Tampereen ammattikorkeakoulu

Tekoälyn vaikutus tietoturvallisuuteen

Eetu Nikula

OPINNÄYTETYÖ
Toukokuu 2025

Tietojenkäsittelyn tutkinto-ohjelma
Ohjelmistotuotanto

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittelyn tutkinto-ohjelma
Ohjelmistotuotanto

Nikula Eetu
Tekoälyn vaikutus tietoturvallisuuteen

Opinnäytetyö 35 sivua
Toukokuu 2025

Tämän opinnäytetyön tavoitteena oli selvittää, miten tekoäly vaikuttaa tietoturvallisuuteen ja minkälaisia mahdollisuuksia tai haasteita se tuo mukanaan. Työssä tarkastellaan sekä tekoälyn hyödyntämistä tietoturvan parantamiseksi että uusia uhkia, joita tekoäly voi mahdollistaa. Työssä käydään läpi tietoturvan keskeiset käsitteet, tekoälyn toimintaperiaatteet sekä generatiivisen tekoälyn mahdollisuudet ja tämän merkitys tietoturvassa. Lisäksi työssä käsitellään tietosuojaa ja lainsäädäntöä, kuten GDPR:ää, EU:n tekoälyasetusta ja NIS 2 -direktiiviä, jotka ohjaavat tekoälyn käyttöä ja asettavat vaatimuksia henkilötietojen käsittelylle.

Opinnäytetyössä tuodaan esille, miten tekoälyä voidaan käyttää esimerkiksi haittaohjelmien tunnistamiseen, poikkeavuuksien havaitsemiseen ja automatisoituun reagointiin tietoturvauhkien torjumiseksi. Samalla tarkastellaan, miten tekoälyyn liittyvät riskit, kuten syväväärennökset ja muut tekoälyhuijaukset, voivat vaikeuttaa tietoturvariskien tunnistamisessa. Työssä pohditaan myös tulevaisuuden näkymiä, kuten tekoälyn luomia energiavaikutuksia ja tulevaisuuden huolestuttavia uhkia.

Tutkimus osoitti, että tekoälyllä on merkittävä rooli tulevaisuudessa, mutta sen hyödyntäminen vaatii huolellista riskienhallintaa ja vastuullista käyttöä. Maailmanlaajuinen yhteistyö tulee olemaan tärkeää, jotta tekoälyn vaikutukset kyberuhkien muodossa saadaan pidettyä kurissa. Työ tarjoaa kattavan katsauksen ja auttaa ymmärtämään kokonaisuuden, kuinka tekoäly voi toimia sekä tietoturvan vahvistajana että uusien uhkien mahdollistajana.

Asiasanat: tekoäly, tietoturvallisuus, kyberuhkat, generatiivinen tekoäly

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Software Production

Nikula, Eetu
The impact of artificial intelligence (AI) on cybersecurity

Bachelor's thesis 35 pages
May 2025

The aim of this thesis was to explore how artificial intelligence (AI) impacts on cybersecurity, highlighting both the opportunities it offers and the challenges it presents. It investigated how AI can be used to enhance cybersecurity, such as through malware detection and anomaly recognition as well as how it introduces new threats.

Key cybersecurity concepts are reviewed alongside the fundamentals of AI and the potential of generative AI. The thesis also addresses data protection and relevant legislation, such as the GDPR, the EU AI act, and the NIS 2 directive, which guide the responsible use of AI and impose the requirements for personal data processing.

The research reveals that while AI holds a significant role in the future of cybersecurity, its use must be guided by careful risk management and responsible implementation. Global cooperation will be essential to mitigate emerging cyber threats. This work provides a comprehensive overview and deeper understanding of how AI can act as both a security enhancer and a source of novel threats.

Key words: artificial intelligence, information security, cyber threats, generative artificial intelligence

SISÄLLYS

ERITYISSANASTO

Identity theft	Identiteettivarkaus
Malware	Haittaohjelma
ChatBot	Keskustelurobotti
GenAI	Generatiivinen tekoäly
AI	Tekoäly
	Artificial intelligence
GDPR	EU:n tietosuoja-asetus
	General Data Protection Regulation
APTs	Kohdistetut hyökkäykset
	Advanced Persistent Threats
Enterprise GenAI	Yrityksille suunnattu räätälöitävä chatbot
IoT-laite	Internet of Things
	Internettiin yhdistettävä laite, joka vastaanottaa tai lähettää dataa
OSINT	Avointen tietolähteiden tiedustelua
	Open Source Intelligence
NIS	Kyberturvallisuusdirektiivi
	Network and Information Security
Phishing	Tietojenkalastelu

1 JOHDANTO

Tekoäly (AI), eli Artificial intelligence on muuttanut merkittävästi tietoturvan luonnetta sekä mahdollistamalla uusia puolustuskeinoja että synnyttäen uusia uhkia. Sen nopea kehitys on tuonut mukanaan merkittäviä hyötyjä, kuten automatisoidun uhkien tunnistamisen ja nopean reagoinnin. Nopea reagointi uhkiin on tuonut myös hyökkääjälle entistä tehokkaammat menetelmät, joka on tehnyt puolustamisesta tekoälyavusteisilla työkaluilla entistä tärkeämpää.

Tämän opinnäytetyön tavoitteena on analysoida tekoälyn vaikutuksia nykyaikaisen tietoturvan toimintaan sekä arvioida, miten tulevaisuudessa voidaan hyödyntää tekoälyä tietoturvan tukemiseksi. Työssä tarkastellaan laajasti nykyhetken tärkeimpiä ja ajankohtaisempia aiheita liittyen tekoälyyn ja tietoturvallisuuteen.

Opinnäytetyön alussa käsitellään keskeiset käsitteet, joiden pohjalta syvennytään laajemmin itse aiheeseen. Tekoälyyn liittyy vahvasti myös lainsäädäntö ja tietosuoja, joka on myös osana tutkielmaa. Tekoäly ja kyberrikollisuus liitettynä yhteen on hyvin ajankohtainen aihe. Tämän pohjalta keskitytään yleisimpiin huijauksiin ja loukkauksiin, mitä maailmalla tapahtuu. Tekoälyn tulevaisuuden näkymät ja niihin reagointi ovat aiheuttaneet paljon keskustelua tietoturva-alalla ja myös näitä asioita tutkitaan tässä opinnäytetyössä.

Tekoäly ja tietoturva aihealueena on hyvin laaja. Tämän vuoksi opinnäytetyö on pyritty rajaamaan suurimmaksi osin tarkastelemaan tekoälyn ja tietoturvallisuuden välistä yhteyttä. Erityisesti sitä, miten tekoäly on vaikuttanut tietoturvallisuuteen hyötyjen ja uhkien muodossa.

2 TIETOTURVA

Tietoturvalla tarkoitetaan tiedon saatavuuden, eheyden ja luottamuksellisuuden turvaamista. Saatavuudella tarkoitetaan, että tieto on saatavilla ja hyödynnettävissä tarvittaessa. Eheydellä tarkoitetaan tiedon täsmällisyyttä ja sen vastaavuutta alkuperäiseen tietoon. Luottamuksellisuus puolestaan tarkoittaa, että tiedon käsittelyssä varmistetaan luvattomien henkilöiden pääsyn estäminen tietoihin tai järjestelmiin. (Sanastokeskus 2018, 16.)

Tietoturvan toteuttamiseen liittyy useita konkreettisia järjestelyjä. Näihin kuuluvat fyysiset suojaukset kuten kulunvalvonta ja tilojen lukitus. Digitaalisia suojatoimia ovat muun muassa, tiedostojen ja asiakirjojen turvallinen säilytys, arkaluonteisen tiedon asianmukainen hävittäminen, tietojen salaus ja säännöllinen varmuuskopiointi. Teknisinä suojauksina käytetään palomuureja, virustorjuntaohjelmistoja ja digitaalisia varmenteita, kuten kaksivaiheista tunnistusta. (Sanastokeskus 2018, 16.)

Tietoturvan käsite kattaa laajan alueen, johon sisältyy tietoaineistojen, laitteiston, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen. Tietoturvallisuus viittaa tilanteeseen, jossa organisaation tietoturvariskit on tunnistettu ja hallinnassa. Tämä edellyttää organisaatiolta toimenpiteitä, jotta tietoturvallisuus olisi mahdollisimman tehokasta. Huomioon otettavia osa-alueita ovat muun muassa riskien tunnistaminen ja oikeanlainen tietoturvastrategia. (Sanastokeskus 2018, 16.)

2.1 Tietoturvauhkat

Yleisimpiä tietoturva uhkia ovat:

- Tietojenkalastelu (phishing): Tämä tapahtuu yleisimmin sähköpostin, tekstiviestien tai puheluiden välityksellä. Osa kalastelusta voi tapahtua myös suoraan erilaisten verkkosivustojen tai mainoksien kautta. Näihin kaikkiin on mahdollista tänä päivänä suojautua oikeanlaisen tietoturvapalvelun avulla. Kuluttajille, mutta myös yrityksille, esimerkiksi F-Secure tarjoaa omaa huijausturvapalvelua, joka tunnistaa väärät linkit ja huijaussivustot. Palvelu tarjoaa myös tekstiviestisuojauksen, joka suodattaa mahdolliset huijaukset suoraan puhelimen roskapostikansioon. Täytyy kuitenkin muistaa, että huijaukset paranevat koko ajan ja näiden edellä täytyy pysyä.

- Identiteettivarkaudet: Identiteettivarkauden (identity theft) uhriksi on mahdollista joutua, jos tietosi vuotavat. Tietoihin voivat kuulua nimi, puhelinnumero, syntymäaika, sosiaaliturvatunnus, osoite ja luottokorttinumero (What is identity theft 2023). Usein tietojen menetys johtuu tietojenkalastelusta tai haittaohjelmasta, jonka avulla pääsee verkkotileillesi.

