Tampereen ammattikorkeakoulu

Tekoälyn käyttö kyberturvallisuudessa

Roni Ilomäki

OPINNÄYTETYÖ
Huhtikuu 2025

Tietotekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

ILOMÄKI, RONI:
Tekoälyn käyttö kyberturvallisuudessa

Opinnäytetyö 22 sivua, joista liitteitä 1 sivu
Huhtikuu 2025

Opinnäytetyössä tutkittiin tekoälyn käyttöä kyberturvallisuudessa. Työn alussa tutustuttiin tekoälyn sekä kyberturvallisuuden määritelmiin. Lisäksi työssä tutkittiin molempien sovelluksia ja miten tekoälyä hyödynnetään osana kyberturvallisuutta kehittämään alaa ja toisaalta arveluttaviin tarkoituksiin. Lopuksi tutustuttiin tekoälyn tulevaisuuteen kyberturvallisuudessa.

Työssä selvitettiin ajankohtaisimpia asioita tekoälyn soveltamiseen kyberturvallisuudessa sekä miten tekoälyn rooli tulee todennäköisesti kasvamaan ja tuomaan uusia hyötyjä ja teknillisiä sekä eettisiä haasteita. Tavoitteena oli saada mahdollisimman ajankohtainen tutkimus tekoälyn tämänhetkisistä sekä tulevaisuuden hyödyistä ja haasteista kyberturvallisuudessa, vaikka tekoälyn merkitys muuttuukin jatkuvasti sen nopean kehityksen ansiosta.

Tuloksena saatiin kattava ja selkeä kuva ajankohtaisista menetelmistä, miten tekoälyä hyödynnetään kyberturvallisuudessa ja miten sitä kannattaisi käyttää hyväksi kehittämään entistä tehokkaampia kyberturvallisuusratkaisuja esimerkiksi automatisoinnin avulla. Tekoälyn jatkuva oppiminen ja suurien tietomäärien käsittely auttaa tunnistamaan uhkia nopeasti suurista tietovirroista ja verkkoliikenteestä. Tulevaisuudessa varsinkin suurten kielimallien hyödyntäminen on olennainen osa kyberturvallisuutta. Tämän lisäksi saatiin selville monia uhkia, joita tekoäly voi kyberturvallisuudessa tuoda sekä suurille organisaatioille että tietokonejärjestelmien keskivertokäyttäjille nyt ja tulevaisuudessa. Näistä olennaisimpina uhkina nousivat sosiaaliset manipulointihuijaukset, kuten tietojenkalastelu ja tekoälyn käyttäminen erilaisten haittaohjelmien kirjoittamiseen.

Asiasanat: tekoäly, kyberturvallisuus, koneoppiminen

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in ICT Engineering
Telecommunications and Networks

ILOMÄKI, RONI:
The Use of Artificial Intelligence in Cybersecurity

Bachelor's thesis 22 pages, appendices 1 page
April 2025

The thesis explored the use of artificial intelligence (AI) in cybersecurity. At the beginning of the work, the definitions of both artificial intelligence and cybersecurity were examined. In addition, the thesis investigated the applications of both fields and how AI is utilized in cybersecurity for both beneficial and malicious purposes. Finally, the future of artificial intelligence in cybersecurity was discussed.

The study addressed the most current aspects of applying AI in cybersecurity, as well as how the role of AI is likely to grow, bringing new benefits along with technical and ethical challenges. The aim was to produce an up-to-date overview of the current and future advantages and challenges of AI in cybersecurity, despite the fact that the significance of AI continues to evolve rapidly due to its fast-paced development.

As a result, a comprehensive and clear picture was formed of the current methods by which AI is utilized in cybersecurity and how it could be effectively used to develop even more efficient cybersecurity solutions, for example through automation. Continuous learning by AI and its ability to process large amounts of data help to quickly identify threats from vast data streams and network traffic. In the future, the utilization of large language models will be an essential part of cybersecurity. In addition, several threats posed by AI to both large organizations and average users of computer systems, now and in the future, were identified. The most prominent threats identified were social engineering attacks, such as phishing, and the use of AI to write various types of malwares.

Key words: artificial intelligence, cybersecurity, machine learning

SISÄLLYS

ERITYISSANASTO

tekoäly	kyky, jolla tietokonejärjestelmät voivat suorittaa ihmiselle tyypillisiä tehtäviä
kyberturvallisuus	digitaalisten järjestelmien, verkkojen ja tietojen suojaaminen luvattomalta käytöltä, häiriöiltä ja vahingoilta
koneoppiminen	tekoälyn osa-alue, jossa tietokone oppii tunnistamaan kuvioita ja tekemään päätöksiä datan perusteella ilman erikseen ohjelmoituja sääntöjä
syväoppiminen	koneoppimisen osa-alue, jossa keinotekoiset neuroverkot oppivat monimutkaisia kuvioita ja esitysmalleja suurista tietoaineistoista kerroksellisten rakenteidensa avulla
suuret kielimallit	tekoälyyn perustuvia järjestelmiä, jotka on koulutettu valtavilla tekstiaineistoilla ymmärtämään ja tuottamaan luonnollista kieltä ihmisen kaltaisesti
generatiivinen tekoäly	tekoälyn osa-alue, joka pystyy luomaan uutta sisältöä, kuten kuvia, ääntä tai videoita, oppimiensa mallien pohjalta
palvelunestohyökkäys	kyberhyökkäys, jossa verkkopalvelu pyritään kaatamaan tai tekemään käyttökelvottomaksi ylikuormittamalla se liikenteellä

