

Kalle Vesanterä

**JULKISTEN JA AVOINTEN LÄHTEIDEN TIEDUSTELUN (OSINT)
HYÖDYNTÄMINEN KYBERTURVALLISUUDEN
YLLÄPITÄMISESSÄ**

Tiedonhankinta osana päätöksentekoa ja järjestelmien teknistä turvaamista

**Pienoistutkielma
CENTRIA-AMMATTIKORKEAKOULU
Insinööri, tieto- ja viestintätekniikka (AMK)
Maaliskuu 2026**



SISÄLLYS

1 JOHDANTO.....	1
2 AVOINTEN LÄHTEIDEN TIEDUSTELU (OSINT).....	2
2.1 Avointen lähteiden tiedustelu osana kyberturvallisuutta.....	3
2.2 Tietolähteiden valitseminen.....	3
3 AVOIMISTA LÄHTEISTÄ SAADUN INFORMAATION HYÖDYNTÄMINEN.....	5
4 TOTEUTUKSET KÄYTÄNNÖSSÄ.....	6
4.1 Osana järjestelmäkokonaisuuksia.....	6
4.2 Teoreettisia tiedonhankinta- ja käsittelytapoja.....	8
5 POHDINTA.....	9
LÄHTEET.....	10

1 JOHDANTO

Kyberturvallisuuteen liittyvä uhkaympäristön kartoitus on kriittinen osa jokaisen tietoympäristöjen turvallisuuden parissa työskentelevän henkilön työtä. Päätösten teko jokaisella asteella, aina teknisestä ja taktisesta toteutuksesta strategisiin suuntaviivoihin asti, vaatii tuekseen informaatiota, jonka pohjalta päätäntää voidaan tehdä. Yksi osa tätä informaation hankintaketjua on julkisista ja avoimista lähteistä tapahtuva tiedon kerääminen.

Tämä tieto kattaa alleen laajoja kyberuhkaympäristöä koskevia raportointeja, kuten myös tarkkaan tekniseen toteutukseen lukeutuvia vaarantumisindikaattoritietoja. Näiden avulla turvallisuuden parissa työskentelevä henkilöstö pystyy varautumaan ja suojautumaan erilaisilta uhkakuvilta, joita ympäristö sisältää. Toteutuneiden uhkakuvien tunnistaminen ja näihin reagoiminen vaatii vastaavasti informaatiota koko skaalalta, jotta toimenpiteet ovat oikeita.

Avoimista lähteistä saatu tieto osana uhkakuvakartoitusta on merkittävässä roolissa. Kyseinen kategoria tiedustelussa on kuitenkin todella moninainen ja siihen nojautuvien järjestelmien kehittäminen vaatii syvää ymmärrystä sen sisällöstä. Tätä kyseistä kehitystyötä ajatellen, pyrittiin tutkielmassa selvittämään tätä alaa kokonaisuutena. Tutkielman aikana saatiin tietoa avointen lähteiden tiedustelun yhteydestä ja käyttökohteista osana kyberturvallisuusjärjestelmiä, tiedonhankintamenetelmistä ja lähteistä, sekä olemassa olevista toteutuksista osana erinäisiä järjestelmäekosysteemejä. Näistä ja muista teoreettisista järjestelmäkuvauksista koostettu korkean tason tiedon voidaan ajatella toimivan alustana, josta syventyä kuhunkin aiheeseen tulevan kehitystyön aikana.

2 AVOINTEN LÄHTEIDEN TIEDUSTELU (OSINT)

Kun puhumme avointen lähteiden tiedustelusta (open source intelligence, OSINT) terminä, vastassa on laaja konsepti, joka kattaa alleen monia erilaisia käyttökohteita ja tiedonhankintalähteitä sekä -menetelmiä. Avointen lähteiden tiedustelu voidaan määritellä informaation hankkimiseksi julkisesti saatavilla olevista lähteistä. Näitä lähteitä voivat olla muun muassa julkinen internet, uutisjulkaisut, sosiaalinen media sekä tutkimusartikkelit ja -julkaisut. Vaikka termi sisältää sanan tiedustelu, eroaa se oleellisesti vakoilusta. Avointen lähteiden tiedustelu on erilaisista tiedonhankintamenetelmistä tavanomaisin ja sitä voi harjoittaa kuka tahansa. (Hwang, Lee, Kim, Lee & Kim 2022.)

