Tampereen yliopisto

Aarne Vuoristo

KYBERTURVALLISUUDEN PARANTAMINEN TEKOÄLYN AVULLA

Kandidaatintyö
Johtamisen ja talouden tiedekunta
Tarkastaja: Jussi Myllärniemi
12/2024

TIIVISTELMÄ

Aarne Vuoristo: Kyberturvallisuuden parantaminen tekoälyn avulla
Kandidaatintyö
Tampereen yliopisto
Tietojohtaminen
Joulukuu 2024

Kyberturvallisuuden merkitys on digitalisaation takia viimeisten vuosien aikana ja työmarkkinoilla on tällä hetkellä suuri pula kyberturvallisuudenammattilaisista. Tekoälyn eri sovellukset voivat auttaa organisaatioita niin parantamaan kyberturvallisuuttaan kuin helpottamaan omaa työntekijäpulaansa.
Tämä tutkimus on tehty kirjallisuuskatsauksena ja sen tarkoituksena oli koota tietoa tämänhetkisestä tilanteesta, miten tekoälyä hyödynnetään tällä hetkellä eri organisaatioissa ja millaisia hyötyjä ja riskejä siihen liittyy. Artikkelit, joita työssä on käytetty ovat pääsääntöisesti alle 5 vuotta vanhoja vertaisarvioituja julkaisuja, jonka avulla on varmistettu, että lähteet ovat mahdollisimman ajankohtaisia. Tekoälyn kehitys on ollut viimeisen 10 vuoden aikana hyvin nopeaa ja yli 5 vuotta vanhoissa teksteissä tekoälyyn liittyvät asiat voivat olla jo vanhentuneita.
Tutkimuksen tulokset osoittavat, että tekoälyn avulla kybertuvallisuutta voidaan parantaa, kustannuksia voidaan vähentää ja henkilöstöpulaa voidaan helpottaa. Tekoälyn käyttämiseen liittyy myös riskejä ja sen käyttöönotto voi olla vaikeaa erityisesti organisaatioissa, jossa ei ole entuudestaan kokemusta tekoälyn käytöstä.

Avainsanat: Kyberturvallisuus, tekoäly, koneoppiminen, kyberturvallisuusstrategia, AI integraatio

ABSTRACT

Aarne Vuoristo: Improving cybersecurity with using Artificial Intelligence
Bachelor's thesis
Tampere University
Degree Program of Information and Knowledge Management
December 2024

The importance of cybersecurity has grown in recent years due to digitalization and there is currently a significant shortage of cybersecurity professionals in the organizations. Various applications of Artificial Intelligence can help organizations not only improve their cybersecurity but also relieve their staff shortages.

This study has been conducted as a literature review with the goal of gathering information about the current state of how AI is being utilized in different organizations and the benefits and risks associated with it. The articles used in this study are primarily peer-reviewed publications less than five years old, ensuring that the sources are as up to date as possible. The development of AI has been rapid over the past ten years, and materials older than five years may already be outdated regarding AI-related topics.

The results of the study indicate that AI can enhance cybersecurity, reduce costs, and mitigate staff shortages. However, there are risks associated with the use of AI, and its implementation can be challenging, particularly for organizations with no prior experience in utilizing AI.

Keywords: Cybersecurity, Artificial Intelligence, AI, Machine Learning, Cybersecurity strategy, AI integration

ALKUSANAT

Tämä työ on kirjoitettu syksyllä 2024 osana tietojohtamisen opintoja. Halusin tehdä työni kyberturvallisuuteen liittyen, koska koen sen hyvin ajankohtaiseksi ja tärkeäksi aihealueeksi. Liitin aiheeni koskemaan myös tekoälyä, sillä halusin oppia ilmiöstä lisää ja siitä sai kiinnostavan kokonaisuuden työn aiheeksi. Haluan kiittää kandidaatintyön ohjaajaa, sekä kaikkia, jotka ovat auttaneet minua työni kanssa seminaaritilaisuuksissa.

Tampereella, 11.12.2024

Aarne Vuoristo

TEKOÄLYN KÄYTTÖ OPINNÄYTTEESSÄ

Opinnäytteessäni on käytetty tekoälysovelluksia:

☐ Ei
☒ Kyllä

Ilmoitukseni mukaan olen käyttänyt opinnäytteessäni tutkielmaprosessin aikana seuraavia tekoälysovelluksia:

Tekoälysovellusten nimet ja versiot: ScopusAI

Käyttötarkoitus: ScopusAI:n avulla on etsitty tietoa hyödyntämällä erilaisia hakulausekkeita. Tekoäly etsii hakulausekkeisiin sopivia tieteellisiä tekstejä tietokannasta ja tekee niiden avulla lyhyen koosteen, jossa ilmenee, millaisia asioita artikkelissa käsitellään.
Tekoälyn avulla on vain etsitty mahdollisia tietolähteitä aineiston etsintävaiheessa.

Osiot, joissa tekoälyä on käytetty: Aineiston hankinta ja rajaus. Aineistoa on karsittu pois, jos tekoälyn tekemä tiivistelmä artikkelista ei käsittele haluttua aihetta.

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

SISÄLLYSLUETTELO

KESKEISET KÄSITTEET

Tietoturva (information security) tarkoittaa järjestelyjä, kuten asiakirjojen turvallista säilytystä ja hävittämistä sekä laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaamista, joiden avulla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus (Kuha, S et al. 2023).

Esineiden internet, IOT (Internet of Things) on käsite, jolla tarkoitetaan erilaisia laitteita tai niiden

muodostamaa kokonaisuutta, joihin on yhdistetty internet (SAP 2024). Esineet ovat varustettu erilaisilla antureilla, jolloin ne pystyvät keräämään dataa ja lähettämään sitä eteenpäin. Esineiden internetin tarkoituksena on muodostaa kokonaisuuksia, joiden avulla käyttäjä voi automatisoida toimintaa tai saada tietoa laitteen toiminnasta.

Kyberturvallisuus (cyber security) tarkoittaa toimia, jolla turvataan ja suojellaan laitteita, tietojärjestelmiä ja tietoa hyökkäyksiltä (F-Secure 2024). Kyberturvallisuuden merkitys on viime vuosien aikana korostunut huomattavasti. Erityisesti esineiden internetin lisääntyessä, sekä digitalisaation seurauksena, kyberturvallisuuden merkitys korostunut.

Tekoäly (Artificial Intelligence, *AI*) on tietokonejärjestelmä, joka jäljittelee ihmisen kognitiivisia toimintoja. Järjestelmä pystyy oppimaan, päättelemään ja ratkaisemaan ongelmia (Copeland 2024). Tekoäly pystyy suorittamaan tehtäviä ja käyttämään niiden suorittamiseen sille syötettävää dataa tai internetistä löytyvää materiaalia.

Tunkeilijan havaitsemisjärjestelmä IDS tarkoittaa järjestelmää, joka havaitsee, jos verkkoon kohdistuu hyökkäysyritys (Paloalto 2024). Ohjelma tarkkailee haluttua verkkoa erilaisilla sensoreilla ja analysoi sen pohjalta onko verkon käytössä jotain normaalista poikkeavaa.

Tietoturva-aukko (Vulnerabilities) tarkoittaa haavoittuvuutta tietojärjestelmässä, jonka avulla ulkopuolinen pääsee tekemään toimia tietojärjestelmään, joita sen ei pitäisi normaalisti päästä tekemään (Owasp 2024). Tietoturva-aukkoja on tyypillisesti ohjelmistoissa, mutta niitä voi myös esiintyä laitteissa.

Tietovuotojärjestelmä (Data Leak Protection) on järjestelmä, joka tarkkailee ja analysoi organisaation sisällä ja sen ulkopuolelle liikkuvaa data ja varmistaa, ettei sitä päädy ulkopuolisille. Tietovuotojärjestelmä myös tarkkailee tietoverkkoon liitettäviä laitteita ja varmistaa, ettei tietoverkkoon liity ulkopuolisia käyttäjiä, jotka yrittävät saada organisaation tietoja haltuunsa. (Pytel 2024)

1. JOHDANTO

Kyberturvallisuudesta on tullut yksi keskeisimmistä teemoista digitaalisessa yhteiskunnassa, jossa yhä suurempi osa yksilöiden ja organisaatioiden toiminnasta on sidottu erilaisiin tietojärjestelmiin ja verkkoihin. Yksityishenkilöt, julkiset organisaatiot ja yritykset käsittelevät ja hyödyntävät päivittäin valtavia määriä dataa, jolloin he ovat alttiita jatkuvasti erilaisille kyber- ja tietoturvallisuusriskeille. Nämä uhat voivat aiheuttaa vakavia taloudellisia menetyksiä, henkilökohtaisten tietojen vuotamista tai kansallisen turvallisuuden vaarantumista. (Florackis et al. 2023) Kyberturvallisuuden avulla voidaan turvata tietoverkkojen ja -järjestelmien toimivuus ja turvallinen käyttö, mikä on edellytys digitaaliselle yhteiskunnalle.