1 JOHDANTO

Nyky-yhteiskunta on vahvasti riippuvainen sähköisistä järjestelmistä ja internetistä ja myös valtioiden kriittinen infrastruktuuri tukeutuu niihin. Tästä syystä kyberturvallisuuden merkitystä ei voi liikaa painottaa. On helppo kuvitella, millaisia seurauksia olisi, jos yhteiskunnan kannalta keskeiset palvelut yhtäkkiä lamaantuisivat esimerkiksi kyberhyökkäyksen takia. (F-secure 2023).

Tekoälyllä on kasvava rooli kyberturvallisuudessa sekä hyökkääjien että puolustajien näkökulmasta. Rikolliset hyödyntävät tekoälyä esimerkiksi entistä vakuuttavampien tietojenkalasteluhuijausten luomiseen ja haavoittuvuuksien tunnistamiseen, mikä nopeuttaa ja tehostaa hyökkäyksiä. Toisaalta tekoäly auttaa myös puolustuksessa tunnistamalla poikkeavaa verkkoliikennettä, automatisoimalla tietoturvatoimia ja parantamalla reagointinopeutta uhkiin. Tulevaisuudessa tekoälyn rooli kyberhyökkäysten ja -puolustuksen välisessä kilpajuoksussa kasvaa, ja sen tehokkuus riippuu pitkälti siitä, kuinka laadukasta dataa se saa käyttöönsä.

Opinnäytetyössä tutustutaankin tekoälyn käyttöön kyberturvallisuudessa. Työssä käydään läpi tekoälyn ja kyberturvallisuuden määritelmät ja sovellukset nykymaailmassa ja mitä hyötyjä ja uhkia niihin liittyy. Työssä käydään myös läpi tekoälyn hyödyntämistä etenkin kyberturvallisuuden saralta ja miten sitä voidaan käyttää sekä hyviin että vääriin tarkoituksiin. Lopussa käydään läpi miltä tulevaisuus näyttää tekoälyn osalta kyberturvallisuudessa.

2 TEKOÄLY

Tekoäly on nyky-yhteiskunnassa esillä erittäin monilla eri osa-alueilla ja sitä hyödynnetäänkin laajasti, mutta se tuo kuitenkin mukanaan myös monia uhkia ja eettisiä kysymyksiä.

2.1 Määritelmä

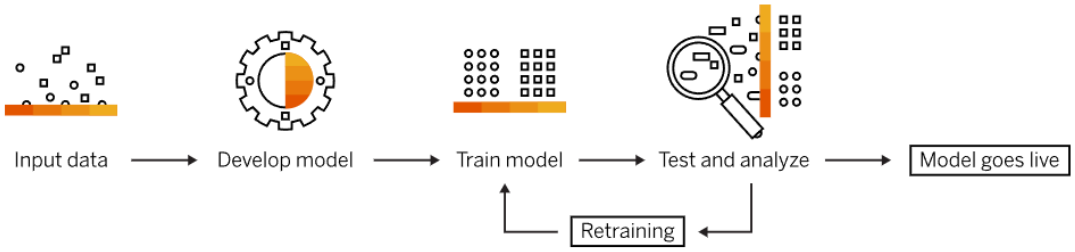
Tekoälyllä viitataan kykyyn, jolla koneet, kuten tietokonejärjestelmät voivat suorittaa ihmisille tai eläimille tyypillisiä tehtäviä. Tekoälyn ”älykkyys” viittaa sen kykyyn tehdä päätöksiä, ratkaista ongelmia, tunnistaa merkityksiä, yleistää, suunnitella ja oppia kokemuksesta. (Traficom 2024).

Suurin osa nykyisistä tekoälyn sovelluksista on vielä kaukana ihmisen älykkyydestä, eikä niillä ole kykyä itsenäisesti suunnitella tai toteuttaa kyberhyökkäyksiä. Sen sijaan koneoppimiseen perustuvat järjestelmät suoriutuvat hyvin monista tehtävistä, jotka on perinteisesti yhdistetty ihmisen älyllisiin kykyihin. Näitä ovat esimerkiksi kuvien tunnistaminen, tekstien kääntäminen sekä strategisten pelien, kuten shakin pelaaminen. (Traficom 2024).

Viime vuosina koneoppiminen on edistynyt huomattavasti, mikä on lisännyt sen saamaa huomiota. Nykyään tekoälyyn liittyvä julkinen keskustelu keskittyykin useasti juuri koneoppimisen sovelluksiin ja termiä ”tekoäly” käytetäänkin usein tarkoittamaan nimenomaan koneoppimista. (Traficom 2024).