Avointen lähteiden tiedustelua tekevätkin esimerkiksi journalistit, liiketoiminta-analyytikot sekä erilaiset viranomaiset. Avointen lähteiden tiedustelua hyödynnetään myös kadonneiden ihmisten etsimiseen erilaisten ryhmittymien ja voittoa tavoittelemattomien yhdistysten puolesta. Tätä toimintaa on myös pilotoitu koulutuskäyttöön kyberturvallisuuden opiskelijoille. (Dincelli, Yayla & van Slyke 2023.) Puhdas tiedonhankinta ei kuitenkaan tarkoita, että toimintaa voidaan kutsua tiedusteluksi, vaan saatua tietoa pitää käsitellä ja tämän paikkansapitävyys tulee varmistaa.

Tiedustelumenetelmiä käsitellessä, tulee eettinen ja moraalinen puoli huomioida aina kun tietoa lähdetään hankkimaan ja käsittelemään. Informaation paikkansapitävyydestä varmistuminen korostuu erityisesti avoimista lähteistä saatavan tiedon osalta. Esimerkiksi journalismin kautta tarkasteltuna, voidaan todeta etiikan olevan erittäin tärkeässä roolissa. Väärään tietoon luottaminen voi vääristää käsiteltävän aiheen lopputulosta ja siitä seuraavia reaktioita. (Loehrke, Al-Kaisy, Kenausis, Terrill & Smits 2021.) Kyberturvallisuuden näkökulmasta, piittaamaton pimeän verkon haittaohjelmamarkkinapaikkojen hyödyntäminen voi tukea järjestäytyntä rikollisuutta tai jopa kansainvälistä terrorismia (Europol 2017, 2025). Koostetun lähdeinformaation tai käsitellyn informaation päätyminen väärin käsiin voi aiheuttaa epätoivottuja ja vahingollisia lopputulemia niin henkilökohtaisella kuin organisaatiotasolla. Kun reaali maailman tiedustelua peilataan kyberturvallisuuden käyttökohteisiin, tulee samat eettiset periaatteet huomioida.

2.1 Avointen lähteiden tiedustelu osana kyberturvallisuutta

Erilaisten tietojärjestelmien ja -ympäristöjen turvallisuuden ylläpitäminen pohjautuu monelta eri kantilta jo valmiiksi avointen lähteiden tiedusteluun. Esimerkiksi haittaohjelmien torjuntaan tarkoitettut ohjelmistot hyödyntävät erilaisten haittaohjelmien indikaattoritietoja, joita kyberturvallisuusyhteisö alana jakaa avoimesti keskenään. Myös päivittäisen internet-liikenteen suodatus organisaation järjestelmissä voi usein pohjautua vastaavanlaiseen avoimesti jaettuun dataan, jolloin haitalliset tai epäilyttävät sivustot voidaan estää. Yleisesti nämä tunnistetiedot voidaan asettaa vaarantumisindikaattorien kategorian alle (Paine, Whitehouse, Firefly, Sellwood & Shaw 2023).

Avoimista lähteistä saatu tietomassa erilaisista vaarantumisindikaattoreista voidaan käsitellä ja täten kohdistaa oikeaan käyttökohteeseen suojaamaan organisaation tietojärjestelmiä. Toisaalta, jos organisaation tietojärjestelmiin on jo kohdistunut jonkinlainen hyökkäys, voidaan vaarantumisindikaattorien avulla selvittää mitä on tapahtunut ja miten tapahtumasta selvittää.

Näiden kahden ääripäiden välille käyttökohteita mahtuu lukemattomia. Avointen lähteiden tiedusteluun perustuvaa informaatiota voidaan hyödyntää jopa reaaliaikaisesti organisaation päivittäisessä toiminnassa. Koostetusta ja käsitellystä datamassasta saaduilla tiedoilla varustetut järjestelmät voivat huomata sellaisia indikaattoreita, jotka viittaavat hyökkäyksiin valmistautumiseen tai organisaation sisältä tulevaan uhkaan.