- Haittaohjelmat: Haittaohjelma (malware), viittaa ohjelmaan, jonka tarkoituksena on aiheuttaa vahinkoa tai häiritä tietokoneiden, tietoverkkojen ja mobiililaitteiden toimintaa (What is malware 2022). Haittaohjelmien vaikutukset voivat olla hyvin laajoja ja näistä isoimpia voivat olla, esimerkiksi, henkilötietojen varastaminen tai rahojen varastaminen tililtä. Tilille pääsy tarkoittaa sitä, että henkilötiedot vuotavat samalla. Tämä mahdollistaa huijareille suuremman mahdollisuuden identiteettivarkautta varten.

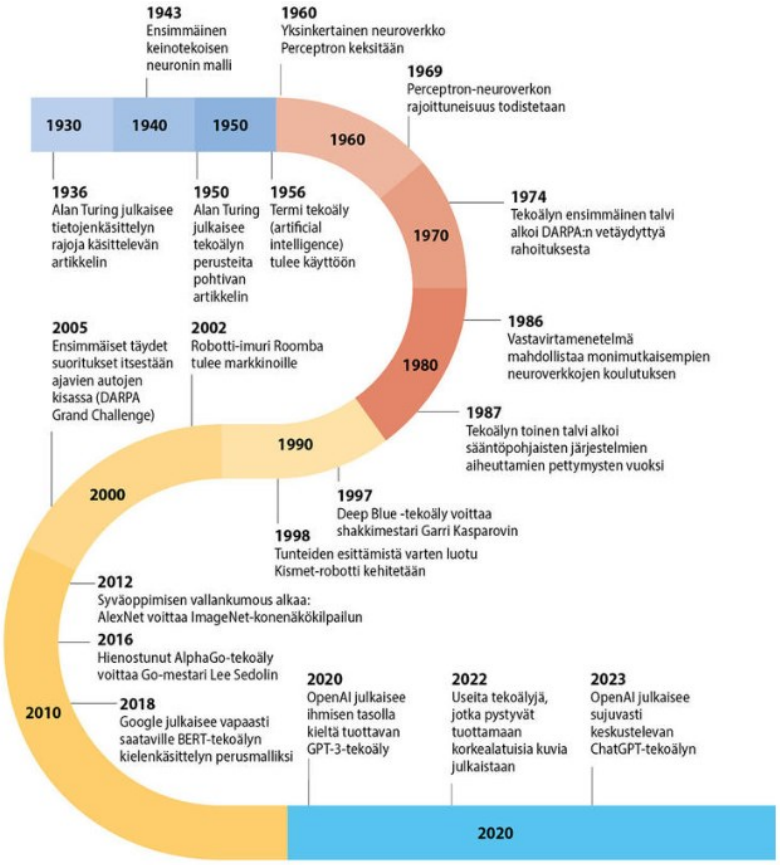
- Kohdistetut hyökkäykset: Kohdistetut hyökkäykset, jotka tunnetaan myös nimellä advanced persistent threats (APTs), tarkoittavat kyberhyökkäyksiä, jotka on räätälöity tietylle henkilölle, organisaatiolle tai toimialalle (VPN Unlimited, n.d). Hyökkäykset ovat usein hyvin vaikea tunnistaa, sillä nämä pyritään tekemään jälkeä jättämättä. Hyökkäykset suunnitellaan ja toteutetaan pyrkimyksenä varastaa arkaluontoista tietoa, joka tekee niistä vahingollisempia.

- Palvelunestohyökkäykset: palvelunestohyökkäys (denial of service attack) on hyökkäys, jolla pahantahtoinen toimija pyrkii estämään verkkoresurssin tai palvelun käytön häiritsemällä sen toimintaa (Toimintaohje - Palvelunestohyökkäys 2022). Hyökkäys voidaan toteuttaa useammalla eri tavalla. Nykyään hyökkäysmenetelmänä käytetään usein hajautettua hyökkäystä. Liikenne lähetetään useasta eri lähteestä samanaikaisesti. Yksi osa hyökkäyksen taustalla on palvelun kuormittaminen, joka mahdollistetaan hajautetulla hyökkäyksellä käyttäen useita eri laitteita, jotka ovat kaapattu hyökkäyskäyttöön. Usein kaapatun laitteen omistaja ei ole tästä tietoinen.

3 TEKOÄLY

Tekoälyllä (AI, artificial intelligence), tarkoitetaan koneen kykyä käyttää perinteisesti ihmisen älyyn liitettyjä taitoja, kuten päättelyä, oppimista, suunnittelemista tai luomista (Guillot 2023). Tekoäly kerää tietoa, ja oppii sen perusteella tuottamaan nopeamman ja resurssitehokkaamman työn tuloksen. Kerätyn tiedon perusteella tekoälyjärjestelmät kykenevät muokkaamaan järjestelmää tehokkaammaksi ja täten pystyvät tiettyyn pisteeseen työskentelemään itsenäisesti.

Tekoäly itsessään mielletään uudeksi asiaksi niin kuin se osaltaan onkin. Uuden aikakauden tekoäly on huomattavasti tehokkaampi ja automatisoidumpi kuin aikanaan. Tekoälyn kehityksen historia on kuitenkin alkanut jo 1940- ja 1950-luvuilta lähtien. Tällöin on otettu käyttöön ensimmäiset digitaaliset tietokoneet, joiden myötä tekoäly alkoi kehittyä. Kehitys on kuitenkin ollut erittäin hidasta ja vasta 2000- luvulla on alkanut syntyä ihmisten arkeen vaikuttavia innovaatioita. (Kolari & Kallio 2023, 1.2.)



KUVIO 1. Tekoäly 123. Tekoälyn kehitys (Kolari & Kallio 2023, 1.2.1).

Tekoälystä on tullut osa normaalia arkielämää. Suurin osa ihmisistä käyttää ehkä tiedostamattaankin useita tekoälypohjaisia palveluita. Näitä voivat olla esimerkiksi sosiaaliseen median tai navigointiin käytettävät sovellukset. Sosiaalisen median sovellukset oppivat tunnistamaan kohderyhmiin pohjautuvat videot, kuvat ja henkilöt. Navigointisovellukset pystyvät ehdottamaan tiettyä reittiä pohjautuen tekoälyyn perustuvaa dataa seuraten, joka tässä tapauksessa on voisi olla nopein reitti. Sama sovellus saattaa alkaa tunnistamaan käyttäjän kodin sijainnin tai mihin aikaan käyttäjä usein menee tiettyyn paikkaan. Moniin käyttämistämme sovelluksista tekoäly liittyy tavalla tai toisella. (Kolari & Kallio 2023, 2.1.)

3.1 Tekoälyn hyödyntäminen tietoturvassa

Tekoäly on muuttanut tietoturvallisuutta automatisoimalla tehtäviä, analysoimalla suuria tietojoukkoja ja ottamalla käyttöön älykkäitä algoritmeja, jotka parantavat uhkien havaitsemista ja reaaliaikaisia vastauksia (Islam 2024, 2.5.)

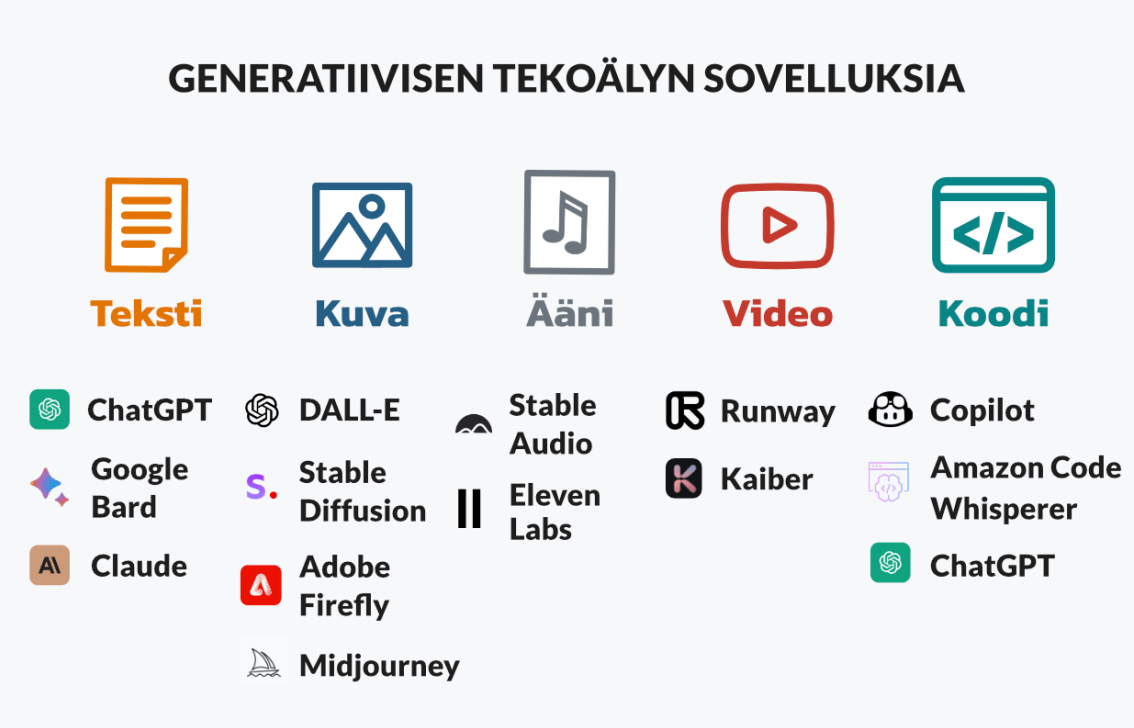
Järjestelmien nopea mukautuminen antaa etua kyberuhkiin. Koneoppimisen hyödyntäminen tietoturvassa on tuonut valtavasti mahdollisuuksia. Tätä on pystytty hyödyntämään haittaohjelmien, kiristysohjelmien ja muiden uhkien havaitsemiseen ja tunnistamiseen, jotta tietoturvaloukkauksia ei pääsisi tulemaan. Näiden järjestelmien avulla voidaan reaaliajassa tunnistaa poikkeavia verkkotoimintoja, kuten bottien toimintaa tai tietojen luvatonta siirtoa. Lisäksi on olemassa järjestelmiä, joita käytetään uusien ja tuntemattomien haittaohjelmien havaitsemiseen syväoppimisen avulla, mikä parantaa kykyä reagoida kehittyneisiin uhkiin. (Islam 2024, 2.5.1.)