2.1.1 Koneoppiminen

Koneoppimisen avulla tietokoneet voivat oppia ilman, että niitä tarvitsee erikseen ohjelmoida jokaista tehtävää varten. Erityisesti syväoppimisen kehitys on ollut keskeinen tekijä tekoälyn nopeassa yleistymisessä viime vuosina. Koneoppiminen perustuu siihen, että tietojärjestelmät opetetaan hyödyntämään algoritmeja toistuvien kuvioiden tunnistamiseen datasta, minkä ansiosta ne voivat tehdä ennusteita ja päätöksiä itsenäisesti. (Viitaila n.d.).



KUVA 1. Miten koneoppimisprosessi toimii. (SAP n.d.).

Koneoppiminen voidaan jakaa kolmeen päätyyppiin: valvottuun, valvomattomaan ja vahvistavaan oppimiseen:

Valvotuksi oppimiseksi kutsutaan sitä, kun koneita opetetaan käyttämällä dataa, johon on lisätty selitteitä tai luokittelutietoja. Esimerkiksi kuviin voidaan liittää tietoja siitä, mitä ne esittävät. Koneen algoritmi oppii tunnistamaan nämä selitteet ja löytämään samankaltaisia piirteitä uudesta datasta. Jos esimerkiksi joukko kuvia on merkitty ”koira” -tunnisteella, kone oppii yhdistämään nämä piirteet koiriin ja tunnistamaan vastaavanlaiset kuvat koiriksi. (Viitaila n.d.).

Valvomattomassa oppimisessa koneet analysoivat dataa, jossa ei ole valmiita selitteitä ja pyrkivät tunnistamaan siinä toistuvia rakenteita tai samankaltaisuuksia. Toisin kuin valvotussa oppimisessa, algoritmia ei ole ohjelmoitu etsimään tiettyjä asioita (esimerkiksi koirakuvia). Sen sijaan se ryhmittelee datan osiin sen perusteella, mitkä esimerkit muistuttavat toisiaan. (Viitaila n.d.).

Vahvistavassa oppimisessa kone oppii kokeilemalla eri tapoja suorittaa tehtävä ja saa palautetta onnistumisista ja virheistä. Tämän avulla se kehittää lopulta tehokkaimman tavan toimia. Esimerkiksi Microsoft hyödyntää tätä menetelmää pelien tekoälyhahmojen kehittämisessä. (Viitaila n.d.).

2.1.2 Syväoppiminen

Syväoppiminen on koneoppimismenetelmä, joka suoriutuu erinomaisesti erilaisten luonnollisten tietojen, kuten tekstin, kuvien, äänen ja videon, automaattisesta käsittelystä. Viime vuosien edistysaskeleet syväoppimisessa ovat olleet keskeinen tekijä tekoälyn ja koneoppimisen suosion kasvussa. Näillä menetelmillä on saavutettu poikkeuksellisen hyvä suorituskyky monimutkaisissa tehtävissä, kuten kuvantunnistuksessa, konekääntämisessä ja strategiapelien hallinnassa. Syväoppimismallit pystyvät päättelemään, ratkaisemaan ongelmia, tunnistamaan merkityksiä ja oppimaan itsenäisesti pelkän datan avulla. Tämä kehitys on ollut mahdollinen algoritmien parantumisen, suurten tietoaineistojen saatavuuden ja laskentatehon halpenemisen ansiosta. (Traficom 2024).

2.2 Sovellukset

Tekoälyllä on nyky-yhteiskunnassa useita sovelluksia erilaisilla toimialoilla, kuten esimerkiksi terveydenhuollossa, logistiikassa, markkinoinnissa ja teollisuudessa. Näihin kaikkiin löytyy erilaisia hyötyjä, mutta myös uhkia ja eettisiä kysymyksiä.

Terveydenhuollossa tekoäly auttaa lääkäreitä diagnosoimaan sairauksia tarkemmin ja nopeammin. Esimerkiksi röntgen- ja magneettikuvien analysointi tekoälyn avulla voi havaita varhaisia merkkejä sairauksista, jotka saattaisivat jäädä huomaamatta perinteisessä tutkimuksessa. Lisäksi tekoälyä käytetään uusien lääkkeiden kehittämisessä ja hoitosuunnitelmien personoinnissa, mikä parantaa potilaiden saamaa hoitoa.

Liikenteessä ja logistiikassa tekoäly tehostaa kuljetuksia ja parantaa liikenneturvallisuutta. Itseajavat autot hyödyntävät tekoälyä ympäristön havainnointiin ja päätöksentekoon, mikä voi vähentää liikenne onnettomuuksia. Lisäksi lentoyhtiöt ja rahtiliikenne käyttävät tekoälyä reittien optimointiin, polttoaineen kulutuksen vähentämiseen ja toimitusten nopeuttamiseen, mikä säästää aikaa ja resursseja

Asiakaspalvelussa ja markkinoinnissa tekoäly on jo laajasti käytössä. Chatbotit ja virtuaaliavustajat auttavat käyttäjiä vastaamalla kysymyksiin ja tarjoamalla suosituksia. Verkkokaupat ja suoratoistopalvelut hyödyntävät tekoälyä analysoidakseen asiakkaiden mieltymyksiä ja suositellakseen heille sopivia tuotteita tai sisältöä. Tämä tekee ostokokemuksesta henkilökohtaisemman ja parantaa asiakastyytyväisyyttä.

