Tampereen yliopisto

Miika Vuorenmaa

LUVATTOMIEN DRONEJEN TORJUNTA

Informaatioteknologian ja viestinnän tiedekunta
Kandidaatintyö
Kesäkuu 2019

TIIVISTELMÄ

Miika Vuorenmaa: Luvattomien dronejen torjunta
Kandidaatintyö
Tampereen yliopisto
Sähkötekniikka
Tarkastaja: TkT Taneli Riihonen
Kesäkuu 2019

Kandidaatintyön aiheena on luvattomien dronejen torjunta. Aihetta rajattiin siten, että työssä keskitytään vain sähkö- ja tietoteknisiin ratkaisuihin, minkä takia kineettisiä vaikutusmenetelmiä ei käsitellä ollenkaan. Työn ensimmäinen tavoite on tutustua yleisesti teknisiin menetelmiin ja niiden toimintaperiaatteisiin, joita hyödyntämällä luvattomat dronet voidaan havaita ja torjua. Tarkoituksena on löytää viranomaisille soveltuvia valvonta- ja torjuntalaitteita, jotka ovat toimintavarmoja ja turvallisia. Toinen tavoite on esitellä dronetorjuntateknologiaan erikoistuneita yrityksiä ja tutustua niiden kaupallisten tuotteiden teknisiin ratkaisuihin sekä vertailla niitä keskenään.

Valvonta- ja torjuntamenetelmien periaatteiden ymmärtäminen vaatii osittain dronen tekniikan tuntemista, joten aluksi tutustutaan yleisesti dronelennokkeihin. Tekniikan ohella käsitellään muutamia dronemalleja ja käyttötarkoituksia sekä perustellaan luvattomien dronejen torjunnan merkitys mahdollisilla uhkatilanteilla.

Työn ensimmäisessä osiossa tutustutaan neljään valvontamenetelmään, joita on käsitelty aiheeseen liittyvissä tieteellisissä artikkeleissa. Ne perustuvat akustiikkaan, optiikkaan, radiotekniikkaan ja tutkaan. Jokaisen menetelmän perusperiaatteet käydään läpi ja samalla arvioidaan niiden soveltumista dronevalvontaan. Dronetorjunnassa käsitellään pääasiassa radiohäirintää ja dronen hakkerointia, jonka avulla drone on mahdollista kaapata. Näiden lisäksi pohditaan muita mahdollisia torjuntamenetelmiä.

Työn toisessa osiossa listataan markkinoilla olevia yrityksiä, jotka tarjoavat viranomaisille dronetorjuntaan soveltuvia teknisiä laitteita. Vertailu jaetaan laitteiden käyttötarkoituksien mukaisesti kolmeen kategoriaan, jotka ovat valvonta- ja torjuntalaitteet sekä torjuntajärjestelmät. Jokaiseen kategoriaan valitaan satunnaisesti aina kolme tuotetta eri yritysten tuotevalikoimista siten, että niitä on mahdollista vertailla keskenään. Kuvien avulla havainnollistetaan laitteiden fyysinen toteutus. Vertailussa tarkastellaan erityisesti toiminta-aluetta ja teknistä toteutusta. Lisäksi huomioidaan muita käyttötarkoitukseen olennaisesti liittyviä tekijöitä.

Vertailua varten suoritetussa tiedonhankinnassa huomattiin, että kaupallisista laitteista ei ole saatavilla tarkkoja teknisiä yksityiskohtia, minkä takia työssä joudutaan luottamaan yritysten verkkosivuilla ja datalehdillä esitettyihin tietoihin. Myös laitteiden testiolosuhteista on hyvin vähän tietoa saatavilla, vaikka ympäristö vaikuttaa jokaisen torjunta- ja valvontamenetelmän toimintaan. Samalla vertailussa tuli esiin se, että radiovalvontaa ja -häirintää hyödynnetään kaupallisissa ratkaisuissa kaikkein eniten. Jokaisessa kategoriassa vertailtavat laitteet saavuttavat lähes saman toimintasäteen, vaikka niiden tekniset ratkaisut eroavat jonkin verran toisistaan. Lisäksi havainnot osoittavat, että kaupallisten tuotteiden ominaisuudet eivät täysin vastaa tieteellisten tutkimusten tuloksia.

Avainsanat: drone, UAV, lennokki, kuvauskopteri, autonomia, tunnistaminen, valvonta, radiokuuntelu, tutka, mikro-Doppler, torjunta, radiohäirintä, hakkerointi

ALKUSANAT

Valitsin kandidaatintyön aiheen Tampereen yliopiston sähkötekniikan yksikön aihepankista, koska aihe liittyy keskeisesti omiin opintoihin ja on erittäin ajankohtainen. Työ kytkeytyy yksikössä käynnissä olevaan Ulla Tuomisen säätiön rahoittamaan hankkeeseen "Haitallisten dronejen elektroninen torjunta". Motivaatiota työn tekemiselle toi mahdollisuus yhdistää elektroniikka, tietoliikenne- ja radiotekniikka. Työn ohella tarjoutui myös mahdollisuus tutustua tarkemmin sähkömagneettiseen ja radiotaajuuksiseen häirintään, joiden perusteet olen opiskellut varusmiespalveluksen aikana palvellessani viestijoukoissa.

Dronet olivat itselle suhteellisen tuttuja ennen työn aloittamista, mutta työn aikana oma tietymys varsinkin dronen tekniikasta kasvoi huomattavasti. Samalla kiinnostuin droneharrastuksesta ja suunnitelmissa on oman dronelennokin hankinta. Erityisen mielenkiintoinen uusi asia oli mikro-Doppler-ilmiö ja sen hyödyntäminen dronen havaitsemisessa.

Haluan kiittää tekniikan tohtori Taneli Riihosta erinomaisesta kandidaatintyön ohjauksesta. Ohjaustapaamisissa sain aina hyviä neuvoja ja ideoita, jotka auttoivat työn toteutuksessa, ja pystyin kehittämään omaa tieteellistä kirjoittamista.

Tampereella, 17. kesäkuuta 2019

Miika Vuorenmaa

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

BVLOS	Beyond Visual Line of Sight
EMP	Electromagnetic Pulse
EVLOS	Extended Visual Line of Sight
FPV	First Person View
HEL	High Energy Laser
Hexacopter	Kuusimoottorinen kopteri
LOS	Line of Sight
MAC	Media Access Control
Octocopter	Kahdeksenmoottorinen kopteri
Quadcopter	Nelimoottorinen kopteri
RC	Radio Control
RF	Radio Frequency
RPAS	Remotely Piloted Aircraft System
RPM	Rotations per Minute
RSS	Received Signal Strength
RTH	Return-to-Home
UAV	Unmanned Aerial Vehicle
VLOS	Visual Line of Sight
VR	Virtual Reality
WLAN	Wireless Local Area Network

1 JOHDANTO

Dronet eli miehittämättömät kauko-ohjattavat lennokit ovat yleistyneet nopeasti, ja niiden suosio on kasvanut huomattavasti viimeisen viiden vuoden aikana. Yleisin syy dronen hankintaan on harrastustoiminta. Myös monet eri alojen yritykset ja viranomaistahot ovat alkaneet hyödyntämään droneja osana omaa toimintaansa. Samalla nämä suositut kuvauskopterit ja lennokit ovat luoneet uuden turvallisuusuhan. Tällä hetkellä eri alojen viranomaiset tarvitsevat nopeasti uusia teknisiä ratkaisuja, joilla voidaan havaita, estää ja torjua dronejen luvaton käyttö. Erityisesti tarvetta olisi ratkaisuille, jotka ovat toimintavarmoja ja toimivat turvallisesti riippumatta käyttöympäristöstä. Autonomiset järjestelmät lisäisivät kustannustehokkuutta, koska valvontahenkilöstöä ei tarvita. Dronelennokkien havaitsemisesta ja torjunnasta ei saa aiheutua vahinkoa, vaaratilanteita tai häiriötä ihmisille tai ympäröivälle infrastruktuurille.

Dronelennokkien aiheuttamista uhkatilanteista ja väärinkäytöstä on uutisoitu paljon ulkomailla ja kotimaassa, minkä perusteella dronelennokkien aiheuttamaa uhkaa voidaan pitää todellisena. Suomessa on jo varauduttu näihin uusiin uhkatilanteisin muuttamalla poliisin, puolustusvoimien ja rajavartiolaitoksen toimintatapoja. Asiasta on tehty lakimuutos, joka astui voimaan alkuvuodesta 2019. Sen myötä viranomaisilla on nyt oikeus puuttua droneilla aiheutettuihin uhkatilanteisiin ja luvattomaan käyttöön.

