uusia keinoja ja uusien menetelmien kehittämistä niiden torjumiseksi. Tällainen kehitys on välttämätöntä tietojen ja tietojärjestelmien suojelemiseksi yhä monimutkaistuvassa digitaalisessa maailmassa. Kyberhyökkäysten ja -uhkien edistyessä ja lisääntyessä on tärkeää pysyä kehityksen mukana myös puolustuksessa. Wendzel ym. (2022) mukaan eräs ehdotettu edistysaskel on kehittää uusia tunkeutumisen havaitsemisen muotoja. Lisäksi he toteavat, että nämä menetelmät perustuvat koneoppimiseen ja mahdollistavat poikkeamien havaitsemisen, liikenteen normalisoinnin tai aktiivisten vartijoiden käytön, joiden avulla hyökkäyksiä voidaan tunnistaa ja estää. (Wendzel ym., 2022.)

Zheng ym. (2022) lisäävät, että perinteisten puolustustekniikoiden tarjoama turvallisuus riittää tiettyyn pisteeseen asti, mutta monipuolisten ja jatkuvasti kehittyvien hyökkäysten alla perinteinen kyberpuolustus yksinään on riittämätön. Tämän vuoksi perinteisen puolustuksen rinnalle tarvitaan muutakin puolustusta, joka poistaisi puolustuksen passiivisuuden. Yksi tarjolla oleva menetelmä siihen on dynaaminen puolustus. Zheng ym. (2022) määrittelevät, että dynaaminen puolustus perustuu jäljittelevään puolustukseen sekä liikkuvaan kohdepuolustukseen. Heidän mukaansa jäljittelevä puolustus (*Mimic Defense,*

MD) pyrkii mitätöimään hyökkäyksen muuttamalla verkkojärjestelmän rakennetta. Lisäksi he toteavat, että liikkuvan kohdepuolustuksen (*Moving Target Defense, MTD*) tarkoitus on hämmentää kyberhyökkääjiä jatkuvilla muutoksilla, minkä seurauksena hyökkäykset vaikeutuvat muun muassa kasvavien kustannusten, monimutkaisuuden ja epäonnistumisasteen takia. (Zheng ym., 2022.) Liikkuvan maalin periaatteessa muutetaan tietojärjestelmää ja ympäristöä siten, että hyökkäyksen epävarmuus lisääntyy. Epävarmuuden lisääntyminen vaikeuttaa kyberhyökkäyksen onnistumista sekä kasvattaa sen riskejä ja resurssikustannuksia. Dynaamisia puolustusmekanismeja tutkitaan ja esitellään vain hyvin pienissä määrin tutkimusalan teoksissa. Niiden tutkiminen olisi kuitenkin äärimmäisen tärkeää, jotta löydettäisiin uusia keinoja vastata alati kehittyviin kyberhyökkäyksiin.

Kyberpuolustus käsittää kolme toisiaan täydentävää luokkaa, jotka ovat ennakoiva, aktiivinen ja uudistuva (Galinec ym., 2017). Ennakoiva kyberpuolustus pyrkii tunnistamaan kyberpuolustuksen aukot ja haavoittuvuudet ennakkoon sekä ennaltaehkäisemään niiden hyväksikäyttöä. Ennakoiva kyberpuolustus sisältää esimerkiksi riskianalyysin ja haavoittuvuuksien skannauksen sekä henkilöstön kouluttamisen. Aktiivinen kyberpuolustus tarkoittaa hyökkäyksen aikana toteutettuja toimenpiteitä, joiden tavoitteena on minimoida vahingot ja pysäyttää hyökkäys. Aktiiviseen kyberpuolustukseen sisältyy muun muassa hälytysjärjestelmien käyttö, hyökkääjän liikkeiden ja toimien seuranta sekä tietojen suojaus. Uudistuva kyberpuolustus pyrkii palauttamaan hyökkäyksen tai vahingon kohteena olleet järjestelmät normaaliin tilaan hyökkäyksen jälkeen. Uudistuva kyberpuolustus sisältää esimerkiksi järjestelmän uudelleenrakentamisen ja tietojen palauttamisen varmuuskopioista.

4 TEKOÄLYN HYÖDYNTÄMINEN KYBERPUOLUSTUKSESSA

Tekoäly on yksi viime vuosikymmenien merkittävimmistä teknologisista innovaatioista, eikä kyberpuolustus ole poikkeus tälle trendille, vaan tekoälyn kehittyminen ja sen laajamittainen alojen valtaaminen on vaikuttanut merkittävästi myös kyberpuolustukseen. Kuten edellä mainittu, kyberhyökkäykset kehittyvät jatkuvasti, minkä vuoksi myös kyberpuolustuksen on pysyttävä kehityksessä mukana. Kyberhyökkäykset ovat tällä hetkellä kyberpuolustusta edistyneempiä, joten hyökkäyksen ja puolustuksen välinen edistyneisyyden kuilu pitäisi saada kurottua umpeen. Potentiaalisin ratkaisu kuilun umpeen kuromiseksi on tekoälyn hyödyntäminen kyberpuolustuksessa. Hyökkäyksissä käytetty tekoäly kuitenkin hankaloittaa tilannetta entisestään. Edelleen on epävarmuutta, kuinka puolustautua tekoälyllä varustettuja kyberhyökkäyksiä vastaan.