2.2 Tietolähteiden valitseminen

Uhkaympäristön kartoittamiseen soveltuvia tietolähteitä on monenlaisia. Tavoitteesta ja kohteesta riippuen, voi olla tarkoituksenmukaista keskittyä vain tietynlaisiin informaatiokanaviin, jotta käsiteltävän informaation määrää voidaan rajata. Yleisesti uhkakuvan kartoittamisessa on kuitenkin hyvä yhdistellä erityyppisiä lähteitä, joiden pohjalta muodostuva kokonaiskuva voi hyödyttää koko organisaation uhkamallin käsittelyä ja päivittämistä.

Jos tarkoituksena on yleismaailmallinen tilannetietoisuuden ylläpitäminen ja uhkaympäristön kartoittaminen, voi olla järkevää kohdistaa tiedonkeruu viranomaisten ja tietoturvayhtiöiden julkaisemiin tilannekatsauksiin, uhkaympäristöraportteihin ja teknisiin analyysihin. (Kyberturvallisuuskeskus 2026.) Ammatillisten uutislähteiden hyödyntäminen voi toimia helposti

lähestyttävänä tapana tilannetietoisuuden ylläpitämisessä, joista tarpeen vaatiessa syventyminen on myös mahdollista matalalla kynnyksellä.

Teknisesti tarkempaan käyttöön puolestaan voidaan hyödyntää erilaisia Threat Intelligence -syötteitä ja haavoittuvuustietokantoja, jotka antavat tarkkaa tietoa eri tasoihin uhkiin, uhkatoimijoihin ja tunnettuihin haavoittuvuuksiin liittyen (The MITRE Corporation 2026; National Institute of Standards and Technology 2024). Näiden tietolähteiden tarjoamaa informaatiota voidaan käsitellä suoraan koneellisesti, muodostaen vaarantumisindikaattoreita syötettäväksi integroituihin järjestelmiin. Yhdistettynä ihmisten tekemään korkeamman tason työhön, voidaan näitä hyödyntää myös uhkakuviin reagoinnin priorisoinnissa, sekä mahdollisesti toteutuneiden uhkien tunnistamisessa. Syötteestä riippuen saatava tieto voi olla hyvinkin reaaliaikaista.

Reaaliaikaisen tilannetietouden tueksi sosiaalisen median kanavien, pikaviestintäpalveluiden ja keskustelufoorumien seuraaminen niin avoimessa kuin pimeässä verkossa voi antaa reaaliaikaista indikaattoritietoa nousevista, todennäköisistä ja toteutuneista uhkakuvista. Lisäksi sosiaaliset lähteet voivat nopeasti koostaa vaikeasti selvitettäviä yksityiskohtaisia kokonaisuuksia. (Shin, Shim, Kim, Lee, Kang & Hwang 2021; Alzahrani, Lee & Kim 2024.) Tarkkailtavasta alustasta ja käyttötarkoituksesta riippuen, voidaan tätä tehdä automatisoidusti tai manuaalisesti. Tiedon oikeellisuuden varmistaminen on lisäksi erityisen tärkeää.

3 AVOIMISTA LÄHTEISTÄ SAADUN INFORMAATION HYÖDYNTÄMINEN

Hankitun tiedon taso ja käyttökohde määrittävät pitkälti sen millaisiin käyttökohteisiin sitä voidaan hyödyntää. Käytännönläheisesti ajatellen, korkean tason tilannetietoisuuden ylläpitäminen vaatii sitä vastaavia lähteitä ja tiedonhankintamenetelmiä, mutta näistä ei ole välttämättä suurta hyötyä käynnissä olevan kyberhyökkäyksen analysoinnissa. Lähempänä matalaa teknistä tasoa toimittaessa, kuten organisaation tietojärjestelmien aktiivista suojausta suoritettaessa, on hankittava informaatio syytä rajata juuri tähän käyttökohteeseen. Kumpikaan näistä ääripäistä ei kuitenkaan sulje toista pois, vaan tapauksiin varautuminen ja niiden tutkiminen voi vaatia koko informaatiokaalan hyödyntämistä.

