Droonien havaitseminen ja torjunta: Teknologiat, haasteet ja tulevaisuuden näkymät

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Teknillinen tiedekunta
Joulukuu 2025
Aarne Ollila

TURUN YLIOPISTO
Tietotekniikan laitos

Aarne Ollila: Droonien havaitseminen ja torjunta: Teknologiat, haasteet ja tulevaisuuden näkymät

TkK-tutkielma, 25 s.
Teknillinen tiedekunta
Joulukuu 2025

Drooniteknologian nopea kehitys on tuonut mukanaan sekä merkittäviä hyötyjä että uusia turvallisuusuhkia. Tässä tutkielmassa tarkastellaan eri teknologioiden tehokkuutta droonien havaitsemisessa ja neutraloimisessa erilaisissa ympäristöissä, sekä analysoidaan erityisesti fyysisten ja pehmeiden torjuntakeinojen synergistä käyttöä. Tutkielma keskittyy myös drooniparvien muodostamiin erityishaasteisiin, jotka vaativat nykyisiä järjestelmiä monimutkaisempia ratkaisuja. Tulokset osoittavat, että mikään yksittäinen teknologia ei tarjoa täydellistä ratkaisua kaikkiin tilanteisiin. Tehokkaimmat ratkaisut perustuvat monikerroksiseen puolustusjärjestelmään, jossa yhdistetään sensorifuusiota, tekoälyä ja erilaisia torjuntateknologioita. Tutkimuksen perusteella tulevaisuuden droonien torjunta edellyttää jatkuvaa teknologista innovaatiota sekä kansainvälisen sääntelyn kehittämistä.

Asiasanat: drooni, drooniparvi, droonien torjunta, droonien havaitseminen

Sisällys

1 Johdanto

1.1 Tutkielman tarkoitus

Drooniteknologia on kehittynyt nopeasti viime vuosina, tuoden mukanaan merkittäviä mahdollisuuksia, mutta samalla myös uusia uhkia turvallisuudelle. Sotilaallinen ja kaupallinen droonien käyttö, erityisesti Ukrainan sodassa nähtyjen tapausten myötä, on korostanut tarvetta tehokkaille havaitsemis- ja torjuntajärjestelmille. Tämän tutkielman tavoitteena on tunnistaa ja analysoida eri teknologioiden tehokkuutta droonien havaitsemisessa ja neutraloimisessa vaihtelevissa ympäristöissä. Lisäksi tutkitaan erityisesti fyysisten ja pehmeiden torjuntakeinojen yhdistämistä ja niiden mahdollista synergistä käyttöä. Tutkimuksessa kiinnitetään huomiota drooniparvien muodostamiin uhkiin, joiden torjuminen edellyttää nykyisiä järjestelmiä monimutkaisempia ratkaisuja. Työn tulokset tarjoavat kattavan kuvan droonien torjunnan nykytilasta ja tulevaisuuden haasteista, sekä mahdollistavat tehokkaampien torjuntajärjestelmien suunnittelun ja toteutuksen.

1.2 Tutkimuskysymykset

TK 1: Mitkä teknologiat ovat tehokkaimpia droonien tunnistamiseen ja neutraloimiseen erilaisissa ympäristöissä?

TK 2: Miten pehmeät torjuntakeinot voivat täydentää fyysisiä torjuntakeinoja?

TK 3: Millaisia haasteita drooniparvet aiheuttavat nykyisille torjuntajärjestelmille?

1.3 Tutkielman rakenne

Tutkielma koostuu neljästä pääluvusta. Johdannon jälkeen luvussa kaksi käsitellään työn taustaa, perehtyen droonien monipuolisiin käyttötarkoituksiin sekä niihin liittyviin turvallisuusuhkiin ja eettisiin kysymyksiin. Lisäksi luvussa esitellään tarkemmin droonien havaitsemiseen ja torjuntaan käytettävät perinteiset ja uudet teknologiat, mukaan lukien fyysiset ja pehmeät torjuntakeinot sekä erityisesti drooniparvien asettamat erityishaasteet. Luku kolme keskittyy tutkimuksen aineistoon ja tuloksiin, joissa vertaillaan eri havaitsemis- ja torjuntateknologioiden tehokkuutta ja soveltuvuutta erilaisissa uhkatilanteissa ja ympäristöissä. Tutkimuksessa huomioidaan myös tekoälyn rooli torjuntaratkaisuissa. Viimeisessä neljännessä luvussa tiivistetään tutkimuksen keskeiset havainnot ja esitetään johtopäätökset sekä suositukset droonien torjuntateknologioiden kehittämiseksi.

2 Tausta

Droonit ovat mullistaneet monia aloja viime vuosina. Niitä käytetään tavarankuljetuksessa, maataloudessa, valokuvaamisessa sekä sotilaallisissa tehtävissä. Niiden pieni koko, matalat kustannukset, helppokäyttöisyys ja sovellettavuus luo lähes loputtomat mahdollisuudet eri käyttötarkoituksiin [1]. Hyödyllisyyden vastakohtana droonit luovat keskustelua droonien eettisyydestä ja oikeudenmukaisuudesta. Pienen koon ansiosta vakoilu ja tiedustelu on entistä helpompaa, mikä on turvallisuusriski esimerkiksi ihmisten yksityisyydelle [2]. Sotatilanteessa etäohjatut droonit aiheuttavat psykologisen ja moraalisen etäisyyden ohjaajan ja kohteen välille. Tämä haastaa kansainvälistä oikeutta kuin myös sodankäynnin periaatteita [3].

2.1 Droonien uhkakuvat ja käyttötarkoitukset

Drooniteknologian yleistyminen on lisännyt niiden käyttötarkoituksia sekä sotilaallisella, että kaupallisella sektorilla. Käyttötarkoituksia ovat esimerkiksi tiedustelu-, tavarankuljetus- ja valvontatehtävät [1]. Ukrainan sota on korostanut droonien merkitystä nykyaikaisessa sodankäynnissä, missä drooneja on käytetty tiedustelu- ja hyökkäysvälineinä [4]. Drooneja käyttävät valtiollisten toimijoiden lisäksi myös yksityiset toimijat, kuten terroristijärjestöt [5]. Vaikka drooneja käytetään hyödyllisiin tehtäviin, niiden ominaisuudet tekevät niistä potentiaalisia myös väärinkäytöille. Pienikokoiset droonit ovat vaikeasti havaittavia ja muodostavat vakavan turvallisuusriskin lentoliikenteelle, infrastruktuurille ja ihmisten yksityisyydelle [2].

2.1.1 Droonien turvallisuusuhat

Droonien käyttöä lisää niiden monipuolisuus ja matalat kustannukset. Drooneja on helppo mukauttaa käyttötarkoituksen mukaan, ne voivat kantaa esimerkiksi räjähteitä tai haitallisia kemikaaleja. Tämän tyyppistä käyttöä on ollut esimerkiksi Ukrainassa, jossa droonien merkitys tiedustelussa ja hyökkäyksissä on korostunut. Drooneja käytetään myös laittomaan toimintaan, kuten salakuljetukseen ja vakoiluun [2].

Drooneilla tehdyt fyysiset hyökkäykset ovat yleistyneet Ukrainassa. Vastaavanlainen hyökkäys tapahtui vuonna 2018, kun Venezuelan presidentti oli iskun kohteena [6]. Drooneja on käytetty myös kyberhyökkäysten apuvälineinä: vuonna 2021 Tesla Model X:n ovet hakkeroitiin droonin avustuksella [7]. Lisäksi drooneilla voidaan aiheuttaa merkittävää häiriötä; Gatwickin lentokenttä jouduttiin sulkemaan droonihavaintojen vuoksi 33 tunniksi, ja sulkemisesta aiheutui arviolta 50 miljoonan punnan tappiot [8]. Pienen kokonsa ansiosta droonit soveltuvat tehokkaasti tiedusteluun, esimerkiksi vuonna 2019 drooniparvi seurasi Yhdysvaltain sotalaivoja Kalifornian rannikolla noin 90 minuutin ajan [9]. Näiden esimerkkien valossa droonien nopea kehitys ja monipuoliset käyttötavat luovat uusia turvallisuusuhkia, joihin yhteiskunnan ja viranomaisten on varauduttava tehokkaasti ja ennakoivasti.