COVID-19-pandemia kiihdytti digitaalisten ratkaisujen kehittämistä entisestään. Pandemian aiheuttamat rajoitukset ja sosiaalisen etäisyyden pitäminen toisiin johti monilla työpaikoilla etätyöhön ja uusien etätyökäytäntöjen luomiseen. Niin julkisella, kuin yksityisellä sektorilla tarvittiin uusia digitaalisia palveluita, jotka mahdollistivat asioinnin ilman fyysistä kontaktia. Digitalisaation nopeutuminen lisäsi myös kyberturvallisuuden tarvetta entisestään ja monissa organisaatioissa tarvittiin uusia keinoja suojautua kyberhyökkäyksiltä uudessa toimintaympäristössä. Lanka esittää tutkimuksessaan (2024), että kyberhyökkäyksien määrä on yli kaksinkertaistunut pandemian aikana ja jälkeen. Hän myös mainitsee, että taloudelliset tappiot, joita kyberhyökkäykset ovat aiheuttaneet globaalisti ovat yli nelinkertaistuneet vuodesta 2017.

Evans ja Reeder (2010) toteuttivat yli vuosikymmenen sitten tutkimuksen, jonka mukaan tietoturva-ammattilaisista on pulaa alalla. Ala kasvaa koko ajan ja alalle tarvitaankin jatkuvasti lisää uusia tekijöitä. Kyberturvallisuuden ammattilaisista on pulaa, joka tuottaa ongelmia monille organisaatioille parantaa heidän kyberturvallisuuttaan (Glas, M. et al. 2023). Organisaatioiden kyberturvaosaajien pulaa voitaisiin helpottaa hyödyntämällä kyberturvallisuuteen tekoälyä. Tekoälyn auttaisi organisaatioita automatisoimaan osan työvaiheista, jolloin työntekijöiden työtaakka helpottaisi.

Tekoälyn kehitys on kehittynyt valtavasti viimeisen vuosikymmenen aikana. Tekoälyn hyödyntäminen mahdollistaa uusien liiketoiminnallisia mahdollisuuksia, ja sen avulla voidaan parantaa ja tehostaa nykyisä toimintoja. (Collins et al. 2021) Tekoälyä pystytään hyödyntämään monenlaisissa kohteissa, kuten itseohjautuvien autojen kehityksessä (Tesla 2024) ja lääketieteessä diagnoosin tunnistamisessa tai hoitokeinojen

valitsemisessa (Alowais et al. 2023). Tämän työn tarkoituksena on tutkia erilaisia mahdollisuuksia hyödyntää tekoälyä kyberturvallisuuden parantamiseen ja tarkastella kriittisesti, millaisia hyötyjä ja riskejä siihen sisältyy, sekä voidaanko organisaatioiden työvoimapulaa helpottaa tekoälyä hyödyntämällä.

1.1 Tutkimuksen tausta

Tutkimuksen aiheeksi on valittu kyberturvallisuuden parantaminen tekoälyn avulla. Digitalisaation myötä organisaatioiden, sekä yksityishenkilöiden jokapäiväinen toiminta on hyvin riippuvaista digitaalisista palveluista (Abbas et al. 2022). Monet palvelut, kuten verkkopankki ja Kansaneläkelaitos, vaativat sähköisen tunnistautumisen käyttäjältään, että hän pääsee sisään järjestelmään ja käyttämään palvelua omalla henkilöllisyydellään.

Palveluiden toimiminen digitaalisesti verkossa luo uusia mahdollisuuksia, mutta se myös altistaa ne täysin uusille vaaroille, kuten kyberhyökkäyksille. Internetistä riippuvaiset toiminnot ovat nykypäivänä yleisiä, jolloin niiden toimivuus ja turvallinen käyttö on varmistettava. Myös iso osa valtiollisista kriittisestä infrastruktuurista on sähköistetty ja liitettynä internettiin mikä luo tarpeen turvata niiden toimivuus myös erilaisten kriisien aikana, jotta kansallinen turvallisuus säilyy. (F-Secure 2024)

Tekoälyn hyödyntäminen kyberturvallisuuteen voisi sekä parantaa nykyistä kyberturvallisuutta, mutta myös helpottaa alalla esiintyvää pulaa osaavista työntekijöistä. Tekoälyn avulla ainakin osan ihmisen tekemästä työtaakasta voisi ulkoistaa tekoälylle, jolloin pula kyberturva-ammattilaisista voisi helpottua.

1.2 Tutkimusongelma

Tässä kandidaatintyössä tutkitaan tekoälyn hyödyntämismahdollisuuksia kyberturvallisuuden parantamiseen. Tutkimuksen tarkoituksena on koota tietoa alan kirjallisuudesta ja nykytilanteesta, miten tekoälyä hyödynnetään organisaatioissa kyberturvallisuuden parantamiseen.

Päätutkimuskysymyksenä on

- Miten tekoälyä voidaan hyödyntää kyberturvallisuuden parantamiseen?

Päätutkimuskysymystä on tutkimuksessa tarkennettu hyödyntämällä alakysymyksiä, jotka ovat

- Mitä kyberturvallisuudella tarkoitetaan ja miten sitä voidaan parantaa?

- Mitä hyötyjä tekoäly tuo kyberturvallisuuden parantamiseen?
- Millaisia vaaroja tai riskejä tekoälyn käyttö sisältää?
- Miten tekoälyä hyödynnetään tällä hetkellä kyberturvallisuuden parantamiseen?

Tutkimusta tehtiin etsimällä tutkimuskysymykseen vastaus hyödyntämällä tieteellisiä artikkeleja aihealueesta. Alatutkimuskysymyksiä hyödyntämällä aihetta on pilkottu pienempiin osiin, jonka tutkimus etenee sujuvasti ja tutkimuskysymykseen on helpompi löytää vastauksia.

1.3 Tutkimuksen rakenne

Tutkimuksen toisessa osiossa esitellään valitut tutkimusmenetelmät, sekä tutkimuksessa käytetty aineisto ja miten se on valittu. Tutkimuksen kolmas osio keskittyy kyberturvallisuuteen. Osiossa määritellään kyberturvallisuus, sekä esitellään, miten kyberturvallisuuteen voidaan vaikuttaa ja miten sitä voidaan parantaa.

Työn neljäs osio keskittyy tekoälyyn. Osion ensimmäisessä luvussa määritellään tekoäly käsitteenä ja esitellään, miten tekoälyä voidaan hyödyntää erilaisissa käyttötarkoituksissa. Seuraava luku keskittyy esittelemään, kuinka tekoälyä voidaan hyödyntää kyberturvallisuuteen liittyvissä asioissa.

Viimeisessä osiossa on tehty yhteenveto tutkimuksen keskeisistä löydöistä ja koottu yhteen, miten tekoälyä voidaan hyödyntää kyberturvallisuuden parantamiseen. Viimeisessä luvussa on esitetty mahdollisia jatkotutkimusaiheita.

2. TUTKIMUSMENETELMÄT JA -AINEISTO

2.1 Tutkimusmenetelmä

Kandidaatintyön tutkimusmenetelmänä on kirjallisuuskatsaus, jonka aineistona on käytetty pääasiallisesti vertaisarvioituja tieteellisiä artikkeleja. Tutkimusongelmaan on lähdetty etsimään vastauksia lukemalla useita tieteellisiä artikkeleja, jotka käsittelevät aihealuetta.

Alkuvaiheessa tietoa etsiessä on myös hyödynnetty Scopus AI:ta, jonka avulla löysi hyviä artikkeleja, joiden avulla pystyin luomaan hyvän viitekehyksen, jonka ympärille tutkimusta lähdettiin tekemään. Scopus AI:lla on etsitty lähteitä esimerkiksi hakulauseilla ”Can you make cybersecurity better using ai? ja ”is artificial intelligence being used to cybersecurity?”.