Tekoälyn hyödyntäminen kyberpuolustuksessa tarjoaa merkittäviä mahdollisuuksia, mutta se tuo mukanaan myös haasteita. Yksi keskeisistä haasteista on tietosuoja, sillä tekoäly vaatii paljon dataa ja tietoa toimiakseen. Tieto voi olla arkaluontoista, joten on tärkeää huolehtia, että tietoja käsitellään oikein ja huolellisesti.

Tässä luvussa tutkitaan tekoälyn hyödyntämistä kyberpuolustuksessa. Alaluvuissa tutkitaan sitä, millainen rooli tekoälyllä on nykypäivän kyberpuolustuksessa ja millaisia mahdollisuuksia tekoälyllä on tulevaisuudessa ja kuinka tekoälyä voidaan hyödyntää kyberpuolustuksessa entistä tehokkaammin.

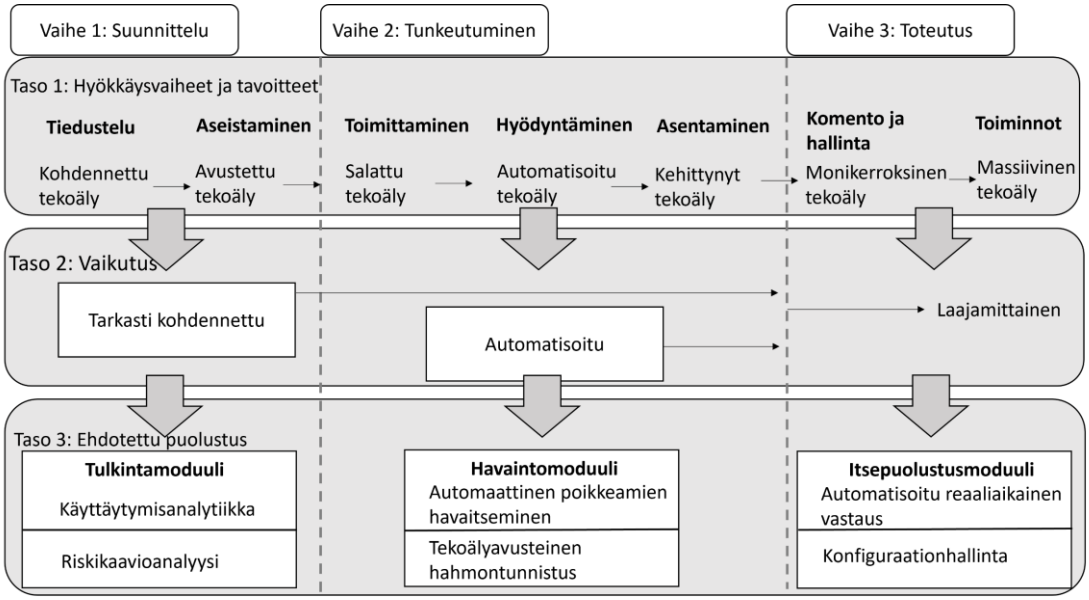
Kun ymmärretään tekoälyn hyödyntäminen kyberhyökkäyksissä, voidaan löytää parhaat puolustusmenetelmät niitä vastaan. Kaloudin ja Lin (2020) mukaan tekoälyyn perustuvia verkkohyökkäyksiä ei ole tutkittu vielä riittävästi vastustajan toimien ymmärtämiseksi.

4.1 Tekoälyn rooli kyberpuolustuksessa

Tekoälyä pidetään kyberpuolustuksen ja -turvallisuuden lupaavimpana teknologiana, mutta myös pahantahtoiset hyökkääjät hyötyvät siitä. Tekoälyn kehitys on tuonut mukanaan valtavia määriä uusia hyökkäysmenetelmiä ja -tapoja. Tekoäly mahdollistaa esimerkiksi hyvin kohdennettuja hyökkäysoperaatioita haitallisiin tarkoituksiin ja tekoälytekniikoita voidaan käyttää yhdessä perinteisten hyökkäystekniikoiden kanssa tehokkuuden lisäämiseksi, eikä nykyiset puolustusmenetelmät riitä vastaamaan hyökkäysten edistyneisyyteen (Kaloudi & Li, 2020). Toisaalta Candolinin (2022) mukaan myös kyberoperaatioiden suojausratkaisuissa hyödynnetään tekoälyä ja koneoppimista koko ajan enemmän. Tekoälyn avulla voidaan löytää uhkia entistä varhaisemmassa vaiheessa sekä nopeuttaa kyberpuolustuksen reaktioaikoja. Tarkoma (2017) kiteyttää, että tekoäly mahdollistaa uhkien ja hyökkäysten ennakoinnin ja niiden vaikutukset sekä verkkohyökkäysten tunnistamisen ja estämisen. Tekoälyratkaisut mahdollistavat paremman automatisoinnin ja tuen päätöksentekoon, mutta samalla syntyy uusia haasteita järjestelmien toiminnan varmistamiseen ja suojaamiseen liittyen.