Tekoäly ja automaatio mullistavat uhkien metsästystä etsimällä automaattisesti järjestelmiin liittyviä resursseja, luomalla dynaamisia lähtökohtia sekä tunnistaen ja ilmoittaen poikkeavuuksista reaaliajassa. Nämä tekniikat käsittelevät valtavia tietomääriä korostaakseen haitallisia tapahtumia ja tunnistaakseen merkit mahdollisista tietoturvaloukkauksista. Kehittyneet järjestelmät mahdollistavat ennakoivan uhkien havaitsemisen ja niiden lieventämisen ennen kuin ne aiheuttavat merkittäviä vahinkoja. (Islam 2024, 2.5.2.)

Tekoäly ei ainoastaan auta suojamaan järjestelmiä, vaan myös ennustamaan mahdolliset uhkat ja haavoittuvuudet ennen niiden eskaloitumista. Ennakoiva lähestymistapa perustuu siihen, että tekoäly analysoi tietoja ja tunnistaa niistä kuvioita, jotka voivat viitata tuleviin uhkiin. Kehittyneet poikkeamien havaitsemisjärjestelmät mahdollistavat tietoturvahäiriöiden ennustamisen jo ennen niiden toteutumista, ja käyttäytymisanalytiikkaa hyödyntävät järjestelmät mallintavat normaalia verkkokäyttäytymistä tunnistaakseen mahdollisia poikkeamia, jotka voivat olla merkki uhkasta. Tekoälypohjaiset riskipisteytysjärjestelmät taas arvioivat hyväksikäytön todennäköisyyttä ja auttavat organisaatioita priorisoimaan korjaustoimenpiteitä tehokkaammin. Ennakoivia oivalluksia tarjoavat tietoturvakeskukset hyödyntävät tekoälyä tuottaakseen ajantasaista tietoa mahdollisista uhkista, ja uhkatietoalustat ennustavat uusia uhkia analysoimalla laajoja tietomassoja. Näiden teknologioiden hyödyntäminen parantaa organisaatioiden kykyä ennakoida ja torjua kyberuhkia, mikä mahdollistaa nopeamman reagoinnin ja hyökkäysriskien minimoimisen. (Islam 2024, 2.5.6.)

3.2 Generatiivinen tekoäly

Generatiivinen tekoäly, eli GenAI on suunniteltu tuottamaan uutta sisältöä tekstin, äänen, kuvien tai videoiden muodossa. (Kallio 2025). Alustoja voidaan hyödyntää muun muassa käsikirjoitukseen, novelleihin, romaaneihin tai ohjelmistokehittäjien käyttöön. Generatiivisen tekoälyn taustalla on, että kone kykenisi luomaan ja ratkaisemaan samoja asioita kuin ihminen, mutta tekisi sen huomattavasti tehokkaammin ja nopeammin.



KUVIO 2. Generatiivisen tekoälyn sovelluksia (Kallio 2025).

Generatiiviselle tekoälyohjelmalle voi kertoa kohdennetusti asian mitä haluaa tämän tuottavan. Siltä voi myös kysyä kehitysehdotuksia valmiina olevaan tuotokseen. Tekoäly muistaa tuotetun tekstin, mikä helpottaa uusien muutosten tekemisen jo kerran muutettuun tekstiin.

Suurin osa generatiivisista tekoälyistä perustuvat syväoppimiseen, eli menetelmään, joka opettaa tietokoneita oppimaan ja tekemään päätöksiä itsenäisesti ilman, että niitä erikseen ohjelmoidaan. Nämä mallit on koulutettu suurella datamäärällä. Datan avulla keskustelurobotilla on yleensä erittäin hyvä käsitys siitä, minkälaista tekstiä haluaa sen tuottavan tai minkälaiseksi jo olemassa olevan

tekstin muuttaa. Keskustelurobotilta voit siis kysyä käsikirjoitusta esimerkiksi dokumentin tekoon aiheesta koirien sairaudet. (Caulfield 2023.)

3.2.1 Generatiivinen tekoäly ja tietoturva

Generatiivinen tekoäly mahdollistaa tietoturvalle kehittyneitä menetelmiä uhkien havaitsemiseksi. Tämä antaa myös paremmat mahdollisuudet tehdä analyysejä monimutkaisemmasta datasta. Tällöin voi saada nopeamman ja tarkemman tunnistamisen tietoturvauhkiin. Tietoturvahyökkäysten edellä voi olla vaikea pysyä, mutta tekoälyn avulla se on helpompaa ja nopeampaa. (How Can Generative AI be Used in Cybersecurity 2025.)

Generatiivisen tekoälyn avulla on mahdollista luoda malleja, jotka pysyvät ajan tasalla epätavallisista kyberuhkiin viittaavista uhkista. Tämän ansiosta turvajärjestelmien on mahdollista reagoida nopeammin ja tehokkaammin kuin perinteiset järjestelmät. Tämä mukautuu uusiin ja kehittyviin uhkiin, joka mahdollistaa tunnistusmekanismien pysyä edellä mahdollisilta hyökkääjiltä. Tästä on suuresti hyötyä tietoturvatiimeille, jotta heillä on mahdollisuus suunnitella omaa puolustusmekanismiaan tulevia hyökkäyksiä vastaan. (What is generative AI in cybersecurity, n.d.)

Tietoturvaa parantavia tekoälysovelluksia on useita. Osa näistä on generatiivisia, joita voidaan käyttää jo tuotetun koodin parantamiseksi tai uhkien havaitsemiseen. Yleisiä generatiivisia tekoäly sovelluksia, joiden avulla koodin tietoturvauhkat ja virheet voidaan tarkastaa helposti, ovat muun muassa GitHub Copilot ja OpenAI ChatGPT. Microsoft Security Copilot sen sijaan mahdollistaa Microsoft-ekosysteemiä käyttäville hyvin laajan virtuaaliavustajan, joka tehostaa työnkulkua ja suojaa samalla ohjelmistoa, jotta uhkia ei pääsisi tulemaan. Tämä priorisoi uhkia reaaliajassa, joka on hyvin tärkeää, jotta yritykset pysyvät ajan tasalla kaikista uhkista ja mahdollisista vuodoista.

Tietoturvaparannuksia voidaan miettiä myös toisesta näkökulmasta. Yritys voi järjestää työntekijöilleen esimerkkejä kyberrikollisten käyttämistä taktiikoista generatiivisella tekoälyllä. Näitä voi olla esimerkiksi tietojenkalasteluhyökkäykset tai anonymisoidut kopiot yrityksen tiedoista. Tietoturvatiimit voivat hyödyntää näitä

koulutustarkoitukseen, jonka tarkoituksena on tunnistaa ja välttää mahdolliset tietojenkalasteluhuijaukset. Tämä parantaa luonnollisesti yrityksen yleistä tietoturvatietoisuutta. (Padhy 2024.)

3.2.2 Generatiivisen tekoälyn vahvuudet ja rajoitukset

Generatiivinen tekoäly on nopeasti kehittyvä teknologia-ala, mutta se on vielä keskeneräinen osittain. Tuotettu teksti voi olla väärää tai vanhentunutta tietoa, joka tekee lähteiden varmentamisesta tärkeää. On kuitenkin myös paljon asioita, missä se on erittäin tehokas työkalu.

Scribbr:n artikkelissa (What is Generative AI 2023) Caulfield listaa, vahvuuksiksi muun muassa joustavuuden useiden eri asioiden käyttöön, joka avaa mahdollisuuksia käyttää tätä monissa eri tilanteissa. Asioiden tutkiminen on tehty hyvin helpoksi, sillä generatiivinen tekoäly tekee sen hyvin nopeasti ja tehokkaasti. On kuitenkin myös rajoituksia, joita ovat muun muassa virheelliset vastaukset tai kuvien muodossa virheelliset yksityiskohdat, kuten liian monta sormea henkilön kädessä. (Caulfield 2023.)

Aiemmin rajoituksiin on kuulunut myös lähteiden puuttuminen tai näiden löytäminen. Tänä päivänä näihin on kuitenkin tullut isoja muutoksia. Lähteiden etsiminen ja jopa tuotettuun tekstiin viittaus on mahdollinen GenAI työkaluilla. Näistä esimerkkinä ChatGPT ja perplexity AI. Lähdeviittaukset on kuitenkin hyvä tarkistaa suoraan viitatusta tekstistä.

Generatiivinen tekoäly voi vaikeuttaa yrityksen sisällä generatiivisten tekoälyalustojen käyttöä julkisen datan hyödyntämisen takia. Tätä näkökulmaa voi miettiä myös tietynlaisena rajoituksena. Yrityksillä on paljon asiakkaiden tietoja ja myös yrityksen sisäisiä tietoja, joista täytyy pitää erityisen tärkeää huolta, jotta nämä ei pääse vuotamaan. On tärkeää, että yritys on asettanut oman tietosuojastrategian, missä on tarkkaan määritelty minkälaista dataa voi syöttää tekoälyalustalle. Salasanat, käyttäjätunnukset ja yrityksen salassa pidettävät tiedot, kuten erilaiset luvut, jotka eivät saa vuotaa, on hyvin tärkeää suodattaa pois ennen tämän laittamista julkista dataa hyödyntävälle tekoälyalustalle.