2.1.2 Droonien sotilaallinen käyttö

Droonit pystyvät pysymään ilmassa pitkiä aikoja, mikä mahdollistaa kohteen seurannan ja reaaliaikaisen tiedon keräämisen. Tämän avulla voidaan tehdä parempia taktisia päätöksiä ja valita kohteet tarkemmin. Pitkään jatkuneen tarkkailun ansiosta droonit voivat tunnistaa kohteen varmemmin ja suorittaa tarkan iskun. Droonit eivät tarvitse lentäjää, joten ne mahdollistavat sotatoimien laajentamisen alueille, joihin ihmisen lähettäminen voisi olla liian riskialtista. Etenkin tämä ominaisuus on muuttanut merkittävästi sotatoimien suunnittelua ja toteutusta. Droonien käyttö

sopii parhaiten operaatioihin, joissa vastapuolella ei ole käytössä viimeaikaisia kehittyneitä ilmatorjuntajärjestelmiä [10]. Drooneja voidaan käyttää myös viestinnässä, ja ne voivat korvata kalliita satelliittiyhteyksiä ja toimia langattomien sotilasverkkojen viestintäsolmuina. Tästä on erityisesti hyötyä vaikeissa ympäristöissä, kuten vuoristoalueilla, joihin perinteisten viestiasemien perustaminen on haastavaa [11]. Ukrainan sodassa sotilaat ovat käyttäneet pienikokoisia kaupallisia drooneja, joiden avulla tehdään tiedustelua, seurataan taistelukentän tapahtumia sekä pudotetaan räjähteitä viholliskohteisiin. Erityisen suosittu droonimalli on ollut DJI Mavic –nelikopteri, jonka globaalista tuotannosta Ukraina osti 60 prosenttia lokakuussa 2023. Drooneja käytetään myös yhden suunnan iskuissa, joissa drooni toimii kertakäyttöisenä itsetuho-ammuksena.

Droonit voivat tulevaisuudessa toimia yhdessä miehistön kanssa, mutta tämä edellyttää autonomian tasapainottamista, eli ihmisen ja järjestelmän välisen päätöksenteon ja vastuunjaon hallittua määrittämistä [4]. Tasapainottamisella tarkoitetaan sitä, että droonit kykenevät toimimaan riittävän itsenäisesti nopeasti muuttuvissa tilanteissa, mutta säilyttävät samalla mahdollisuuden ihmisen ohjaukseen ja valvontaan. Droonien sotilaallinen käyttö on jo merkittävästi muokannut sodankäyntiä: niiden avulla voidaan toteuttaa vaarallisia operaatioita, joihin ihmisen lähettäminen olisi riskialtista. Tulevaisuudessa autonomian lisääntyessä on entistä tärkeämpää löytää oikea suhde ihmisen ja koneen väliseen päätöksentekoon sekä kommunikaatioon.

2.1.3 Droonien oikeudelliset ja eettiset haasteet

Droonien yleistyessä herää kysymyksiä oikeudellisista ja eettisistä haasteista. Erityisesti keskustelua herättävät täysin autonomiset droonit, jotka voivat suorittaa hyökkäyksiä ilman ihmisen välitöntä ohjausta. Suurin kysymys liittyy vastuuseen, jos drooni tekee virheen, onko vastuu ohjelmoijalla, ohjaajalla vai valtiolla. Täysin

autonomisten asejärjestelmien kannattaja Ronald C. Arkin esittää, että kehittyvä tekoäly voisi tulevaisuudessa tehdä parempia eettisiä päätöksiä kuin ihminen, koska koneet eivät tunne pelkoa, kostoa tai muita tunteita, jotka voivat vaikuttaa päätöksentekoon [3]. Kuitenkin vuonna 2020 järjestetyssä kansainvälisessä kyselyssä 62 prosenttia vastusti autonomisten tappavien asejärjestelmien käyttöä [12]. Toinen lähestymistapa on Human-Macine Partership -malli, jossa ihminen säilyttää täyden kontrollin kriittisissä päätöksissä ja on itse juridisesti vastuussa. Droonien etäohjattavuus tuo mukanaan lisähaasteen eettiseen näkökulmaan. Ohjaajan ei itse tarvitse olla kosketuksessa taistelukenttään, mikä luo psykologisen ja moraalisen etäisyyden ohjaajan ja kohteen välille. Tämä voi johtaa siihen, että hyökkäyksen tekeminen on helpompaa ja tappaminen tuntuu vähemmän henkilökohtaiselta.

Droonien etäohjatun käytön vuoksi niiden soveltaminen kansainväliseen oikeuteen on monimutkaista. Asiantuntijoiden mukaan droonihyökkäykset voivat rikkoa sodankäynninperiaatteita, kuten suhteellisuutta ja erottelua sotilaallisen ja siviilikohteen välillä. Tämä johtuu siitä ettei ohjaaja pysty arvioimaan tilannetta yhtä hyvin kuin taistelukentällä oleva sotilas [3]. Näiden haasteiden vuoksi droonien käyttö sodassa edellyttää selkeämpää kansainvälistä säätelyä. Teknologian kehittyessä on ratkaistava, kuinka autonomisten järjestelmien päätöksenteko sovitetaan yhteen kansainvälisten oikeuksien ja sodan eettisten periaatteiden kanssa.

2.2 Droonien havaitsemis- ja torjuntakeinot

Droonien havaitsemista vaikeuttaa droonien pieni koko ja kevyt runko, jolloin perinteiset tutkajärjestelmät voivat erehtyä luulemaan drooneja linnuiksi. Erityisen haastavaa on havaita matalalla lentävät droonit [13]. Droonien torjunta voidaan rajata kahteen luokkaan; fyysisiin ja pehmeisiin torjuntakeinoihin. Fyysisten torjuntakeinojen tarkoitus on tuhota drooni fyysisesti. Fyysiset torjuntakeinot sisältävät esimerkiksi mikroaaltotekniikalla tai laserin käytön [14]. Pehmeillä keinoilla kuten

häirinnällä pyritään säilyttämään droonin forensiset tiedot, jolloin droonista voidaan tutkia sen käyttämä teknologia, ja selvittämään sen alkuperäinen lentoreitti [15].

2.2.1 Havaitsemisteknologiat: Perinteiset ja uudet teknologiat

Perinteiset havaitsemisteknologiat

Perinteisiin havaitsemisteknologioihin kuuluvat tutkat, akustiset sensorit, kuvapohjaiset järjestelmät ja radiofrekvenssianalyysi. Perinteiset teknologiat ovat yleisesti halvempia, mutta yksittäin käytettyinä ne eivät sovellu kaikkiin tilanteisiin.