Teknisellä tasolla voidaankin siis keskittyä vaarantumisindikaattoritietojen hankintaan näihin erikoistuneista lähteistä, rajaamalla parametrit relevantteihin indikaattoritietoihin (Alzahrani ym. 2024). Tämän tukeminen korkean tason lähteistä saatavalla informaatiolla voi helpottaa rajaamista. Erilaiset uhkatyypit ja uhkatoimijoiden tekniset ja taktiset menetelmät voivat vaihdella muun muassa organisaation toimialueen, maantieteellisen tason ja muuttuvien trendien mukaisesti (Lee, Mujammami & Kim 2025.), jolloin tietynlaisiin vaarantumisindikaattoreihin osataan pureutua tarkemmin. Muuttuvien taktiikoiden, tekniikoiden ja toimintatapojen sekä hyökkäystrendien kannalta ajan tasalla pysyminen niin teknisellä kuin korkealla tasolla tulee hyödyttämään nousevilta uhkilta suojautumista.

Tavoitteen mukaan, trendien seuranta voi tukea strategisten uhka-arviointien suorittamista niin organisaatiotasolla, kuten myös kansallisella ja ylikansallisella tasolla. Näiden uhka-arviointien pohjalta siirtyminen alemman tason taktiseen ja operatiiviseen toimintaan tulee osaltaan helpottamaan päätöksen tekoa ja resurssien rajaamista oikeisiin kohteisiin. Kohdistamalla korkean tason seurannassa saatuja parametrejä matalan tason toimintaan, on mahdollista löytää tarkalta tekniseltä tasolta jopa yksittäisiin haittaohjelmiin liittyvää informaatiota (Shin ym. 2021.), joka vertaisarvioituna ja varmistettuna muun informaation kanssa pitää suurelta osin paikkaansa. Tähän käyttöön voidaan hyödyntää myös sosiaalisen median seuranta, jonka avulla myös piilossa olevaa informaatiota voidaan saada hyödynnettäväksi ja käsiteltäväksi (Lee ym. 2025.). Erityisen hyödyllistä tämä voi olla kriittisillä liiketoiminnan aloilla, joilla toteutuneista kyberuhkista ulospäin viestiminen on harvinaista.

4 TOTEUTUKSET KÄYTÄNNÖSSÄ

Avointen lähteiden tiedusteluun ja tiedonhankintaan perustuvia kyberturvallisuusjärjestelmiä on kehitetty ja käytetty pitkään. Yksi tavallisimmista tavoista organisaation tietoverkkoja suojaavaan liikenteen suodatuksen on käyttää erilaisia koostettuja listoja, jotka sisältävät indikaattoritietoja haitalliseksi todetuista verkkosivustoista ja palvelimista. Tämän ohella haittaohjelmasuojaukset toimivat usein indikaattoritietojen perusteella. Toisaalta korkean tason tiedon jakaminen auttaa turvallisuushenkilöstöä ja järjestelmäylläpitäjiä ymmärtämään erilaisia teknisiä uhkia sekä varautumaan erilaisten toimijoiden menetelmiin ja nouseviin uhkiin.

Informaation määrän ollessa jatkuvasti kasvava, on tämän työn helpottamiseksi kehitetty erilaisia järjestelmiä, jotka käyttökohteensa mukaan saattavat toimia itsenäisesti tai osana muuta turvallisuusekosysteemiä. Internetin sosiaalisten alustojen kasvaessa myös niiden merkitys osana kyberturvallisuuden uhkaympäristöä on noussut merkittäväksi osaksi tiedonhankintaekosysteemiä. Informaatiomassan kasvun ja sosiaalisten ilmiöiden informaation käsittelyn on todettu olevan merkittävä osa jopa sotilaallisiin käyttökohteisiin luotuja strategisia määritelmiä (Ahlskog, Berrier & MacDougall 2023), eikä sen merkitystä käytännön tason kyberturvallisuuden ylläpitämisessä kannata ohittaa.