Mirsky ym. (2021) toteavat, että viime aikoina on keskitytty työskentelemään tekoälypohjaisten järjestelmien turvallisuuden parantamiseksi. Erityisesti tekoälyyn kohdistuvia hyökkäyksiä on pyritty tunnistamaan ja niiden vaikutuksia on pyritty lieventämään. (Mirsky ym., 2021.) Tämä on tärkeää, jotta voidaan kehittää puolustusmenetelmiä estämään vahingolliset hyökkäykset ja suojata tekoälypohjaisia järjestelmiä. Tekoälyn hyödyntäminen kyberpuolustuksessa on tärkeää etenkin hyökkäyksen alkuvaiheessa, sillä Mirsky ym. (2021) mukaan tekoälyn vaikutus on suurin edellä esitetyn tappoketjun alkuvaiheessa, koska hyökkääjä pystyy hyödyntämään ympäristöä harjoitellakseen ja testatakseen hyökkäyksen tekoälymallejaan.

Kaloudi ja Li (2020) ehdottavat kuviossa 7 havainnollistettua kolmiportaista kyberuhkien viitekehystä, jonka avulla ymmärrettäisiin paremmin tekoälypohjaisia kyberhyökkäyksiä. Mallin avulla voitaisiin tutkia uhkia sekä niiden luokituksia ja vaikutuksia. Viitekehys kuvaa vastustajan toimia tämän näkökulmasta. Mallin ensimmäinen taso tunnistaa hyökkääjän tavoitteiden ajankohdat, toinen taso luokittelee tekoälyteknologioiden vaikutuksen hyökkäyksen vaiheen mukaan ja kolmannella tasolla esitetään erilaisia puolustusmenetelmiä. Viitekehys auttaa tekoälypohjaisten kyberhyökkäysten torjumista ja puolustamista tekoälyn keinoin. (Kaloudi & Li, 2020.)



KUVIO 6: Kolmiportainen kyberuhkien viitekehys (Kaloudi & Li, 2020).

Koneoppimistekniikoiden avulla on mahdollista kouluttaa agentti, joka kykenee puolustamaan itsenäisesti järjestelmää (Applebaum ym., 2022). Ventren (2020) mukaan autonomisen aktiivisen kyberpuolustuksen avulla voidaan havaita, määritellä, analysoida ja lieventää kyberuhkia ilman ihmisen välitöntä puuttumista. Kaloudi ja Li (2020) täsmentävät, että autonomisen kyberpuolustuksen avulla voidaan oppia kokemuksista kybertaistelussa hyökkääjien ja puolustajien välillä. Applebaum ym. (2022) lisäävät, että autonomisen kyberpuolustuksen tutkimus on kestänyt jo vuosikymmeniä ja se on kehittynyt asiantuntijajärjestelmien käytöstä vahvistusoppimisen käyttöön.

Kaloudin ja Lin (2020) mukaan tekoälyä käytetään tällä hetkellä kyberhyökkäysten torjumisessa usein eri tavoin. Se auttaa havaitsemaan poikkeavan verkkoliikenteen, arvioimaan haavoittuvuuksia, luokittelemaan haittaohjelmia, havaitsemaan tietojenkalasteluhyökkäyksiä sekä tunnistamaan bottiverkkoliikenteen. (Kaloudi & Li, 2020.) Vähäkainu ja Lehto (2019) lisäävät tekoälyn käyttötarkoituksiin kyberpuolustuksessa havaitsemisen ja torjumisen lisäksi myös kyberhyökkäysten tutkimisen.

Luvun lopuksi esittelen muutaman jo käytössä olevan tekoälypohjaisen ratkaisun kyberpuolustukseen. Valitsin alla esitetyt ratkaisut niiden tunnettuuden perusteella. Esittelemäni ratkaisut ovat:

- AI2-alusta
- CylanceProtect
- Darktrace Cyber AI loop

Conner-Simonsin (2016) mukaan AI2 on MIT:n tutkijoiden ja PatternExin kehittämä kyberhyökkäysten ennustamiseen kehitetty tekoälyalusta. Järjestelmä kykenee ennustamaan jopa 85 prosenttia kyberhyökkäyksistä, mikä on noin kolme kertaa aiempia tutkimuksia parempi. Järjestelmä ennakoi hyökkäyksiä havaitsemalla epäilyttävän toiminnan koneoppimisen avulla. Järjestelmä luo uusia malleja muutamassa tunnissa, minkä vuoksi sen nopeus havaita epäilyttävä toiminta voi parantua merkittävästi. (Conner-Simons, 2016.)

Vähäkainun ja Lehdon (2019) mukaan CylanceProtect, jonka on kehittänyt Cylance inc., on integroitu älykäs työkalu, joka torjuu tietoturvauhkat ja haittaohjelmat tietoturvakontrollin ja tekoälyn avulla. Työkalu kykenee myös estämään nollapäivähyökkäyksiä ja suojaamaan laitetta ilman käyttäjän häiriintymistä. (Vähäkainu & Lehto, 2019.)