Tutkateknologian etuna on pitkä kantama ja toimivuus kaikissa sääolosuhteissa. Tutkan haasteena on erottaa pienet droonit esimerkiksi linnuista, mikä voi johtaa vääriin hälytyksiin. [16]

Akustiset sensorit ovat tehokkaita lyhyillä etäisyyksillä, ne soveltuvat parhaiten hiljaisiin ympäristöihin. Akustisten sensoreiden haasteena on niiden herkkyys ympäristön äänille ja melulle, kuten tuulelle ja liikenteelle. [14]

Kuvapohjaiset järjestelmät sisältää kamerat ja lämpökamerat. Kuvapohjaisten järjestelmien käytössä voidaan hyödyntää syväoppimista tunnistuksen ja havaitsemisen parantamiseksi. Kuvapohjaiset järjestelmät vaativat hyvän näkyvyyden, mikä rajaa niiden käytön vain hyviin sääolosuhteisiin. [17]

Radiofrekvenssianalyysi (RF-analyysi) tunnistaa droonien radiolinkkisignaalit tehokkaasti, mutta se ei toimi autonomisesti lentäviin drooneihin, mitkä eivät tarvitse radiolinkkiä. [14]

Uudet havaitsemisteknologiat

Uusiin havaitsemisteknologioihin kuuluvat lidar eli valotutka, erilaiset sensorifuusiot ja monianturijärjestelmät, sekä tekoälypohjaiset menetelmät. Uudet teknologiat ovat yleisesti kalliita ja niiden juridinen sääntely on osittain epäselvää.

Valotutka tarjoaa erittäin tarkkaa kolmiulotteista tunnistusta. Valotutka on kallis ja altis sääolosuhteille. Valotutkan kantama on noin 2000 metriä. [18]

Sensorifuusion ja monianturijärjestelmien etuna on tarkkuus ja luotettavuus erityisesti haastavissa olosuhteissa. Teknologian tarkoitus on yhdistää erilaisia sensoreita kuten tutkaa, kameroita, valotutkaa ja RF-analyysiä. Teknologian haasteena on sen monimutkaisuus ja järjestelmien korkea hinta. [17]

Tekoälypohjaiset menetelmät kykenevät tehokkaasti erottelemaan erilaisia kohteita toisistaan koneoppimisen avulla. Tekoäly toimii muiden sensoreiden taustalla ohjelmana, joka käy läpi sensorien tarjoamaa dataa. Tekoälypohjaiset menetelmät ovat riippuvaisia koulutusdatasta, ja niiden sääntelyn epäselvyydet hidastavat käyttöönottoa. [17]

Taulukko 2.1: Havaitsemisteknologioiden vertailu [17]

	Hyödyt	**Haitat**	**Hinta**
Tutka	Toimii huonoissa näkyvyysolosuhteissa. Pitkä kantama (2 km pienille lentokoneille; 1 km drooneille).	Korkein hinta, paino ja virrankulutus. Käytetään enimmäkseen GBDAA:ssa.	$5K–1M+
Kuvapohjaiset järjestelmät	Kevyt, edullinen ja pienikulutuksinen. Vaihteleva kantama, kykenee pitkän kantaman havaitsemiseen (riippuu optiikasta).	Rajoittuu selkeisiin sääolosuhteisiin. 3D-havainnointi vaatii useita sensoreita.	< $1K–100K
LiDAR	Toimii hieman heikossa näkyvyydessä. Parempi kuin kamerat etäisyyden arvioinnissa. Teknologia kehittyy nopeasti autoalan ansiosta.	Kalliimpi kuin kamerat. IR-spektrin haasteet (esim. silmäturvallisuus, väärien hälytysten riski).	< $5K–100K
RF-analyysi	Toimii huonoissa näkyvyysolosuhteissa. Pitkä kantama (jopa 3 km). Tarkkaa tietoa droonista.	Tunnistaa vain tunnetut kaupalliset RF-signaalit. Vaatii useita sensoreita droonin tarkan paikannuksen mahdollistamiseksi.	$1K–10K
Akustinen	Kevyt ja halpa.	Kehittyvä teknologia; ei vielä tarpeeksi käyttöä.	$1K–20K (arvio)

2.2.2 Fyysiset torjuntateknologiat

Fyysiset torjuntakeinot tarkoittaa droonien pysäyttämistä ja tuhoamista fyysisesti, nämä keinot ovat yleensä aggressiivisia.

Korkean energian laseraseet tuhoavat droonin sähköoptiset järjestelmät tai fyysisen rakenteen. Laser säteen kohdistaminen esimerkiksi droonin propulsioon aiheuttaa droonin putoamisen. Laserit ovat tarkkoja ja edullisia verrattuna perinteisiin ohjuksiin. Laserin etuja ovat välitön vaikutus ja tarkkuus, ne ovat tehokkaita myös drooniparvia vastaan. [19]

Mikroaaltotekniikka tarkoittaa korkeatehoisen mikroaaltosäteilyn käyttöä droonien elektroniikan ja viestintäjärjestelmien tuhoamiseen. Menetelmällä voidaan myös häiritä droonin hallintaa. Mikroaaltotekniikka on tehokas jos droonien määrä tai

ketteryys vaikeuttaa esimerkiksi verkkojen tai suoran tulituksen käyttöä. Tekniikan käyttöä rajoittaa esimerkiksi ympäristötekijät, koska mikroaaltosäteily voi vaikuttaa myös muihin elektronisiin järjestelmiin kuten matkapuhelimiin. [19]

Kineettinen vaikuttaminen tarkoittaa perinteisten aseiden tai ohjusten käyttöä. Tämä aiheuttaa vaaraa sivullisille erityisesti kaupunkialueilla. Perinteisistä aseista haulikko toimii hyvin matalalla lentäviä drooneja vastaan. Yleisesti suoraa tulitusta käyttävät sotilaat, joilla ei ole muita torjuntavälineitä, ja droonin pysäyttäminen nopeasti on välttämätöntä. Ohjusten käyttäminen drooneja vastaan ei ole kustannustehokasta, koska droonit ovat todella halpoja ohjuksiin verrattuna [13]. Kustannustehokkaampi keino on käyttää toista droonia droonin tuhoamiseen. Droonilla voidaan törmätä suoraan toiseen drooniin, tai siihen voidaan kiinnittää räjähde joka räjäytetään tarpeeksi lähellä haitallista droonia, jolloin sirpalevaikutus tuhoaa droonin työntövoiman. [20] Tämä taktiikka on laajasti käytössä Ukrainan sodassa.

2.2.3 Pehmeät torjuntateknologiat

Pehmeät torjuntakeinot tarkoittavat droonin neutralointia ilman fyysistä tuhoa. Näin voidaan säilyttää arvokkaat forensiset tiedot ja minimoida sivullisille aiheutuvat riskit.

Verkkojärjestelmät toimivat joko yksittäisillä drooneilla tai drooniparvilla. Droonit kantavat verkkoa, jolla on tarkoitus pyydystää haitallinen drooni suoraan ilmasta. Verkkoa voidaan joko vetää droonien perässä tai se voidaan ampua droonin kyydistä kohti haitallista droonia. Verkkojen tulee olla riittävän suuria, mutta kuitenkin kevyitä jotta droonit jaksavat kantaa niitä. Drooniparvella toimivassa verkkojärjestelmässä on tärkeä huomioida droonien kyky klusteroitua, eli ne voivat järjestäytyä itsenäisesti havaittuaan haitallisen droonin. Koska verkko on fyysinen

elementti, sitä on käytännössä mahdoton häiritä. Verkkoja käytetään myös passiivisesti ripustamalla niitä kriittisten alueiden ympärille. [21]

Häirinnän (Jamming) tarkoituksena on häiritä droonin ja ohjaimen välistä kommunikaatiota radiotaajuushäirinnällä. Häirinnällä saavutetaan droonin pysähtyminen tai palaaminen lähtöpaikkaan. Jos drooni on ohjelmoitu palaamaan lähtöpaikkaan yhteyden katkettua, se tarjoaa arvokasta tiedustelutietoa viranomaisille. Häirintää on erilaisia tyyppejä, joista energiatehokkain ja tarkin on protokollatietoinen häirintä. Protokollatietoinen häirintä tunnistaa ja häiritsee tiettyjä protokollia, kun taas laajemmalla alueella toimiva pyyhkäisyhäirintä (sweep jamming) lähettää häirintäsignaalia sokeasti ympärilleen. Häirintää käytettäessä on huomioitava, että se rajoittaa myös omien joukkojen ja laitteiden toimintaa häirinnän alueella. Häirintä voi haitata myös sivullisia elektronisia laitteita. Häirinnän kehitystä hidastaa juridinen sääntely joissain maissa. [14]