Droneista yleisesti on tehty suhteellisen paljon tutkimusta ja opinnäytetöitä viime vuosien aikana. Aikaisemmissa tutkimuksissa on laajasti käsitelty dronen soveltumista eri alojen käyttöön. Dronejen hyödyntämistä on tarkasteltu muun muassa valokuvauksen, rakentamisen, ympäristösuunnittelun ja metsätalouden näkökulmista. Toistaiseksi suomenkielisessä tieteellisessä tutkimuksessa ei ole ehditty perehtymään dronejen havainnointiin ja torjuntaan. Asiaan liittyvää kaupallista tuotekehitystä on tapahtunut, mikä näkyy markkinoilla olevista yrityksistä ja niiden dronevalvonta- ja torjuntalaitteista.

Kandidaatintyön päätarkoitus on tutustua dronelennokkien havaitsemisen ja torjunnan perusperiaatteisiin ja tehdä kattava kirjallisuusselvitys kotimaassa ja ulkomailla toimivien yritysten tuotteiden teknisistä ratkaisuista, jotka soveltuvat siviiliviranomaisten käyttöön. Toiseksi on tarkoitus vertailla alan yritysten samantyyppisiä tuotteita keskenään ja arvioida niiden soveltuvuutta eri käyttöympäristöissä.

Droneja voidaan käytännössä torjua lukuisilla eri tavoilla, mutta tässä työssä on tarkoitus keskittyä teknisiin menetelmiin ja laitteisiin, jotka pohjautuvat elektroniikkaan sekä langattoman tiedonsiirron ja radiotekniikan hyödyntämiseen. Tämän takia työn ulkopuolelle

rajataan kaikki sellaiset torjuntamenetelmät, jotka perustuvat täysin kineettiseen vaikuttamiseen. Pois suljettuja menetelmiä ovat dronen alasampuminen käsiaseella tai ilmatorjunnan avulla, erilaiset maasta tai ilmasta laukaistavat verkonheittimet sekä dronen sieppaamiseen koulutetut kotkat ja haukat.

Työn sisältö on järjestetty siten, että seuraavassa luvussa tutustutaan ensin yleisesti droneihin ja perustellaan niiden aiheuttama turvallisuusuhka. Luvussa 3 käsitellään neljää erilaista valvontamenetelmää, joita hyödyntämällä dronet ovat mahdollista havaita. Luvussa 4 tarkastellaan teknisiä menetelmiä, joilla luvattoman dronen eteneminen voidaan pysäyttää. Luvussa 5 yhdistyy osittain aikaisempien lukujen sisällöt, kun vertaillaan dronetorjuntaan erikoistuneiden yritysten kaupallisia ratkaisuja keskenään. Lopuksi luvussa 6 esitetään työn havainnot, keskeiset johtopäätökset ja pohditaan mahdollisia jatkotutkimuksia. Aineisto tutkimukseen on kerätty lähes kokonaisuudessaan sähköisistä lähteistä, koska dronelennokkeihin liittyvää painettua kirjallisuutta on hyvin niukasti saatavilla.

2 DRONELENNOKIT

Dronelennokilla tarkoitetaan miehittämätöntä ilma-alusta (engl. UAV, Unmanned Aerial Vehicle), jota ohjataan pääasiassa maasta käsin. Arkikielessä droneista saatetaan puhua hieman vaihtelevilla nimillä, joilla kaikilla kuitenkin viitataan samaan asiaan. Yleisempiä nimityksiä ovat muun muassa drooni, lennokki tai kuvaus-, neli-, heksa-, okto- ja multikopteri sekä muut johdannaiset termit. Eri nimityksiä käytetään riippuen asiayhteydestä ja kuvaamaan esimerkiksi dronen rakennetta tai käyttötarkoitusta. Ammattilaiskäytön yhteydessä käytetään termiä RPAS (engl. Remotely Piloted Aircraft System), jolla tarkoitetaan kauko-ohjatun ilma-aluksen käytön kokonaisjärjestelmää ja siihen oleellisesti liittyviä laitteita. [16]

Suomessa kuka tahansa voi ostaa dronelennokin ja aloittaa lennätysharrastuksen ilman mitään ennakkovaatimuksia [16]. Dronen hankinta on todella helppoa, koska suurimpien kotimaassa toimivien elektroniikkaliikkeiden ja tavaratalojen tuotevalikoimista löytyy suhteellisen paljon erilaisia vaihtoehtoja. Tuotteen voi noutaa suoraan liikkeestä tai tilata verkkokaupan kautta. Mikäli kotimaan valikoima vaikuttaa suppealta, dronen voi myös tilata ulkomaalaisesta verkkokaupasta. Euroopan ulkopuolelta tilatessa pitäisi varmistua, että kyseinen tuote täyttää eurooppalaiset säädökset ja se on CE-hyväksytty [58]. Valitettavasti kaikki harrastajat eivät kuitenkaan noudata tätä säädöstä, minkä takia käytössä on myös laitteita, jotka eivät ole CE-merkittyjä. Lisäksi saatavilla on erilaisia rakennussarjoja, joiden avulla käyttäjä kykenee rakentamaan oman dronelennokkinsa [1, 3].

Dronen hankintahinta voi vaihdella suuresti. Halvimmat markkinoilla olevat tuotteet maksavat alle 100 euroa, ja kalleimpien mallien hinta voi olla yli 3000 euroa [3, 39, 61]. Suurien hintaerojen takia koptereiden ominaisuuksien välillä on myös suuria toiminnallisia eroja. Yleensä laatu, toimintasäde, lentoaika, ohjelmistot ja muut ulkoiset varusteet paranevat, mitä korkeamman hintaluokan tuotteesta on kyse. Kuluttajan ei kuitenkaan kannata tehdä ostopäätöstä pelkän hinnan perusteella, koska joissain kuluttujalaitteissa on käyttötarkoitusta ajatellen huomattavasti paremmat varusteet, mikä näkyy selvästi laitteen hinnoittelussa. Samalla kaupallisten dronejen hinnat ovat laskeneet, kun teknologia on yleistynyt ja kehittynyt [49]. Näin ollen lennokit voidaan jakaa karkeasti kolmeen eri kategoriaan niiden hinnan ja käyttötarkoituksen perusteella.

Matalan hintaluokan tuotteet ovat kokoluokaltaan pieniä ja soveltuvat sisä- tai ulkokäyttöön. Laitteet ovat hyvin kevyitä, eivätkä kykene aiheuttamaan suurta vahinkoa törmäyksen sattuessa. Toimintasäde on yleensä 10–100 m riippuen kopterin mallista. Useimmissa tuotteissa varusteena on kamera, jota voidaan hyödyntää valo- ja videokuvauksessa.

(a) *Itse koottu drone [3]* ***(b)*** *DJI Mavic Air [61]* ***(c)*** *DJI Inspire 2 [39]*

Kuva 2.1. *Kolme eri hintaluokan dronelennokkia*

Joukossa on myös paljon lasten leluiksi tarkoitettuja tuotteita. Kuvassa 2.1a on lapsille suunniteltu ja Lego-palikoita vastaavista osista koottava drone. Laite on varustettu erillisellä suojakehikolla, jolla estetään potkureiden rikkoutuminen törmäyksessä. Tuotteen myyntihinta Amazon-verkkokaupassa on noin 30 euroa. [3]

Kuvassa 2.1b on harrastekäyttöön soveltuva kuvauskopteri, jonka myyntihinta Verkkokauppa.comin verkkosivuilla on noin 670 euroa. Kyseisen hintaluokan droneissa ominaisuudet ovat parantuneet huomattavasti verrattuna halvempiin laitteisiin. Toimintasäde on kasvanut useampaan kilometriin, laitteessa on GPS-paikannin ja kameran laatu ja ominaisuudet ovat parantuneet. Ohjelmistosta saattaa löytyä muun muassa automaattinen törmäyksen esto, automaattinen lähtöpaikkaan palaaminen (engl. RTH, Return-to-Home) ja autopilotti [14]. Kuluttajalaitteet soveltuvat kuitenkin huonosti ammatti- ja tutkimuskäyttöön, koska ne saattavat palauttaa epätarkan sijainnin, josta kuva on otettu, mikä vaikuttaa suoraan esimerkiksi karttojen sekä mittaustulosten tarkkuuteen ja luotettavuuteen. Ongelma saattaa johtua siitä, että laitteissa ei ole kuvauspisteiden hallintaa, minkä takia kuvia otetaan laitteen liikkuessa. Epätarkkoja kuvia ja tuloksia joudutaan korjaamaan jälkikäsittelyn yhteydessä, mistä aiheutuu luonnollisesti ylimääräistä työtä tai huonossa tapauksessa mittaukset ovat tehtävä uudestaan. [49]