On olemassa kuitenkin hieman tietoturvallisempiakin ratkaisuja. Yrityksille on luotu Enterprise tekoälyavusteisia kehitysympäristöjä täysin yrityksen sisäiseen käyttöön, johon voi kutsua vain tiimin jäseniä. Tämä mahdollistaa tietoturvallisemman ratkaisun käyttää tekoälyavusteisia alustoja, jolloin tiedon vuotaminen on paljon epätodennäköisempää. Tieto ei siis pääse vuotamaan julkista dataa hyödyntäville alustoille.

4 TIETOSUOJA JA LAINSÄÄDÄNTÖ

4.1 Tietosuoja-asetus (GDPR)

Euroopan unioni on rakentanut laajan ja johdonmukaisen sääntelykehyksen kyberturvallisuuden vahvistamiseksi sekä digitaalisen infrastruktuurin suojaamiseksi kaikissa jäsenvaltioissa. Vuonna 2018 tullut yleinen tietosuoja-asetus (GDPR) määrittää tarkat säännöt henkilötietojen käsittelylle ja edellyttää organisaatioilta vahvoja turvatoimia sekä velvoittaa ilmoittamaan tietoturvaloukkauksista 72 tunnin kuluessa tämän tapahtumisesta. Vaatimuksia sovelletaan sekä eurooppalaisiin organisaatioihin, jotka käsittelevät ihmisten henkilötietoja EU:ssa, että EU:n ulkopuolisiin organisaatioihin, mikäli tietojen käsittely kohdistuu EU:n alueella asuviin ihmisiin. (Yleinen tietosuoja-asetus 2025.)

4.2 GDPR ja tekoäly: vaatimustenmukaisuus ja haasteet

Tekoälyn käyttö on tuonut tarpeen valvoa tarkemmin henkilötietojen ja esimerkiksi yrityksen sisäisiä tietoja, jotta nämä ei pääsisi vuotamaan. Generatiivinen tekoäly varsinkin oppii syötetyn datan perusteella, ja tarjoaa opitun datan perusteella tuloksia. Tekoälyjärjestelmä ei välttämättä käsittele järjestelmään syötettyä tietoa tietosuoja-asetusten mukaisesti. Tieto voi siis vuotaa yrityksen ulkopuolelle inhimillisestä virheestä, jota ei pysty palauttamaan. Suuri osa tekoälyalustoista on yhdysvaltalaisilla yrityksillä hallussa ja tällöin GDPR pitää ottaa huomioon siinä, minkälaista dataa näihin syöttää. On siis mahdollista, että nämä pääsisivät vuotamaan Euroopan ulkopuolelle, mikäli tätä ei noudata ja tällöin rikkoisi suoraan GDPR:n vaatimuksia.

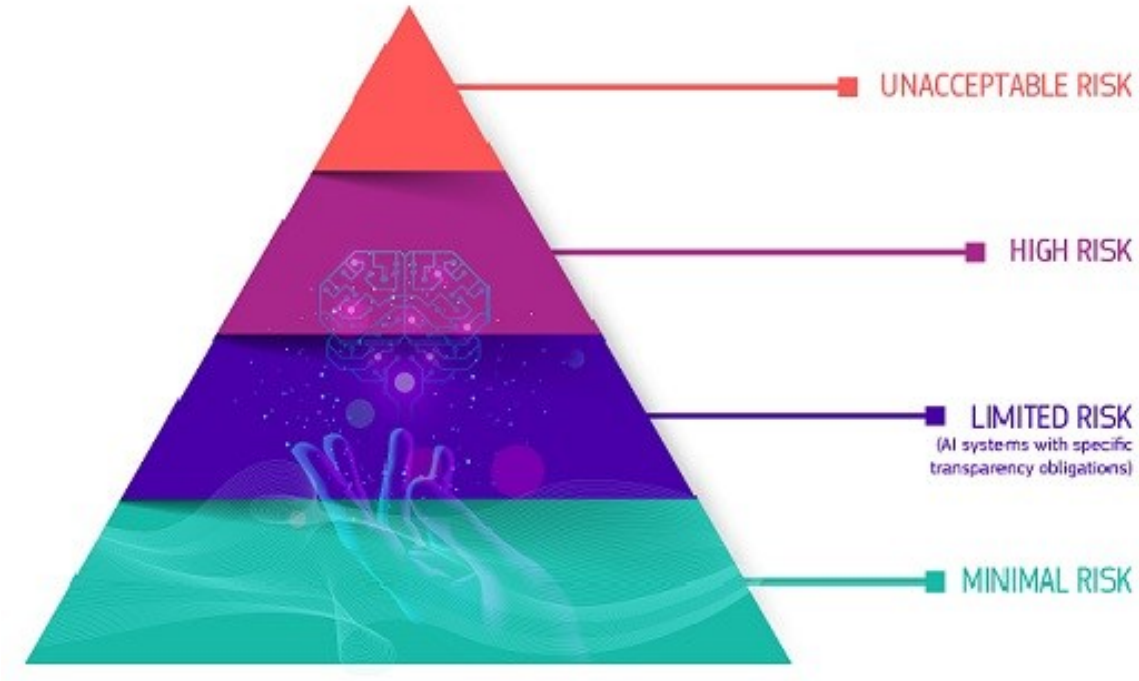
Tekoäly voi olla haastava yhtälö GDPR:n ja tekoälyn sovittamisessa yhteen, mutta tämä on kuitenkin tehtävissä oikeanlaisilla toimilla. GDPR:n keskeisiä vaatimuksia ovat muun muassa tiedon minimointi, tarkistussidonnaisuus ja läpinäkyvyys. Tekoälykehittäjien on siis varmennettava, että järjestelmät keräävät vain välttämättömiä tietoja ja niin, että käyttäjä on tietoinen siitä, miten hänen tietojaan käytetään. Vaatimusten noudattaminen pitävät huolen, että tietosuojariskit pysyvät kurissa ja pystyvät täten noudattamaan GDPR:n vaatimuksia. Tietosuojaris-

kien tarkempi tehostaminen on suositeltavaa. Näitä voidaan hallita erilaisilla toimilla, kuten tietojen tarkemmalla peittämisellä, kehittämällä selkeitä tietosuojakäytäntöjä ja varmistamalla, että tekoälyjärjestelmät ovat läpinäkyviä ja selitettävissä. (Privaon n.d.)

4.3 EU:n tekoälysäädös

EU:n tekoälysäädös on maailman ensimmäinen kattava lainsäädäntö tekoälyjärjestelmien käytön sääntelemiseksi. Asetus astui voimaan 1. elokuuta 2024 ja sen soveltaminen on käynnistynyt portaittain kahden vuoden siirtymäajalla. Kieltoja ja tekoälylukutaitovelvoitteita alettiin soveltamaan 2. helmikuuta 2025 alkaen. Lisäksi yleiskäytännöllisiä tekoälymalleja koskevia hallintosääntöjä ja velvoitteita koskeva säädäntö on tulossa 2. elokuuta 2025 alkaen. Säänneltyihin tuotteisiin lisättyjä suuririskisiä tekoälyjärjestelmiä koskee pidennetty siirtymäaika, joka jatkuu 2. elokuuta 2027 saakka. (Euroopan komissio 2025.)

Tekoälyasetuksen ensisijaisena tavoitteena on edistää luotettavaa tekoälyä Euroopassa. Lainsäädäntö perustuu riskipohjaiseen lähestymistapaan, jossa tekoälyjärjestelmät jaetaan neljään luokkaan niiden aiheuttaman riskin mukaisesti. Kyseisiä luokkia ovat kielletyt järjestelmät, korkean riskin järjestelmät, läpinäkyvyysriskin omaavat järjestelmät ja vähäisen tai olemattoman riskin järjestelmät. Kaikki tekoälyjärjestelmät, joita pidetään selvänä uhkana ihmisten turvallisuudelle, toimeentulolle ja oikeuksille, kuuluvat kiellettyihin järjestelmiin. On olemassa myös tekoälyn käyttötapauksia, jotka voivat aiheuttaa vakavaa riskiä terveydelle, turvallisuudelle tai perusoikeuksille, jotka luokitellaan korkean riskin luokkaan. Läpinäkyvyysriskin omaavissa järjestelmissä on suuressa osassa tekoälyn käytön läpinäkyvyyden puute. Tämä tarkoittaa sitä, että järjestelmissä ei välttämättä kerrota ihmisille, että he ovat vuorovaikutuksessa koneen kanssa. Kaikkiin luokkiin paitsi vähäisen tai olemattoman riskin omaaviin järjestelmiin on tulossa muutoksia tekoälysäädöksessä. Vähäisen tai olemattoman riskin kohdalla on katsottu, että näitä ei tarvitse säädellä hyvin pienen riskin vuoksi. (Euroopan komissio 2025.)



KUVIO 3. Riskiluokat (Euroopan komissio 2025).

4.4 NIS 2 -direktiivi

NIS 2 -direktiivillä luodaan yhtenäinen oikeudellinen kehys kyberturvallisuuden ylläpitämiseksi 18 kriittisellä alalla kaikkialla EU:ssa. Säännöksessä kehotetaan jäsenvaltioita määrittelemään kansalliset kyberturvallisuusstrategiat ja tekemään yhteistyötä EU:n kanssa rajatylittävää reagointia ja täytäntöönpanon valvontaa varten (Euroopan unioni 2025.)

NIS 2 korvaa aiemman NIS- direktiivin laajentamalla soveltamisalaa, selkeyttämällä sääntöjä ja vahvistamalla valvontavälineitä. Direktiivi edellyttää, että jäsenvaltiot parantavat kyberturvallisuusvalmiuksiaan, ottavat käyttöön riskienhallintatoimenpiteitä ja raportointivaatimuksia useille eri toimialoille sekä vahvistavat yhteistyötä, tietojen jakamista ja valvontaa. Jokaisen jäsenvaltion on laadittava kansallinen kyberturvallisuusstrategia, joka kattaa muun muassa toimitusketjun turvallisuuden, haavoittuvuuksien hallinnan sekä kyberturvallisuuskoulutuksen. Lisäksi jäsenvaltioiden on ylläpidettävä ja päivitettävä luetteloa keskeisten palvelujen tarjoajista varmistaakseen, että nämä toimijat noudattavat direktiivin vaatimuksia. (Euroopan unioni 2025.)