Satelliittipaikannushuijauksessa (GNSS-spoofing, GNSS-huijaus) droonille lähetetään väärää sijaintitietoa, jolla drooni harhautetaan lentämään turvalliselle alueelle tai laskeutumaan turvallisesti. Tekniikka sopii erityisesti kaupunkialueille, joissa fyysinen torjunta ei ole turvallista. GNSS-huijaus on teknisesti vaikea toteuttaa, eikä se toimi kaikkiin drooneihin. Tekniikka toimiessaan voisi olla erityisen tehokas autonomisesti satelliittipaikannuksen avulla toimivien drooniparvien torjuntaan. [15]

Drooni vs. drooni menetelmä (Attacker hunter drone, AHD) käyttää tekoälyä ja GNSS-huijausta. ”Metsästäjä drooni” ohjaa GNSS-huijauksen avulla haitallisen droonin turvalliselle vyöhykkeelle, jossa drooni voidaan torjua. Menetelmä käyttää vahvistusoppimista (Q-learning) nopeasti mukautuvaan ja tehokkaaseen toimintaan. Menetelmällä saadaan minimoitua vahingot ja mahdollistamaan forensisten tietojen säilyttämisen. [15]

Etäidentifikaatio (Drone Remote Identification, DRI) tarkoittaa droonien tunnistamista ja lainmukaisuuden varmistamista etänä. Tekniikka toimii käytännössä ennalta ehkäisevänä protokollana, jossa jokainen drooni lähettää tunnistustietojaan. Tiedoista selviää droonin rekisteröinti, lentolupa ja muut oleelliset tiedot. Etäidentifikaation tarkoituksena on tunnistaa drooni nopeasti ja luotettavasti, sekä erottaa lailliset ja luvattomat droonit toisistaan ennen torjuntatoimien käynnistämistä. Etäidentifikaation jälkeen tilanteen arvioimiseksi käytetään toimintaprotokollaa jonka vaiheet ovat seuraavat:

- Toleranssi, vähemmän kriittisessä tilanteessa voidaan antaa droonille hetki aikaa korjata tilanne. Esimerkiksi tunnistautua tai korjata lentoreitti.
- Välitön esto, kriittisessä tilanteessa drooni pysäytetään välittömästi, jos uhka arvioidaan vakavaksi ja välittömäksi.
- Viivästetty esto, käytetään tilanteissa joissa drooni ei aiheuta välitöntä uhkaa mutta sen toiminta vaatii kuitenkin lisäselvitystä.

Etäidentifikaatio ja protokollapohjainen torjunta vähentää virheellisiä päätöksiä järjestelmällisten toimintatapojen ansiosta. Lisäksi ne huomioivat lailliset näkökulmat ja vähentää sivullisille aiheutuvaa vaaraa. Menetelmä on myös nopea ja luotettava, identifikaatio kestää vähimmillään muutamia sekunteja. Menetelmän haasteena on tarve reaaliaikaiselle yhteistyölle operatiivisten järjestelmien sekä viranomaisten kanssa. Lisäksi järjestelmän täytyy kyetä erottamaan tekniset ongelmat ja oikeutetut poikkeukset toisistaan. [22]

Taulukko 2.2: Torjuntajärjestelmien vertailu [23]

Torjuntajärjestelmä	**Toimintasäde**	**Kustannus**	**Teknologian kehitysaste**	**Sivulliset vahingot**	**Kyky torjua drooniparvia**
Ilmatorjuntaohjus	Kaukana	Korkea	Korkea	Suuri	Huono
Laserase	Kaukana	Matala	Matala	Pieni	Hyvä
Mikroaaltotekniikka	Kaukana	Matala	Matala	Pieni	Hyvä
Pehmeät torjuntakeinot	Kaukana	Matala	Korkea	Pieni	Hyvä
Verkko	Lähellä	Matala	Korkea	Pieni	Huono

2.3 Drooniparvien kehitys ja niiden vaikutus torjuntajärjestelmissä

Drooniparvien nopea teknologinen kehitys perustuu tekoälyyn, autonomiaan ja hajautettuun viestintään, joiden avulla droonit voivat toimia yhdessä koordinoidusti ilman keskitettyä ohjausta [24]. Parvet tarjoavat uudenlaisia mahdollisuuksia sodankäyntiin hyödyntämällä määrällistä ylivoimaa, nopeutta ja älyä [25]. Tämä on haastanut perinteiset torjuntateknologiat, jotka eivät ole suunniteltu kohtaamaan samanaikaisesti toimivia, monimuotoisia ja älykkäitä uhkia. Kehityksen myötä drooniparvet ovat vaikuttaneet merkittävästi sekä hyökkäys- että puolustusstrategioihin taistelukentällä [26].

2.3.1 Drooniparvien teknologinen kehitys

Droonien autonomisuus mahdollistaa laajat itsenäiset ja älykkäät operaatiot, joissa yksittäisen droonin tehtävät vaihtelevat tiedustelusta taisteluyksiköihin ja viestinnän varmistajiin [24]. Drooniparvien teknologinen kehitys on ollut nopeaa ja monipuolista. Se perustuu vahvasti tekoälyn, viestintäteknologian ja autonomisten järjestelmien kehittymiseen. Parviteknologian ytimessä on kyky hajautettuun päätöksentekoon ja kommunikaatioon, minkä ansiosta droonit voivat toimia yhdessä koordinoidusti ilman keskitettyä ohjausta.

Valtiot kuten Iso-Britannia, Venäjä, Kiina ja Yhdysvallat, ovat investoineet parviteknologiaan. Esimerkiksi Yhdysvaltojen LOCUST- ja Gremlins-ohjelmat kehittävät halpoja ja helposti monistettavia droonialustoja joita voidaan käyttää suurissa parvissa. Parvista kehitetään pääasiassa heterogeenisiä, jolloin parvi koostuu eri tehtäviä suorittavista drooneista. Heterogeenisyyden ansiosta drooniparvet voivat toteuttaa ja mukautua monimutkaisiin operaatioihin. [24]

2.3.2 Drooniparvien strateginen käyttö ja vaikutus sodankäynnissä

Drooniparvet muuttavat sodankäynnin strategisia asetelmia hyödyntämällä massaa, nopeutta, älyä ja koordinaatiota. Parviteknologia mahdollistaa uudenlaisen sodankäyntimallin, jossa suuri määrä itsenäisesti koordinoituja drooneja voi toteuttaa monipuolisia operaatioita ilman jatkuvaa ihmisen ohjausta [25]. Parvien strategisiin ominaisuuksiin kuuluvat määrällinen ylivoima, heterogeenisyys ja korkea resiliensi: ne muodostavat hajautetun verkoston, jossa yksittäisten droonien menetys ei merkittävästi heikennä koko parven toimintakykyä. Tällainen rakenne mahdollistaa koordinoidut ja hajautetut hyökkäykset, jotka kuormittavat vihollisen puolustusjärjestelmiä ja lisäävät todennäköisyyttä, että osa drooneista läpäisee puolustuslinjat. Parvet ovat usein heterogeenisiä, ne voivat koostua eri tyypin drooneista, joiden tehtäviä ovat hyökkäys, tiedustelu, viestintä ja elektroninen sodankäynti [24].