Darktracen (2023) mukaan heidän Cyber AI Loop on itseoppivalla tekoälyllä toimiva kokonaisratkaisu kyberuhkia ja -hyökkäyksiä vastaan. Se löytää ja tunnistaa uusia, perinteisen tietoturvan kiertäviä kyberuhkia. Ratkaisu on alan ensimmäinen kokonaisuusratkaisu kyberpuolustukseen. Se estää ja havaitsee kyberuhkat ja -hyökkäykset sekä reagoi niihin. Vuoden 2023 aikana ratkaisu täydentyy neljännellä osa-alueella eli toipumisella, joka parantaa järjestelmien toimintakunnon kyberhyökkäysten jälkeen. (Darktrace, 2023.)

Yhteenvetona voidaan todeta, että tekoälyn hyödyntäminen kyberpuolustuksen apuna ja tukena ei täysin poista tai pysäytä kyberhyökkäyksiä, mutta lieventää niiden tehokkuutta ja vaikutusta. Koska tekoäly ja tutkimus sen parissa kehittyvät ekspotentiaalisesti, myös tekoälyn mahdollisuudet kyberpuolustuksessa lisääntyvät jatkuvasti. Tekoälyn hyödyntämisen merkitys kyberpuolustuksessa kasvaa myös tekoälypohjaisten hyökkäysten jatkuvan edistymisen ja lisääntymisen seurauksena. Tekoäly tullee näyttelemään isoa roolia kyberhyökkäyksen ja kyberpuolustuksen välisen kuilun umpeen kuromisessa.

4.2 Tekoälyn tulevaisuudennäkymät kyberpuolustuksessa

Tekoälyä käytetään apuna niin kyberhyökkäyksissä kuin -puolustuksessakin. Tulevaisuuden taistelukentällä tekoälyjen välinen taistelu tulee yleistymään entisestään. Tämän alaluvun tarkoituksena on tutkia, miten tekoälyä voidaan tulevaisuudessa hyödyntää kyberpuolustuksen tukena.

Suuren datan analysointiin tarkoitetut tekniikat, eli niin kutsutut big data analytiikat, ovat yksi tulevaisuuden lupaavista kyberpuolustuksen menetelmistä. Kumarin ym. (2022) mukaan Big Data Analytics on teknologinen läpimurto, jonka avulla voidaan suojautua monimutkaisilta ja kehittyneiltä kyberhyökkäyksiltä. Useat tahot ja organisaatiot ympäri maailmaa kehittävät big dataan perustuvia järjestelmiä, joiden avulla voidaan tehokkaasti analysoida suuria datamassoja tarvittavan tiedustelutiedon saamiseksi. Datamassojen analysoinnin avulla voidaan tunnistaa varhaisessa vaiheessa mahdollisia hyökkäyksiä ja uhkia, jotta niitä vastaan voidaan puolustautua. (Kumar ym., 2022.) Erittäin lupaava ratkaisu tulevaisuuden kyberpuolustukseen lienee big datan, tekoälyn, koneoppimisen ja

syväoppimisen yhdistäminen ja soveltaminen. Ratkaisu vaatii kuitenkin runsaasti resursseja, joten se tarvitsee huolellista suunnittelua ja hallintaa.

Kyberpuolustusjärjestelmien autonomisuus, monimutkaisuus ja laajuus aiheuttavat uusia hyökkäysstrategioita ja autonomiset älykkäät haittaohjelmat kehittyvät koko ajan (Théron & Kott, 2019). Autonomiset älykkäät haittaohjelmat käyttävät useita eri hyökkäystekniikoita, minkä vuoksi ne voivat levitä laajalle. Ne ovat vielä melko harvinaisia, mutta ne myös kehittyvät jatkuvasti, minkä vuoksi niitä vastaan on kehitettävä puolustusmenetelmiä. Théron ja Kott (2019) ehdottavat autonomisten älykkäiden haittaohjelmien puolustukseen autonomista kyberpuolustusta. Autonominen kyberpuolustus on uusi tekniikka, joka pyrkii ennakoiden vastaamaan hyökkäyksiin nopeasti ja tehokkaasti. Se toteutetaan autonomisten älykkäiden kyberpuolustusagenttien avulla. Autonomisten älykkäiden kyberpuolustusagenttien viisi tehtävää ovat järjestelmän valvominen, verkkohyökkäysten havaitseminen, vastatoimien laatiminen, taktinen toteuttaminen ja ihmiselle raportointi. Autonominen kyberpuolustus on visio järjestelmien entistä itsenäisempään toimintaan ja sitä kautta nopeampaan reagointiin mahdollisin uhkiin ja hyökkäyksiin. (Théron & Kott, 2019.)

Seker (2019) linjaa, että kyberpuolustusjärjestelmän tulisi tarjota vähintään kolme kyberturvallisuuden tasoa. Ensimmäinen taso kattaa perinteiset kyberpuolustusmenetelmät, toinen taso ennakoivat menetelmät ja kolmas taso kokonaisvaltaisen arvioinnin, puolustuksen hallinnan ja puolustusmenetelmien mukauttamisen. Tekoälyteknologioilla varustetuilla järjestelmillä on suuri rooli kyberturvallisuustasojen tarjoamisessa. (Seker, 2019.) Varhaisvaroitusjärjestelmä on järjestelmä, joka havaitsee mahdolliset uhkat ennen niiden muuttumista kriittiseksi. Seker (2019) toteaa, että tekoälyn käyttötarkoitus ennakoinnissa ja varhaisen vaiheen varoituksessa on kehittää älykäs apujärjestelmä, jonka avulla voidaan havaita mahdollisimman aikaisin lähi- ja laajakaistaverkossa tapahtuvat verkkohyökkäykset.