Direktiivi sisältää myös säännöksiä valvonnasta, täytäntöönpanosta ja vapaaehtoisista vertaisarvioinneista, joiden tavoitteena on parantaa keskinäistä luottamusta ja kyberturvallisuusvalmiuksia EU:ssa. Lisäksi direktiivi korostaa ylimmän johdon vastuuta kyberturvallisuusriskien hallinnassa. Direktiivillä perustetaan myös tietoturvaloukkauksiin reagoivien ja niitä tutkivien yksiköiden verkosto, jonka tehtävänä on vaihtaa tietoja kyberuhkista ja reagoida poikkeamiin. Laajamittaisten kyberturvallisuuspoikkeamien varalta direktiivi perustaa Euroopan kyberkriisien yhteysorganisaatioiden verkoston, joka tukee koordinoitua hallintaa ja tietojenvaihtoa jäsenvaltioiden ja EU:n toimielinten välillä. (Euroopan unioni 2025.)

NIS 2- direktiivi velvoittaa poikkeamien ilmoittamista ja riskienhallinta toimenpiteitä, mikä edistää myös tekoälypohjaisten järjestelmien turvallisuutta. Jokaisen jäsenvaltion kyberturvallisuusstrategia tulee vahvistamaan EU:n yhteistyötä jäsenvaltioiden kanssa, joka edesauttaa tekoälyn tuomien uhkien havaitsemisessa ja torjumisessa.

5 TEKOÄLY TYÖKALUNA KYBERRIKOLLISUUDESSA

Tekoäly on mahdollistanut monen tietoturvaa ylläpitävän ratkaisun ohituksen. Tekoälystä on tullut keskeinen osa yritysten työkalupakkia, mutta tämä on myös mahdollistanut vaarallisen aseen kyberrikollisten toiminnassa. Vaikka sovellukset on suunniteltu hyväntahtoisiin tarkoituksiin, kuten tiedonhakuun, uuden luomiseen tai vaikkapa tietoturvan parantamiseksi, on tämä tuonut myös kyberhyökkäyksiä mahdollistavat uhkat.

Tekoälyn tuomia etuja ja parannuksia hyökkäystarkoituksiin on useita. Ennen tekoälyä hyökkääjät ovat joutuneet käyttämään paljon enemmän vaivaa ja aikaa hyökkäyksen toteutukseen. Hyökkäyksen suunnittelussa ja toteutuksessa on käytetty suhteellisen yksinkertaisia työkaluja. Asiantuntijuus on ollut siis isossa roolissa hyökkäyksien toteutuksessa.

Tekoälyn tuomat muutokset kyberhyökkäyksiin, voidaan jakaa kolmeen osaan, joita ovat automatisointi, työkalujen parantaminen ja tehostaminen, sekä uusien kykyjen mahdollistaminen, kuten painallusten tunnistaminen näppäimistöllä liikkeen perusteella. Nämä kaikki tuovat hyökkääjälle isoja etuja ja antaa suuremman mahdollisuuden hyökkäyksen onnistumiselle. (Aksela, Marchal, Patel, Rosenstedt 2022, 9.)

5.1 Hyökkäyksiin käytettävät tekoälyn mahdollistamat tekniikat

Tekoälyyn perustuvat kyberhyökkäykset hyödyntävät kehittyneitä koneoppimisalgoritmeja ja tekoälytekniikoita automatisoidakseen, nopeuttaakseen ja tehostaakseen hyökkäyksen eri vaiheita. Näihin sisältyy muun muassa automatisoitu haavoittuvuuksien tunnistaminen, adaptiivinen hyökkäysten suunnittelu, hyökkäyspolkujen edistäminen, takaovien luominen järjestelmiin, tietojen suodattaminen, sekä kohdennettu järjestelmähäirintä. (Stanham 2025.)

Stanham listaa artikkelissa (AI-powered cyberattacks 2025), viisi pääominaisuutta kyberhyökkäyksille, jotka toimivat tekoälyllä. Ensimmäinen näistä on hyökkäysten automaatio, jossa tekoäly- ja generatiivisten tekoälyä tukevien työkalujen

lisääntyvä saatavuus mahdollistaa hyökkäysten tutkimuksen ja toteutuksen automatisoinnin. Automaatio tekee itsessään hyökkäyksistä kattavampia, nopeampia ja muovautuvampia. Työmäärä tämän ansiosta on huomattavasti pienempi ja lisää hyökkäyksien itseohjautuvuutta. (Tekoälyn mahdollistamat kyberhyökkäykset, 2022.)

Tehokas tiedonkeruu on näistä toinen, jossa tekoäly nopeuttaa tiedustelua, jossa etsitään kohteita, haavoittuvuuksia ja omaisuutta. Tiedustelun osana on käytetty OSINT-prosessia (Open Source Intelligence), eli avoimien tietolähteiden tiedustelua. Tämä on pystytty täysin automatisoimaan tekoälyn avulla, joka tekee tiedustelun kohteille huomattavasti helpommaksi. Prosessi pitää sisällään tietojen keräämisen, analysoinnin ja yhteenvedon. Tietojen kerääminen tapahtuu kattavasti muun muassa, verkkosivuilta ja sosiaalisesta mediasta. Näiden avulla on mahdollista selvittää esimerkiksi laajempia tietoja yksilöistä, yrityksestä tai heidän työntekijöistään. (Reznikov 2024.)

Räätälöinti on kolmas ominaisuus, jossa tekoäly kerää ja analysoi julkisia tietoja luodakseen personoituja, osuvia ja ajankohtaisia viestejä, joita voidaan käyttää tietojenkalasteluhyökkäyksille ja muille suunnittelutekniikoita hyödyntäville hyökkäyksille. Oppimisen vahvistaminen on neljäs. AI-algoritmit oppivat ja mukautuvat reealiajassa. Tämä tarkoittaa sitä, että vaikka työkalut kehittyvät jatkuvasti ja tarjoavat tarkempia näkemyksiä käyttäjille, ne myös kehittyvät auttamaan vastustajia eli hyökkääjiä. Tekniikoiden parantaminen ja hyökkääjän suojautuminen havaitsemiselta on tehty helpommaksi. (Stanham 2025.)

Työntekijöihin kohdistaminen on näistä viimeinen. Tekoälyä voidaan käyttää tunnistamaan organisaation henkilöitä. Aiemmin mainitussa OSINT-prosessissa voidaan näin tehdä. Työntekijöihin kohdistamisella pyritään saamaan pääsy arkaluontoisiin tietoihin. Työntekijöillä, joihin nämä kohdistuvat, on usein pääsy näihin tai heillä on laaja käyttöoikeus järjestelmään.

5.2 Verkkojen haavoittuvuus

Haavoittuvien verkkojen etsiminen hyökkääjille on tehty huomattavasti helpommaksi tekoälypohjaisilla työkaluilla. Työkalut skannaavat verkkoja 24/7, etsien avoimia portteja. Nämä kykenevät etsimään heikosti suojattuja IoT-laitteita (Internet of Things), joita voi olla mikä vaan laite, joka voidaan yhdistää internetiin datan vastaanottamiseksi tai lähettämiseksi. Järjestelmät kykenevät tarkistamaan myös vanhentuneita laitteita, jossa suojaus on olematon, kuten tietokoneen vanhentuneet käyttöjärjestelmät. (Balaganesh 2023.)

IoT-laitteiden yleistyminen korostaa tekoälyn merkitystä laitteiden turvaamiseksi. Tekoälyratkaisut puolustukseen ovat välttämättömiä, jotta avoimien porttien tiedustelu voidaan havaita ajoissa. Suojausmenetelmiä hyökkäyksiä varten on kuitenkin kehitetty. Nämä kykenevät analysoimaan poikkeavuuksia ja havaitsemaan hyökkäykset ajoissa, jotta suurempia vahinkoja ei pääsisi tulemaan. (Islam 2024, 2.5.4.)

5.3 Tekoälyhuijaukset

Tekoälyhuijaukset lisääntyvät ja teknologian kehittyessä tekevät näistä huomattavasti vaikeammin tunnistettavia. Erityisesti tekoäly on avannut uusia mahdollisuuksia huijareille. Tekoälyä voidaan hyödyntää muun muassa huijaussivustojen luontiin, väärennettyihin mainoksiin, syväväärennöksiin, viestihuijauksiin sekä huijauspuheluihin.

5.3.1 Uskottavat huijaussivustot yhdistettynä väärennettyyn mainontaan

Huijaussivustoja pystytään luomaan tänä päivänä helposti ja edullisesti. Ennen generatiivisten tekoälyalustojen tuloa, huijaussivustojen tekeminen vaati huomattavasti enemmän aikaa ja taitoa. Tänä päivänä kuka vain voi avata generatiivisen tekoälyalustan, jonka voit pyytää tekemään samankaltaisen nettisivuston kuin alkuperäinen oikea sivusto on. Oikeilla kysymyksillä ja tiedolla mitä haluat tehdä, tekee se sinulle hyvin aidon oloisen sivuston, joka jäljittelee tarkasti aitoa sivustoa. Tietynlaista ammattitaitoa tämä kuitenkin vaatii, jotta saa sen näyttämään katsojan silmään oikealta sivustolta.