Drooniparvet vaikuttavat taistelukentän dynamiikkaan. Parvet lisäävät sodankäynnin tempoa, mikä voi johtaa ”flash war” -tilanteeseen. Se tarkoittaa tilannetta jossa sodan tempo ja päätöksentekosykli nopeutuu niin paljon, ettei ihmisenpäätöksenteko pysy mukana [25]. Ihmisen jääminen jalkoihin päätöksenteossa haastaa kansainvälisiä oikeuksia ja sodankäynnin periaatteita. Kuka on vastuussa autonomisen droonin tekemästä sotarikoksesta [3]? Drooniparvet eivät ole vain hyökkäyksellinen teknologia; niitä käytetään myös vastadroonijärjestelminä. Puolustusparvet voivat

saartaa ja hajottaa vihollisen hyökkäävät parvet tai häiritä niiden kommunikaatiota ja pakottaa ne epäedullisiin sijainteihin. Tärkeänä etuna on kyky toimia autonomisesti ja hajautetusti ilman satelliittipaikannusta, mikä tekee parvesta erityisen kestävän vihollisen elektronista sodankäyntiä vastaan [26].

2.3.3 Drooniparvien vaikutus torjuntateknologioihin

Drooniparvien yleistyminen ja teknologinen kehittyminen aiheuttaa merkittäviä haasteita perinteisille puolustusjärjestelmille. Perinteiset ilmatorjuntaratkaisut ovat suunniteltu suuria yksittäisiä kohteita vastaan ja osoittautuneet tehottomiksi drooniparvien muodostamaa uhkaa vastaan [23]. Esimerkiksi 14. syyskuuta 2019 Saudi Aramcon kahteen öljyjalostamoon tehtiin hyökkäys, joissa käytettiin noin kymmenen droonin parvea [24]. Hyökkäys aiheutti merkittävää tuhoa infrastruktuurille ja häiritsi maailmanlaajuista öljyntuotantoa. Tapaus korosti drooniparvien kykyä hyökätä tehokkaasti erittäin suojattuihin kohteisiin.

Elektronisen sodankäynnin merkitys kasvaa drooniparvien torjunnassa. Vihollisen kommunikaation hajottaminen on tehokas tapa lamauttaa drooniparven toimintakyky [26]. Drooniparvien nopeus ja autonomisuus ovat pakottaneet kehittämään tekoälyyn perustuvia, automatisoituja ja nopeammin reagoivia torjuntajärjestelmiä [25]. Ratkaisu voisi olla yhdistelmä erilaisia torjuntateknologioita kuten fyysisiä torjuntamenetelmiä, sensorifuusiota, elektronista häirintää ja tekoälypohjaisia seurantamenetelmiä, jotka ovat kehittymässä tehokkaaksi vastaukseksi drooniparvien aiheuttamaan uhkaan [24].

3 Aineisto ja tulokset

3.1 Havaitsemisteknologiat ja niiden tehokkuus

Viime vuosien kehitys droonien käytössä sekä niiden yleistyminen siviili- ja sotilaskäytössä luovat tarpeen tehokkaalle ja luotettavalle droonien havainnoinnille ja tunnistamiselle. Erilaiset uhkatilanteet edellyttävät, että käytettävät havainnointiteknologiat kykenevät vastaamaan monenlaisiin toimintaympäristöihin. [4]

3.1.1 Havaitsemisteknologioiden vertailu

Droonien havaitsemiseen vaikuttavat merkittävästi toimintaympäristö sekä uhkan luonne. Tutkajärjestelmät erottuvat pitkällä havaintoetäisyydellä sekä kyvyllä havaita drooneja myös haastavissa sää- ja näkyvyysolosuhteissa, mutta pienikokoisten droonien havaitseminen voi olla ongelmallista [17]. Akustiset sensorit ovat tehokkaita havaitsemaan drooneja lyhyellä kantamalla säästä riippumatta, mutta niiden suorituskykyyn vaikuttaa merkittävästi ympäristön melutaso [14]. Kuvapohjaiset järjestelmät tarjoavat tarkan visuaalisen tunnistuksen, mutta eri tilanteisiin tarvitaan erilaisia kameroita [16]. Esimerkiksi lämpökamera toimii hyvin pimeällä, mutta sen voi olla haastava tunnistaa vähälämpöisiä drooneja. Perinteistä kameraa käyttäessä näkyvyyden on oltava hyvä, mikä rajaa sen käyttöä vain hyvään keliin. Radiotaajuusjärjestelmät kykenevät tunnistamaan droonien aktiivisen radioliikenteen [14]. Radioliikenteen perusteella on mahdollista tunnistaa myös droonin toimintatila, eli

onko drooni esimerkiksi leijumassa paikallaan tai palaamassa tukikohtaan. Radiotaajuusjärjestelmät eivät tunnista automaattisesti tai kuidun avulla lentäviä drooneja. Ympäristötekijät kuten urbaanit alueet ja sääolosuhteet ovat suurin rajoite erilaisille havaitsemisteknologioille [16]. Ratkaisuksi ympäristötekijöihin kehitetään moniteknologisia ratkaisuja yhdistämällä jo olemassa olevia sensoreita.

3.1.2 Moniteknologiset ratkaisut

Moniteknologiset ratkaisut ovat nousseet yhä keskeisimmiksi droonien havainnointijärjestelmissä, koska yksittäiset sensoriteknologiat eivät tarjoa täydellistä ratkaisua kaikkiin tilanteisiin [16]. Tutkan pitkän kantaman havainnointi voidaan yhdistää kuvapohjaisiin ja akustisiin sensoreihin, jolloin saavutetaan kattava havainnointi sekä pitkällä että lyhyellä etäisyydellä [17]. Lisäämällä samaan ratkaisuun radiotaajuusteknologia, saadaan tietoa radioliikennettä käyttävistä drooneista, joiden toimintatila voidaan selvittää [14].

Teknologioiden yhdistäminen lisää kustannuksia ja kompleksisuutta, mikä tuo mukanaan haasteita järjestelmän ylläpidossa ja integraatiossa [16]. Teknologioiden oikeaoppinen integrointi ja optimointi ovat kriittisiä tehokkaan ja taloudellisesti järkevän moniteknologisen ratkaisun kehittämisessä.

3.1.3 Tekoälyn rooli havaitsemisessa

Tekoälyllä on tärkeä rooli droonien havainnoinnin ja luokittelu tehostamisessa. Koneoppimisen avulla voidaan analysoida ja yhdistää nopeasti eri sensoreista saatavaa tietoa, mikä parantaa havainnointijärjestelmän kykyä tunnistaa drooneja ja niiden toimintatilaa [22]. Erityisesti radiotaajuusteknologian yhteydessä tekoäly mahdollistaa tarkemman droonien lentotilan tunnistamisen, mikä auttaa arvioimaan droonin uhkapotentiaalia [14]. Lisäksi tekoäly tukee drooniparvien hallintaa ja torjuntaa, sillä se kykenee käsittelemään laajoja tietomääriä nopeasti ja tekemään autonomisia pää-

töksiä dynaamisissa tilanteissa [26]. Esimerkiksi vahvistusoppiminen (reinforcement learning) tarjoaa menetelmiä, joilla torjuntajärjestelmät voivat nopeasti mukautua droonien vaihteleviin toimintatapoihin ja ohjata droonit pois herkiltä alueilta [15]. Tekoälyn kehityksen myötä droonien havainnointijärjestelmien kyky tunnistaa ja ennakoida uhkia paranee ja nopeutuu merkittävästi [22].

3.2 Torjuntakeinojen tehokkuuden vertailu eri uhkatilanteissa

Eri torjuntakeinojen tehokkuus riippuu siitä, millaista uhkaa vastaan ja millaisessa ympäristössä niitä käytetään. Esimerkiksi laseraseiden ja korkeatehoisten mikroaaltojen tehokkuus korostuu pienien, nopeasti liikkuvien ja vaikeasti havaittavien droonien torjunnassa [19]. Pienten droonien torjunnassa perinteiset fyysiset torjuntakeinot, kuten tykit ja ohjukset ovat liian kalliita ja ne aiheuttavat merkittävän riskin oheisvahingoista [21].