Teollisuudessa älykkäät robotit ja automaatiojärjestelmät tehostavat tuotantoprosesseja ja vähentävät inhimillisten virheiden riskiä. Lisäksi tekoäly auttaa ennakoimaan laitteiden huoltotarpeita, mikä voi estää kalliit tuotantokatkokset. Tekoäly auttaa myös laadunvalvonnassa, jossa koneoppimismallit tarkkailevat valmistus prosessia ja havaitsevat poikkeamat, kuten virheet tai vialliset tuotteet, jo ennen kuin ne päätyvät markkinoille.

Tekoälyn sovelluksiin liittyy myös uhkia ja eettisiä kysymyksiä, kuten terveydenhuollossa, jos esimerkiksi tietomurto sattuu tapahtumaan. Automaatio voi myös korvata monia työtehtäviä, mikä herättää kysymyksiä siitä, miten työntekijöitä tuetaan muutoksessa. Lisäksi tekoälyn tekemistä virheistä, kuten itseajavien autojen onnettomuuksista, on epäselvää kuka kantaa vastuun: ohjelmoija, käyttäjä vai valmistaja. Näiden haasteiden ratkaiseminen edellyttää eettisiä periaatteita, sääntelyä ja vastuullista tekoälyn kehitystä.

3 KYBERTURVALLISUUS

Kyberturvallisuus tarkoittaa digitaalisten järjestelmien, verkkojen ja tietojen suojaamista kyberuhkia, kuten hakkerointia, haittaohjelmia ja tietojenkalastelua, vastaan. Sen merkitys kasvaa jatkuvasti, sillä kehittyvät teknologiat tuovat sekä uusia suojausmahdollisuuksia että entistä kehittyneempiä kyberuhkia.

3.1 Määritelmä

Kyberturvallisuus tarkoittaa tietokone järjestelmien ja verkkojen suojaamista digitaalisilta uhkilta. Se sisältää monenlaisia keinoja, kuten salasanojen hallinnan ja tekoälyyn perustuvat tietoturvaratkaisut. Sen ansiosta voimme käyttää internetiä turvallisesti esimerkiksi verkkokaupoissa, viestinnässä ja selailussa. (NordVPN n.d.).

Tietoturvallisuus/tietoturva sekoitetaan usein arkisessa puheessa käsitteenä kyberturvallisuuteen. Vaikka nämä käsitteet liittyvät toisiinsa, niillä on merkittäviä eroja. Kyberturvallisuus keskittyy tietojen, järjestelmien ja laitteiden suojaamiseen erityisesti verkkoympäristössä. Tietoturvallisuus puolestaan kattaa tiedon suojauksen laajemmin, mukaan lukien sen fyysisen säilyttämisen ja pääsyn rajoittamisen myös digitaalisuuden ulkopuolella. Näiden kahden turvallisuuden muodot kohtaavat erilaisia uhkia. Kyberturvallisuus pyrkii estämään esimerkiksi haittaohjelmien aiheuttamia vahinkoja, kun taas tietoturvaan kuuluu myös kaikenlaisen tiedon levittämisen hallinta sekä väärän tiedon torjunta. Näiden erojen vuoksi kyberturvallisuutta voi pitää yhtenä tietoturvan osa-alueena. (F-secure 2023)

3.2 Uhkat

Koska sekä yksityishenkilöiden että yritysten tietoja on tallennettuna verkkoon monessa eri paikassa ja eri muodoissa, verkkorikolliset pyrkivät hyödyntämään tietoturvan heikkouksia. Myös ihmisten inhimilliset virheet ja huolimattomuus muodostavat uhan kyberturvallisuudelle. Lisäksi internet on keskeinen osa rahaliikennettä, ja lähes kaikki hoitavat pankkiasiansa verkossa, mikä avaa rikollisille

uusia mahdollisuuksia, kuten pankkitietojen varastamisen. Seuraavaksi käsitellään joitakin yleisiä kyberturvallisuusuhkia, joihin on hyvä varautua. (F-secure 2023).

Vaikka käyttäjällä olisi suojanaan esimerkiksi antivirus-ohjelma, verkkorikolliset voivat silti päästä käsiksi tietoihin, jos uhri itse luovuttaa ne huijauksen seurauksena. Yksi yleisimmistä tavoista varastaa pankkitunnuksia, henkilötietoja ja salasanoja on tietojenkalastelu (englanniksi phishing). Tämä voi tapahtua esimerkiksi sähköpostin tai verkkosivuston kautta ja onnistuneessa huijauksessa rikolliset saattavat myös houkutella uhrin lataamaan haittaohjelman laitteelleen. (F-secure 2023).

Tietomurrot, joissa päästään käsiksi suurten ihmisjoukkojen henkilötietoihin, ovat herättäneet paljon huomiota myös Suomessa. Yritysten, jotka säilyttävät asiakastietoja, on suhtauduttava tietomurtoihin vakavasti, sillä ne voivat aiheuttaa merkittäviä taloudellisia tappioita ja vahingoittaa yrityksen mainetta. Mitä enemmän ihmisten tietoja tallennetaan tietokantoihin, sitä suurempi on tietomurtojen riski. (F-secure 2023).