Kuvassa 2.1c on ammattikäyttöön suunniteltu pitkän kantaman kopteri, jonka myyntihinta Multitronicin verkkosivuilla on noin 3300 euroa [39]. Myyntihinta ei sisällä kameraa tai muita lisälaitteita, joten todelliset kustannukset nousevat vieläkin korkeammiksi. Ammattilaitteet ovat suunniteltu siten, että ne kestävät pitkäaikaista käyttöä, minkä lisäksi valmistajat tarjoavat usein esimerkiksi huolto-, varaosa- ja korjauspalveluita. Muita etuja ovat muun muassa käytännöllisyys, muokattavuus, toimintavarmuus, erilaisten hyötykuormien kiinnittäminen ja pitkä toimintasäde. [49]

2.1 Dronen tekniikka

Dronet ovat radio-ohjattuja eli RC-laitteita (engl. Radio-Control), joiden ohjausjärjestelmien on täytettävä yleiset liikenne- ja viestintävirasto Traficomin asettamat määräykset käytettävällä taajuusalueella. Ohjauslaite voi olla perinteinen radio-ohjain tai nykyaikainen videonäytöllinen ohjausasema, joka välittää reaaliaikaista lentodataa. Datan avul-

la lentäjä saa jatkuvaa tilannetietoa lento-olosuhteista ja dronen järjestelmistä. Lento-olosuhteisiin liittyvää dataa voivat olla esimerkiksi tuulen nopeus ja suunta. Roottorien pyörimisnopeus, lentokorkeus, yhteyssignaalin laatu, akun kesto ja arvioitu lentoaika ovat järjestelmätietoja, joiden pohjalta lentäjä kykenee arvioimaan lentotapahtumaa ja tekemään päätöksiä. [14, 58]

Yleisimmät taajuusalueet ovat 2400–2483,5 MHz ja 5725–5875 MHz, joita käytetään dronen ohjaukseen. Traficom on luokitellut nämä luvasta vapaiden radiolaitteiden käyttötaajuuksiksi. Taajuuskaistoilla on asetettu rajoituksia käytettävien lähettimien lähetystehoille ja toimintasuhteille, jolloin ne eivät häiritse muita vastaavia laitteita. Tyypillisesti 2,4 GHz:n taajuusalue on dronen ohjaussignaalin käytössä ja dronen liitetty hyötykuorma toimii esimerkiksi 5,8 GHz:n alueella. Hyötykuormalla tarkoitetaan droneen liitettäviä lisälaitteita, jotka eivät liity dronen ohjaamiseen. Näitä lisälaitteita ovat muun muassa valonheittimet, sensorit, mittalaitteet, video- ja lämpökamerat. [16, 58]

Dronen ja radio-ohjaimen välinen radioliikenne on toteutettu tyypillisesti hyödyntäen taajuushyppelyä (engl. FH, Frequency Hopping), minkä ansiosta useat erilaiset laitteet voivat käyttää samaa taajuusaluetta. Taajuushyppelyssä käytettävissä oleva taajuuskaista jaetaan pienempiin osiin, joita kutsutaan kanaviksi. Jokaisella kanavalla on tietty taajuus ja leveys. Radioliikenne tapahtuu siten, että radiosignaali jaetaan pieniin osiin ja nämä osat lähetetään kanavien kautta tietyin aikavälein. Yksittäisen lähetyksen jälkeen siirrytään aina seuraavalle kanavalle. Kanavien hyppelyjärjestys voi olla joko ennalta määritelty tai satunnainen, jolloin sekä radiolähettimen että -vastaanottimen on tunnettava käytettävä pseudosatunnaisuus. Lisäksi on täysin mahdollista, että kaksi erilaista laitetta käyttävät hetkellisesti samaa kanavaa täsmälleen samaan aikaan. Tästä ei kuitenkaan seuraa suurempia ongelmia, koska radioliikenteellä on käytössä useita muita kanavia, joiden lukumäärää kasvattamalla on mahdollista pienentää samanaikaisten lähetysten todennäköisyyttä. [45, 50]

Dronet lentävät vaakatasossa pyörivien potkurien avulla. Yksittäisen potkurin pyörimisnopeus tavallisessa lentotilanteessa saattaa olla noin 7500-10500 kierrosta minuutissa (engl. RPM, Rotations per Minute) [40]. Jokaista potkuria pyörittää yleensä oma sähkömoottori, joka saa virtansa dronen akuista. Tyypillisesti droneissa käytetään litiumpohjaisia akkuja, koska ne kykenevät tuottamaan enemmän tehoa painoyksikköä kohden kuin vanhemmat nikkelipohjaiset akut. Käytettävät akut ovat suhteellisen kevyitä ja niillä on korkea energiatiheys. [13, 14, 57] Akkujen kapasiteetilla on keskeinen merkitys dronen lentoaikaan, joka riippuu muun muassa akkujen lukumäärästä, dronen mallista, lisälaitteista ja painosta. Yleisesti lentoaika vaihtelee välillä 10-30 minuuttia, jos vertaillaan eri dronetyyppejä [3, 39]. Lentoaikaa on hankala pidentää, koska ylimääräisen akun lisääminen kasvattaa akkujen kokonaiskapasiteettia, mutta samalla laitteen kokonaispaino kasvaa, minkä takia potkureita pyörittävien moottorien tehonkulutus kasvaa. Yksinkertainen ratkaisu tähän ongelmaan on vaihtoakut, mutta dronen täytyy laskeutua sellaiseen paikkaan, missä vaihto voidaan suorittaa.

Jos drone menettää yhteyden ohjauslaitteeseen, niin se voi toimia tilanteessa periaatteessa kolmella eri tavalla, jotka riippuvat dronen tyypistä ja lentotilan asetuksista. Ensimmäinen vaihtoehto on se, että drone pysähtyy leijumaan sen hetkiseen paikkaansa ja odottaa signaalin uudelleenyhdistymistä. Toiseksi se voi suorittaa hätälaskeutumisen suoraan alaspäin, mikä ei ota yleensä huomioon alla sijaitsevaa ympäristöä tai esteitä. Hätälaskeutuminen tyypillisesti tapahtuu, kun dronen akuista virta on loppumassa. Tarkoituksena on saada drone maahan hallitusti, jolloin suurilta vahingoilta olisi mahdollisuus välttyä. Kolmas toimintatapa on automaattinen kotiin palaaminen (engl. RTH, Return-to-Home), joka vaatii toimiakseen GPS-signaalin. Tässä yhteydessä "dronen koti" on yleensä lähtöpaikka, josta lentosuoritus on aloitettu. Ohjelmistoa muokkaamalla kotipaikaksi voidaan asettaa myös jokin muu kiinteä sijainti, joka ei ole lähtöpaikka. [13, 14, 38]

Dronet voivat lentää myös itsenäisesti eli autonomisesti, mikä ei vaadi lentosuorituksen aikana lentäjältä ohjauskomentoja tai muita toimenpiteitä. Ennen lentosuoritusta pitää kuitenkin määritellä dronelle sen lentoreitti, jonka voi esimerkiksi luoda puhelimeen ladattavan sovelluksen avulla. Sovelluksessa on graafinen käyttöliittymä ja kartta, johon lentäjä voi muutaman painalluksen avulla lisätä koordinaattipisteitä, jotka määrittelevät dronen lentoreitin [39]. Autonominen lentäminen toimii parhaiten, kun dronella on käytössä vahva GPS-signaali. Dronen autonomisuutta voidaan hyödyntää esimerkiksi tilanteissa, jossa drone suorittaa valvontatehtävää ennalta määriteltyä reittiä pitkin. [21]

Jos GPS-signaali on heikko tai sitä ei ole käytettävissä, niin drone voi lentää siihen kiinnitetyn kameran avulla. Kyseessä on visuaalinen navigointi ja paikannus, joka kameran ja muiden sensorien avulla mittaa ja analysoi ympäristöä. Informaation perusteella drone yrittää valita optimaalisen lentoreitin. Navigoinnin aikana drone reagoi esteisiin ja säätää jatkuvasti ohjaustaan siten, että se pysyy turvallisella reitillä. Visuaalista navigointia hyödyntäen drone kykenee esimerkiksi lentämään metsäpolkua pitkin tai palaamaan automaattisesti lähtöpaikkaansa. [21, 56]

2.2 Virkistys- ja hyötykäyttö

Tekniikan kehittyessä ja hintojen laskiessa dronelennokkien suosio on ollut tasaisessa kasvussa. Suurin painopiste on ollut ensi alkuun harrastekäyttö, mutta dronejen käyttö yritystoiminnan tukena on koko ajan lisääntymässä. Tulevaisuudessa suurimmat dronemarkkinat saattavat olla maatalous, teollisuus ja tavaraliikenne [29]. Parin viimeisen vuoden aikana myös yritysten lisäksi ja viranomaiset kuten Suomen poliisi ja rajavartiolaitos ovat kiinnostuneet kopterien tuomista hyödyistä [32, 35]. Amatööri- ja ammattilaiskäyttö eroavat toisistaan, koska ammattikäyttäjillä on suuremmat velvollisuudet ja eri asema amatöörikäyttäjiin nähden lain edessä. Ammattikäyttäjät tarvitsevat toiminnan aloittamiseksi muun muassa asiaan kuuluvat vakuutukset ja luvat, jotka eivät ole pakollisia harrastajille. Joissain tapauksissa ammattilentäjältä saatetaan vaatia myös erillistä RPAS-kurssin suorittamista, jolla todetaan lentäjän teoreettinen ja käytännön osaaminen [35].