Tekoäly tosiaan pystyy luomaan aidon oloisia sivustoja, jotka jäljittelevät oikeita sivustoja. Suurelle osaa sivustoista voi ostaa omaa mainostilaa. Tämän kaltaiset sivustot pystyvätkin huijaamaan markkinoijat ajattelemaan, että he sijoittavat mainoksiaan hyvämaineisille alustoille, josta on heille hyötyä. Generatiivinen tekoäly voi myös väärentää näyttökertoja luomalla väärennettyjä käyttäjämerkkijonoja, joka voi myös näyttää käyttäjän silmiin lupaavalta alustalta. (Intergral Ad Science 2024.)

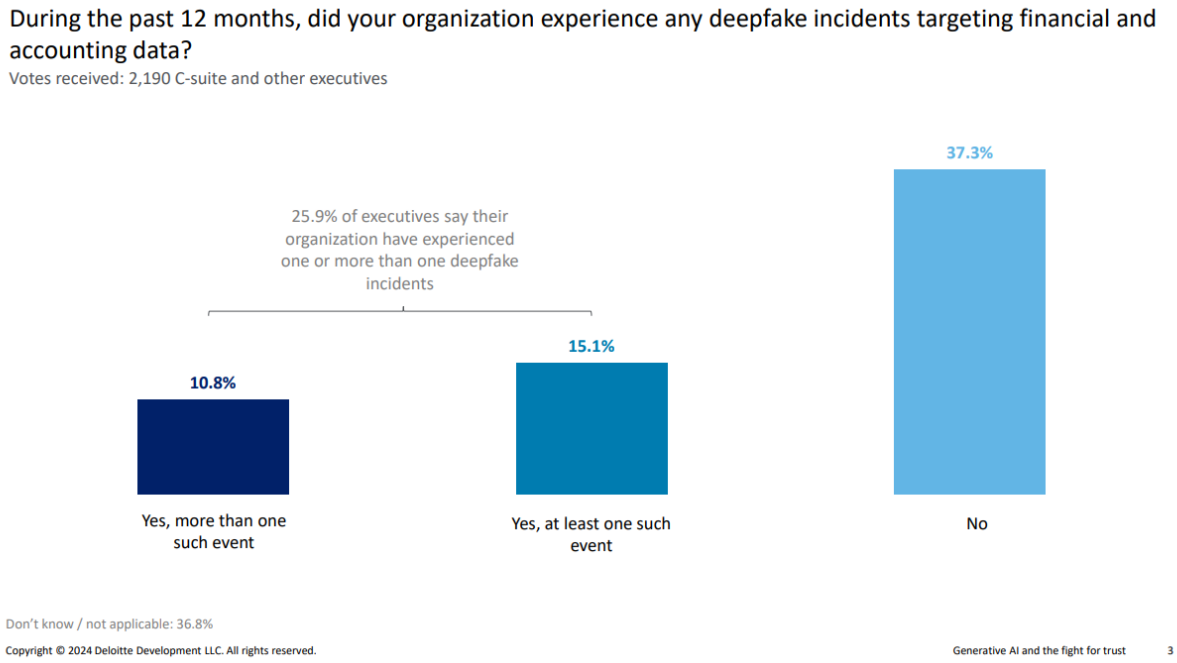
Google tai sosiaalisen median alustat tarjoavat mainostilaa yrityksille, joiden kautta moni vierailee mainostajan sivustolla. Mainostajien sivustoja pidetään usein luotettavina, kuten ne usein ovatkin. Osa näistä saattaa kuitenkin johtaa mahdollisille huijaussivustoille. Kaikilta alustoilta löytyy oma tiimi mainoksien varmentamiseksi, mutta tekoäly on tuonut haasteita näiden varmentamiseksi. Mainokset ovat niin hyvin kirjoitettuja ja aidon oloisia, joka mahdollistaa myös näiden vuotamisen alustoille, joita ihmiset pitävät luotettavina.

5.3.2 Syväväärennökset (Deepfake)

Syväväärennös, eli deepfake on tekoälyn luoma video-, kuva- tai äänitiedosto, jonka tarkoituksena on huijata ihmisiä (Stanham 2025). Syväväärennöksiä käytetään usein pelkästään hauskan videon luomiseen tai hämmentämään ihmisiä. Osa videoista ja kuvista ovat kuitenkin tehty huijaamaan ihmisiä esimerkiksi valeuutisten kautta. Näitä voidaan käyttää korkean profiilin henkilöiden herjauskampanjoina tai kyberhyökkäyksissä. (Stanham 2025.)

Sosiaalisen median kautta syväväärennös videoita ja kuvia esiintyy hyvin paljon. Syväväärennöksissä ihmisiä kehotetaan esimerkiksi sijoittamaan johonkin tiettyyn kohteeseen, joka on videoon muokatun henkilön mukaan täydellinen tapa tehdä rahaa. Tuntemattoman suusta kukaan ei tähän kiinnittäisi kummemmin huomiota, mutta kun kyseessä on vaikutusvaltainen henkilö, kiinnittää se ihmisen huomion. Videosta voi olla vaikeaa tunnistaa väärennös, sillä usein ääni ja suun liikkeet saadaan näyttämään hyvin aidolta.

Syväväärennökset kehittyvät entistä vaarallisemmiksi ja helpommin saavutettaviksi, mikä saa petostapaukset lisääntymään tulevaisuudessa. Deloitte julkaisi vuonna 2024, kyselyn yhdysvaltaisille johtajille, jossa tiedusteltiin, onko heidän organisaatiossaan ollut syväväärennöstapauksia. Kyselyssä tuli ilmi, että yli 25 % kertoi kohdanneensa organisaation sisällä tapahtuneisiin syväväärennöstapauksiin. (Deloitte 2024.)



KUVIO 4. Kohdistetut syväväärennös tapaukset yhdysvaltalaisille johtajille (Deloitte 2024).

5.3.3 Viestihuijaukset

Viestihuijaukset ovat olleet jo pitkään osana huijareiden taktiikoita, mutta aiemmin ne on jouduttu tekemään hieman monimutkaisemmin ja näkyvämmin. Aiemmin käytössä on usein ollut automaattisesti ohjelmoituja, roskapostia lähettäviä botteja. Tekstin muotoilu on tehty huomattavasti tehokkaammaksi tekoälyn avulla, johon onkin siirrytty. Tekoäly on kykeneväinen kirjoittamaan hyvin selkeää suomen kieltä, jossa myös kielioppi on huomioitu suhteellisen hyvin. Tässä kuitenkin on vielä jonkin verran virheitä, jolloin tarkkasilmäisimmät osaavatkin tunnistaa huijauksen jo pelkästä tekstistä. (Tekoälyhuijaukset 2024.)

Viestihuijaukset toimivat pääasiassa sähköpostin ja tekstiviestien kautta. Suurin osa sähköposteista menee suoraan roskapostikansioon, joka meneekin usein

täysin ohi, jos sinne on jotain saapunut. Tekstiviestihuijaukset ovatkin sitten toinen asia. Ilman erillistä suodatusohjelmaa suurin osa tekstiviesteistä tulee läpi, joka antaa huijareille mahdollisuuden onnistua entistä tehokkaammin. F-Securen artikkelissa (Yleisiä tekstiviestihuijauksia 2024) McAuley mainitsee, että jopa 12 prosenttia kyberrikoksista on tekstiviestihuijauksilla tehtyjä. Heidän tavoitteenaan on saada henkilöä klikkaamaan harkitsemattomasti jotain linkkiä, joka vie uskottavan näköiselle sivustolle. Tämä saattaa johtaa henkilötietojen varastamiseen tai pankin kautta rahojen viemiseen.

5.3.4 Esimerkkejä huijaussähköpostista ja huijaustekstiviestistä

Tätä opinnäytetyötä varten pyydettiin generatiivista tekoälyä kirjoittamaan esimerkit huijaussähköpostista ja huijaustekstiviestistä. Tekstin luonnissa on käytetty OpenAI:n ChatGPT keskustelurobottia. Tästä tämä suoriutui erinomaisesti. Viestit ovat kirjoitettu erittäin hyvällä suomen kielellä, eikä kieliopillisia virheitä ole juurikaan. Tietyistä merkeistä voi huomata, että nämä tulevat väärän lähettäjän kautta.

ChatGPT:n Nordean nimissä luodusta huijaussähköpostista huomaa suoraan erikoisen sähköpostiosoitteen. Samalla tästä voi huomata, että viesti yrittää luoda kiireen tuntua ja uhkaa tilin sulkemisella pysyvästi.

ChatGPT:n Postin nimissä luodusta tekstiviestihuijauksesta huomaamme saman ominaisuuden, joka välittää kiireen tuntua. Lisäksi viestissä pyydetään maksamaan käsittelymaksu, joka on hyvin yleinen keino huijata pankkitunnukset ja henkilötiedot.

Voisitko kirjoittaa minulle phishing sähköpostin, joka tulee lähettäjältä nordea?

Tässä on esimerkki huijaussähköpostista, joka esiintyy Nordean lähettämänä:

Lähettäjä: Nordea security@nordea-verification.com
Aihe: ⚠️ **Tärkeä ilmoitus: Tilisi käyttö on rajoitettu**

Hyvä asiakas,

Olemme havainneet epätavallista toimintaa pankkitililläsi. Turvallisuussyistä tilisi käyttö on väliaikaisesti rajoitettu, kunnes vahvistat henkilöllisyytesi.

Voit palauttaa tilisi normaalin käytön vahvistamalla tietosi alla olevan turvallisen linkin kautta:

🔹 Vahvista tilisi nyt

Huomioithan, että jos et suorita vahvistusta 24 tunnin kuluessa, tilisi voi jäädä pysyvästi estetyksi.

Kiitos yhteistyöstäsi.

Ystävällisin terveisin,
Nordea Asiakaspalvelu
📞 0200 5000 (24/7)

KUVA 1. ChatGPT Nordea tietojenkalastelu sähköposti.

Voisitko tehdä minulle esimerkin huijaustekstiviestistä, joka tulee postin kautta?