Lee ja Kim (2021) esittävät lohkoketjuteknologiaa hyödyntävän kyberpuolustusmenetelmän. Heidän mukaansa lohkoketjuteknologia on yksi potentiaalinen tulevaisuuden kyberpuolustuksen kehittyvistä teknologioista. Sen soveltaminen kyberpuolustuksessa olisi iso harppaus sen tarjoamien hyötyjen ansiosta:

- Näkyvyys: Lohkoketjun hajautetun ja jaetun pääkirjarakenteen myötä se tarjoaa tietojen näkyvyyttä.
- Todennettavuus: Lohkoketjun avulla voidaan varmistaa tiedon todennettavuus.
- Yhden vikapisteen poistaminen: Hajautetussa lohkoketjuympäristössä ei ole ainoastaan yhtä keskitettyä ohjauspalvelinta, joka olisi yksi vikapiste.
- Tarkastettavuus: Lohkoketjun jatkuvan haschchain-tietorakenteen eli lohkojen yksilöllisten tunnisteiden ansiosta tietojen muokkaaminen ja poistaminen kesken lohkojen on lähes mahdotonta, mikä mahdollistaa järjestelmän tietojen tarkastettavuuden kyberpuolustuksen näkökulmasta.

Lohkoketjuteknologian käyttöönotto kyberpuolustuksen kontekstissa vaatii kuitenkin edelleen lisätutkimusta ja kehitystä, sillä siinä on edelleen joitain haasteita ja rajoituksia. (Lee & Kim, 2021.)

Yksi potentiaalisimmista tekoälyn tulevaisuuden sovelluksista kyberpuolustuksessa on tekoälyn kyky oppia ja sopeutua jatkuvasti muuttuviin uhkiin. Niiden avulla tekoäly voi kehittää ennakoivan puolustusmekanismin, joka havaitsee ja tunnistaa uhkia ennen niiden toteutumista. Sen tuomat edut verrattuna nykyiseen reaktiiviseen puolustukseen auttaisivat kaventamaan kyberhyökkäyksen ja -puolustuksen välillä olevaa edistyneisyyden kuilua.

Big data -analytiikoiden, autonomisen kyberpuolustuksen ja lohkoketjuteknologian potentiaali tulevaisuuden kyberpuolustuksessa on valtava. Edellä mainittujen tekniikoiden hyödyntäminen on kustannuksiltaan vaativia, sillä ne vaativat runsaasti resursseja ja erikoistunutta osaamista. Big data -analytiikan hyödyntäminen puolustuksessa vaatii merkittäviä tallennus- ja tietokoneresursseja, jotta voidaan kerätä, tallentaa ja käsitellä suuria tietomassoja. Autonominen kyberpuolustus vaatii kehittyneitä algoritmeja ja automaatiojärjestelmiä, jotka voivat olla vaativia ja monimutkaisia toteutettavia. Lohkoketjuteknologian käyttöönotto kyberpuolustuksessa taas vaatii etenkin tietoteknisiä resursseja, kuten palvelimia, tietokoneita ja verkkoja. Tästä kaikesta huolimatta edellä mainittujen tekniikoiden hyödyntäminen tulevaisuuden kyberpuolustuksessa on hyödyllistä, sillä ne pystyvät parantamaan kyberpuolustuksen tehokkuutta ja sitä myöten kyberympäristöjen turvallisuutta merkittävästi.

5 YHTEENVETO

Tässä kandidaatintutkielmassa tarkasteltiin tekoälyä, kyberpuolustusta sekä tekoälyn hyödyntämistä kyberpuolustuksessa. Tutkielman tavoitteena oli kuvailla tekoälyn käyttöä kyberpuolustuksessa ja kartoittaa mahdollisia tulevaisuuden suuntauksia. Jatkuvasti edistyvät kyberhyökkäykset ovat herättäneet viime vuosina huolta. Tekoälyä käytetään hyökkäyksissä laajalti, mikä omalta osaltaan vaikuttanee siihen, että kyberhyökkäykset ovat tutkielmaa kirjoitettaessa jopa kyberpuolustusta edistyneempiä. Toisaalta tekoälyn on havaittu tarjoavan merkittäviä mahdollisuuksia myös puolustukseen. Tämän kirjallisuuskatsauksena toteutetun tutkielman tavoitteena oli tutkia tekoälyn hyödyntämistä kyberpuolustuksessa ratkaisten seuraavat tutkimusongelmat:

- Mikä on tekoälyn rooli kyberpuolustuksessa?
- Miten tekoälyä voidaan hyödyntää tulevaisuuden kyberpuolustuksessa?