2.2.1 Amatöörikäyttö

Suosituimpia droneharrastuksia ovat pitkään olleet valo- ja videokuvaus, joihin kuvauskopteri soveltuu todella hyvin. Ilmasta saadaan helposti näyttäviä valokuvia ja päästään kuvaamaan paikkoja ja alueita, joihin muuten olisi hankalaa tai jopa vaarallista mennä. Drone voidaan asettaa seuraamaan tai kiertämään kohdetta ennalta määrätyltä etäisyydeltä. Esimerkiksi kuvan 2.1b laitteesta löytyvät nämä ominaisuudet, joiden lisäksi kopteri osaa itsenäisesti väistää esteitä samalla, kun se seuraa ja kuvaa kohdetta [14]. Videokuvauksen automatisoinnin avulla henkilö pystyy keskittymään kuvattavaan aktiviteettiin, joka voi olla esimerkiksi urheilusuoritus.

Viime aikoina esille on tullut myös kokonaan uusia harrustusmuotoja, joista eräs on FPV-lento (engl. First Person View). Kyseessä on taitolento, jossa lennokkia ohjataan yleensä VR-lasien (engl. Virtual Reality) avulla sisä- tai ulkoradalla. Radalla on erilaisia esteitä ja reittejä, joilla testataan muun muassa lentäjän ohjaustaitoja ja reaktionopeutta [55]. Lentäjä näkee tilanteen vain ja ainoastaan dronen kameran kautta, minkä takia lentäjällä pitää olla mukana tähystäjä, kun lennetään ulkona. Rajoittuneen näkökentän takia lentäjä ei kykene havaitsemaan ylhäältä, alhaalta, takaa tai sivuilta lähestyviä vaaroja. Tähystäjän tehtävä on varoittaa näistä vaara- ja uhkatilanteista. Tämä perustuu yleisiin lentoturvallisuusmääräyksiin, joilla pyritään välttämään ilmaliikenneonnettomuuksia [16].

Dronea voidaan hyödyntää osana muuta harrastustoimintaa, joka voi olla esimerkiksi metsästys. Ilmasta voidaan tarkkailla alueen eläinten liikkumista ja käyttäytymistä. Dronella saatetaan päästä jopa todella lähelle eläimiä, jotka normaalisti pelkäävät ihmistä ja kohtaustilanteessa juoksisivat pakoon. Hirvet ja muut isommat eläimet eivät osaa pelätä dronea, koska ne eivät ole aikaisemmin kohdanneet ilmasta lähestyvää uhkaa. Talvella on mahdollista myös eläinten jälkien seuraaminen, mikä muuten voi olla hankalaa, jos maassa on paljon lunta.

2.2.2 Ammattilaiskäyttö

Dronejen hyödyntämisestä ammatti- ja viranomaiskäytössä on viime aikoina saatu paljon positiivista palautetta. Dronet soveltuvat todella hyvin erilaisiin pelastus- ja etsintätehtävien suorittamiseen. Alueelta saadaan dronen kameran avulla reaaliaikaista tilannekuvaa, jonka perusteella voidaan paikantaa eksyneitä ihmisiä ja ohjata pelastushenkilökunta paikalle. Erityisen hyödyllisiä ovat lennokkeihin kiinnitettävät lisälaitteet, kuten valonheittimet ja lämpökamerat. Näillä välineillä voidaan operoida myös vaativissa olosuhteissa.

Rajavartiolaitos on testannut dronelennokkien soveltumista rajavartioston tehtäviin. Tarkoituksena on uudistaa valvontakalustoa vastaamaan tämän päivän teknologiaa, millä henkilöstö pystyy suorittamaan valvontatehtäviä entistä tehokkaammin. Esimerkiksi lämpökameralla varustettu drone onnistui löytämään kadoksissa olleen vanhuksen. [32]

Suomen poliisi on myös aloittanut omat henkilöstökoulutukset järjestämällä RPAS-kaukoohjaajakursseja, joiden tarkoituksena on opettaa dronen käyttöä. Samalla poliisilaitoksille tehdään laitehankintoja, jotka tehostavat poliisin työtä, minkä seurauksena resursseja vapautuu muiden tehtävien hoitamiseen. Poliisilla on vastaavia kokemuksia dronen hyödyntämisestä kadonneen henkilön etsinnöissä kuin rajavartiolaitoksella. [35]

Ammattikäyttöön soveltuvista droneista tehdään tällä hetkellä paljon erilaisia tutkimuksia ja liiketoimintasuunnitelmia, joissa kartoitetaan laitteiden soveltuvuutta ja käyttömahdollisuuksia [2, 8, 23, 51] Laitteita testataan myös käytännössä ja kehitetään vastaamaan käyttötarkoitusta. Toistaiseksi kaikkia sovelluskohteita ei ole löydetty tai ehditty selvittämään.

2.3 Luvaton käyttö ja uhkatilanteet

Dronen lennättäminen on mukava harrastus, mutta se ei ole sallittua kaikissa paikoissa. Kiellettyihin alueisiin kuuluvat muun muassa valtioiden rajavyöhykkeet, yleisötapahtumat, vankilat sekä lentokentät ja niiden lähialueet. Tarkemmin kieltoalueita on mahdollista tarkastella osoitteessa *droneinfo.fi* tai lataamalla kyseinen sovellus älypuhelimeen. Sivustolla on paljon muita yleisiä turvallisen lennättämisen ohjeita, jotka kannattaa lukea ennen harrastuksen aloittamista. [16]

Henkilö saattaa syyllistyä dronen luvattomaan käyttöön tahallisesti tai tahattomasti. Luvattomalla käytöllä tarkoitetaan tilanteita, joissa dronea käytetään rikoksentekovälineenä. Mahdollisia rikoksia, joihin dronelentäjä voi syyllistyä, ovat muun muassa kotirauhan rikkominen, salakatselu, yritysvakoilu, vaaran aiheuttaminen, salakuljetus ja ilmaliikenteen häirintä. Rangaistukset määrätään rikosseuraamuslain perusteella, mikäli rikoksen tunnusmerkit täyttyvät. [16]

Erilaisia uhkatilanteita voi syntyä ja aiheutua monella eri tavalla. Kaupalliset dronet kykenevät aiheuttamaan vaaraa ja vahinkoa ilman, että teko olisi suunniteltu tai tahallinen. Esimerkiksi holtittoman lentämisen seurauksena kopteri voi törmätä lähellä olevaan ajoneuvoon tai ihmiseen. Vahinkojen suuruudet riippuvat dronen massasta ja lentonopeudesta. Tyypillinen kuvauskopterin massa on noin 1-2 kg ja lentonopeus voi olla kymmeniä metrejä per sekunti [13, 14]. Jos drone törmää ihmiseen, niin henkilövahingot ovat yleensä vakavat. Fyysisen törmäyksen lisäksi pitää huomioida laitteen terävien potkurien pyörimisestä aiheutuva silpoutuminen. Aina ei ole kyse tahallisesta teosta tai huolimattomuudesta, koska vaaratilanne voi aiheutua laitteen toimintahäiriön seurauksena, jolloin lentäjällä on hyvin vähän mahdollisuuksia estää vahingon syntyminen.