2.2 Tutkimusaineisto

Tutkimusaineistoa on etsitty pääasiallisesti Andor-, Scopus ja Google Scholar -tietojärjestelmistä hyödyntämällä niiden hakuominaisuuksia. Lähteitä on etsitty pääsääntöiseksi vain englanniksi, sillä alan kirjallisuus on ensisijaisesti kirjoitettu englanniksi. Mahdollisimman ajankohtaisten ja luotettavien lähteiden löytämiseksi hakua on rajattu niin, että se sisältää vain tieteellisiä vertaisarvioituja tekstejä. Lisäksi hakuvaiheessa on karsittu lähteitä myös julkaisuvuoden perusteellä, jotta lähteet olisivat mahdollisimman ajankohtaisia. Tietolähteitä etsiessä eri tietokannoista rajaukseksi on valittu vuodesta 2019 eteenpäin tehdyt vertaisarvioidut julkaisut. Tutkimusaineisto on valikoitu niin, että se sisältää vain maksimissaan 5 vuotta vanhoja julkaisuja, koska tutkimusmateriaalia löytyy eri tietokannoista todella paljon ja siksi, että tekoäly kehitys on ollut viime vuosina hyvin nopeaa ja tässä kirjallisuuskatsauksessa on haluttu käyttää mahdollisimman ajankohtaista aineistoa hyväksi. Yli 5 vuotta vanhat julkaisut tekoälyyn liittyen voivat sisältää jo vanhentunutta tietoa.

Tutkimusaineistoa kerätessä mielenkiintoiset ja ajankohtaiset julkaisut, joiden otsikot ovat osuvia ja liittyneet tutkimusongelmaan ovat valikoituneet tarkempaan tarkasteluun, jolloin niiden tekstien tiivistelmät ja johtopäätökset ovat luettu tarkemmin läpi ja tutkittu soveltuuko julkaisu ja sen aihealue tutkimukseen. Soveltuvat lähteet ovat otettu ylös, jotta niihin palaaminen myöhemmin on helpompaa. Myös hyviä hakusanoja ja hakusuodattimia on kirjattu ylös muistiin. Seuraavassa taulukossa on esimerkkejä käytetyistä hakusanoista. Aihealueena tekoäly ja kyberturvallisuus ovat olleet viime vuosina

hyvin tutkittuja aiheita, jonka seurauksena niistä löytyy hyvin paljon erilaisia tutkimusraportteja ja artikkeleja.

Hakulauseke	Andor	Scopus	Google Scholar
"cybersecurity" AND ("artificial intelligence" OR "AI")	5 228	4 204	17 800
“robust cybersecurity” AND ("artificial intelligence" OR "AI")	34	48	1 300
cybersecurity AND ("machine learning" OR "deep learning")	5 158	8 116	17 300
“utilizing AI in cybersecurity”	79	150	13 000
utilizing ("AI" OR "artificial intelligence") in cybersecurity AND threat	49	28	9 400

***Taulukko 1**: Hakulausekkeilla löytyvien artikkelien määrät eri tietokannoissa*

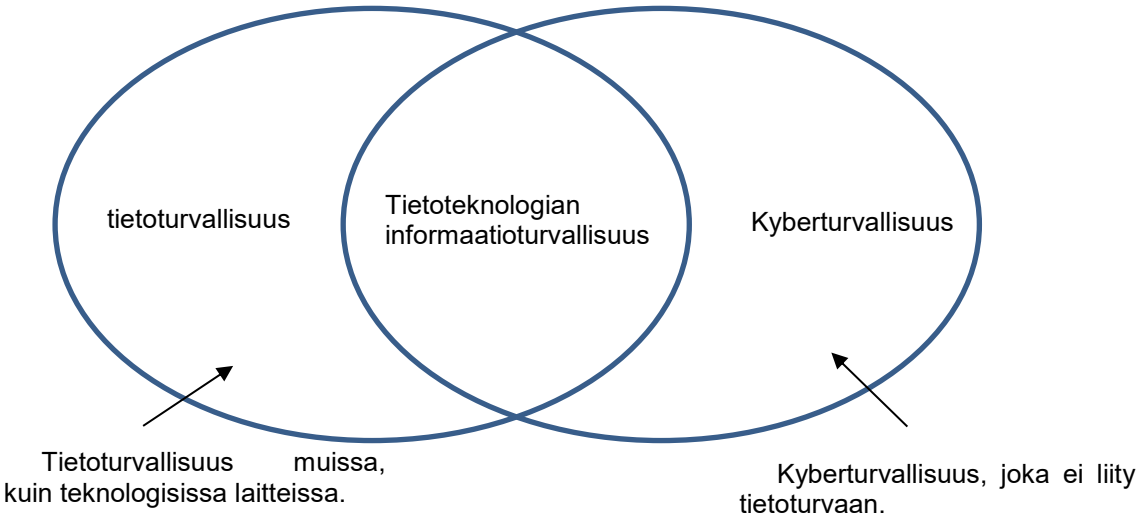
Yllä olevasta taulukosta huomataan, että englanninkielistä aineistoa on hyvin paljon tietokannoissa saatavilla. Hakulausekkeiden sanavalinnat pohjautuvat alan kirjallisuuteen ja niissä säännöllisesti esiintyviin sanavalintoihin, kuten ”*robust*”. Hakulausekkeissa on hyödynnetty tietokantojen Boolen operaattoreita AND ja OR, jonka avulla hakulausekkeet ovat tarkempia ja rajaavat aineistoa tehokkaammin.

3. KYBERTURVALLISUUS

Kyberturvallisuus tarkoittaa toimia, joita tarvitaan verkko- ja tietojärjestelmien, niiden käyttäjien ja asianosaisten henkilöiden suojaamiseksi kyberhyökkäyksiltä (Eurooppa-neuvosto 2024; F-Secure 2024). Kyberturvallisuus (cybersecurity) ja tietoturvallisuus (information security) ovat käsitteinä hyvin lähellä toisiaan ja arkikielessä niitä saatetaan käyttää ristiin.

Tietoturvallisuusuudella tarkoitetaan tiedon saatavuuden, luottauksellisuuden ja eheyden ylläpitämistä (Helenius 2024). Tietoturvan tehtävänä on huolehtia, ettei tieto ole vääristynyttä ja että siihen ei pääse ulkopuoliset käsiksi. Tieto voi olla niin digitaalisessa kuin fyysisessä muodossa, jolloin tietoturvalla eri ulottuvuuksia digitaalisen ja fyysisen maailman välillä.

Koska kyberturvallisuus keskittyy vain digitaaliseen ympäristöön, voidaan katsoa, että se on käsitteenä suppeampi termi kuin tietoturvallisuus. Alla olevassa kuvassa 1 on kuvattu tietoturvallisuuden ja kyberturvallisuuden käsitteitä venn-diagrammin avulla ja havainnollistettu, kuinka termit liittyvät toisiinsa.



Kuva 1. *Venn-diagrammi tieto- ja kyberturvallisuuden käsitteistä*

Helenius kuvaa Kyberturvallisuus 1 -kurssilla, että kyberturvallisuuden määritelmä ei ole yhtä konkreettinen kuin tietotuvallisuuden, vaan sillä kuvataan abstraktimpaa tavoitetilaa (Helenius 2024). Sarker (2022) kuvaa kyberturvallisuutta 0-toleranssi alaksi. Tämä tar-

koittaa sitä, että 1 onnistunut kyberhyökkäys voi lamauttaa koko organisaation ja aiheuttaa suuret vahingot koko organisaatiolle. Tästä syystä kyberturvallisuuden tulisi olla hyvin kokonaisvaltainen ja ennakoiva järjestelmä, jolla varmistetaan, että kyberhyökkäyksiä kohtaan osataan varautua ja torjua.