Tässä on esimerkki huijaustekstiviestistä, joka esiintyy postin lähettämänä:

Lähettäjä: Posti
Viestin sisältö:

📦 **Pakettisi toimitus on keskeytetty!**
Emme voineet toimittaa pakettiasi puutteellisten osoitetietojen vuoksi. Vahvista toimitustiedot ja maksa pieni käsittelymaksu (1,90€) alla olevan linkin kautta, jotta paketti voidaan toimittaa:

🔹 Päivitä tiedot

Jos et päivitä tietoja 24 tunnin kuluessa, paketti palautetaan lähettäjälle.

Kiitos,
Posti

KUVA 2. ChatGPT Posti tekstiviestihuijaus.

5.3.5 Puhelut tekoälyn avustamana

AI-äänen kloonaus on mullistanut huijaukset puheluiden kautta. Tekoäly mahdollistaa äänen väärentämisen entistä uskottavammin ja monipuolisemmin. Nykyään huijarit pystyvät luomaan tekoälyavusteisesti täysin keinotekoisia ääninäytteitä, jotka kuulostavat aidolta ja saavat ne lausumaan halutun sisällön. Lisäksi teknologia mahdollistaa tietyn henkilön äänen jäljittelyn, jolloin huijauksessa voidaan esiintyä jonkun tunnetun henkilön äänellä. Tämä tekee tästä entistä huolestuttavampaa, sillä nämä ovat huomattavasti vaikeammin tunnistettavia. Ääntä voidaan väärentää hyödyntämällä julkisia videoita esimerkiksi sosiaalisesta mediasta. (Tekoälyhuijaukset 2024.)

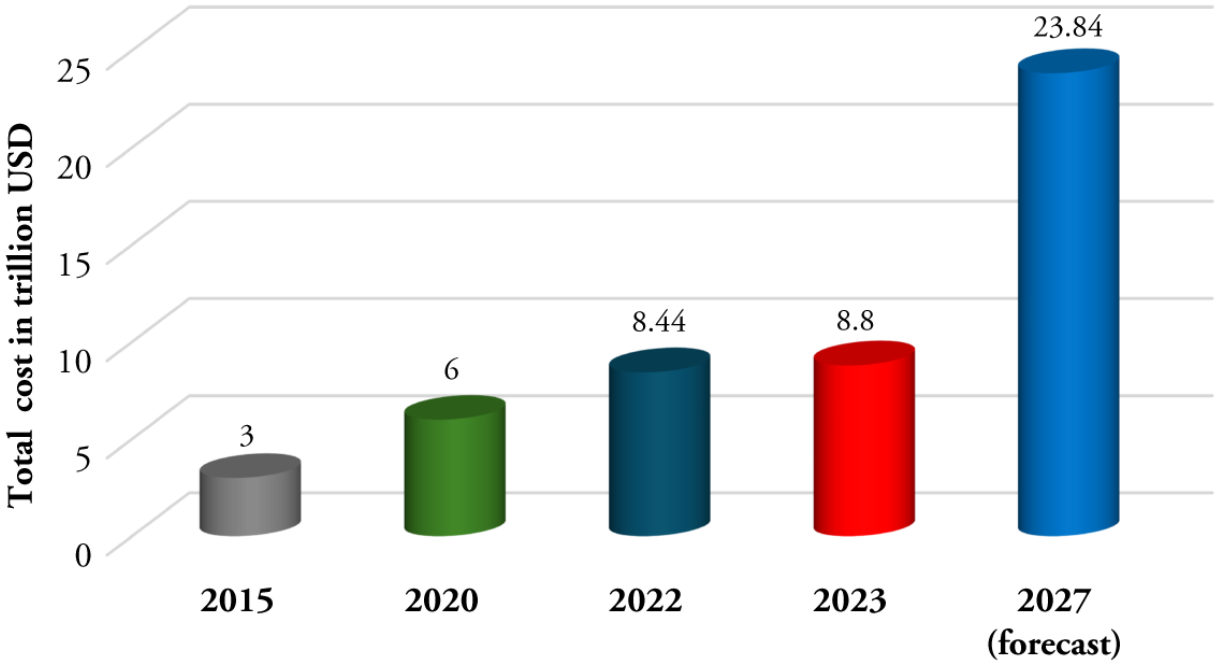
Äänenkloonauksella tapahtuneita kyberhuijauksia on tapahtunut useita. Nämä voivat esimerkiksi soittaa sinulle hätääntyneen puhelun toisen läheisen henkilön äänellä kertoakseen, että hänet on kidnapattu ja ainut millä hänet vapautettaisiin, on maksamalla huijarin vaatima summa. Näissä tilanteissa on hyvin vaikeaa arvioida, onko tilanne tosi. Usein näissä tilanteissa uhri on kuitenkin älynnyt soittaa läheiselleen varmistaakseen asian.

5.4 Kyberrikollisuuden maailmanlaajuiset vaikutukset

Kyberturvallisuudella on ollut merkittävä vaikutus maailmanlaajuisesti, erityisesti tietoverkkorikollisuuden taloudellisten seurausten kautta. Vuonna 2023 tietoverkkorikollisuuden aiheuttamat taloudelliset menetykset nousivat noin 8 biljoonaan dollariin, joka vastaa noin 7,36 biljoonaa euroina. Ennusteiden mukaan summa tulee kasvamaan 23,84 biljoonaan dollariin vuoteen 2027 mennessä. Tämä kehitys korostaa tarvetta tehostaa kyberturvallisuustoimenpiteitä, sillä kasvu on huomattavaa verrattuna vuoden 2015 3 biljoonaan dollariin. (Islam 2024, 2.2.1.)

Kyberrikollisuuden ja sen vaikutusten voimakas kasvu johtuu useista tekijöistä. Kyberhyökkäykset kohdistuvat usein kriittiseen dataan, mikä voi lamauttaa yritysten ja valtion toimintaa. Taloudelliset varkaudet sisältävät suorat pankkivarkau-

det, vilpilliset liiketoimet ja muut manipulaatiot, jotka häiritsevät liiketoimintaa aiheuttaen suuria tuottavuuden menetyksiä. Henkilö- ja taloustietojen varastaminen on myös hyvin yleistä. Siihen liittyy arkaluonteisten tietojen varastamista, identiteettivarkauksia, pimeässä verkossa tapahtuvaa myyntiä tai muita petoksia, joista aiheutuu suuria menetyksiä. Suurin osa voimakkaan kasvun tekijöistä viittaa vahvasti tekoälyn mahdollistamiin hyökkäyksiin, joka voikin olla yksi syy voimakkaasti kasvaville tappioille rahallisesti. (Islam 2024, 2.2.1.)



KUVIO 5. Maailmanlaajuiset taloudelliset menetykset (Islam 2024, 2.2.1).

6 TULEVAISUUDEN NÄKYMÄT JA HAASTEET

Kyberturvallisuuden kehitystä ohjaa tekoälyn nopea käyttöönotto, jonka on tehnyt hyökkäysten monimutkaistuminen, nopeutuminen ja laajeneminen. Tekoälyn saatavuuden parantuminen ja niihin kohdistuva kasvanut kiinnostus viittaa vahvasti trendin jatkumiseen tulevaisuudessakin. (Tekoälypohjaiset kyberturvallisuusratkaisut 2024.)

6.1 Tulevaisuuden huolestuttavat uhkat

Tekoälyn laajentuvan käytön myötä on noussut esiin useita merkittäviä haavoittuvuuksia. Järjestelmiin liittyy vinoumia, heikkoa selitettävyyttä sekä turvallisuus- ja yksityisyysongelmia. Tekoälyjärjestelmät ovat entistä alttiimpia uusille, vihamielisiksi koneoppimishyökkäyksiksi kutsutuille tietoturvariskeille, jotka vaikuttavat vain tekoälyyn perustuviin järjestelmiin. (Marchal & Nawrotek 2024, 39.)

Tekoälyä käytetään yhä useammin sekä hyökkäyksissä että puolustuksessa. Hyökkääjät hyödyntävät sitä kiertääkseen perinteisiä turvajärjestelmiä, mikä vaatii vastaavasti tekoälypohjaisia puolustusmekanismeja. Tekoälypohjaisissa puolustusmekanismeissa on kuitenkin varmennettava se, että ne ovat yhtä turvallisia ja joustavia kuin ei-tekoälyä käyttävät järjestelmät. Koneoppimishyökkäykset tulevat hyvin todennäköisesti lisääntymään huomattavasti jo entisestään, joka painottaa tekoälypohjaisten puolustusmekanismien käyttöönottoa. (Marchal & Nawrotek 2024, 39.)

Tulevaisuuden tekoälypohjaiset kyberuhat haastavat perinteiset tietoturvaratkaisut ja synnyttävät uusia riskejä, jotka vaikuttavat sekä järjestelmien eheyteen että ennusteiden luotettavuuteen. Nämä uhat tulevat vaatimaan tulevaisuudessa jatkuvaa seurantaa sekä organisaation tietoturvastrategioiden muuttamista jo entisestään.

6.2 Suurten organisaatioiden etuudet kyberturvallisuusympäristössä

Vuonna 2025 suurilla ja vakiintuneilla organisaatioilla on merkittävä etulyöntiasema kyberturvallisuusympäristössä verrattuna tekoälyä hyödyntäviin uusiin yrityksiin. Tämä etu juontuu juuriltaan näiden organisaatioiden laajasta asiakaskunnasta ja kattavista datavaroista, jotka sisältävät runsaasti korkealaatuista dataa. Laajat tiedonkeruumenetelmät ja pitkän aikavälin datankeruu mahdollistavat tekoälymallien kattavan koulutuksen, mikä puolestaan parantaa niiden ennustustarkkuutta ja toiminnan tehokkuutta. Uusien toimijoiden on huomattavasti vaikeampi kerätä vastaavanlaista datamäärää lyhyessä ajassa, joka on merkittävä haaste tekoälymallien suorituskyvyn kannalta. (Uusiteknologia 2024.)