Pehmeät torjuntakeinot, kuten häirintä ja GNSS-huijaus soveltuvat parhaiten ympäristöihin, joissa fyysisten torjuntakeinojen käyttö on liian riskialtista [13]. Tällaisia ympäristöjä ovat esimerkiksi urbaanit alueet ja kriittisten infrastruktuurien läheisyys.

Droonien torjunnassa käytetään myös toisia drooneja. Esimerkiksi vastadrooniparvien kaltaiset integroidut fyysiset menetelmät osoittavat suurta potentiaalia [26]. Vastadrooniparvet kykenevät mukautumaan joustavasti erilaisiin uhkatilanteisiin ja minimoimaan riskejä ympäristölle

3.2.1 Fyysisten torjuntakeinojen soveltuvuus ja rajoitteet

Fyysiset torjuntamenetelmät kuten laseraseet, mikroaaltotekniikka ja ohjusjärjestelmät tarjoavat nopean ja usein varman keinon droonien neutralointiin. Laseraseiden

etuja ovat tarkkuus, nopea reagointiaika ja pieni oheisvahinkoriski [19]. Laseraseiden rajoitteena on ympäristö ja tarve suurelle energiantuotolle.

Mikroaaltotekniikalla pyritään lamauttamaan droonin elektroniikka ja viestintäjärjestelmät [21]. Mikroaaltotekniikka soveltuu hyvin tilanteisiin, joissa droonien suuri määrä tai niiden ketteryys vaikeuttavat verkkojen tai kineettisten aseiden käyttöä. Toisaalta mikroaaltojen käyttöä rajoittavat ympäristötekijät. Urbaanissa ympäristössä mikroaallot voivat vaikuttaa haitallisesti myös muihin elektronisiin järjestelmiin, kuten matkapuhelimiin.

Perinteiset ampuma-aseet ja ohjukset ovat tehokkaita suurten ja matalalla lentävien droonien torjunnassa, mutta niiden käyttö on kallista ja niihin liittyy merkittävä oheisvahinkojenriski [21]. Kustannustehokkaampi vaihtoehto on käyttää toista droonia haitallisen droonin torjumiseksi joko törmäämällä tai räjähtämällä lähellä [27]. Fyysistentorjuntakeinojen tarkoitus on tuhota droonin propulsio, tai muilla keinoin tehdä siitä kyvytön jatkamaan tehtäväänsä. Fyysisten torjuntakeinojen lisäksi drooneja voidaan torjua pehmeillä keinoilla.

3.2.2 Pehmeiden torjuntakeinojen soveltuvuus ja rajoitteet

Fyysisten torjuntakeinojen lisäksi drooneja voidaan torjua pehmeillä keinoilla. Pehmeiden torjuntakeinojen ideana on säilyttää droonin forensiset tiedot, joista voidaan myöhemmin kerätä arvokasta dataa. Pehmeitä keinoja käytetään myös tilanteissa, joissa fyysisten torjuntakeinojen käyttö aiheuttaa liiallista riskiä.

Häirintä on tehokastapa estää droonien ohjaus- ja navigointiyhteydet. Häirintä on kuitenkin riippuvainen siitä, että haitallinen drooni käyttää näitä signaaleja [21]. Esimerkiksi Ukrainan sodassa käytetty valokuituyhteyden avulla operoiva drooni on immuuni radiotaajuushäirinnälle [28].

GNSS-huijaus, jossa drooni harhautetaan pois kohdealueelta lähettämällä sille väärää sijaintitietoa, on tehokas tapa hallita drooneja vahingoittamatta niitä [21].

Kyberhyökkäyksen avulla drooneja voidaan ottaa haltuun tai lamauttaa, mutta niiden toiminta perustuu siihen että droonien tietoliikennejärjestelmissä on tunnettuja haavoittuvuuksia [13].

Verkot ovat periaatteessa fyysisiä torjuntakeinoja, mutta niillä on merkittäviä pehmeiden torjuntakeinojen ominaisuuksia. Verkoilla on matala oheisvahinkoriski ja niitä käyttämällä droonin forensiset tiedot saadaan säilytettyä [26]. Verkkoja voidaan hyödyntää useilla eri tavoilla: maasta käsin tykeillä tai ampuma-aseilla, droonista laukaistuna tai drooniparven kuljettamana. Verkkoja käytetään myös passiivisesti asentamalla niitä kriittisten kohteiden läheisyyteen.

3.2.3 Teknologioiden integrointi ja monikerroksisen puolustuksen rakentaminen

Droonien torjunnassa tehokkuus perustuu teknologioiden yhdistämiseen monikerroksiseksi puolustusjärjestelmäksi, jossa pehmeät ja fyysiset keinot täydentävät toisiaan eri uhkatilanteiden vaiheissa [21]. Monikerroksisessa puolustusjärjestelmässä tavoitteena on havaita ja neutraloida droonit mahdollisimman aikaisessa vaiheessa. Tämä vähentää fyysisten torjuntakeinojen tarvetta, jotka ovat yleensä kustannuksiltaan ja riskeiltään suurempia.

Monikerroksisuutta voidaan kuvata sipulinkuorimallilla. Mallissa torjuntakeinot kovenevat mitä syvemmälle uhka etenee. Uloin kuori muodostuu pehmeistä keinoista kuten radiotaajuus- ja GNSS-häirinnästä, joilla pyritään estämään droonin pääsy suojatulle alueelle ilman fyysisiä keinoja [21]. Mikäli uhka läpäisee uloimman kuoren, keskimmäinen kerros aktivoituu. Keskimmäiseen kerrokseen kuuluvat esimerkiksi korkeatehoiset mikroaaltoaseet ja verkot, jotka lamauttavat tai pysäyttävät droonin fyysisesti, mutta ilman suurempaa uhkaa ympäristölle [26]. Viimeisenä ja sisimpänä kerroksena toimivat kineettiset aseet, kuten laserit ja ohjukset [19]. Viimeisen kerroksen tavoitteena on tuhota drooni lopullisesti kriittisessä tilanteessa.

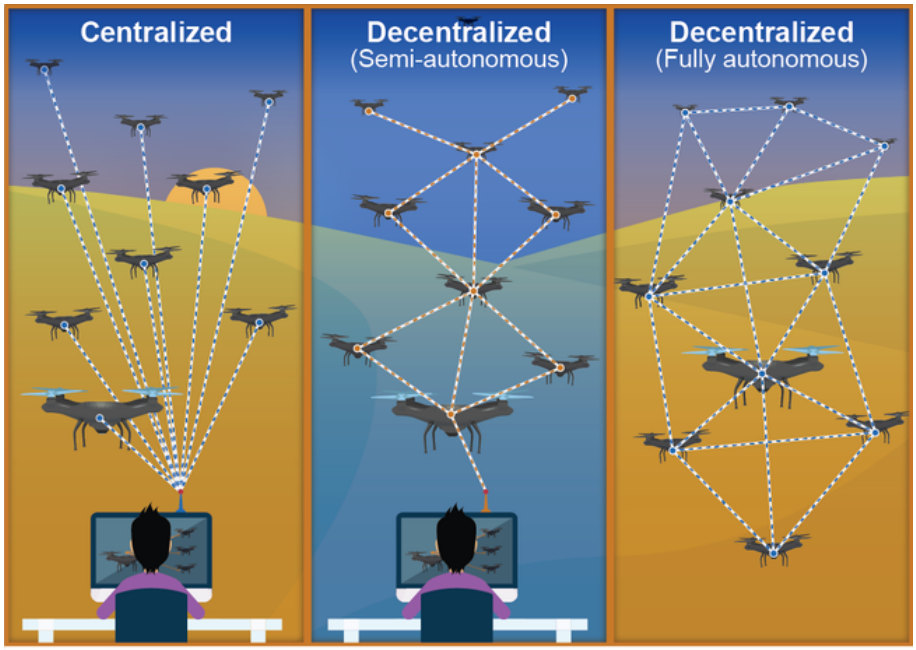
Teknologioiden yhteistoiminta vaatii tekoälyä toimiakseen. Erilaiset sensorit syöttävät dataa yhteen järjestelmään, jossa tekoäly käsittelee tiedon reaaliaikaisesti ja ehdottaa parasta torjuntakeinoa tilanteeseen [21]. Tekoäly myös kohdentaa resursseja ja priorisoi uhkia. Tekoäly mahdollistaa järjestelmän automatisoinnin, jolloin se voi toimia myös silloin kun operatiivista henkilökuntaa ei ole saatavilla. Tämä sensorifuusio mahdollistaa dynaamisen päätöksenteon, mikä on keskeistä nopeasti liikkuvien droonien torjunnassa.