3.1 Käyttäjän vaikutus kyberturvallisuuteen

Käyttäjän vaikutus kyberturvallisuuteen on valtava. Suurin osa kyberhyökkäyksistä kohdistuu nykyään suoraan käyttäjään ja sen toimintaan, eikä itse laitteeseen tai tietoverkkoon, sillä käyttäjän toiminnasta löytyy yleensä eniten haavoittuvuuksia. (Mashiane & Kritzinger 2018). Ihminen pystyy omalla käytöksellään tahallaan tai tahattomasti vaikuttamaan negatiivisesti omaan tai organisaationsa kyberturvallisuuteen, vaikka laite tai tietoverkko olisi muuten turvallinen käyttää ja kyberturvallinen. Käyttäjän tulisi ymmärtää, että hänen toiminnallaan on hyvin suuri vaikutus hänen omaan kyberturvallisuuteensa ja esimerkiksi organisaatioissa toimiessaan hän käytös voi pahimmassa tapauksessa vaarantaa koko organisaation toiminnan. (Li et al. 2019)

Organisaatiot pystyvät suojautumaan erilaisilta kyberuhilta esimerkiksi rajoittamalla työntekijän pääsyä vaarallisille sivustoille, vaatimalla käyttäjältä riittävän turvallista salasanaa ja vaihtamaan sitä säännöllisesti tai käyttämällä erilaisia tietovuotojärjestelmiä (Li et al. 2019). Inhimilliset virheet, sekä huolimattomuus vaikeuttavat kyberturvallisuuden ylläpitoa ja se on suuri haaste organisaatioissa, vaikka siellä olisi käytössä todella hyvät suojaukset verkkoihin ja tietojärjestelmiin.

Li et al. (2019) mukaan turvatoimet tietoturvan ja kyberturvallisuuden eivät aina pysty toimimaan tehokkaasti, koska työntekijät eivät kiinnitä tarpeeksi huomiota heidän organisaationsa tietoturvakäytäntöihin. Monet työntekijät saattavat myös aliarvioida tietoturvariskejä, vaikka he saisivat koulutusta aiheesta ja saisivat ohjeet, miten tulisi toimia vaarantamatta tietoturvaa.

Monet laitteet saavat päivityksiä niiden ohjelmistoon vielä sen jälkeen, kun se on ostettu kaupasta. Näillä päivityksillä usein parannetaan laitteen tietoturvaa ja tukitaan tietoturvaaukkoja, jos laitteesta tällaisia on löytynyt. Käyttäjän tulisi pitää huolta, että laite on aina päivitetty uusimpaan versioon, koska muuten laitteen käyttö voi vaarantaa oman, sekä pahimmillaan kaikkien muiden samassa verkossa olevien käyttäjien kyberturvallisuuden.

3.2 Teknisten laitteiden kyberturvallisuus

Esineiden internet on mahdollistanut ihmisille arkielämään uusia innovaatioita, kuten älypuhelimet ja kellot. Internettiin yhdistetyt laitteet ovat mahdollistaneet ihmisille uusia mukavuuksia ja voi tehostaa niiden käyttöä, mutta se myös altistaa laitteet uusille kyberuhille.

Digitalisaation ja esineiden internetin takia yhä useampi laite on liitettynä internettiin ja ne ovat integroitu jokapäiväiseen elämään. Älylaitteet mahdollistavat monia mukavuuksia ja niiden avulla voidaan automatisoida monia toimintoja, sekä optimoida ja säästää energiaa. (Tenkanen et al. 2018) Älykodin avulla voidaan automatisoida, sekä esimerkiksi käyttää erilaisia toimintoja etänä älypuhelimen avulla, kuten valojen sammuttaminen tai ulko-oven lukitseminen, mutta ne myös altistavat laitteet uusille täysin uusille kyberturvallisuusuhille. Vaikka älykodin sovellukset voivat lisätä perinteistä turvallisuutta erilaisilla uusilla keksinnöillä, kuten älylukoilla, niihin liittyvät tietoturva- ja kyberturvallisuusriskit kasvavat merkitsevästi (Tenkanen et al. 2018).

Kun kodin älylaitteet yhdistetään internettiin, yleensä ne laitetaan kaikki samaan langattomaan verkkoon. Tämä mahdollistaa laitteiden toimimisen hyvin yhteen ja niiden välisen tiedonsiirron, mutta samalla niiden tietoturva, sekä kyberturvallisuus heikkenee. Koska kaikki laitteet ovat liitettynä samaan verkkoon, altistuvat kaikki laitteet vaaralle, jos verkkoon pääsee tunkeilija. (Tenkanen et al. 2018) Kyberhyökkäyksen kohteena voi olla mikä vain laite, joka on liitettynä samaan tietoverkkoon, kuten esimerkiksi kopiokone. Jos kopiokoneen oma kyberturva ei ole riittävän hyvä, tämä altistaa kyseisen laitteen kyberhyökkäyksille, mutta myös tämän laitteen kautta koko tietoverkko voi olla vaarassa ja verkon kautta hyökkääjä voi päästä käsiksi muihin laitteisiin ja tietovarastoihin.

Vaikka kyberturvallisuudella tarkoitetaan vain suojaamista digitaalisia uhkia vastaan, sillä voi olla myös hyvin suoria vaikutuksia fyysiseen turvallisuuteen. Kriittisen infrastruktuurin, kuten energiaverkkojen suojaamattomuus voi johtaa energiaverkkojen kaatumiseen, jolloin laajat sähkökatkokset voivat estää sairaaloiden tai muiden yhteiskunnallisesti kriittisten toimintojen toimivuuden. Myös älykotien järjestelmiin, kuten lukitusjärjestelmään tai turvallisuusvalvontajärjestelmiin kohdistuvat hyökkäykset voivat vaarantaa ihmisten fyysisen turvallisuuden.

Vaikka kyberhyökkäykset kohdistuvat usein laitteisiin, jotka ovat yhdistettynä internettiin, myös muihin sähköisin laitteisiin voi kohdistua hyökkäysyrityksiä. Laitteisiin voidaan

päästä käsiksi fyysisesti esimerkiksi USB-portin kautta, joka voi mahdollistaa ulkopuolisen pääsyn laitteeseen ja sen tietoihin.

3.3 Kyberturvallisuuden parantaminen

Kyberturvallisuus koostuu monesta eri osa-alueesta, jotka yhdessä muodostavat holistisen kokonaisuuden, jonka avulla kyberhyökkäyksiä pystytään torjumaan ja ennakoimaan, mutta myös minimoimaan mahdolliset vahingot. Ihmiset ovat käyttäjän roolissa isossa vastuussa niin omasta kuin myös organisaatioiden kyberturvallisuudesta. Kyberturvallisuutta parantaessa on otettava huomioon ihmiset ja niiden käytös.

Ihmiset nähdään usein heikoimpana lenkkinä kyberturvallisuuden ylläpitämisessä, mutta hyvällä koulutuksella ja harjoittelulla he voivat olla myös ensimmäisenä vaikuttamassa positiivisesti kyberturvallisuuteen (Zimmermann 2019). Ihmisten koulutuksella on valtava merkitys ja heidän toimintansa vaikuttaa suoraan turvallisuuteen organisaatioissa. Koska suurin osa kyberhyökkäyksistä kohdistetaan suoraan tai epäsuorasti käyttäjään, on tärkeää, että hän ymmärtää kyberturvallisuuden perusperiaatteita ja osaa toimia turvallisesti ilman että vaarantaa kyberturvallisuutta organisaatiossa (Mashiane & Kritzinger 2018). Kouluttamalla ihmisiä ja opettamalla heidät toimimaan verkossa ja eri tietojärjestelmissä on tärkeä osa kyberturvallisuuden parantamista.

On myös hyvin tärkeää, että kehittää järjestelmistä ihmisläheisempiä ja ottaa suunnitteluvaiheessa huomioon, että järjestelmän käyttäjät ovat ihmisiä ja he voivat tehdä inhimillisiä virheitä varsinkin, jos käyttäjällä ei ole aikaisempaa kokemusta tai osaamista liittyen järjestelmiin tai kyberturvallisuuteen. (Zimmermann 2019) Tämä lisää järjestelmien helppokäyttöisyyttä ja mahdollistaa käyttäjien turvallisen toimimisen.

Organisaatioissa tietoturvaa voidaan parantaa ottamalla käyttöön käytäntöjä ja strategioita, joilla lähdetään parantamaan kyberturvallisuutta organisaatioissa järjestelmällisesti ja määrätietoisesti.