Tekoälyn käyttö on myös hyvin kallista. Suurilla organisaatioilla on mahdollisuus rakentaa oikeanlainen puolustus tekoälyn avulla tehtyjä hyökkäyksiä vastaan suurella datamäärällä, mutta myös mahdollisuudella investoimalla suurempia määriä rahaa. Oikeanlainen tietoturvatiimi on suuri etu. Tämä mahdollistaa järjestelmien ylläpidon ja jatkuvan valvonnan, jotta mahdolliset kyberhyökkäykset tunnistetaan madollisimman nopeasti.

7 POHDINTA

7.1 Johtopäätökset

Opinnäytetyössä tutkittiin ajankohtaisia tekoälyn tuomia haasteita ja hyötyjä kohdistuen tietoturvallisuuteen. Tutkimusmenetelmänä käytettiin artikkeleiden, tutkimusten ja kirjallisuuden tuomia näkemyksiä. Tutkimuksesta käy hyvin ilmi, että tekoälyn tuomat vaikutukset ovat hyvin suuret. Suuressa osassa hyökkäyksistä käy ilmi, että tavalla tai toisella näihin on hyödynnetty tekoälyä. Suojausmenetelmät ovat tämän mukana luonnollisesti kehittyneet myös hurjasti. Uhkien edellä on vaikea pysyä, mutta tekoälyn tuomat ennakoivat työkalut auttavat uhkien rajoittamisessa ja estämisessä.

Generatiivisen tekoälyn tuomat vaikutukset ovat toinen asia. Tämä antaa isoja hyötyjä monissa asioissa muun muassa tietoturvan parantamisessa, mutta yleistyvät huijausmenetelmät ovat entistä helpommin toteutettavissa generatiivista tekoälyä hyödyntäen. Huijausviestit ja väärennetyt sivustot ovat olleet jo jonkin aikaa pinnalla. Näihin on voitu reagoida viestien suodatusohjelmilla ja sivuston aitouden paljastavilla selaimeen tuotavilla työkaluilla. Syväväärennös tapaukset sen sijaan on kysymysmerkki. Monet näistä on helppo tunnistaa, mikäli kyseessä on video tai kuva. Kun tämän tilalle tulee tekoälyn mahdollistama äänenkloonaus puheluissa tai ääniviesteissä, voi se olla vaikea tunnistaa syväväärennökseksi.

Säätelyn asettaminen kansainvälisesti tulee olemaan tärkeää, jotta uhkia osataan tunnistaa entistä paremmin. Tutkiessani aihetta tarkemmin monia sääntelyitä on jo toteutettu, ja ne edesauttavat uhkien edellä pysymisessä. Maailmanlaajuinen yhteistyö tulee olemaan myös hyvin tärkeää. Tutkimuksessa käy ilmi kyberrikollisuuden taloudellinen vaikutus maailmanlaajuisesti, joka on isompi kuin olisin voinut kuvitella. Lukemat tämän osalta on ennustettu nousevan moninkertaiseksi jo nykyisestään, ja se kertoo sääntelyn tärkeydestä.

7.2 Oma oppiminen ja tutkimusmenetelmät

Valitsin opinnäytetyön aiheen, koska halusin täydentää omaa näkemystäni tekoälyn tuomista vaikutuksista tietoturvallisuuteen. Olin tutkinut aihetta hieman jo aiemmin ja jo silloin kävi hyvin nopeasti ilmi, että vaikutukset ovat suuret. Aihe on suhteellisen tuore, joka tuotti hieman haasteita aiheeseen liittyvää kirjallisuutta etsiessä. Sen vuoksi lähdin tutkimaan pääasiassa artikkeleiden ja tutkimusten kautta. Tuoreiden artikkeleiden ja tutkimusten kautta luotettavaa ja ajankohtaista sisältöä löytyi kuitenkin hyvin.

Opinnäytetyö antoi erittäin kattavan käsityksen tämänhetkisestä tilanteesta. Tutkimuksen kautta sain myös hyvän käsityksen, mihin tekoäly tulee viemään kyberrikollisuutta tulevaisuudessa ja kuinka uhkia voidaan välttää. Opinnäytetyö vastasi ajankohtaisimpiin aiheisiin, mutta tiettyjä osa-alueita olisi voinut tutkia tarkemmin, muun muassa tulevaisuuden uhkat ja vaikutukset.

LÄHTEET

Aksela, M., Marchal, S., Patel, A. & Rosenstedt, L. 2022. Tekoälyn mahdollistamat kyberhyökkäykset. Traficom. Viitattu 7.5.2025. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/TRAFICOM_Teko%C3%A4lyn_mahdollistamat_kyberhy%C3%B6kk%C3%A4ykset%202022-12-12_web.pdf

Balaganesh. 2023. Shodan and Censys: Finding hidden parts on the internet with special search engines. gbhackers. Viitattu 15.3.2025. https://gbhackers.com/shoda-censys-internet/

Caulfield, J. 2023. What is Generative AI? Scribbr. Viitattu 20.3.2025. https://www.scribbr.com/ai-tools/generative-ai/

Deloitte. 2024. Generative AI and the fight for trust. Viitattu 7.5.2025. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/Advisory/us-generative-ai-and-the-fight-for-trust.pdf

Euroopan unioni. 2025. NIS 2 -direktiivi: verkko- ja tietojärjestelmien kyberturvallisuutta koskevat uudet säännöt. Viitattu 21.4.2025. https://digital-strategy.ec.europa.eu/fi/policies/nis2-directive

Euroopan unioni. 2025. Yleinen tietosuoja-asetus. Viitattu 21.4.2025. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm

Euroopan komissio. 2025. Tekoälysäädös. Viitattu 30.3.2025. https://digital-strategy.ec.europa.eu/fi/policies/regulatory-framework-ai

F-Secure. 2022. Mikä on haittaohjelma? Näin pysyt turvassa vaarallisilta ohjelmilta. Viitattu 7.3.2025. https://www.f-secure.com/fi/articles/what-is-malware

F-Secure. 2023. Mikä on identiteettivarkaus? Viitattu 7.3.2025. https://www.f-secure.com/fi/articles/what-is-identity-theft

Guillot, J, D. 2023. Mitä tekoäly on ja mihin sitä käytetään. Euroopan parlamentti. Viitattu 7.3.2025. https://www.europarl.europa.eu/pdfs/news/expert/2020/9/story/20200827STO85804/20200827STO85804_fi.pdf

Islam, M, R. 2024. Generative AI, Cybersecurity, and Ethics. E-kirja. Wiley.

Kuluttajaliitto. 2024. Tekoälyhuijaukset. Viitattu 21.4.2025. https://www.kuluttajaliitto.fi/materiaalit/tekoalyhuijaukset/?utm_source=chatgpt.com

Kolari, J. & Kallio, A. 2023. Tekoäly 123. Matkaopas tulevaisuuteen. E-kirja. Docendo.

Kallio, S. 2025. Mitä on generatiivinen tekoäly – GenAI Opas (2025). Santeri Kallio. Viitattu 14.5.2025. https://santerikallio.com/genai-opas/?utm_source=chatgpt.com

McAuley, C. 2024. Yleisiä tekstiviestihuijauksia: varo näitä huijausviestejä. F-Secure. Viitattu 21.4.2025. https://www.f-secure.com/fi/articles/trending-fake-sms-scam-text-messages-you-should-ignore

Marchal, S. & Nawrotek, B. 2024. Tekoälypohjaiset kyberturvallisuusratkaisut. Traficom. Viitattu. 7.5.2025. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Teko%C3%A4lypohjaiset%20kyberturvallisuusratkaisut_FI.pdf

Privaon. n.d. GDPR ja tekoäly – mitä tietosuojasta täytyy tietää nyt? Viitattu 5.3.2025. https://privaon.com/fi/gdpr-ja-tekoaly-mita-tietosuojasta-taytyy-tietaa-nyt/

Padhy, R, P. 2024. Generative AI use cases in cybersecurity. LinkedIn. Viitattu 23.3.2025. https://www.linkedin.com/pulse/generative-ai-use-cases-cybersecurity-dr-rabi-prasad-ynlvc

Palo Alto Networks. n.d. What is Generative AI in cybersecurity? Viitattu 23.3.2025. https://www.paloaltonetworks.com/cyberpedia/generative-ai-in-cybersecurity

Reznikov, R. 2024. Artificial intelligence in cyberattacks. positive technologies. Viitattu 19.3.2025. https://global.ptsecurity.com/analytics/artificial-intelligence-in-cyberattacks

Sanastokeskus. 2018. Kyberturvallisuuden sanasto. Viitattu 5.3.2025. https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf?file=pdf/Kyberturvallisuuden_sanasto.pdf

Stanham, L. 2025. AI-Powered Cyberattacks. Crowd Strike. Viitattu 7.5.2025. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/

Swimlane. 2025. How Can Generative AI be Used in Cybersecurity. Viitattu 5.3.2025. https://swimlane.com/blog/how-can-generative-ai-be-used-in-cybersecurity/

Traficom. 2022. Toimintaohje – Palvelunestohyökkäys. Viitattu 7.3.2025. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Palvelunestohy%C3%B6kk%C3%A4ysToimintaohje.pdf

Uusiteknologia. 2024. Kyberturvallisuuden ja tekoälyn tärkeimmät trendit 2025. Verkkosivu. Viitattu 21.4.2025. https://www.uusiteknologia.fi/2024/11/20/kyberturvallisuuden-ja-tekoalyn-tarkeimmat-trendit-2025/

VPN Unlimited. n.d. Kohdistetut hyökkäykset. Viitattu 7.3.2025. https://www.vpnunlimited.com/fi/help/cybersecurity/targeted-attacks?srsltid=AfmBOoq-iQP-vmDEm_8Zb5NP9oqsrWhus3TLtLKcwk0iT-wqix_yjCnQM