3.3 Drooniparvet ja niiden tuottamat haasteet

Drooniparvien yleistyminen sodankäynnissä ja niiden edustama teknologinen murros ovat tuoneet merkittäviä haasteita nykyisille torjuntajärjestelmille. Näitä ovat erityisesti parvien korkea autonomisuus, dynaaminen yhteistoiminta ja suuri lukumäärä, mikä asettaa uusia vaatimuksia niin havainto- kuin torjuntamenetelmille. [23]

3.3.1 Drooniparvien dynaaminen käyttäytyminen ja torjunta

Drooniparvet toimivat tyypillisesti dynaamisesti ja adaptiivisesti. Parvet hyödyntävät autonomista koordinaatiota sekä hajautettua päätöksentekoa [23]. Parvien kyky muodostaa nopeasti uusia taktiikoita, sekä vaihtaa tehtäviä kesken operaation vaikeuttaa ennustettavuutta ja torjuntaa. Tämä edellyttää torjuntajärjestelmiltä kykyä jatkuvaan uhka-analyysiin, nopeaan reagointiin ja joustavaan toimintaan [21]. Perinteiset staattiset puolustusjärjestelmät eivät pysty riittävän tarkasti seuraamaan parvien liikettä tai mukautumaan niiden muuttuviin taktiikoihin. Lisäksi drooniparvien käyttämä hajautettu viestintä ja tekoälyyn perustuva koordinointi vaikeuttavat yksittäisten droonien neutraloimista, sillä parvi voi uudelleenorganisoitua ja jatkaa tehtävänsä suorittamista vaikka osa yksiköistä tuhottaisiin [23].



Kuva 3.1: Drooniparven toiminta voi olla keskitettyä, hajautettua (osittain autonomista) tai hajautettua (täysin autonomista) [29]

3.3.2 Torjuntajärjestelmien sopeutuminen drooniparviin

Torjuntajärjestelmien on sopeuduttava drooniparvien muodostamiin uusiin uhkakuviin. Tämä edellyttää entistä laajempaa sensorifuusiota, korkeampaa automaatiotasoa ja tekoälypohjaista uhka-analyysiä [21]. Näiden avulla voidaan tunnistaa drooniparvien toimintamalleja ja ennakoida niiden seuraavia liikkeitä. Tehokkaana ratkaisuna on havaittu vastadrooniparvet, jotka kykenevät reagoimaan nopeasti uhkan liikkeisiin ja sopeutumaan niiden toimintatapoihin [26]. Vastadrooniparvet voivat esimerkiksi piirittää haitallisen parven, jolloin vihollisen droonien toimintamahdollisuuksia saadaan rajoitettua. Torjuntajärjestelmiin täytyy myös integroida elektronista häirintää ja kineettisiä aseita [19]. Niiden yhdistäminen uusien droonipohjaisten torjuntaratkaisujen kanssa saavutetaan parempi reagointinopeus ja joustavuus

3.3.3 Tulevaisuuden haasteet ja ratkaisut drooniparvien torjunnassa

Vaikka nykyiset torjuntajärjestelmät kehittyvät nopeasti, drooniparvien teknologinen kehitys aiheuttaa jatkuvasti uusia haasteita. Merkittävästi haastetta lisää tekoälyn ja autonomisuuden kasvu drooniparvissa, nämä vaikeuttaa drooniparvien ennakointia ja torjuntaa entisestään [21]. Ratkaisuna korostuvat tekoälyavusteiset ja autonomiset torjuntajärjestelmät. Näihin perustuva järjestelmä kykenisi itsenäisesti tunnistamaan, seuraamaan ja ennakoimaan drooniparvien käyttäytymistä ja tekemään itsenäisiä päätöksiä vastatoimista. Tulevaisuuden ratkaisuja voivat olla myös uudenlaiset elektroniset ja kyberpohjaiset torjuntamenetelmät, joiden avulla häiritään drooniparvien sisäistä viestintää ja tekoälyn toimintaa [13]. Lisäksi drooniparvien torjunnan ja toiminnan kehittyessä on välttämätöntä kehittää kasainvälisesti yhteisiä normeja ja sääntöjä, jotta niiden käyttöä ja vastatoimia voidaan hallita tehokkaasti myös kansainvälisellä tasolla.

4 Yhteenveto

Tässä tutkielmassa tarkasteltiin droonien havaitsemiseen ja torjuntaan käytettäviä teknologioita sekä tuotiin esille niiden tehokkuutta erilaisissa uhkatilanteissa. Tutkielman perusteella voidaan todeta, ettei mikään yksittäinen havaitsemis- tai torjuntateknologia tarjoa täydellistä ratkaisua kaikissa ympäristöissä, vaan tehokas torjunta vaatii teknologioiden yhdistämistä monikerroksiseksi puolustusjärjestelmäksi.

Havaitsemisteknologioiden osalta tutkat, kuvapohjaiset järjestelmät ja radiotaajuusanalyysi osoittautuivat hyödyllisiksi eri olosuhteissa, mutta niiden rajoitukset vaativat sensorifuusion ja tekoälyn hyödyntämistä luotettavuuden ja tunnistustarkkuuden parantamiseksi. Erityisesti tekoälyn rooli havaitsemisessa korostui sen kyvyssä analysoida nopeasti ja luotettavasti eri sensorien tuottamaa dataa.

Fyysisten ja pehmeiden torjuntakeinojen vertailussa havaittiin, että fyysiset menetelmät, kuten laseraseet ja mikroaaltotekniikka, tarjoavat nopean ja tehokkaan vasteen, mutta niiden käyttöön liittyy merkittäviä ympäristöön ja kustannuksiin liittyviä rajoitteita. Pehmeät menetelmät, kuten GNSS-huijaus ja radiotaajuushäirintä, mahdollistavat droonien neutraloinnin turvallisemmin ja säilyttäen arvokkaat forensiset tiedot, mutta niiden teho riippuu vahvasti droonin käyttämästä teknologiasta ja autonomiatasosta.

Drooniparvien lisääntyminen ja niiden dynaaminen käyttäytyminen luovat erityisen suuren haasteen nykyisille torjuntajärjestelmille. Parvien torjunta edellyttää torjuntajärjestelmiltä kykyä reaaliaikaiseen analyysiin, adaptiivisuuteen sekä tek-

nologiseen monipuolisuuteen. Vastadrooniparvet ja tekoälypohjainen sensorifuusio nousivat lupaaviksi keinoiksi vastata drooniparvien muodostamiin haasteisiin.