Vuonna 2015 luvaton drone putosi katsomoon kesken U.S. Open tennisturnauksen. Kukaan ei loukkaantunut onnettomuudessa, koska törmäyshetkellä kyseinen osa katsomoa oli tyhjillään. Ihmiset luulivat törmäystä ensiksi pommi-iskuksi, minkä takia tapauksesta aiheutui lyhyt keskeytys peliin, yleistä hämmennystä ja pelkoa. [62]

Suurimpien laitevalmistajien droneista löytyy geofence-ominaisuus, joka luo virtuaalisen raja-aidan maantieteellisen kohteen ympärille. Rajatulla tai estetyllä alueella sijaitseva kohde voi olla esimerkiksi voimalaitos, vankila tai lentokenttä. Geofence on osana dronen ohjelmistoa ja se tarvitsee toimiakseen GPS-paikannuksen. Yksinkertainen geofence voidaan toteuttaa myös pelkän korkeusrajoittimen avulla, millä estetään törmäykset esimerkiksi lentokoneiden ja helikopterien kanssa. Kyseessä ei ole kuitenkaan pakollinen ominaisuus, minkä takia sitä ei ole kaikissa kaupallisissa droneissa. Valmistajat, kuten DJI, ovat vapaaehtoisesti lisänneet geofence-ominaisuuden parantaakseen yleistä turvallisuutta. Geofence-tietokanta sisältää paljon tärkeitä kohteita Suomessa ja ulkomailla, mutta kaikkia paikallisia lentokieltoalueita ei sieltä valitettavasti löydy. Tämän takia ominaisuuteen pitää suhtautua varauksella, koska merkityt alueet eivät aina täytä kaikkia turvallisuusmääräyksiä tai pahimmassa tapauksessa alueen maantieteellinen sijainti on virheellisesti merkitty. [12, 14] Luvattomaksi käytöksi lasketaan myös tilanteet, jossa lentäjä tahallaan kytkee geofence-toiminnon pois päältä ja lentää rajoitetulle alueelle.

Dronelennokkia voidaan myös fyysisesti muokata terrorismiin tai rikokseen soveltuvaksi, missä alustana on usein kaupallinen tuote. Kuormana voi räjähteitä tai salakuljetettavaa tavaraa. Dronen kantokyky on rajallinen, mutta se on kuitenkin riittävä siirtämään pieniä käsiaseita tai huumaus- ja räjähdysaineita. Tämän tyyppinen uhka on erittäin vaikea torjua, koska ilmassa korkealla lentävää dronea on hankala pysäyttää ja tekijä voi olla kaukana rikospaikasta. Yleensä rikokset tapahtuvat todella nopeasti, mikä vaikeuttaa tilanteisiin varautumista. [50]

Vuoden 2018 aikana nousi esiin pari uutista ulkomailta, jotka saavuttivat laajaa medianäkyvyyttä. Ensimmäinen uutinen oli Venezuelan presidentti Nicolás Maduroa vastaan kohdistunut droneisku, kun hän oli pitämässä puhetta sotilasseremoniassa. Räjähteillä varustettu drone lensi presidenttiä kohti ja räjähti lähellä, mutta isku epäonnistui. [60] Toinen tapaus sattui Gatwickin lentokentällä pahimman jouluruuhkan aikana. Lentoliikenne oli täysin pysähdyksissä lähes 36 tuntia, koska lentokentän alueella ja sen lähistöllä tehtiin lukuisia dronehavaintoja. Kyseessä oli nähtävästi tahallinen teko, jolla haluttiin aiheuttaa häiriötä ja sekasortoa. [54]

3 HAVAITSEMINEN JA VALVONTA

Dronen havaitseminen on vaikea tehtävä, koska dronet ovat pieniä, lentävät hitaasti ja matalalla. Havaitseminen toteutetaan hyödyntämällä teknisiä valvontamenetelmiä, jotka perustuvat akustiikkaan, optiikkaan, radiotekniikkaan ja tutkaan. Tässä luvussa tutustutaan näihin laajasti käytettyihin ja yleisesti tunnettuihin valvontamenetelmiin sekä niiden keskeisiin toimintaperiaatteisiin, joita hyödyntämällä luvattoman dronen havaitseminen on mahdollista. [50, 53] Jokaisella menetelmällä on omat vahvuudet ja heikkoudet, mutta kaikilla on yksi yhteinen tavoite, joka on dronen havaitseminen mahdollisimman pitkältä etäisyydeltä ja luotettavasti. Näitä valvontamenetelmiä hyödynnetään kaupallisissa dronen torjuntajärjestelmissä, minkä takia toimintaperiaatteiden ymmärtäminen auttaa myös kaupallisten ratkaisujen vertailussa.

Menetelmä	Dronen ominaisuus	Valvontasäde	Vahvuudet	Haasteet
Akustiikka	Potkurien ääni	30-300 m	Yksinkertainen Halpa	Korkea taustamelu Lyhyt valvontasäde
Optiikka	Ulkomuoto ja liike	100-1000 m	Kohteen tunnistus	Pienet kohteet Huono resoluutio Sääolosuhteet
Radio	Langaton yhteys	1000 m	Tunnetut taajuusalueet	Muut radiolaitteet Radioaaltojen heijastuminen Autonomiset dronet
Tutka	Mikro-Doppler	3000 m	Pitkä valvonsäde	Kohteen pieni heijastuspinta Kaupunkiympäristö Matala lentokorkeus

Taulukko 3.1. *Valvontamenetelmät [27, 40, 53]*

Taulukossa 3.1 on esitetty yhteenveto eri valvontamenetelmistä. Dronen ominaisuus kertoo, mihin kyseinen valvontamenetelmän toiminta perustuu. Valvontasäteen, vahvuuksien ja haasteiden avulla on helppo vertailla ja arvioida eri valvontamenetelmiä keskenään. Tässä luvussa eri menetelmät ovat esitetty kasvavan valvontasäteen mukaisessa järjestyksessä. Seuraavissa alaluvuissa tutustutaan jokaiseen valvontamentelmään tarkemmin.

3.1 Akustinen valvonta

Akustinen valvonta perustuu kohteen tuottaman äänisignaalin hyödyntämiseen. Signaalin havainnointi tarvitsee järjestelmän, johon on kytketty jonkinlainen akustinen sensori eli yleensä mikrofoni. Havaittua signaalia käsitellään äänitekniikan algoritmeilla ja tarkastellaan taajuus- ja aikatasossa, minkä avulla voidaan määrittää kohteen akustinen jälki, jonka perusteella eri dronemallit voidaan erotella toisistaan. [20, 53]

Dronen akustinen jälki syntyy, kun lentäessä sähkömoottorit pyörittävät laitteen potkureita. Ihminen kykenee havaitsemaan potkurien pyörimisestä aiheutuvan äänen kuuloaistinsa avulla ja sen perusteella kykenee paikantamaan dronen. Ääni kuulostaa eräänlaiselta surinalta, josta on kuitenkin todella vaikeaa pelkän ihmiskuulon avulla määritellä mitään teknisiä ominaisuuksia tai tehdä muita johtopäätöksiä. Tämä ei ole kuitenkaan ongelma akustiselle valvontajärjestelmälle, joka kykenee analysoimaan ääntä huomattavasti tarkemmin, minkä perusteella dronesta ja sen liikkumisesta saadaan enemmän informaatioita. Laitetietojen lisäksi akustisen valvonnan avulla voidaan arvioida kohteen sijaintia sekä liike- ja saapumissuuntaa, joita hyödynnetään dronen paikantamisessa. [53]

Eri dronetyyppien akustisia jälkiä voidaan tallentaa tietokantoihin, joista voidaan tehdä vertailuhakuja. Tietokannan luomisessa hyödynnetään yleensä koneoppimista, jota hyödyntäen järjestelmälle opetetaan useiden erilaisten dronetyyppien akustisia jälkiä. Havaittua akustista jälkeä verrataan tietokantaan aikaisemmin lisättyihin näytteisiin. Mikäli riittävän hyvä vastaavuus löytyy tietokannasta, niin saadaan selville kyseisen laitteen tyyppi ja tekniset tiedot. Usein pelkkä akustinen jälki ei ole riittävä vahva ominaisuus varmaan tunnistukseen. Tietokantajärjestelmä vaatii myös jatkuvaa päivittämistä ja tietojen aktiivista lisäämistä, kun uusia dronemalleja tulee markkinoille. Yleisimpien dronemallien akustiset jäljet ovat suhteellisen hyvin tiedossa, mutta haasteita aiheuttavat mm. uudet, harvinaiset tai itse rakennetut dronet. [53]

Akustiset valvontajärjestelmät ovat halpoja ja helposti asennettavia, mutta niiden keskeinen ongelma on ylimääräinen taustamelu valvontaympäristössä [53]. Taustamelu voi syntyä usean eri äänilähteen yhteisvaikutuksesta, mikä koostuu esimerkiksi alueen liikenteestä, ihmisistä, koneista ja tapahtumista. Tämän takia yksittäisen kohteen tuottamaa akustista signaalia on hankala havaita ja erotella muista äänilähteistä siten, että signaalia voitaisiin vielä käyttää osana luotettavaa tunnistusta ja paikantamista.