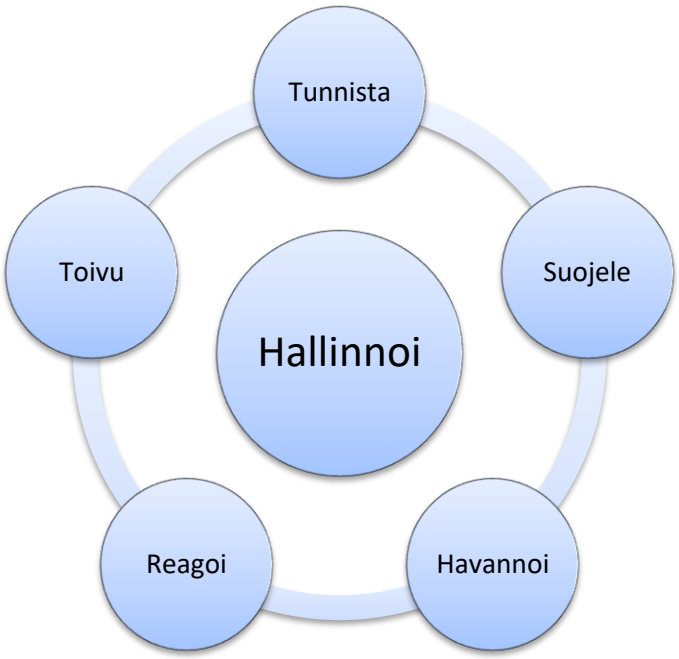
Hyödyntämällä saatavilla olevia kyberturvallisuusstandardeja organisaatiot voivat varmistaa, että heidän käytäntönsä ovat turvallisia. Yksittäiset standardit eivät kuitenkaan välttämättä kata koko organisaation toimintaa, jolloin heidän on usein hyödyllistä yhdistää useampaa eri standardia, jolloin he voivat varmistaa, että heidän toimintansa on varmasti turvassa kyberhyökkäyksiltä. (Taherdoost 2022)

Yhdysvalloissa NIST (The National institute of Standards and Technology at the U.S. Department of Commerce) eli kansallinen standardien ja teknologian instituutti on kehittänyt viitekehyksen, jonka tarkoituksena on auttaa organisaatioita hallitsemaan kyberturvallisuutta. (Taherdoost 2022)

vallisuuteen liittyviä riskejä. Viitekehyksen tarkoituksena on auttaa erikokoisia organisaatioita ymmärtämään ja hallitsemaan omaa kyberturvallisuuttaan ja varmistamaan, että heidän oma suojauksensa tietoverkkoihin ja laitteisiin on hyvällä tasolla. (U.S. Department of Commerce 2024) Alun perin kriittisen infrastruktuurin suojaamiseen kehitetty viitekehys on levinnyt myös muuhun käyttöön sen soveltuvuuden vuoksi.

NIST:n kehittämä viitekehys CSF (Cyber Security Framework) on päivitetty helmikuussa 2024 versioon 2.0 ja sen mukana viitekehykseen on lisätty hallinnoinnin osa-alue (governance). Päivityksen myötä viitekehys auttaa integroimaan organisaatioiden kyberturvallisuuden paremmin osaksi liiketoimintaa. Tämä viitekehys onkin hyvin suosittu ja useat organisaatiot käyttävät sitä omassa toiminnassaan.

CSF 2.0 koostuu kuudesta osa-alueesta, jonka tarkoituksena on tarjota organisaatioille kokonaisvaltainen rakenne kyberturvallisuuden parantamiseen. Malli on kuvattu alla olevassa kuvassa 2 ja se tehty instituutin oman havainnekuvan pohjalta. Ensimmäinen osa-alue on viitekehyksen ydin, hallinnoi. Tämän osa-alueen tarkoituksena on sitoa kyberturvallisuusstrategia osaksi organisaation laajempaa riskienhallintaa ja visiota. Viitekehyksen ulkokehällä olevat osa-alueet tunnista (indentify), suojele (protect), havainnoi (detect), reagoi (respond) ja toivu (recover) muodostavat kokonaisuuden, joka auttaa organisaatioita luomaan strategian, joka ennakoi ja auttaa varautumaan mahdollisiin riskeihin, mutta myös mahdollisiin kyberhyökkäyksiin. (U.S. Department of Commerce 2024)



Kuva 2. *NIST 2.0 viitekehys.*

Euroopan unionin kyberturvallisuusvirasto ENISA (European Union Agency For Cybersecurity) on virasto, joka säätelee Euroopan unionin jäsenvaltioita kyberturvallisuuteen liittyen. ENISA on määrittänyt esimerkiksi kyberturvallisuussertifikaatin, jonka tarkoituksena on varmistaa, että EU:n alueella myydyissä ja käytetyissä laitteissa on huomioitu kyberturvallisuus ja että niitä on turvallista käyttää. Sertifikaatti yhtenäistää EU:n alueella toimivien tahojen kyberturvallisuuskäytäntöjä ja auttaa varmistamaan, että organisaatiot ja eri tahot ovat suojautuneet riittävän hyvin mahdollisia kyberhyökkäyksiä vastaan. (Euroopan komissio 2024)

ENISAN kehittämä viitekehys auttaa Euroopan unionin maita kehittämään kyberturvallisuusstrategian kansallisella tasolla. Strategiamalli on jaettu neljään päävaiheeseen. Ensimmäisessä vaiheessa kehitetään strategia, jonka mukaan kyberturvallisuutta lähdetään kehittämään. Tämän jälkeen toisessa vaiheessa otetaan käyttöön käytännössä tämä kehitetty strategia ja lähdetään toteuttamaan strategian mukaisia vaiheita. Kolmannessa vaiheessa arvioidaan strategiaa ja sen toimivuutta käytännössä ja tutkitaan, tarvitseeko mallia muuttaa. Viimeinen vaihe keskittyy ylläpitämään käytössä olevaa strategiaa. Viitekehys esitetty alla olevassa kuvassa 3.

Kuva 3. *ENISA:n kyberturvallisuuden strategian elinkaarimalli (ENISA 2016)*

Jokaiseen vaiheeseen liittyy palautteen kerääminen ja vaiheen kehittäminen paremmaksi. Strategiamalli pohjautuu jatkuvaan kehittämiseen, jonka avulla varmistetaan, että kyberturvallisuus ei jää kansallisella tasolla jälkeen kehityksestä. (ENISA 2024)

.

4. TEKOÄLY

4.1 Tekoäly ja sen määritelmä

Tekoäly on tietokonejärjestelmä, joka jäljittelee ihmisen kognitiivisia toimintoja. Järjestelmä pystyy oppimaan, päättelemään ja ratkaisemaan sille annettuja ongelmia (Copeland 2024). Tekoäly pystyy suorittamaan tehtäviä ja käyttämään niiden suorittamiseen sille syötettävää dataa tai internetistä löytyvää materiaalia. Tekoäly ei pysty kuitenkaan tehdä johtopäätöksiä tai ratkaisemaan ongelmia, joita sitä ei ole suunniteltu tekemään (Vähä-Sipilä et al. 2021).

Tekoälyn vahvuus ihmiseen verrattuna on sen kyky käsitellä dataa nopeammin ja väsymättä (Vähä-Sipilä et al. 2021). Tekoälyä voidaan hyödyntää esimerkiksi toistuvien rutiinitehtävien automatisointiin tai koneoppimiseen ja analytiikkaan, jossa tekoäly hyödyntää valtavaa määrää dataa ja analysoi sitä.

Koneoppimista voidaan pitää tekoälyn yhtenä alalajina (Vartiainen et al. 2021; Zhou, Z. & Liu, S. 2021). Koneoppimisella tarkoitetaan tietokoneen kykyä tehdä päätöksiä ilman, että niitä on erikseen ohjelmoitu jokaista tilannetta varten (Vartiainen et al. 2021). Koneoppimisessa tekoälymallit rakennetaan syöttämällä tietokoneelle dataa ja sen pohjalta opetetaan, miten tällaista dataa pitäisi analysoida. Jatkossa tietokone osaa samantyyppisissä ongelmissa ratkaista ongelman tai analysoida dataa pohjautuen opetettuun mallin. Koneoppimisen yksi suurimmista hyödyistä on sen soveltuvuus, jossa kyseistä ilmiötä ei ymmärretä tarpeeksi hyvin tai sen mallintaminen on liian työlästä, mutta siitä on saatavilla riittävästi dataa (Vartiainen et al. 2021).

Tekoälyn läpimurto tapahtui 2010-luvun alussa, kun digitaalisen datan määrä alkoi lisääntyä räjähdysmäisesti ja tietokoneiden laskentateho alkoi parantua vauhdilla (Vartiainen et al. 2021; Emmert-Streib et al. 2020). Syväoppiminen (eng. deep learning) on yksi koneoppimisen opetusmalli, jonka juuret ulottuvat 1950-luvulle, mutta tietokoneiden laskentatehon parantuessa se on mahdollistanut tekoälyjen suuren kehityksen 2010-luvun aikana. Syväoppimisessa tietokone muodostaa monikerroksisia keinotekoisia neuroverkkoja ja hyödyntää niitä datan analysointiin ja päätöksentekoon. (Emmert-Streib et al. 2020) Syväoppimisen avulla tekoäly pystyy käsittelemään suuria määriä dataa ja tunnistamaan, sekä analysoimaan sen perusteella monimutkaisia riippuvuussuhteita datasta.