Tutkimuksen keskeisimpänä havaintona on, että tekoälyn merkitys kyberpuolustuksessa on suuri. Sen avulla pystytään havaitsemaan ja tunnistamaan uhkat entistä varhaisemmassa vaiheessa sekä nopeuttamaan kyberpuolustuksen reagointiaikoja. Vaikka tekoälyn hyödyntäminen kyberpuolustuksen apuna ei täysin poista tai pysäytä kyberhyökkäyksiä, mutta tekoälyyn pohjautuvilla menetelmillä voidaan lieventää hyökkäysten tehokkuutta ja vaikutusta. Tulevaisuudessa tekoälyn merkitys puolustuksessa kasvaa entisestään, sillä sen avulla kyberpuolustus vahvistuu monin tavoin. Tekoäly voi auttaa tunnistamaan, ennakoimaan ja estämään uhkia ja hyökkäyksiä sekä tarjota reaaliaikaista vastetta hyökkäyksiin ja havaita haavoittuvuuksia. Tulevaisuuden kyberpuolustuksessa lupaavia sovellusalueita ovat muun muassa big data -analytiikat, autonominen kyberpuolustus ja lohkoketjuteknologia.

Tutkielman ensimmäisessä sisältöluvussa määriteltiin tekoäly, tarkasteltiin sen historiaa sekä tutkittiin sen tekniikoita. Ensimmäisen sisältöluvun perusteella voidaan todeta, että tekoälyn määrittely on erittäin haastavaa, eikä sille löydy yhtä, yleisesti hyväksyttyä määritelmää. Tekoälyn juurten voidaan katsoa ulottuvan aina 1900-luvun alkuun tai puoliväliin saakka, mutta varsinaista

huomiota tekoäly sai ensimmäisen kerran vasta 1950-luvulla. Tekoälyllä on useita erilaisia tekniikoita. Ensimmäisessä sisältöluvussa esiteltiin näistä koneoppiminen, syväoppiminen, vahvistusoppiminen, neuroverkot sekä luonnollisen kielen käsittely. Nämä tekniikat ovat yleisiä, laajalti eri sovelluksissa käytettyjä tekoälyn tekniikoita, jotka voivat tarjota kyberpuolustukseen mahdollisuuksia. Nämä tekniikat valikoituivat tutkielmaan, sillä niiden merkitys nykypäivän kyberpuolustuksessa on merkittävä. Edellä mainitut tekniikat tarjoavat myös laajoja tutkimusmahdollisuuksia tulevaisuuden kyberpuolustukselle.

Tutkielman toisessa sisältöluvussa määriteltiin kyberpuolustus, tarkasteltiin kyberpuolustuksessa käytettyjä menetelmiä sekä kyberuhkien tunnistamista ja torjumista. Kyberpuolustus on toisaalta tiedustelun, suojautumisen ja vaikuttamisen yhdistelmä, ja toisaalta se sisältää tietoturvan, kansallisen puolustuksen, kyberturvallisuuden sekä tieto- ja viestintäteknologian turvallisuuden. Sisältöluvussa tarkastellaan perinteisten reaktiivisten puolustusmenetelmien lisäksi sen kanssa yhtenäisesti toimivia aktiivisia ja ennakoivia puolustusmenetelmiä. Jotta kokonaisvaltainen puolustus voidaan saavuttaa, näiden kolmen puolustusmenetelmän täytyy toimia yhtenäisesti kyberpuolustuksessa. Toisen sisältöluvun viimeisessä alakappaleessa käsiteltiin kyberuhkia sekä niiden tunnistamista ja puolustamista. Kybertiedustelu ja uhkatiedustelu ovat tärkeimmät elementit kyberuhkien tunnistamiselle ja varhaisen vaiheen havaitsemiselle. Uusia uhkia syntyy entistä kehittyneempien tekniikoiden ja menetelmien myötä. Kyberuhkien torjumista varten eri osapuolten välinen yhteistoiminta tulee olla entistä koordinoidumpaa, läpinäkyvämpää ja nopeampaa.

Tutkielman viimeisessä sisältökappaleessa tarkasteltiin tekoälyn hyödyntämistä kyberpuolustuksessa. Aluksi tarkasteltiin tekoälyn roolia nykypäivän kyberpuolustuksessa, minkä jälkeen tutkittiin, kuinka tekoälyä voidaan hyödyntää tulevaisuuden kyberpuolustuksessa. Tekoäly on yksi lupaavimmista teknologioista kyberpuolustuksessa.

Tutkielman keskeiset tulokset osoittavat, että tekoälyä ja sen tekniikoita hyödynnetään kaikkien muiden alojen lisäksi laajalti myös kyberpuolustuksessa. Toisaalta tekoälyn kaikkea potentiaalia kyberpuolustuksen saralla ei olla vielä tunnistettu, vaan se pystyy tarjoamaan tulevaisuuden kyberpuolustukseen paljon nykyistä enemmän. Vaikka tutkielma osoittaa tekoälyn hyödyntämisen mahdollisuuksia nykypäivän ja tulevaisuuden kyberpuolustuksessa, lisätutkimusta tarvitaan, jotta kaikki tekoälyn potentiaali kyberpuolustuksen alalla saadaan hyödynnettyä. Yhteenvetona voidaan todeta tutkimuksen tulosten tukiessa aiempaa aiheen tutkimusta siltä kannalta, että tekoälyä voidaan hyödyntää laajalti kyberpuolustuksessa, ja sen rooli tulevaisuuden kyberpuolustuksessa voi kasvaa entisestään.