4.1 Osana järjestelmäkokonaisuuksia

Avointen lähteiden tiedustelun ja tiedonhankinnan tavoitteesta riippuen erilaisia järjestelmiä on kehitetty tukemaan kyseisiä tavoitteita. Hyvin usein nämä toimivat osana jonkinlaista kokonaisvaltaisempaa järjestelmäkokonaisuutta tai -ekosysteemiä. Turvallisuusjärjestelmät ovat hyvin usein monimutkaisia, joten tämän tyyppisen informaation hyödyntäminen saattaa toimia usealla eri osa-alueella samassa kokonaisuudessa. Informaation jakamista ja hyödyntämistä helpottamaan on kehitetty erilaisia järjestelmiä, kuten Malware Incident Sharing Platform (MISP) (Wagner, Dulaunoy, Wagener & Iklody 2016). MISP on kehitetty mahdollistamaan muun muassa indikaattoritietojen, kyberuhkatiedon ja haavoittuvuustietojen jakaminen eri organisaatioiden, viranomaisten ja muiden toimijoiden välillä.

MISP:iin pohjautuvia järjestelmiä on luotu tukemaan kyberturvallisuusinformaation jakamista ja hyödyntämistä eri kokoisille organisaatioille. Pienten yritysten ja organisaatioiden ongelmaksi tunnistettu kyberturvallisuusrasite on ongelma, jonka ratkaisemiseksi avointa tiedonjakoa on hyödynnetty. Eurooppalainen GEIGER-pilvipalvelu on kehitetty kansantajuisesti työkaluksi tätä rasitetta helpottamaan. GEIGER pyrkii hyödyntämään suuren kyberturvallisuusyhteisön suorittamaa uhkatietojen jakamisesta syntynyttä informaatiomassaa, käsitellen sen pienille organisaatioille sopivaksi, hyödynnettäväksi kokonaisuudeksi (van Haastrecht, Golpur, Tzismadia, Kab, Priboi, David, Răcățăian, Brinkhuis & Spruit 2021). Työn tavoitteena on parantaa kokonaisvaltaista tietoturva-asemointia myös kohteissa, joissa asiantuntijuutta tähän ei välttämättä ole.

Vastaavaa kyberuhkainformaatiota voidaan hyödyntää ja kerätä erilaisten toimijoiden puolesta. Indikaattoritietojen keräämiseksi kehitettyjä järjestelmiä voidaan valjastaa keräämään granulaarista tietoa yksittäisen organisaation sisällä, tai vaihtoehtoisesti yleisempien laajalti käytettyjen kokonaisuuksien kartoittamiseksi. Hunaja-ansa järjestelmiä voidaan käyttää laajan alueellisen turvallisuuskartoituksen luomiseen ja tämän avulla saatu indikaattoritieto voidaan jakaa muun muassa MISP:in avulla muille toimijoille. (Alzahrani ym. 2024.) Yhdistettynä avointen lähteiden tiedustelun avulla saatuihin parametreihin voidaan informaatiota käsittelemällä monitoroida aktiivista kyberuhkaympäristöä.

Indikaattoritietoon perustuva sosiaalisen median tarkkailu voi antaa vertailtaen tarkkaa lisätietoa laajoista tapahtumista, joiden seuranta perinteisin menetelmin olisi hidasta ja vaivalloista. Erilaisten uhkatoimijoiden ja jatkuvien edistyneiden uhkatoimijoiden tunnistaminen, näiden toiminta-alueen, taktisten ja teknisten menetelmien kartoittaminen on osoittautunut mahdolliseksi sosiaalisen median tiedustelun avulla (Shin ym. 2021; Lee ym. 2025). Tämän kaltaisen informaation yhdistäminen muihin tietolähteisiin voi luoda kokonaisuuden, joka oikein käsiteltynä ja luokiteltuna voi auttaa kokonaisvaltaisesti laajan kyberturvallisuusympäristön turvaamista. Tietojen jakaminen muun muassa MISP:in avulla voi auttaa jopa sellaisia tahoja, joita kyberturvallisuusrasite koskettaa kaikista eniten.