Äänilähde	Äänenvoimakkuus [dB]
Lentokoneen nousu	120-140
Rock-konsertti	110-120
Moottorisaha	100-110
Yleisötapahtuma	90-105
Kaupungin keskusta	80
Drone	70-80
Normaali keskustelu	50-60
Hiljainen maaseutu	20-30

Taulukko 3.2. *Melutasot [7, 25, 36]*

Taulukossa 3.2 on listattu erilaisia äänilähteitä, jotka saattavat aiheuttaa taustamelua akustisen valvontalaitteen ympäristössä. Vertailukohtana on drone, jonka tuottama äänisignaali pitäisi pystyä erottamaan muusta ympäröivästä taustamelusta. Vertailussa pitää huomata äänenvoimakkuudet ovat esitetty desibeleissä, joka on logaritminen asteikko. Taulukon perusteella voidaan todeta, että drone on suhteellisen äänekäs laite, mutta työkoneista ja tapahtumista aiheutuva melu on silti huomattavasti suurempi. Akustinen valvonta toimii parhaiten, kun valvontaympäristö on hiljaista maaseutua vastaava paikka.

Taustamelu vaikuttaa akustisen valvonnan havainnointisäteeseen. Erään tutkimuksen mukaan luotettavia havaintoja saatiin 40–300 m etäisyydeltä, mikä johtuu tutkimuksessa käytetyistä droneista ja ympäristöstä [40, 53]. Esteettömässä ja avoimessa maastossa saavutetaan parhaimmat tulokset, jos drone lentää kasvillisuuden yläpuolella. Valvontajärjestelmän toiminnalle erityisen haastavia ovat ympäristöt, joissa on paljon rakennuksia tai kasvillisuutta. Kohteen ja valvontajärjestelmän väliin jäävät esteet vaimentavat akustisen signaalin voimakkuutta ja aiheuttavat ääniaaltojen heijastumista. [20]

Dronen äänisignaalin vaimentumista voidaan tarkastella teoriassa, jos oletetaan, että ääni etenee vapaassa tilassa ja äänen intensiteetti jakaantuu tasaisesti pallopinnalle. Tarkastellaan tilannetta, jossa kohteena on drone ja sen tuottaman äänisignaalin voimakkuus on 80 dB metrin etäisyydeltä mitattuna. Valvontaympäristö on hiljainen maaseutu, jonka taustamelun voimakkuus on 30 dB. Tarkoituksena on laskea etäisyys, jolla dronen tuottama äänisignaalin voimakkuus on pudonnut taustamelun tasolle. Etäisyys voidaan ratkaista kaavasta

$$L_2 = L_1 + \left| 20 \cdot \log \frac{r_1}{r_2} \right|, \tag{3.1}$$

missä L_2 on uusi äänenvoimakkuus, L_1 on alkuperäinen äänenvoimakkuus, r_1 on alkuperäinen etäisyys ja r_2 on uusi etäisyys. Tästä kaavasta saadaan muodostettua etäisyyden r_2 lauseke, johon tunnetut lukuarvot voidaan sijoittaa:

$$r_2 = r_1 \cdot 10^{\frac{|L_1 - L_2|}{20}} = 1\mathrm{m} \cdot 10^{\frac{|80\mathrm{dB} - 30\mathrm{dB}|}{20}} \approx 316\mathrm{m}$$

Tulokseksi saadaan runsaat 300 metriä, mikä vastaa hyvin edellä esitetyn tutkimuksen maksimietäisyyttä. Todellisuudessa dronen äänisignaalin voimakkuus täytyy olla hieman taustamelua korkeampi, jolloin se voidaan havaita. Lisäksi akustisessa valvonnassa kyetään rajaamaan taajuusaluetta siten, että esimerkiksi matalat taajuudet jäävät kokonaan tarkastelualueen ulkopuolelle.

Akustisen valvonnan tehokkuutta voidaan arvioida tarkastelemalla tilannetta, jossa luvaton drone havaitaan 200 m etäisyydeltä ja sen oletetaan liikkuvan nopeudella 65 km/h [14], mikä on toisaalta noin 18 m/s. Kyseisellä nopeudella 200 m matkaan dronelta kuluu noin 11-12 sekuntia, mikä tarkoittaa, että kohteen torjunnalle ja vastavaikuttamiselle jää hyvin vähän aikaa. Lisäksi torjunta-ajassa pitää ottaa huomioon äänen etenemisnopeus, koska ääni kulkee ilmassa noin 340 m/s. Tässä tilanteessa dronella olisi vielä 0,5 sekunnin etumatka. Edellä mainittujen asioiden takia yksittäisellä akustisella sensorilla toteutetut valvontajärjestelmät eivät ole käytännöllisiä. Parempi ratkaisu olisi muodostaa akustisista sensoreista kehä kohteen ympärille. Näin saadaan luotua huomattavasti suurempi valvonta-alue, minkä seurauksena on enemmän aikaa vastavaikuttamiselle.

3.2 Optinen valvonta

Optinen valvonta perustuu kameralaitteiden hyödyntämiseen, missä niiden dataa joko analysoidaan tietokoneiden kuvankäsittelyalgoritmien avulla tai videokuva välitetään suoraan valvontakeskukseen, jossa ihminen seuraa valvontakameroiden live-kuvaa. Videokameroiden lisäksi valvonnassa on mahdollista hyödyntää muita optisia laitteita, kuten lämpökameroita ja valonvahvistimia. Ideaalisessa tilanteessa valvonta olisi täysin autonomista. Optinen valvonta vaatii aina suoran näköyhteyden kohteeseen. [53]

Videokuvassa oleva kohde tunnistetaan sen ulkomuodon ja rakenteen avulla. Keskeisiä ulkoisia ominaisuuksia, jotka vaikuttavat dronen tunnistukseen, ovat kohteen ääriviivat, värit, valot, linjat, geometriset muodot ja reunat [53]. Tunnistuksen yhteydessä on mahdollista saada tietoa kohteeseen kiinnitetystä hyötykuormasta, minkä perusteella voidaan tehdä kohteen uhka-arvio. Kyseessä voi olla väärälle alueelle eksynyt harrastelijan kuvauskopteri tai räjähteillä varustettu ja terroristista tekoa varten suunniteltu drone. [22]

Droneista vapautuva lämpö voidaan havaita lämpökameran avulla. Helposti lämpeneviä osia droneissa ovat esimerkiksi sähkömoottorit, videokamera ja akut. Pienet dronet eivät kuitenkaan tuota kovinkaan paljon lämpöä, mikä on valvontamenetelmän eräs keskeinen ongelma. Lämpökameralla maastossa olevat ihmiset kyetään havaitsemaan noin 300 m matkalta ja vastaava etäisyys käynnissä oleville ajoneuvoille on noin 600 m [40]. Dronet ovat kuitenkin selvästi pienempiä lämpölähteitä kuin ihmiset, minkä takia dronen havaitseminen lämpökameralla saattaa vaikuttaa huonolta ajatukselta. Toisaalta pitää muistaa,

että dronet lentävät taivaalla. Taivas näkyy lämpökamerassa täysin kylmänä taustana, josta yksittäiset lämpölähteet ovat selkeästi erotettavissa. [28]

Drone havaitaan optisella laitteistolla hyödyntämällä liikepohjaista havainnointimenetelmää, jota käytetään myös kohteen seurantaan. Liikepohjaisessa videon tarkastelussa vertaillaan peräkkäisiä kuvia tarkastemalla niissä liikkuvia objekteja, joiden siirtymien perusteella voidaan tehdä arvioita niiden liikesuunnista ja lentokuvioista. Dronen lentokuvio on tyypillisesti hyvin suoraviivainen ja siinä on suhteellisen vähän satunnaisuutta, jos sitä verrataan esimerkiksi eläinten liikkumiseen. [53]

Optinen valvonta on konenäön ja hahmontunnistuksen eräs osa-alue, minkä takia niillä on samat haasteet ja ongelmat. Ensimmäinen ongelma on kohteen erottaminen ympäröivästä taustasta, koska kuvat saattavat olla epätarkkoja eli niiden resoluutio on huono tai kohde sulautuu taustaansa muotojensa tai värityksensä ansiosta. Epätarkoista ja pienistä kuvista ei voida varmasti tunnistaa kohdetta tai virheellisesti tulkitaan jokin vastaava samankokoinen ja muotoinen objekti droneksi. Tunnistustarkkuus parantuu, jos kuvan lisäksi on saatavilla jotain muuta tunnistukseen liittyvää tietoa. Yhdistämällä hahmontunnistuksen ja tiedot lentoradasta kyetään paremmin erottelemaan esim. dronet linnuista, koska lintujen lentoradat ovat enemmän satunnaisia ja niiden ulkoasut eroavat toisistaan. [53]