Pohjautuen tutkielman viimeiseen sisältökappaleeseen, jossa käsiteltiin tekoälyn tulevaisuudennäkymiä kyberpuolustuksessa, jatkotutkimusta vaativat big data- analytiikoiden, autonomisen kyberpuolustuksen sekä lohkoketjuteknologian hyödyntäminen kyberpuolustuksessa. Tässä tutkielmassa näihin perehdyttiin melko pintapuolisesti, minkä vuoksi jatkotutkimukset voisivat syventyä vielä tarkemmin tekniikoiden hyödyntämiseen tulevaisuuden puolustuksessa.

Nämä tulevaisuuden kyberpuolustustekniikat voivat olla ratkaisevassa asemassa kyberpuolustuksen ja -hyökkäyksen välisen edistyneisyyden kuilun kaventamisessa.

LÄHTEET

Ailisto, H., Neuvonen, A., & Seppälä, T. (2018). *Tekoälyn kokonaiskuva ja osaamiskartoitus* (Julkaisusarjan osa 46). Valtioneuvoston kanslia.

Akerkar, R. (2019). *Artificial Intelligence for Business*. Springer International Publishing.

Amthor, P., Fischer, D., Kühnhauser, W. E., & Stelzer, D. (2019). Automated Cyber Threat Sensing and Responding: Integrating Threat Intelligence into Security-Policy-Controlled Systems. Teoksessa *Proceedings of the 14th International Conference on Availability, Reliability and Security* (1–10).

Anyoha, R. (2017, 28. elokuuta). *The History of Artificial Intelligence*. Haettu 9.2.2023 osoitteesta https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/

Applebaum, A., Dennler, C., Dwyer, P., Moskowitz, M., Nguyen, H., Nichols, N., Park, N., Rachwalski, P., Rau, F., Webster, A., & Wolk, M. (2022). Bridging Automated to Autonomous Cyber Defense: Foundational Analysis of Tabular Q-Learning. Teoksessa *Proceedings of the 15th ACM Workshop on Artificial Intelligence and Security* (149–159).

Boden, M. A. (2016). *AI: Its Nature and Future*. Oxford University Press.

Bogue, R. (2014). The role of artificial intelligence in robotics. *Industrial Robot: An International Journal*, *41*(2), 119–123.

Broeders, D. (2021). Private active cyber defense and (international) cyber security – Pushing the line? *Journal of Cybersecurity*, *7*(1).

Candolin, C. (2022). *Lausunto sotateknologian tulevaisuudesta ja sen vaikutuksesta Suomen turvallisuuteen*. Haettu 3.2.2023 osoitteesta https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2022-AK-23127.pdf

Clifford, C. (2018, 13. maaliskuuta). *Elon Musk: 'Mark my words — A.I. is far more dangerous than nukes'*. CNBC. Haettu 18.2.2023 osoitteesta https://www.cnbc.com/2018/03/13/elon-musk-at-sxsw-a-i-is-more-dangerous-than-nuclear-weapons.html

Darktrace. (2023). Haettu 11.2.2023 osoitteesta https://darktrace.com/

Definition of Intelligence. (ei pvm.). Haettu 28.3.2023 osoitteesta https://www.all-words.com/query.php?SearchType=0&Keyword=Intelligence&go-query=Find+it%21&Language=ENG&v_PageSize=25

Eisenstein, J. (2019). *Introduction to Natural Language Processing* (Illustrated edition). The MIT Press.

Fletcher, R. B. & Hattie, J. (2011). *Intelligence and Intelligence Testing*. Taylor & Francis Group. Haettu osoitteesta http://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=668817

Galinec, D., Možnik, D. & Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatika*, *58*(3), 273–286.

Goodfellow, I., Bengio, Y. & Courville, A. (2016). *Deep Learning*. MIT Press.

Haenlein, M. & Kaplan, A. (2019). A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. *California Management Review*, *61*(4), 5–14.

Hammond, P. & Gummer, B. (1.11.2016). *National Cyber Security Strategy 2016-2021*.

Hopgood, A. A. (2021). *Intelligent Systems for Engineers and Scientists: A Practical Guide to Artificial Intelligence* (4. p.). CRC Press.

Hu, Z., Zhu, M. & Liu, P. (2017). Online Algorithms for Adaptive Cyber Defense on Bayesian Attack Graphs. Teoksessa *Proceedings of the 2017 Workshop on Moving Target Defense*, 99–109.

Hänninen, P. (2022). *Robotiikka ja tekoäly* (1. p). Tammertekniikka.

Jääskeläinen, A. (2019). *Mitä tapahtuu huomenna, kun tekoäly poistaa järjettömyydet?* WSOY.

Kaloudi, N. & Li, J. (2020). The AI-Based Cyber Threat Landscape: A Survey. *ACM Computing Surveys (CSUR)*, *53*, 1–34.

Kaplan, J. (2016). *Artificial Intelligence: What Everyone Needs to Know*. Oxford University Press. Haettu osoitteesta http://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=4705973

Koetsier, J. (2017, 6. marraskuuta). *Stephen Hawking Issues Stern Warning On AI: Could Be "Worst Thing" For Humanity*. Forbes. Haettu 5.3.2023 osoitteesta https://www.forbes.com/sites/johnkoetsier/2017/11/06/stephen-hawking-issues-stern-warning-on-ai-could-be-worst-thing-for-humanity/

Koski, O. (2018). Tekoäly ja muuttuva työ. Työpoliittinen aikakauskirja, 1(2018), 11–22.