Organisaation omaa operatiivista turvallisuutta ja hyökkäyspinta-alaa voidaan auditoida ja tarkastella käyttämällä sosiaaliseen median kanaviin kohdistettuja tiedustelumenetelmiä (Matvej, Morić & Papić 2020). Varsinkin sosiaalisten hyökkäysmenetelmien yleistyessä, voidaan organisaatioon kohdistuvia hyökkäyksiä suorittaa tämän työntekijöiden välityksellä. Löytämällä ja tunnistamalla näitä ongelmia, voidaan tämän kaltainen hyökkäyspinta-ala minimoida henkilöstöä kouluttamalla.

4.2 Teoreettisia tiedonhankinta- ja käsittelytapoja

Uhkaympäristön tunteminen vaatii jatkuvaa läsnäoloa siellä, missä mahdolliset uhkat asettuvat havaittaviksi. Perinteisesti käytettyjen tiedonhankintamenetelmien ollessa toimivia, voi kokonaiskuvan informaatiomäärä olla sellainen, ettei manuaalisella työskentelyllä pysty toimimaan sen parissa. Yksittäisen tietolähteen tueksi tulee myös hankkia informaatiota varmistamaan tämän oikeellisuus. Kyberturvallisuuden kannalta tähän muodostuneet kehityssuunnat pohjautuvat pitkälti tekoälyyn ja koneoppimiseen.

Sufi ja Alsulami (2025) ovat kehittäneet vähintään kokeellisella tasolla onnistunutta riskiennustetta ja strategisen näkymän kuvantamista tarjoavan tekoälypohjaisen kehysympäristön. Yhdistettynä tiedonkeräämiseen julkisesti saatavilla olevista tiedonlähteistä, kuten uutisjulkaisuista, on tekoälyn, koneoppimisen ja matemaattisten mallinnuksien avulla saatu kohtuullisen luotettavaa ennusteinformaatiota kyberturvallisuuteen liittyvistä kehityssuunnista. Yhdistettynä olemassa olevaan käsiteltyyn ja luotettavaan tietoon, voidaan tämän kaltaisella tiedonhankinnalla tukea strategista päätöksentekoa. (Sufi & Alsulami 2025.)

Gulbay ja Demirci (2024) ovat luoneet kehysympäristön, joka ei ole vielä kirjoitushetkellä vertaisarvioitu, mutta tulevaisuuden kehityksen kannalta varsin lupaavan oloinen tutkimuksen kohde. Kehysympäristössä edistyneiden jatkuvien uhkien analysointiin on käytetty graafipohjaisiin algoritmeihin perustuvia menetelmiä. Näiden menetelmien avulla on onnistuneesti löydetty erilaisia vaarantumisindikaattoritietoja, joita hyödyntämällä voi olla mahdollista parantaa taktista ja operatiivista valmiutta torjua vastaavanlaisia hyökkäyksiä. (Gulbay & Demirci 2024.)

Koneoppimiseen, tekoälyyn ja data-analytiikkaan perustuvat toimintamallit ja kehysympäristöt ovat käytössä jo jatkuvasti kyberturvallisuuden ylläpitämisessä ja uhkaympäristön kartoituksessa. Näiden soveltamisella laajaan uhkaympäristökartoitukseen voi olla merkittävä tehostava vaikutus tietomäärän lisääntyessä ja nousevien uhkien ennustamisessa.

5 POHDINTA

Kyberturvallisuusmaailma on erittäin monimuotoinen, abstrakti ja paikoin vaikeasti käsitettävä aihepiiri. Tutkielman aikana tehty katsaus avointen lähteiden tiedusteluun osana tätä maailmaa antoi erittäin moninaisen kuvan erilaisista liikkuvista osista, joita turvallisten järjestelmien ylläpitäminen sisältää. Strategisen tilannekuvan yhteys tarkkoihin teknisiin toteutusratkaisuihin ja parametreihin osoittautui olevan paljon läheisempi kuin päälle päin voisi ajatella. Tekniset indikaattoritiedot voidaan jakaa kyberturvallisuusyhteisön parissa nopeasti, jolloin mahdolliset hyökkäykset päästään torjumaan jo ennen kuin ne koskettavat organisaatiota. Toisaalta näiden ymmärtäminen ja käsitteleminen ilman laajaa tilannetietoutta vallitsevasta toiminta- ja uhkaympäristöstä voi olla hankalaa, joten tiedonhankintaa ei kannata ohittaa sen osalta.