DDoS-hyökkäykset eli palvelunestohyökkäykset ovat ilmiö, joka on ollut esillä myös Suomessa viime vuosina. Vaikka nämä hyökkäykset eivät yleensä kohdistu yksittäisiin henkilöihin, niiden vaikutukset voivat näkyä arjessa. Onnistuessaan palvelunestohyökkäys voi kaataa jonkin verkkopalvelun kokonaan tai vähintään hidastaa sen toimintaa merkittävästi, mikä hankaloittaa sen käyttöä. (F-secure 2023).

4 TEKOÄLYN ROOLI KYBERTURVALLISUUDESSA

Tekoälyllä on keskeinen rooli kyberturvallisuudessa, sillä se pystyy analysoimaan suuria tietomääriä nopeasti ja tunnistamaan epäilyttäviä käyttäytymismalleja, jotka voivat viitata tietomurtoihin tai muihin hyökkäyksiin. Se auttaa ennakoimaan uhkia, automatisoimaan vastatoimia ja nopeuttamaan reagointia esimerkiksi palvelunestohyökkäyksiin tai haittaohjelmiin. Lisäksi tekoäly voi oppia jatkuvasti uusia hyökkäystapoja ja mukauttaa puolustusmenetelmiä niiden torjumiseksi.

4.1 Tekoälyn hyödyntäminen kyberturvallisuudessa

Tekoälyn hyödyntäminen kyberturvallisuudessa tuo mukanaan monia etuja organisaatioille, jotka haluavat hallita riskejään. Keskeisiä hyötyjä ovat:

Jatkuva oppiminen: Tekoäly kehittyy jatkuvasti, kun se oppii uudesta datasta. Syväoppimisen ja koneoppimisen kaltaiset tekniikat auttavat tekoälyä tunnistamaan kaavoja, luomaan normaalista toiminnasta vertailukohdan ja havaitsemaan poikkeamat tai epäilyttävän toiminnan. Tämä jatkuva oppiminen vaikeuttaa hyökkääjien mahdollisuuksia ohittaa organisaation puolustusjärjestelmät. (Fortinet n.d.).

Tuntemattomien uhkien tunnistaminen: Kyberrikolliset kehittävät jatkuvasti yhä monimutkaisempia hyökkäystapoja, mikä altistaa organisaatiot uusille, vielä tuntemattomille uhille. Tekoäly auttaa tunnistamaan ja estämään tällaisia uhkia, mukaan lukien haavoittuvuudet, joita ohjelmistotoimittajat eivät ole vielä tunnistaneet tai ehtineet korjata. (Fortinet n.d.).

Laajojen tietomäärien käsittely: Tekoäly pystyy analysoimaan valtavia tietomääriä, joita ihmisten olisi mahdotonta käsitellä tehokkaasti. Tämän ansiosta organisaatiot voivat automaattisesti tunnistaa uusia uhkia laajoista tietovirroista ja verkkoliikenteestä, jotka perinteiset järjestelmät saattaisivat ohittaa. (Fortinet n.d.).

Parempi haavoittuvuuksien hallinta: Tekoäly ei ainoastaan tunnista uusia uhkia, vaan auttaa myös organisaatioita hallitsemaan haavoittuvuuksia tehokkaammin. Se tehostaa järjestelmien arviointia, ongelmanratkaisua ja päätöksentekoa. Lisäksi se voi tunnistaa verkkojen ja järjestelmien heikot kohdat, jotta organisaatiot voivat keskittyä kriittisimpiin turvallisuustehtäviin. (Fortinet n.d.).

Vahvempi kokonaisvaltainen tietoturva: Erilaisten hyökkäysten, kuten palvelunestohyökkäysten (DoS) ja kiristyshaittaohjelmien, manuaalinen hallinta on työlästä ja aikaa vievää. Tekoälyn avulla organisaatiot voivat kuitenkin havaita monenlaisia hyökkäyksiä reaaliajassa, priorisoida riskit tehokkaasti ja estää niitä ennakoivasti. (Fortinet n.d.).

Parempi uhkien tunnistus ja reagointi: Uhkien tunnistaminen on olennainen osa tietojen ja verkkojen suojausta. Tekoälypohjainen kyberturvallisuus mahdollistaa nopean, järjestelmällisen tunnistamattoman datan havaitsemisen ja välittömän reagoinnin uusiin uhkiin. (Fortinet n.d.).

4.2 Tekoälyn teknilliset haasteet kyberturvallisuudessa

Vaikka tekoälyä voidaan hyödyntää kyberturvallisuudessa monin tavoin, sisältää se myös teknillisiä haasteita, jotka on hyvä ottaa huomioon.

4.2.1 Datan laatu ja määrä tekoälyjärjestelmissä

Tekoälyalgoritmit vaativat suuria määriä laadukasta dataa toimiakseen tarkasti ja tehokkaasti. Puutteellinen tai heikkolaatuinen data voi johtaa epätarkkaan uhkien tunnistamiseen ja heikentää tekoälyn suorituskykyä. Korkealaatuinen data takaa tarkat ja luotettavat tulokset, kun taas riittävä datamäärä mahdollistaan tekoälymallien oppimisen ja sopeutumisen uusiin uhkiin niiden kehittyessä. (Paloalto. n.d.).