4.2 Tekoälyn hyödyntäminen kyberturvallisuuteen

Viimeisen 5 vuoden aikana on ollut huomattava nousu tekoälyn hyödyntämisessä kyberturvallisuusalalla. Tämä on johtunut siitä, että käytössä olevan datan määrä on noussut hyvin voimakkaasti ja samaan aikaan erilaiset tekoälyalgoritmit ovat kehittyneet, jonka ansiosta ne ovat käyttökelpoisempia kyberturvallisuuden parantamiseen. Lisäksi kyberuhat ovat muuttuneet yhä monimutkaisemmiksi, jolloin niiden torjumiseen on etsitty uudenlaisia keinoja, joista tekoäly ja sen alalaji koneoppiminen on osoittautunut hyvin käyttökelpoiseksi. (Shanthi 2023)

Kyberturvallisuuteen ja sen ylläpitämiseen liittyy monia tehtäviä, jotka vaativat rutiininomaisia työvaiheita, sekä paljon manuaalista työtä. Tekoälyn avulla tällaisia työvaiheita pystytään kokonaan automatisoimaan, sekä käyttäjä voi tekoälyä voidaan hyödyntää aputyökaluna. (Dambe et al. 2023; Gafni & Levy 2024)

Tekoälyn avulla ei kuitenkaan pystytä kokonaan korvaamaan kyberturva-asiantuntijoita. Gafnin (2024) tekemässä tutkimuksessa tutkittiin ChatGPT 3.5 version hyödyntämistä kyberturvallisuuteen. Tutkimuksessa löydettiin, että tekoälyä pystyttiin hyödyntämään jollain tasolla kaikkiin mekaanisiin ja rutiininomaisiin työvaiheisiin kyberturva-ammattilaisen työssä. Generatiivista tekoälyä, kuten tutkimuksessa käytetty Chat GPT:ä ei kuitenkaan pystytty hyödyntämään organisaation kyberturvallisuusammattilaisen asiantuntijatehtäviin tai johtajan työtehtäviin. Organisaatioissa tekoälyä voidaan hyödyntää auttamaan asiantuntijoita työtaakan kanssa ja automatisoimaan tiettyjä työtehtäviä, mutta tekoälyn avulla kyberturvallisuuden työtehtäviä ei voida kuitenkaan kokonaan korvata (Gafni & Levy 2024).

Verkkohyökkäyksiä vastaan voidaan käyttää tunkeilijan havaitsemisjärjestelmää, jonka avulla voidaan tunnistaa, jos verkkoon kohdistuu hyökkäys. Järjestelmän toiminta perustuu tietoverkon toiminnan seuraamiseen ja se analysoi verkon toimintaa ja pyrkii löytämään sieltä toimintaa, joka muistuttaa tunnettuja verkkohyökkäysmalleja. Hyödyntämällä erilaisia koneoppimismalleja, kuten syväoppimista, tekoälyn avulla voidaan myös tunnistaa normaalista poikkeavaa käytöstä ja hälyttää järjestelmänvalvojaa mahdollisesta uhasta. (Shah 2017) Automatisoitu tunkeilijan havaitsemisjärjestelmä vapauttaa resursseja organisaatiossa ihmiseltä, sekä mahdollistaa suurien datajoukkojen tehokkaan ja nopean analysoimisen.

4.3 Hyödyt

Tekoälyyn liittyvät teknologiat ja sovellukset auttavat organisaatioita tehostamaan ja parantamaan omaa toimintaansa. Hyödyntämällä tekoälyä organisaation kyberturvallisuusstrategiaan voidaan helpottaa tämänhetkistä kroonista työvoimapulaa, pienentää organisaatioiden kustannuksia, sekä vahvistaa nykyistä turvallisuutta.

Manuaalista työtä, kuten datan analysoimista, voidaan automatisoida hyödyntäen tekoälyä. Tekoälyn hyödyllisyys automatisoidessa tulee siitä, että tekoäly pystyy tekemään useita työtehtäviä nopeammin kuin ihminen. Kun ihminen tekee työtä, se voi väsyä ja alkaa tekemään huolimattomuusvirheitä, mutta tekoälyn avulla tällaiset virheet voidaan poistaa. (Akhtar & Rawol 2024)

Automatisoimalla tekoälyllä perinteisiä kyberturvallisuuskäytänteitä, kuten tunkeilijan havaitsemisjärjestelmiä voidaan vähäentää ihmisen tekemiä inhimillisestä huolimattomuudesta tai väsymyksestä aiheutuneiden riskien määrää. Inhimilliset tekijät ovat yksi suurimpia turvallisuusriskeihin liittyviä tekijöitä, jolloin niiden vähentäminen mahdollistaa kyberturvallisuuden parantamisen. (Mashiane & Kritzinger 2018)

Onnistuneella AI:n integroinnilla kyberturvallisuuteen voidaan saada aikaan säästöjä. Kyberturvallisuuden eri prosesseissa ei enää tarvita niin paljon työntekijöitä, jolloin organisaatiot voivat vähentää heidän työvoimakustannuksiaan. (Falowo 2024) Tehokkaan kyberturvallisuuden ansiosta myös riski joutua kyberhyökkäyksen kohteeksi pienenee merkittävästi, jolloin voidaan estää ennakoivasti syntyviä kustannuksia, jos organisaation liiketoiminta estyy.

Koska tekoäly pystyy käsittelemään valtavia datajoukkoja tehokkaasti hyvällä tarkkuudella ja nopeasti, tekoälyä voidaan hyödyntää edistyneissä uhantunnistusjärjestelmissä. Syväoppiminen mahdollistaa tekoälylle muodostaa hyvin kehittyneitä algoritmeja, joilla se pystyy havaitsemaan erikoista tai uhkaavaa käytöstä tietoverkossa. (Tlachenska 2024) Syväoppimisen avulla tekoäly pystyy tekemään monimutkaisia malleja ja algoritmeja, joiden avulla se pystyy oppimaan ja tulkitsemaan valtavia datajoukkoja ja löytämään sieltä uusia havaintoja, joita ihminen ei pystyisi löytämään.

4.4 Haasteet

Tekoälypohjaiset ratkaisut ovat vaikea rakentaa organisaatioissa, koska uusien kyberturvallisuusstrategioiden käyttöönotto on hidasta ja vaatii paljon resursseja. Organisaatioissa, joissa ei entuudestaan ole käytetty tekoälyä missään organisaatioiden toiminnassa, on vaikea lähteä kehittämään tai ottamaan käyttöön, sillä tekoälyratkaissut vaativat erilaisia ammattialisia, jotka osaavat käyttää tekoälyä ja luoda siitä hyödyllisen työkalun kyberturvallisuuskäyttöön. AI:n integroiminen käyttöön vaatii niin työntekijäosaamista, mutta myös infrastruktuurin, joka mahdollistaa tekoälyn käytön organisaatioissa. (Srivastava & Stager 2024). Myös organisaatioiden on hyvin vaikea yrittää integroida tekoälyä nykyisiin kyberturvallisuuskäytäntöihin, sillä tekoälyä ei ole suunniteltu alun perin käytettäväksi niihin.

Tekoälyalgoritmien rakentamien vaatii hyvin paljon laadukasta dataa. Kyberturvallisuusalalla käytettävissä oleva data on kuitenkin usein hyvin vaihtelevaa ja yhteensopimatonta, jonka takia algoritmien rakentamien voi olla hankalaa. Lisäksi dataa ei välttämättä ole aina tarpeeksi käytössä, jolloin algoritmia ei pystytä kehittämään (Nour & Said 2024). Algoritmin toimiessa huonosti sen toimintatarkkuus heikkenee ja se tekee todennäköisemmin vääriä päätelmiä tai hälytyksiä. Tämä luo suuria haasteita automatisoinnille kyberturvallisuusalalla, jos tekoäly ei toimi kunnolla tai sen tekemiin hälytyksiin ei voida luottaa.