Sekä tilannetietoutta että teknistä turvaamista tukemaan kehitettyjen järjestelmien käyttö, lähes minkä tahansa tahon osalta, on avainroolissa turvallisuuden ylläpitämisessä. Suurten toimijoiden tekemä laaja informaation hankinta hyödyttää myös pienyrityksiä, joissa kyberturvallisuustietoutta ei välttämättä ole lainkaan.

Uhkaympäristö kuitenkin kehittyy jatkuvasti, joten tiedonhankintamenetelmien on myös syytä kehittyä samaa tahtia. Erilaisista järjestelmäkokonaisuuksista voidaankin ottaa toimivia palasia, yhdistellen näitä organisaation tarpeen mukaiseksi. Tiedonhankinta sosiaalisesta internetistä osoittautui myös olemaan suuressa roolissa. Tulevaisuuden trendit näkyvät sekä uhkaympäristön kehityksessä, että siltä suojautumisessa. Nousevat uhat tulee kyetä tunnistamaan nopeasti, jolloin informaatiomassan käsitteleminen vaatii tehokkaampia työkaluja.

Tämän tutkielman lopputulokseksi on vaikea määrittää mitään tiettyä oivallusta tai kehityskohdetta. Kuitenkin tulevaisuuden järjestelmien kehittämisen ja turvaamisen kannalta, tutkielman aikana saatu tieto tulee olemaan hyödyllistä resurssien kohdentamisessa. Tutkielman pohjalta löytynyttä informaatiota voidaan hyödyntää niin strategisen ja operatiivisen päätännän tueksi rakennetuissa järjestelmissä, kuin syvään tekniseen toteutukseen pohjautuvissa projekteissa.

LÄHTEET

Ahlskog, B.H., Berrier, S.D., & MacDougall, A.S., 2023. OSINT Strategy 2024-2028. Department of Defense, Defense Intelligence Agency. Saatavissa:

<https://www.dia.mil/Portals/110/Documents/OSINT-Strategy.pdf>. Viitattu 30.3.2026.

Alzahrani, I.Y., Lee, S., & Kim, K., 2024. Enhancing Cyber-Threat Intelligence in the Arab World: Leveraging IoC and MISP Integration. *Electronics (Switzerland)*, 13 (13). Saatavissa:

<https://doi.org/10.3390/electronics13132526>. Viitattu 12.3.2026.

Communications Security Establishment, Centre de la sécurité des telecommunications, 2022. An introduction to the cyber threat environment. Saatavissa:

<https://www.cyber.gc.ca/sites/default/files/ncta-2022-intro-e.pdf>. Viitattu 16.3.2026.

Dincelli, E., Yayla, A., & van Slyke, C. 2023. Ethical Hacking for a Good Cause: Finding Missing People using Crowdsourcing and Open-Source Intelligence (OSINT) Tools. *Communications of the Association for Information Systems*, 53, 1052–1071. Saatavissa:

<https://doi.org/10.17705/1CAIS.05345>. Viitattu 7.5.2026.

Europol, 2017. Massive blow to criminal Dark Web activities after globally coordinated operation.

Saatavissa: <https://www.europol.europa.eu/media-press/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation>. Viitattu 18.3.2026.

Europol, 2025. Steal, deal and repeat - How cybercriminals trade and exploit your data Internet Organised Crime Threat Assessment (IOCTA) 2025. Luxembourg. Publications Office of the European Union. Saatavissa: <https://doi.org/10.2813/4926508>. Viitattu 18.3.2026.

Federal Office for Information Security. Cyber security recommendations by threats, Advanced Persistent Threat. Bonn, Germany. Saatavissa: https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefahren/APT/apt_node.html. Viitattu 16.3.2026.

Gulbay, B. & Demirci, M., 2024. A Framework for Developing Strategic Cyber Threat Intelligence from Advanced Persistent Threat Analysis Reports Using Graph-Based Algorithms. Saatavissa:

<https://doi.org/10.20944/preprints202407.1408.v1>. Viitattu 12.3.2026.

van Haastrecht, M., Golpur, G., Tzismadia, G., Kab, R., Priboi, C., David, D., Răcățian, A., Brinkhuis, M., & Spruit, M., 2021. A Shared Cyber Threat Intelligence Solution for SMEs.