4.2.2 Tekoälyn integrointi vanhoihin järjestelmiin

Tekoälyteknologioiden yhdistäminen olemassa olevaan kyberturvallisuus infrastruktuuriin voi olla monimutkaista. Se edellyttää järjestelmien yhteensopivuutta, tekoäly algoritmien sovittamista nykyisiin ratkaisuihin sekä siirtymän hallintaa ilman, että organisaation toiminta häiriintyy. (Paloalto n.d.).

Tämä prosessi voi olla haastava erityisesti, jos eri järjestelmät eivät ole yhteensopivia. Se saattaa vaatia infrastruktuurin päivittämistä ja datan muotoilua tekoälymallien kanssa yhteensopivaksi. Tämä puolestaan edellyttää merkittävää teknistä osaamista ja huolellista suunnittelua, mikä voi olla monille organisaatioille vaikeaa. (Paloalto. n.d.).

4.2.3 Luotettavuus ja luottamusongelmat

Vaikka tekoälyjärjestelmät ovat tehokkaita, ne eivät ole erehtymättömiä, mikä herättää huolta. Lisäksi tekoälyn päätöksentekoprosessit eivät ole aina läpinäkyviä, mikä vaikeuttaa niiden toimintalogiikan ymmärtämistä ja ennakoimista. Tämä saa monet päätöksentekijät epäröimään tekoälyn käyttöä kriittisissä turvallisuuspäätöksissä, sillä on olemassa riski, että tekoäly ei tunnista uhkaa tai antaa virheellisen hälytyksen. (Paloalto. n.d.).

4.3 Tekoälyn väärinkäyttö kyberturvallisuudessa

Sosiaalisissa manipulointihuijauksissa (social engnineering attack) käytetään psykologista manipulointia, jotta ihmiset saataisiin paljastamaan arkaluonteisia tietoja tai tekemään muita tietoturvaan liittyviä virheitä. Ne kattavat monia erilaisia petostyyppejä, kuten tietojenkalastelun (phishing), äänipohjaisen huijauksen (vishing) ja yrityssähköpostien väärinkäytön (business email compromise). Tekoälyn avulla verkkorikolliset voivat automatisoida monia sosiaalisen manipuloinnin hyökkäystapoja sekä luoda yksilöllisempää, hienostuneempaa ja tehokkaampaa

viestintää, joka hämää uhrinsa helpommin. Tämä mahdollistaa suuremman määrän hyökkäyksiä lyhyemmässä ajassa ja kasvattaa onnistumisen todennäköisyyttä. (Morgan Stanley 2024).

Kyberrikolliset hyödyntävät tekoälyä parantaakseen algoritmejaan, joita käytetään salasanojen murtamiseen. Näiden algoritmien avulla salasanoja pystytään arvaamaan nopeammin ja tarkemmin, mikä tekee hakkeroinnista entistä tehokkaampaa ja kannattavampaa. Tämä voi johtaa entistä suurempaan panostukseen salasanojen murtamiseen rikollisten keskuudessa. (Morgan Stanley 2024).

Deepfake-tekniikalla voidaan tekoälyn avulla muokata kuvia, videoita ja ääntä niin, että ne vaikuttavat aidoilta. Tätä käytetään esimerkiksi väärien videoiden ja äänitteiden luomiseen, joilla voidaan esiintyä toisena henkilönä. Tällaisia väärennettyjä sisältöjä voidaan levittää laajasti ja nopeasti esimerkiksi sosiaalisessa mediassa, mikä voi aiheuttaa pelkoa, hämmennystä ja stressiä niiden katsojissa. Deepfake-sisältöjä voidaan yhdistää myös muihin huijaustaktiikoihin, kuten sosiaaliseen manipulointiin ja kiristykseen. (Morgan Stanley 2024).

Tietomyrkytys (data poisoning) tarkoittaa sitä, että hakkerit manipuloivat tekoälyn oppimaa dataa, jolloin algoritmin tekemät päätökset vääristyvät. Käytännössä tekoälylle syötetään harhaanjohtavaa tietoa, mikä johtaa virheellisiin lopputuloksiin. Tietomyrkytyksen havaitseminen voi olla hidasta ja vaikeaa ja sen aiheuttamat vahingot voivat olla merkittäviä ennen kuin ongelma huomataan ja siihen pystytään puuttumaan. (Morgan Stanley 2024).

5 TEKOÄLYN TULEVAISUUS KYBERTURVALLISUUDESSA

Tekoälyn tulevaisuus kyberturvallisuudessa tulee olemaan merkittävä ja etenkin suurten kielimallien hyödyntäminen on olennainen osa sitä. Tekoälyn jatkuva kehittyminen tuo myös uudenlaisia uhkia tulevaisuudessa, joihin on hyvä varautua.

5.1 Suurten kielimallien hyödyntäminen

Suuret kielimallit (kuten ChatGPT) osaavat ymmärtää ja tuottaa luonnollista kieltä, mikä tekee tekoälyn mahdollisuuksien tutkimisesta huomattavasti helpompaa. Tämä avaa uusia ovia luovalle ja innovatiiviselle työskentelylle erityisesti kyberturvallisuuden alalla. Kokeiluista käytäntöön siirtyminen vaatii kuitenkin asiantuntijoiden mukanaoloa, jotta ideoista saadaan toimivia ja käyttökelpoisia ratkaisuja. Erityisesti niille organisaatioille, jotka eivät ole vielä valmiita hyödyntämään tekoälyä kyberturvallisuudessaan, kielimallit voivat tarjota hyvän aloituspisteen. (Traficom 2024).