Toinen ongelma on ympäristön vaihtuvat sääolot ja vuorokaudenaika, jotka vaikuttavat merkittävästi kohteen tunnistamiseen ja valvontaetäisyyteen. Valonmäärän pienentyessä ja sääolosuhteiden huonontuessa lähes aina havainnointimahdollisuudet heikkenevät. Jos vertaillaan erilaisia sääolosuhteita keskenään, niin on selvää, että parempia havaintoja tehdään selkeä säässä ja hyvässä valaistuksessa kuin sumuisessa ja pimeässä ympäristössä. Asiaan vaikuttaa myös kohteen väritys, koska tummat objektit erottuvat hyvin vaaleaa taustaa vasten ja päinvastoin. Toisaalta pimeässä dronen mahdolliset LED-valot paljastavat sen helposti. Tämä vaatii tunnistusalgoritmeiltä kykyä havaita ja tunnistaa drone useiden erilaisten ominaisuuksien perusteella, mikä puolestaan lisää virheellisen tunnistuksen mahdollisuutta. Edellä mainittujen asioiden takia valvontasäde voi vaihdella välillä 100–1000 m, minkä takia valvontamenetelmän tehokkuus riippuu hyvin paljon ympäristöstä. [38, 53]

Automaattisen valvonnan ongelmia voidaan minimoida, jos valvonta ei ole täysin tietokonetunnistuksen varassa. Käytännössä se tarkoittaa valvontakeskuksen henkilöstöä, joka aktiivisesti seuraa kameroiden lähettämää videokuvaa ja reagoi automaattisen valvonnan lähettämiin ilmoituksiin. Näin virheelliset tunnistukset eivät aiheuta ylimääräisiä torjuntatoimenpiteitä. Kuitenkaan valvontaa ei kannata täysin jättää ihmisten vastuulle, koska ihmisen havainnointikyky on rajallinen. Pienen kohteen havaitseminen on aina haastava tehtävä laajasta ympäristöstä, jolla voidaan tarkoittaa sekä ulkona tapahtuvaa tarkkailua että usean kameran lähettämän videokuvan seuraamista valvontakeskuksessa. Molemmissa tilanteissa ihminen tarvitsee yleensä tietoa dronen sijainnista tai lentosuunnasta, minkä perusteella henkilö osaa rajata etsintäaluetta. [38] Toisaalta ylimääräinen valvontahenkilöstö lisää yrityksen tai laitoksen henkilöstökuluja, minkä takia olisi kustannuste-

hokasta saada koko valvontajärjestelmä täysin autonomiseksi. Usein saattaa olla tarve pelkälle dronevalvonnalle, eikä torjunta ole tilanteesta riippuen aina järkevää tai hyödyllistä.

Taitava lentäjä voi hyödyntää optisen valvonnan heikkouksia ja vaatimusta suorasta näköyhteydestä siten, että drone lähestyy kohdetta hyödyntämällä ympäristön näköesteitä ja kameroiden kuolleita kulmia. Tällaista toimintatapaa käytettiin Gatwickin lentokentän tapauksessa, jossa dronet häiritsivät lentoliikennettä. Lennonjohto ja muut viranomaiset eivät onnistuneet paikantamaan luvattomia droneja, koska lentäjä käytti lentokentän rakennuksia näkösuojana. [54]

3.3 Radiovalvonta

Radiovalvonta perustuu passiiviseen dronelennokin ja RC-lähettimen välisen langattoman tietoliikenteen kuunteluun. Kaupalliset dronet kommunikoivat ohjauslaitteen kanssa käyttäen ennalta määriteltyjä taajuusalueita, mikä perusteella radiovalvonta voidaan kohdistaa niihin. Radiovalvontalaitteen tehtävä on kuunnella määritettyä taajuusaluetta ja etsiä mahdollista radioliikennettä, joka paljastaisi alueella toimivat radiolähettimet. Drone ja sen ohjauslaite ovat molemmat ympärisäteileviä radiolähettimiä ja ne lähettävät dataa keskenään radioaaltojen välityksellä. Radiovalvonnalla pystytään havaitsemaan sekä drone että sen lentäjä. [18, 50]

Radiotaajuuksien kuuntelu on täysin luvallista toimintaa, joten kuka tahansa voi kuunnella ympärillä tapahtuvaa radioliikennettä. Kuuntelu tarvitsee ainoastaan langattoman radiovastaanottimen, minkä takia valvontalaitteiston asentaminen on suhteellisen helppo tehtävä. Useassa tapauksessa tarvitaan vain yksittäinen radiovastaanotin, jos sen sijoittaa riittävän korkealle paikalle, esimerkiksi rakennuksen katolle. Keskeisellä paikalla olevalla radiovalvontalaitteella on suhteellisen pitkä valvontasäde, joka voi olla jopa 1 km [53]. Passiiviseen radiovalvontaan liittyy kuitenkin useita haasteita, jotka voidaan eritellä toisistaan seuraavasti.

- Etäisyys: Signaali heikkenee etäisyyden kasvaessa, minkä takia tarvitaan herkkiä valvontalaitteita, jotka kykevät vahvistamaan signaalia siten, että signaalissa tapahtuvat pienet muutokset on mahdollista havaita. [5, 50]
- Häiriöt: Dronet käyttävät luvasta vapaiden laitteiden RF-aluetta, minkä takia kaistalla on huomattava määrä muuta radioliikennettä, joka vaikeuttaa dronen yksilöintiä. [5]
- Kaupunkiympäristö: Rakennusten ja muiden esteiden vaikutuksesta radiosignaalit heijastuvat, minkä takia radiolähettimen ja valvontalaitteen välille muodostuu useita mahdollisia reittejä. Tämä vaikeuttaa dronen paikantamista. [5, 53]

Dronen tunnistaminen RF-signaalin perusteella on mahdollista, koska dronen ohjaussignaalissa on ainutlaatuisia ominaisuuksia, jotka erottavat sen muista samalla kaistalla lii-

kennöivistä laitteista. Tunnistaminen kuitenkin vaatii, että dronen ohjaussignaali kyetään erottamaan muusta radioliikenteestä. Esimerkiksi 2,4 GHz:n taajuusalueella dronejen lisäksi toimivat WLAN-tukiasemat ja Bluetooth-laitteet. Tämän takia virheellisen tunnistuksen todennäköisyys on suuri, koska kaikki tunnistamattomat RF-lähettimet eivät ole droneja. [53, 59]

Eräs yksinkertainen ratkaisu on skannata laajaa radiotaajuusaluetta (1 MHz–6.8 GHz) ja olettaa, että jokainen tunnistamaton radiolähetin on drone [53]. Jos alueen WLAN-tukiasemat ja muut taajuuskaistan kiinteät laitteet tunnetaan, ne voidaan rajata tarkastelun ulkopuolelle, mikä pienentää virheellisen tunnistuksen todennäköisyyttä. Kuitenkaan kaikki alueella toimivat RF-lähettimet eivät ole droneja, minkä takia menetelmästä aiheutuu paljon virheellisiä tunnistuksia.