Ihmisen ja tekoälyn yhteistyö voi olla myös haaste. Koska tekoälyä käytetään apuvälineenä ja sillä voidaan esimerkiksi automatisoida erilaisia työvaiheita, on tärkeää, että ihminen, joka sitä käyttää voi ymmärtää tekoälyä ja sen tekemiä ratkaisuja. Monet tekoälyn ratkaisut voivat näyttää ihmisestä hyvin kummalliselta, eikä ihminen välttämättä pysty ymmärtämään miten tekoäly on päätynyt tiettyyn ratkaisuun. Tämä luo haasteita kyberammattilaiselle luottaa ja tehdä tekoälyn ehdottamia toimenpiteitä. (Nour & Said 2024)

Algoritmeihin perustuvan päätöksenteon haittapuolena on se, ettei tekoäly pysty perustelemaan omaa valintaansa tällä hetkellä. Algoritmin opetusvaiheessa syötettävän data ei saa olla syrjivää tai vinoutunutta, jotta algoritmi ei opi tekemään päätöksiään esimerkiksi suosimalla jotain valintoja. (Seung 2022) Algoritmeja kehittäessä pitää olla hyvin tarkka ja varovainen datan suhteen, että se vastaa todellisia tilanteita, ettei algoritmi ala syrjiä tai suosia erilaisia tilanteita opetusdatan perusteella.

Tekoälyä voidaan myös hyödyntää kyberhyökkäyksissä, joka luo uusia haasteita organisaatioille suojautua vaaroilta. Shang ennustaa tutkimuksessaan (2024), että kyberhyökkäyksistä tulee tulevaisuudessa entistä monimutkaisempia, sekä vaikeampia torjua, sillä tekoälyn avulla voidaan esimerkiksi etsiä haavoittuvuuksia organisaatioiden kyberturvallisuudesta.

5. YHTEENVETO

5.1 Päätelmät

Monissa organisaatioissa hyödynnetään jo jollain tasolla tekoälyä kyberturvallisuuteen liittyvissä työtehtävissä. Etenkin rutiininomaiset ja paljon mekaanista työtä vaativat työvaiheet voidaan automatisoida hyödyntämällä tekoälyä. Tekoäly on loistava apuväline kyberturvallisuudessa.

Viimeisen 10 vuoden aikana tekoälyn kehitys on ollut todella suurta ja uudet sovellukset ovat mahdollistaneet paljon uusia tekoälyn sovelluskohteita. Uudet koneoppimismallit, kuten syväoppiminen, mahdollistavat uusien ja tehokkaiden hyökkäysten tunnistamis- ja estojärjestelmien valmistamisen. Uudet tekoälyt pystyvät analysoimaan ja hyödyntämään suuria datasettejä tehokkaammin kuin ihminen, jonka ansiosta AI:lla toimivat järjestelmät voivat olla huomattavasti tehokkaampia ja havaita paremmin epänormaalia käytöstä verkossa tai hyökkäysyrityksiä kuin ihmisen.

Kyberturvallisuusalan tämänhetkiseen krooniseen työvoimapulaan tekoäly tarjoaa helpotusta. Tekoälyn avulla manuaalisia työvaiheita voidaan automatisoida, joka vapauttaa resursseja ihmiseltä, jolloin työntekijä voi käyttää oman aikansa tehokkaammin esimerkiksi kriittiseen ajatustyöhön tai ongelmanratkaisuun. Työvaiheiden automatisointi voi vähentää henkilökunnan määrän tarvetta, mutta tekoälyllä ei voida kuitenkaan kokonaan korvata ihmistä kyberturvallisuuden alalla. (Gafni & Levy 2024).

Edellisien kappaleiden nostot tekoälyn hyödyistä kyberturvallisuudessa vastaavat alkuperäiseen tutkimuskysymykseen ”Miten tekoälyä voidaan hyödyntää kyberturvallisuuden parantamiseen?”

Vaikka tekoälystä voidaan saada suuresti apua kyberturvallisuuteen ja tietoturvallisuuteen liittyvissä asioissa, sen käyttöönotto voi olla hankalaa. Erityisesti organisaatioissa, joissa ei ole ennestään käytetty tekoälyä voi olla hyvin vaikea lähteä implementoimaan tekoälyllisiä ratkaisuja, koska näissä orga5.3nisaatioissa ei ole entuudestaan osaamista tai tarvittavaa infrastruktuuria, jonka avulla tekoäly voidaan ottaa käyttöön. Myös tekoälyn hyödyntäminen pitäisi olla organisaatiossa osana kyberturvallisuusstrategiaa, jotta sen käyttö olisi tarkoituksen mukaista ja siitä saataisiin oikeasti hyötyä. Nämä löydökset vastaavat työn alkuperäiseen alatutkimuskysymykseen ”Millaisia vaaroja tai riskejä tekoälyn käyttö sisältää?”

Gafni ja Levy nostavat omassa tutkimuksessaan (2024) esiin mielenkiintoisen kysymyksen, kuinka paljon AI:n hyödyntäminen oikeasti auttaa työntekijää työssään ja auttaako se työntekijää olemaan tehokkaampi omassa työssään. Etenkin organisaatioissa, joissa tekoälyä ei olla totuttu vielä hyödyntämään paljoa ja kulttuuri tekoälyn ympärillä ei ole vielä kovin kehittynyttä voi tekoälyn hyödyntäminen olla varsin tehotonta (Gafni & Levy 2024). Työntekijät saattavat käyttää enemmän aikaa siihen, että ne selvittävät voisiko tekoäly tehdä tietyn työtehtävän, jolloin työn tehokkuus varsinkin alkuvaiheessa voi olla huonoa.

5.2 Tutkimuksen arviointi

Työssä on käytetty vertaisarvioituja tieteellisiä artikkeleja, sekä konferenssijulkaisuja, jonka takia työssä käytetty tieto on luotettavaa. Tutkimuksessa käytetty aineisto on suurimmaksi osaksi hyvin tuoretta ja erityisesti tekoälyyn liittyvät lähteet ovat hyvin uusia, jolla on varmistettu, että tieto on mahdollisimman ajankohtaista ja luotettavaa. Tutkimusmenetelmät ovat avattu tässä työssä ja käytettyjä hakusanoja ja -lausekkeita on avattu tekstissä. Lisäksi pää- ja apututkimuskysymykset ovat kerrottu, jonka perusteella tutkimusta on lähdetty tekemään. Tämän vuoksi tutkimus on varsin toistettava, mutta suuren aineiston ja hieman epätarkan artikkelien rajauksen vuoksi työhön valitut artikkelit voisivat hieman erota toisistaan uudessa tutkimuksessa.

Tässä kirjallisuuskatsauksessa on esitetty kattavasti hyviä ja huonoja puolia tekoälyyn ja sen integroimiseen osaksi kyberturvallisuutta ja työ onnistuu kokoamaan alan kirjallisuudesta tämänhetkisen tilanteen hyvin. Työ laajuuden vuoksi löydetyt havainnot jäävät paikoitellen pintapuolisiksi, mutta työn rajauksen vuoksi työssä vain esitellään tekoälyn hyötyjä ja riskejä kyberturvallisuuteen liittyen. Työn rajaus on perusteltavissa työn laajuudella ja se muodostaa järkevän kokonaisuuden. Vaihtoehtoisesti rajaus olisi voinut keskittyä vain esimerkiksi tekoälyn tuomiin hyötyihin kyberturvallisuudessa, jolloin niihin olisi voitu paneutua tarkemmin, mutta tämä on jätetty mahdolliselle jatkotutkimukselle.

Tutkimusta voidaan pitää onnistuneena, sillä siinä on kerätty alan ajankohtaisesta kirjallisuudesta tietoa, miten tekoälyä voidaan hyödyntää kyberturvallisuuteen ja aihetta on tarkasteltu kriittisesti ja tieto on viitattu useisiin eri lähteisiin. Tutkimus on onnistunut löytämään tietoa ja vastauksia alkuperäisiin tutkimuskysymyksiin.

5.3 Jatkotutkimusideat

Tutkimuksessa käytetyissä lähteistä yleinen konsensus oli, että tekoälyn avulla voidaan tehostaa ja parantaa kyberturvallisuutta merkittävästi. Lisäksi usein artikkeleissa nousi esiin, kuinka tekoälyn avulla työvoimapulaa voidaan helpottaa organisaatioissa automatisoimalla työvaiheita ja kuinka tällä on positiivinen vaikutus organisaatioiden kustannuksiin.

Jatkotutkimuksessa voisi selvittää tekoälyn integroimisen vaikutukset organisaation todellisiin kustannuksiin ja kuinka integrointi tulisi tehdä, että kustannuksia saataisiin todellisuudessa pienennettyä.