Suuret kielimallit eivät tosin välttämättä paranna suoraan uhkien tunnistamista tai päätelaitteiden turvallisuutta erityisesti kehittyneissä järjestelmissä, joissa havaitsemiskyky on keskiössä. Sen sijaan kielimallit voivat selkeyttää monimutkaisia päätöksentekoprosesseja ja tehdä niistä ymmärrettävämpiä käyttäjille. Esimerkiksi käyttäjälle voidaan paremmin perustella, miksi jokin toiminto, kuten tiedoston avaaminen tai verkkosivun käyttö, on estetty. Lisäksi ne voivat auttaa havaitsemisjärjestelmien kehityksessä esimerkiksi tunnistamalla, mistä väärät hälytykset johtuvat. Kielimalleilla voidaan myös tukea perinteisiä turvallisuusratkaisuja, kuten sääntöihin perustuvia uhkien tunnistusjärjestelmiä. Turvallisuusasiantuntijat voisivat kirjoittaa havaintosääntöjä luonnollisella kielellä, ja kielimallit voisivat muuntaa ne tekniseen muotoon, jota järjestelmät ymmärtävät. Tällöin kielimallit voisivat myös parantaa tekoälypohjaisten turvallisuusratkaisujen käytettävyyttä ja automaatiota entisestään. (Traficom 2024).

Suurten kielimallien ensimmäinen merkittävä käyttökohde tulevaisuudessa liittyy todennäköisesti koulutukseen. Niiden avulla voidaan tehokkaasti opettaa perusasioita kyberturvallisuudesta ja mahdollistaa turvallisuuskäytäntöjen harjoittelu

laajassa mittakaavassa. Alkuvaiheessa kielimalleja hyödynnetään myös turvallisuusanalyysin tukena, kuten auttaa ymmärtämään tapahtumien taustoja ja ehdottaa sopivia toimenpiteitä. Ajan myötä niiden käyttö laajenee vaativampiin tehtäviin, kuten uhkatiedusteluun ja haavoittuvuuksien hallintaan. Esimerkiksi ne voivat auttaa löytämään tunnettuja haavoittuvuuksia järjestelmistä ja lähdekoodista tunkeutumistestauksen osana. Pitkällä aikavälillä on mahdollista, että suuret kielimallit pystyvät suoriutumaan tehtävistä, jotka vaativat syvällistä asiantuntemusta. Ne voisivat esimerkiksi tunnistaa täysin uusia haavoittuvuuksia, arvioida organisaation kyberturvallisuuden tasoa tai antaa tarkkoja ehdotuksia poikkeustilanteiden hallintaan. (Traficom 2024).

5.2 Tulevaisuuden uhkat

Tekoäly tulee ensisijaisesti parantamaan kyberrikollisten kykyä sosiaaliseen manipulointiin. Generatiivista tekoälyä voidaan jo nyt hyödyntää uhrien kanssa käytävien vakuuttavien vuorovaikutusten luomiseen, kuten houkuttimena toimivien asiakirjojen laatimiseen ilman kielioppivirheitä tai käännöspuitteita, jotka usein paljastavat tietojenkalasteluyritykset. Tämä kehitys todennäköisesti kiihtyy seuraavien kahden vuoden aikana, kun mallit kehittyvät ja yleistyvät. (National Cyber Security Centre 2024.).

Tekoälyä hyödynnetään jo nyt esimerkiksi haittaohjelmien kirjoittamiseen ja järjestelmien tiedusteluun, ja trendi näyttää jatkuvan. Vaikka edistyneemmät hyökkäykset edellyttävät edelleen asiantuntemusta, tekoäly voi tulevaisuudessa mahdollistaa nykyistä tehokkaammat tunkeutumiset, erityisesti kiristyshaittaohjelmien levittämisen osalta. Tämän vuoksi tekoäly pahentaa entisestään olemassa olevia uhkia. (National Cyber Security Centre 2024.).

Generatiivisten kielimallien kehitys vaikeuttaa huijausten tunnistamista ja lyhentää aikaa, joka kuluu haavoittuvuuksien hyödyntämiseen. Tällä hetkellä tekoälyn tehokas käyttö vaatii merkittäviä resursseja, mutta teknisesti edistyneet valtiot ja organisoidut rikollisryhmät voivat jo hyödyntää sitä laajasti. Muiden toimijoiden kyvyt paranevat vähitellen, erityisesti tiedustelussa ja sosiaalisessa manipuloinnissa. (National Cyber Security Centre 2024.).

Tulevaisuudessa tekoälymallien yleistyminen ja kaupallistaminen madaltavat hyökkäyskynnystä. Julkisesti saatavilla olevat työkalut voivat mahdollistaa kehittyneitä hyökkäyksiä myös vähemmän taitaville rikollisille. Kun koulutusdataa kertyy lisää onnistuneiden murtojen kautta, tekoälyyn perustuvat kyberoperaatiot voivat muuttua entistä nopeammiksi, tarkemmiksi ja laajemmalle levinneiksi. (National Cyber Security Centre 2024.).