Electronics (Switzerland), 10 (23). Saatavissa: <https://doi.org/10.3390/electronics10232913>. Viitattu 30.3.2026.

Hanham, M., 2022. *Setting Your Moral Compass A Workbook for Applied Ethics in OSINT*.

Muscatine, IA. Saatavissa: <https://stanleycenter.org/wp-content/uploads/2022/08/OSINT-Ethics-Workbook-2022.pdf>. Viitattu 18.3.2026.

- Hwang, Y.W., Lee, I.Y., Kim, H., Lee, H., & Kim, D., 2022. Current Status and Security Trend of OSINT. *Wireless Communications and Mobile Computing*. Saatavissa: <https://doi.org/10.1155/2022/1290129>. Viitattu 12.3.2026.
- Lee, S., Mujammami, A.A.H., & Kim, K., 2025. Leveraging Social Networks for Cyber Threat Intelligence: Analyzing Attack Trends and TTPs in the Arab World. *IEEE Access*, 13, 5679–5693. Saatavissa: <https://doi.org/10.1109/ACCESS.2024.3508025>. Viitattu 27.3.2026.
- Locke, G. & Gallagher, P., 2011. Managing information security risk. Gaithersburg, MD: National Institute of Standards and Technology (NIST). Saatavissa: <https://doi.org/10.6028/NIST.SP.800-39>. Viitattu 16.3.2026.
- Loehrke, B., Al-Kaisy, A., Kenausis, L., Terrill, D., & Smits, K., 2021. Feeling the Burden: Ethical Challenges and Practices in Open Source Analysis and Journalism. Muscatine, IW. Saatavissa: https://stanleycenter.org/wp-content/uploads/2022/01/NWRPT-FeelingtheBurden_122-v2.pdf. Viitattu 18.3.2026.
- Matvej, E., Morić, Z., & Papić, S., 2020. Croatian Bank Security Analysis by Publicly Available Data. B. Katalinic. Proceedings of the 31st DAAAM International Symposium. Vienna, Austria. DAAAM International, 0184–0188. Saatavissa: <https://doi.org/10.2507/31st.daaam.proceedings.024>. Viitattu 30.3.2026.
- The MITRE Corporation, 2026. About the CVE Program. Saatavissa: <https://www.cve.org/About/Overview#AbouttheCVEProgram>. Viitattu 26.3.2026.
- National Institute of Standards and Technology (NIST), 2024. National Vulnerability Database - General Information. Saatavissa: <https://nvd.nist.gov/general>. Viitattu: 26.3.2026.
- Kyberturvallisuuskeskus, Liikenne- ja viestintävirasto Traficom, 2026. Tilannekuvatuotteet. Saatavissa: <https://kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/tilannekuvatuotteet>. Viitattu 26.3.2026.
- Paine, K., Whitehouse, O., Firefly, B., Sellwood, J., & Shaw, A., 2023. RFC 9424: Indicators of Compromise (IoCs) and Their Role in Attack Defence. Saatavissa: <https://www.rfc-editor.org/info/rfc9424>. Viitattu 16.3.2026.
- Shin, H., Shim, W., Kim, S., Lee, S., Kang, Y.G., & Hwang, Y.H., 2021. #Twiti: Social listening for threat intelligence. Teoksessa *The Web Conference 2021 - Proceedings of the World Wide Web Conference, WWW 2021*. Association for Computing Machinery, Inc, 92–104. Saatavissa: <https://doi.org/10.1145/3442381.3449797>. Viitattu 12.3.2026.
- Sufi, F. & Alsulami, M., 2025. Quantifying Temporal Dynamics in Global Cyber Threats: A GPT-Driven Framework for Risk Forecasting and Strategic Intelligence. *Mathematics*, 13 (10). Saatavissa: <https://doi.org/10.3390/math13101670>. Viitattu 30.3.2026.
- Wagner, C., Dulaunoy, A., Wagener, G., & Iklody, A., 2016. MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform. Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security. 49–56. Viitattu 30.3.2026.