LÄHTEET

Abbas, H. et al. (2022) Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare. PloS one. 17 (11).

Akhtar, Z & Rawol, A. (2024) Enhancing Cybersecurity through AI-Powered Security Mechanisms. IT journal research and development (Online). 9 (1), 50–67.

AlDaajeh, S. et al. (2022) The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & security.

Alowais, S. et al. (2023) Revolutionizing healthcare: the role of artificial intelligence in clinical practice. BMC Med Educ 23. https://doi.org/10.1186/s12909-023-04698-z

Chen, C. et al. (2020) Editorial: IEEE access special section editorial: Artificial intelligence in cybersecurity. IEEE access.

Collins, C., Dennehy, D., Conboy, K., Mikalef, P. (2021) intelligence in information systems research: A systematic literature review and research agenda. Artikkeli.

Copeland, B. 2024. Britannica, Artificial Intelligence. Viitattu 7.10.2024 Saatavilla https://www.britannica.com/technology/artificial-intelligence

Dambe, S., Gochhait, S., Ray, S. (2023) The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Audit. 3rd International Conference on Advancement in Electronics and Communication Engineering, AECE 2023

Darwiche, A. (2018) Human-Level Intelligence or Animal-Like Abilities? Commun. ACM 61, 10, 56–67.

Emmert-Streib, F. et al. (2020) An Introductory Review of Deep Learning for Prediction Models With Big Data.

Euroopan komissio, ENISA. EU:n kyberturvallisuusasetus. Viitattu 19.11.2024. Saatavilla https://digital-strategy.ec.europa.eu/fi/policies/cybersecurity-act

Eurooppa-neuvosto. Kyberturvallisuus: miten EU torjuu kyberuhkia? Viitattu 24.10.2024 https://www.consilium.europa.eu/fi/policies/cybersecurity/

Evans, K. & Reeder, F. (2010) A human capital crisis in cybersecurity: Technical proficiency matters. CSIS

F-secure. Mitä on kyberturvallisuus? Viitattu 2.10.2024. Saatavilla https://www.f-secure.com/fi/articles/what-is-cyber-security

Falowo O., Botsyoe L., Koshoedo K., Ozer M. (2024) Enhancing Cybersecurity With Artificial Immune Systems and General Intelligence: A New Frontier in Threat Detection and Response. IEEE Access, 12, pp. 123811 - 123822

Ferrag, M. A. et al. (2023) Blockchain and Artificial Intelligence as Enablers of Cyber Security in the Era of IoT and IIoT Applications. Journal of sensor and actuator networks. 12 (3), 40-.

Florackis, C. et al. (2023) Cybersecurity Risk. *The Review of financial studies*. 36 (1), 351–407.

Gafni, R. and Levy, Y. (2024), "The role of artificial intelligence (AI) in improving technical and managerial cybersecurity tasks' efficiency", Information and Computer Security, Vol. ahead-of-print No. ahead-of-print

Glas, M. et al. (2023) Improving cybersecurity skill development through visual programming. Information and computer security. 31 (3), 316–330.

Helenius, M. et al. (2024) COMP.SE.100 Kyberturvallisuus 1. -kurssi. Tampereen yliopisto. Kurssimateriaali.

Jansson, S. & Sihvonen, T. (2018) Kyberturvallisuus valtiollisena toimintaympäristönä ja siihen kohdistuvat uhkat. *Media & viestintä*. 41 (1),

Kuha, S. et al. (2023) Teknologian hyödyntämiseen liittyvä yksityisyydensuoja, tietoturva ja -suoja ikääntyneiden kotipalveluissa: kyselytutkimus johtajille. Finnish Journal of eHealth and eWelfare. Vol. 15 (3)

Kyberturvallisuuskeskus (2023) Tekoälyn soveltamisen kyberturvallisuus ja riskienhallinta. Viitattu 8.10.2024 Saatavilla https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Teko%C3%A4lyn%20soveltamisen%20kyberturvallisuus%20ja%20riskienhallinta.pdf

Lanka, P. et al. (2024) Intelligent Threat Detection—AI-Driven Analysis of Honeypot Data to Counter Cyber Threats. *Electronics (Basel)*. 13 (13), 2465-.

Li, L. et al. "Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior." *International Journal of Information Management*, vol. 45, 2019, pp. 13–24, https://doi.org/10.1016/j.ijinfomgt.2018.10.017.

Mashiane, T., Krizinger, E. (2018) Cybersecurity behaviour: A conceptual taxonomy. International Conference on Information Security Theory and Practices pp.147-156, WISTP. Vol 11469

Nour, S. &Said, S. (2024) Harnessing the Power of AI for Effective Cybersecurity Defense. *6th International Conference on Computing and Informatics (ICCI)*, New Cairo - Cairo, Egypt, 2024, pp. 98-102

Owasp. Vulnerabilities. Viitattu 2.10.2024. Saatavilla https://owasp.org/www-community/vulnerabilities/#

Paloalto. What is an Intrusion Detection System? Viitattu 2.10.2024. Saatavilla https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusiondetection-system-ids

Pytel, G. (2024) Data Leak Prevention – How Does It Work. Viitattu 5.11.2024. Saatavillla https://storware.eu/blog/data-leak-prevention/

SAP. Mikä on esineiden internet (IoT)? Viitattu 2.10.2024 . Saatavilla https://www.sap.com/finland/products/artificial-intelligence/what-is-iot.html

Seung, L. (2022) A black box approach to auditing algorithms. Issues in Information Systems, 23 (2), pp. 75 - 88

Shah, J (2017) Understanding and study of intrusion detection systems for various networks and domains. International Conference on Computer Communication and Informatics, ICCCI 2017.

Shang, Y. (2024) DETECTION AND PREVENTION OF CYBER DEFENSE ATTACKS USING MACHINE LEARNING ALGORITHMS. Scalable Computing, 25 (2), pp. 760 - 769

Shanthi, R., Sasi N., Gouthaman, P. (2023) A New Era of Cybersecurity: The Influence of Artificial Intelligence International Conference on Networking and Communications (ICNWC), Chennai, India, 2023, pp. 1-4.

Sharma, N. & Jindal, N. (2023) Emerging artificial intelligence applications: metaverse, IoT, cybersecurity, healthcare - an overview. Multimedia tools and applications. 83 (19).

Srivastava, A. & Stager, S. (2024) Cognitive Computing with Deep Learning based Cybersecurity Solution for Human Computer Interface Applications. *International Conference on Data Science and Network Security (ICDSNS)*, Tiptur, India, 2024, pp. 1-6

Suomi.fi. Mikä on Suomi.fi-tunnistus. Viitattu 24.10.2024 Saatavilla https://www.suomi.fi/ohjeet-ja-tuki/tunnistus/mika-on-suomifi-tunnistus

Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. Electronics, 11(14), 2181. https://doi.org/10.3390/electronics11142181

Tenkanen, T. et al. (2018) Security Challenges of IoT-Based Smart Home Appliances. Vol. 93. Cham, Switzerland : Springer,.

Tesla. (2024) AI & Robotics. Viitattu 22.10.2024 https://www.tesla.com/AI

U.S. Department of Commerce. (2024) The NIST Cybersecurity Framework (CSF) 2.0. Viitattu 21.11.2024. Saatavilla: https://doi.org/10.6028/NIST.CSWP.29.

Vartiainen, H., Tedre, M., Jormanainen, I., Kahila, J., Valtonen, T. (2021). Tekoäly, koneoppiminen ja teknologinen murros: Kohti datatoimijuutta ja tulevaisuuden design-taitoja. Ainedidaktiikka, 5 (2).

Ventre, D. (2020) Artificial intelligence, cybersecurity and cyber defense. 1st edition. Hoboken, New Jersey: ISTE Ltd / John Wiley and Sons Inc.

Vähä-Sipilä, A., Marchal, S., Aksela, M. (2021) Tekoälyn soveltamisen kyberturvallisuus ja riskienhallinta. Liikenne- ja viestintävirasto Traficom https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Teko%C3%A4lyn%20soveltamisen%20kyberturvallisuus%20ja%20riskienhallinta.pdf

Zhou, Z.-H. & Liu, S. (2021) Machine Learning. 1st Edition 2021. Singapore: Springer.

Zimmermann, V. & Renaud, K. (2019) Moving from a ‘human-as-problem” to a ‘human-as-solution” cybersecurity mindset. *International journal of human-computer studies*.