6 POHDINTA

Tekoälyllä on yhä merkittävämpi rooli kyberturvallisuuden vahvistamisessa. Se pystyy analysoimaan valtavia määriä dataa nopeasti ja tehokkaasti, mikä auttaa tunnistamaan poikkeamia ja mahdollisia uhkia reaaliajassa. Esimerkiksi koneoppimismallit voivat oppia tunnistamaan normaalin verkkoliikenteen ja hälyttää, jos järjestelmässä tapahtuu jotakin poikkeavaa, kuten epätyypillinen kirjautuminen tai tiedonsiirto.

Toisaalta tekoälyn käyttöön liittyy myös haasteita ja riskejä. Kyberrikolliset voivat hyödyntää samaa teknologiaa suunnitellakseen entistä älykkäämpiä ja kohdennetumpia hyökkäyksiä. Lisäksi tekoälyjärjestelmien kouluttaminen vaatii laadukasta ja luotettavaa dataa, sillä virheellinen tai puolueellinen data voi johtaa vääriin hälytyksiin tai väärinymmärryksiin, mikä voi heikentää järjestelmän tehokkuutta.

Tulevaisuudessa tekoälyn rooli kyberturvallisuudessa tulee todennäköisesti kasvamaan entisestään. On tärkeää, että sen kehitystä ohjaavat eettiset periaatteet ja selkeät säännöt, jotta järjestelmät pysyvät turvallisina ja luotettavina. Samalla tarvitaan jatkuvaa ihmisen valvontaa ja asiantuntemusta, jotta tekoäly toimii tukena, eikä korvaajana kyberturvallisuuden varmistamisessa.

LÄHTEET

Liikenne- ja viestintävirasto Traficom Kyberturvallisuuskeskus. 2024. Tekoäly-pohjaiset kyberturvallisuusratkaisut. Pdf-dokumentti. Viitattu 20.2.2025. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Teko%C3%A4lypohjaiset%20kyberturvallisuusratkaisut_FI.pdf

Viitaila, M. n.d. Tekoälyn perusteet: koneoppiminen, työn tulevaisuus ja hyvä vai paha tekoäly. Microsoft. Verkkosivu. Viitattu 25.2.2025. https://pulse.microsoft.com/fi-fi/transform-fi-fi/na/fa2-tekoalyn-perusteet-koneoppiminen-tyon-tulevaisuus-ja-hyva-vai-paha-tekoaly/

F-secure. 2023. Mitä on kyberturvallisuus? Verkkosivu. Viitattu 5.3.2025. https://www.f-secure.com/fi/articles/what-is-cyber-security

NordVPN. n.d. Mitä on kyberturvallisuus? Verkkosivu. Viitattu 5.3.2025. https://nordvpn.com/fi/cybersecurity/what-is-cybersecurity/

SAP. n.d. Mitä koneoppiminen on? Verkkosivu. Viitattu 19.3.2025. https://www.sap.com/finland/products/artificial-intelligence/what-is-machine-learning.html

Fortinet. n.d. Artificial Intelligence (AI) In Cybersecurity. Verkkosivu. Viitattu 26.3.2025. https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity

Palo Alto Networks. n.d. What Are the Barriers to AI Adoption in Cybersecurity? Verkkosivu. Viitattu 28.3.2025. https://www.paloaltonetworks.com/cyberpedia/what-are-barriers-to-ai-adoption-in-cybersecurity

Morgan Stanley. 2024. AI and Cybersecurity: A New Era. Verkkosivu. Viitattu 2.4.2025. https://www.morganstanley.com/articles/ai-cybersecurity-new-era

National Cyber Security Centre. 2024. The near-term impact of AI on the cyber threat. Verkkosivu. Viitattu 16.4.2025. https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

LIITTEET

Liite 1. Tekoälyn kyberturvallisuussovellukset, niiden kyvyt ja kypsyystaso. (Traficom 2024).

Sovellus	Kyvyt	Kypsyys
Uhkien ennaltaehkäisy ja havaitseminen	• Luokittelu • Hahmontunnistus • Ryhmittely	Korkea
Päätelaitteiden ja pilvipalveluiden tietoturva	• Luokittelu • Poikkeamien havaitseminen • Hahmontunnistus • Ryhmittely • Järjestäminen	Korkea
Verkon tietoturva	• Luokittelu • Poikkeamien havaitseminen • Hahmontunnistus	
UEBA	• Käyttäytymisanalyysi • Ryhmittely	Kohtalainen
Turvallisuusanalytiikka (SIEM)	• Hahmontunnistus • Poikkeamien havaitseminen • Tiedonhaku • Järjestäminen • Generointi	Kohtalainen
Uhkatiedustelu	• Luokittelu • Ryhmittely • Tiedonhaku • Generointi	Matala
Haavoittuvuuksien hallinta	• Luokittelu • Hahmontunnistus • Järjestäminen • Generointi	Matala
Vaatimustenmukaisuus ja riskienhallinta	• Luokittelu • Tiedonhaku • Järjestäminen • Generointi	Matala