Kumar, M., Srinivasa, K. G. & Yassine, M. (ei pvm.). *Big Data Analytics for Cyber Security and Advance Persistent Threat Intelligence*. Frontiers. Haettu 23.3.2023, osoitteesta https://www.frontiersin.org/research-topics/37830/big-data-analytics-for-cyber-security-and-advance-persistent-threat-intelligence#overview

Kyberturvallisuuden sanasto – Turvallisuuskomitea. (3.10.2018). https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/

Laari, T., Flyktman, J., Härmä, K., Timonen, J. & Tuovinen, J. (2019.). *Kyberkäsikirja Puolustusvoimien henkilöstölle*. 3(12).

LeCun, Y., Bengio, Y. & Hinton, G. (2015). Deep learning. *Nature*, *521*(7553), 436–444.

Lee, S. & Kim, S. (2022). Blockchain as a Cyber Defense: Opportunities, Applications, and Challenges. *IEEE Access*, *10*, 2602–2618.

Legg, S. & Hutter, M. (2007). Universal Intelligence: A Definition of Machine Intelligence. *Minds and Machines*, *17*(4), 391–444.

Lehto, M. (2021). Digitaalisen kybermaailman ilmiöitä ja määrittelyjä. https://www.jyu.fi/it/fi/hae-opiskelemaan/hakukohteet/kybma/kybermaailma_v15-0.pdf

Li, Y., Jiang, W., Yang, L. & Wu, T. (2018). On neural networks and learning systems for business computing. *Neurocomputing*, *275*, 1150–1159.

Lu, W., Xu, S. & Yi, X. (2013). Optimizing Active Cyber Defense. Teoksessa Wenlian L., Shouhuai X. & Xinlei Y, Decision and Game Theory for Security, LNCS 8252 (206-225). Switzerland: Springer International Publishing.

Mirsky, Y., Demontis, A., Kotak, J., Shankar, R., Deng, G., Yang, L., Zhang, X., Pintor, M., Lee, W., Elovici, Y. & Biggio, B. (2021). The Threat of Offensive AI to Organizations. ACM Comput. Surv, *124*.

Merilehto, A. (2018). *Tekoäly matkaopas johtajalle.* (2. p.). Helsinki: Alma Talent.

NATO. (2016). *NATO Summit Guide*. Warsaw.

Russell, S. J., Norvig, P. & Davis, E. (2010). *Artificial intelligence: a modern approach* (3rd ed). Prentice Hall.

Schmidhuber, J. (2015). Deep Learning in Neural Networks: An Overview. *Neural Networks*, *61*, 85–117.

Seker, E. (2019). Use of Artificial Intelligence Techniques / Applications in Cyber Defense. *IEEE Cyber Science 2019*.

Seker, E. & Ozbenli, H. H. (2018). The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation. *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 1–9.

Siau, K. L. & Yang, Y. (2017). Impact of Artificial Intelligence, Robotics, and Machine Learning on Sales and Marketing. *In Twelve Annual Midwest Association for Information System Conference (MWAIS 2017)*. 48.

Singer, P. W. & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know®*. Oxford University Press.

Syam, N. & Sharma, A. (2018). Waiting for a sales renaissance in the fourth industrial revolution: Machine learning and artificial intelligence in sales research and practice. *Industrial Marketing Management*, *69*, 135–146.

Conner-Simons, A. (2016, 18. huhtikuuta) *System predicts 85 percent of cyber-attacks using input from human experts*. Haettu 21.3.2023 osoitteesta https://news.mit.edu/2016/ai-system-predicts-85-percent-cyber-attacks-using-input-human-experts-0418

Tarkoma, S. (5.12.2017). Tekoäly ja kokonaisturvallisuus. *Maanpuolustus-lehti*. Haettu 25.3.2023 osoitteesta https://www.maanpuolustus-lehti.fi/tekoaly-ja-kokonaisturvallisuus/

Théron, P. & Kott, A. (2019). When Autonomous Intelligent Goodware Will Fight Autonomous Intelligent Malware: A Possible Future of Cyber Defense. *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*, 1–7.

Ventre, D. (2020). *Artificial Intelligence, Cybersecurity and Cyber Defense*. Wiley Data and Cybersecurity.

Vähäkainu, P. & Lehto, M. (2019). *Artificial intelligence in the cyber security environment*. International Conference on Cyber Warfare and Security.

Vähä-Sipilä, A., Marchal, S. & Aksela, M. (2021). *Tekoälyn soveltamisen kyberturvallisuus ja riskienhallinta.* Traficom.

Wendzel, S., Mazurczyk, W., Caviglione, L. & Houmansadr, A. (2022). Emerging topics in defending networked systems. *Future Generation Computer Systems*, *128*, 317–319.

Zheng, Y., Zheng, L., Xiaolong, X. & Qingzhan, Z. (2022). Dynamic defenses in cyber security: Techniques, methods and challenges. *Digital Communications and Networks*, *8*(4), 422–435.

Zibak, A. & Simpson, A. (2019). Cyber Threat Information Sharing: Perceived Benefits and Barriers. Teoksessa *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 1–9. Canterbury, UK.