Tutkielman perusteella voidaan päätellä, että tulevaisuuden torjuntajärjestelmien tehokkuus perustuu vahvasti teknologioiden monikerroksiseen integrointiin ja tekoälyn hyödyntämiseen. Samalla droonien torjunta edellyttää kansainvälisen sääntelyn kehittämistä ja jatkuvaa teknologista innovaatiota vastaamaan kehittyviin uhkiin.

Lähdeluettelo

[1] R. V. Behare ja S. V. Raut, *Drones Using in Military & Civilian Application*, 2024. DOI: 10.5281/ZENODO.14555599.

[2] Z. Oudina, M. Derdour, A. Dib ja M. M. Bouhamed, "Empirical Analysis of the Security Threats and Risks That Drones Face, Represent, and Mitigation", teoksessa *2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, IEEE, 2024. DOI: 10.1109/PAIS62114.2024.10541193.

[3] A. Konert ja T. Balcerzak, "Military Autonomous Drones (UAVs) - from Fantasy to Reality. Legal and Ethical Implications", *Transportation Research Procedia*, vol. 59, 2021. DOI: 10.1016/j.trpro.2021.11.121.

[4] D. Kunertova, "Learning from the Ukrainian Battlefield: Tomorrow's Drone Warfare, Today's Innovation Challenge", ETH Zurich, tekninen raportti, 2024. DOI: 10.3929/ETHZ-B-000690448.

[5] D. G. Barten, D. Tin, H. De Cauwer, R. G. Ciottone ja G. R. Ciottone, "A Counter-Terrorism Medicine Analysis of Drone Attacks", *Prehospital and Disaster Medicine*, vol. 37, nro 2, 2022. DOI: 10.1017/S1049023X22000139.

[6] BBC News. "Venezuela: Military Figures Arrested After Drone 'Attack'". (2018), url: https://www.bbc.com/news/world-latin-america-45190905 (viitattu 02. 04. 2025).

[7] R.-P. Weinmann ja B. Schmotzle. ”TBONE - A Zero-Click Exploit for Tesla MCUs”. (2020), url: https://kunnamon.io/wp-content/uploads/2025/02/tbone-v1.0-redacted.pdf (viitattu 02. 04. 2025).

[8] S. Calder. ”Gatwick Drone Disruption Cost Over £50 Million”. (2019), url: https://www.independent.co.uk/travel/news-and-advice/gatwick-drone-airport-costeasyjet-runway-security-passenger-cancellationa8739841.html (viitattu 02. 04. 2025).

[9] J. Crump. ”‘Unidentified’ Drones Swarming US Warships Raise Alarm”. (2021), url: https://www.independent.co.uk/news/world/americas/drones-us-navywarships-unidentified-b1827342.html (viitattu 02. 04. 2025).

[10] M. W. Lewis, ”Drones and the Boundaries of the Battlefield”, *Texas International Law Journal*, vol. 47, s. 293, 2012. url: https://ssrn.com/abstract=1917461 (viitattu 02. 04. 2025).

[11] M. Gargalakos, ”The Role of Unmanned Aerial Vehicles in Military Communications: Application Scenarios, Current Trends, and Beyond”, *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, vol. 21, nro 3, 2024. DOI: 10.1177/15485129211031668.

[12] J. Hernandez. ”A Military Drone With a Mind of Its Own Was Used in Combat, U.N. Says”. (2021), url: https://www.npr.org/2021/06/01/1002196245/a-u-n-report-suggests-libya-saw-the-first-battlefield-killing-by-an-autonomousd (viitattu 02. 04. 2025).

[13] M. J. Guitton, ”Fighting the Locusts: Implementing Military Countermeasures Against Drones and Drone Swarms”, *Scandinavian Journal of Military Studies*, vol. 4, nro 1, 2021. DOI: 10.31374/sjms.53.

[14] C. J. Swinney ja J. C. Woods, "A Review of Security Incidents and Defence Techniques Relating to the Malicious Use of Small Unmanned Aerial Systems", *IEEE Aerospace and Electronic Systems Magazine*, vol. 37, nro 5, 2022. DOI: 10.1109/MAES.2022.3151308.

[15] D. L. D. Silva, R. Machado, O. L. Coutinho ja F. Antreich, "A Soft-Kill Reinforcement Learning Counter Unmanned Aerial System (C-UAS) With Accelerated Training", *IEEE Access*, vol. 11, 2023. DOI: 10.1109/ACCESS.2023.3253481.

[16] R. N. Kashi, A. Prashanth, S. R. Kashi ja G. Prabhakara, "A Survey and Analysis of Drone Detection Systems Using a Systems Approach Superposed on Scenarios", *Systems Engineering*, vol. 27, nro 3, 2024. DOI: 10.1002/sys.21735.

[17] S. Scheff, *State of the Industry: UAS Sensor Review*, 2021. url: https://ntrs.nasa.gov/api/citations/20210026446/downloads/NASA%20CR%2020210026446.pdf (viitattu 02. 04. 2025).

[18] Quadruped. "LSLIDAR MS03 LiDAR Sensor". (2025), url: https://www.quadruped.de/LSLIDAR-MS03_1 (viitattu 21. 10. 2025).

[19] L. Liao, X. Huang ja F. Xie, "Development Status and Operation Analysis of Laser Weapon in Anti-Drone Warfare", teoksessa *2023 IEEE International Conference on Unmanned Systems (ICUS)*, Hefei, China: IEEE, 2023. DOI: 10.1109/ICUS58632.2023.10318249.

[20] Airsight. "Air to Air CounterDrones and Net Guns". (2025), url: https://www.airsight.com/knowledge-hub/counter-drone-technology/air-to-air (viitattu 25. 05. 2025).

[21] J. Wang, Y. Liu ja H. Song, "Counter-Unmanned Aircraft System(s) (C-UAS): State of the Art, Challenges, and Future Trends", *IEEE Aerospace and Elect-*

ronic Systems Magazine, vol. 36, nro 3, 2021. DOI: 10.1109/MAES.2020.3015537.

[22] A. Shoufan ja E. Damiani, "Contingency Clarification Protocols for Reliable Counter-Drone Operation", *IEEE Transactions on Aerospace and Electronic Systems*, vol. 59, nro 6, 2023. DOI: 10.1109/TAES.2023.3313573.

[23] T. Fan, M. Xiaojing ja Z. Chi, "Development Status of Anti UAV Swarm and Analysis of New Defense System", *Journal of Physics: Conference Series*, vol. 2478, nro 9, 2023. DOI: 10.1088/1742-6596/2478/9/092011.

[24] T. Zieliński, "Factors Determining a Drone Swarm Employment in Military Operations", vol. 7, 2021. DOI: 10.37105/sd.112.

[25] P. Scharre, *Robotics on the Battlefield Part II*, lokakuu 2014.

[26] M. R. Brust, G. Danoy, D. H. Stolfi ja P. Bouvry, "Swarm-Based Counter UAV Defense System", *Discover Internet of Things*, vol. 1, nro 1, 2021. DOI: 10.1007/s43926-021-00002-x.

[27] N. Li, Z. Su, H. Ling, M. Karatas ja Y. Zheng, "Optimization of Air Defense System Deployment Against Reconnaissance Drone Swarms", *Complex System Modeling and Simulation*, vol. 3, nro 2, 2023. DOI: 10.23919/CSMS.2023.0003.

[28] A. Kirkkala. "Uusi ase yllätti sotilaat – tätä droonia ei voi pudottaa häirintälaitteilla". (2024), url: https://www.verkkouutiset.fi/a/uusi-ase-yllatti-sotilaat-tata-droonia-ei-voi-pudottaa-hairintalaitteilla/ (viitattu 07. 05. 2025).

[29] U.S. Government Accountability Office, *Counter-Drone Technology: Agencies Need to Improve Coordination and Address Challenges*, GAO-23-106930, 2023. url: https://www.gao.gov/products/gao-23-106930 (viitattu 25. 06. 2025).