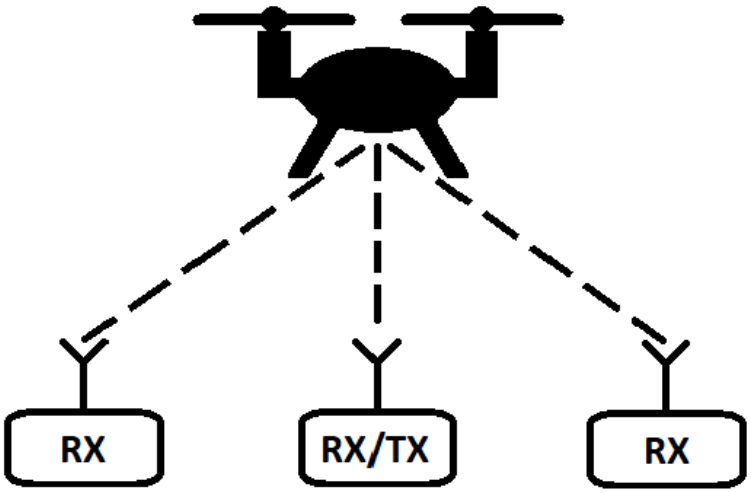
Esimerkiksi WiFi-ohjauksella toimivat dronet voitaisiin tunnistaa sen MAC-osoitteen (Media Access Control) perusteella, mikä kuitenkin vaatii sen, että drone käyttää avointa MAC-osoitetta. Muuten tunnistus ei ole mahdollista. Tämän lisäksi pitäisi olla käytössä tietokanta, jossa on tallennettuna dronejen MAC-osoitteita. Tietokannan vaatii jatkuvaa päivittämistä, kun uusia dronetyyppejä tulee markkinoille. Havaitseminen voidaan myös välttää väärennetyn MAC-osoitteen avulla, mikä on suhteellisen helppo toteuttaa. [40, 53]

Ehkä paras ja tehokkain menetelmä dronen tunnistukseen on RF-spektrin analysointi, koska dronen ja ohjaimen välinen kommunikointi on säännöllistä, minkä perusteella spektrogrammista voidaan erottaa dronelle ominaiset piirteet. Nämä spektrogramissa havaittavat ominaisuudet, kuten tiedonsiirtokanavien lukumäärä, leveys ja taajuus sekä kanavan vaihtumisaika, muodostavat yhdessä dronen RF-jäljen. Dronen paikannus perustuu vastaanotettuun signaalin voimakkuuteen (engl. RSS, Receiced Signal Strength) ja sen tulosuunnan arviointiin. Dronen RF-jälki on edelleen tunnistettavissa, vaikka moottorit sammutetaan ja kamera otetaan pois käytöstä. Ainut vaatimus RF-jäljen havaitsemiselle on se, että dronen ja ohjaimen välinen yhteys on muodostettu. Näin drone voidaan tunnistaa RF-signaalin perusteella jopa kaupunkiympäristössä. [40, 53]

Passiivinen radiovalvonta ei kykene havaitsemaan dronea, joka lentää täysin autonomisesti GPS- tai videopaikannuksen avulla [40]. Toinen mahdollisuus on se, että drone kommunikoi sellaisella taajuusalueella, jota radiovalvonta ei kuuntele [53]. Esimerkiksi dronea on mahdollista ohjata matkapuhelinverkon kautta [37]. Molemmissa tilanteissa dronen RF-jälkeä ei synny olleenkaan, koska drone ei lähetä tai vastaanota radiosignaaleita [40]. Tämän takia pelkästään radiokuunteluun pohjautuvat valvontajärjestelmät eivät ole käytännöllisiä. Yleisin ratkaisu tähän ongelmaan on muodostaa järjestelmiä, jotka koostuvat kahdesta tai kolmesta eri valvontamenetelmästä.

3.4 Tutkavalvonta

Tutkavalvontajärjestelmä koostuu yleensä yhdestä radiolähettimestä ja muutamasta radiovastaanottimesta. Tutkavalvonta on aktiivista radiovalvontaa, jossa radiolähetin lähet-



Kuva 3.1. *Yksinkertainen tutka*

tää jatkuvasti radioaaltoja ympäristöönsä ja vastaanottimet odottavat, että lähetetyt radioaallot heijastuvat jostain pinnasta. Jos heijastuminen tapahtuu, niin valvontalaite kykenee havaitsemaan kohteen saapuvien radioaaltojen perusteella. [27, 40, 53]

Kuvassa 3.1 on esitetty yksinkertaisen tutkan toimintaperiaate. Keskellä on yksikkö, joka kykenee sekä lähettämään että vastaanottamaan radioaaltoja. Tavalliset radiovastaanottimet ovat sijoitettu sen vasemmalle ja oikealle puolelle tietyn etäisyyden päähän toisistaan. Heijastuneet radioaallot saapuvat vastaanottimiin hieman eri aikoihin, minkä perusteella määritetään dronen sijainti ja valvontayksikön suhteen. Doppler-ilmiötä hyödyntäen selvitetään dronen lentosuunta ja -nopeus [24, 27].

Dronen havaitseminen perinteisellä tutkalla ei ole käytännössä mahdollista, koska ne ovat suunniteltu suurien kohteiden, kuten lentokoneiden ja ilma-alusten havaitsemiseen. Lentokoneet lentävät korkealla, nopeasti ja niiden fyysinen pinta-ala on suuri, mistä lähetetty radiosignaali voi heijastua. Dronen tapauksessa mikään edellä mainituista ominaisuuksista ei täyty, minkä vuoksi tilanne on täysin päinvastainen. Tämän takia kyseistä ongelmaa varten tarvitaan erilainen lähestymistapa. [53]

Jos tarkastellaan dronesta syntyvää mikro-Doppler-jälkeä, niin havaitseminen on mahdollista. Jälki on aina erilainen riippuen kohteesta, josta se heijastuu takaisin. Dronen tapauksessa mikro-Doppler-jälki syntyy, kun radiosignaali heijastuu laitteen rungosta tai pyörivistä potkureista. Rungosta heijastunut signaalin ei yksin riitä dronen tunnistamiseen, koska vastaava signaalin heijastuminen voi syntyä lähes mistä tahansa kiinteästä pinnasta. Jos rungosta heijastunutta radiosignaalia analysoidaan tarkemmin, niin siitä on mahdollista havaita dronen rungolle ominainen värinä, joka syntyy, kun laite lentää ilmassa. Potkureista heijastunut signaali on yleensä paljon helpommin tunnistettavissa, koska se eroaa suhteellisen selkeästi esimerkiksi kiinteästä pinnasta tapahtuneesta heijastuksesta. [24, 27, 53]

Analysoimalla mikro-Doppler-jälkeä dronet kyetään erottamaan esimerkiksi linnuista suhteellisen helposti, koska jäljet syntyvät eri tavoin. Linnulla mikro-Doppler-jälki muodostuu

siipien liikkeestä, joka on jaksollista ja tapahtuu pystysuunnassa. Dronen potkurien pyöriminen on huomattavasti nopeampaa verrattuna lintujen siipien liikkeeseen, minkä takia näiden kahden välille syntyy erilaiset mikro-Doppler-jäljet. Lisäksi on mahdollista erottaa eri tyyppiset dronet toisistaan, koska ne ovat rakenteeltaan erilaisia. Rakenteellisia eroja ovat esimerkiksi potkurien lukumäärä, niiden pyörimisnopeus ja dronen ulkomuoto. [27, 40]

Tutkavalvonnan suurinvalvontaetäisyys saattaa olla jopa 3 km, mikä on huomattavasti pitempi verrattuna tässä luvussa aikaisemmin esitettyihin menetelmiin. Mikro-Doppler-menetelmään liittyy kuitenkin haasteita. Esimerkiksi dronen potkurien lavat saattavat olla pieniä ja ohuita, minkä takia niiden heijastuspinta-ala on myös hyvin pieni. Tämän takia pienestä pienestä pinnasta tapahtunut heijastus saattaa helposti sekoittua kohteen taustan ja ympäristön aiheuttamiin heijastuksiin. Dronen erinomainen liikkuvuus aiheuttaa ongelmia, koska se voi leijua paikallaan tai saattaa nopeasti muuttaa liikesuuntaansa. Ilmassa leijuvaa dronea voi olla haastavaa erottaa ympäristön muista kiinteistä objekteista. Nopeiden liikesuuntien muutosten takia dronen lentoreitistä tai -suunnasta ei voi tehdä oletuksia, minkä takia kohteen seuraaminen on haastavaa. [40, 53]

Tutka on aktiivinen sensori, joka toimii yötä päivää ja tuottaa elektromagneettista energiaa. Sääolosuhteet tai vuorokauden aika eivät vaikuta tutkan toimintaan merkittävästi, mutta sillä on kuitenkin eräs merkittävä heikkous. Tutka ei kykene havaitsemaan dronen mikro-Doppler-jälkeä kiinteiden esteiden takaa. Tämän takia tehokkaan tutkan sijoittamista kaupunkiympäristöön pitää harkita. Lisäksi asentamiseen tarvitaan aina erillinen lupa, koska tutkasta aiheutuu ylimääräistä häiriötä ympäristöön. [53]

4 TORJUNTAMENETELMÄT

Luvattomien dronejen torjunnassa yleensä ei ole tarpeellista käyttää sellaisia menetelmiä, jotka aiheuttaisivat dronen rikkoutumisen tai tuhoutumisen. Kohteen pysäyttäminen useimmissa tilanteissa on riittävä vastatoimenpide. [17] On kuitenkin täysin mahdollista, että torjunnan seurauksena drone päätyy tilaan, jossa sen moottorit sammuvat, ja se putoaa maahan. Luvattomalla alueella liikkuva drone halutaan saada turvallisesti ja hallitusti maahan, minkä jälkeen jatkotutkimuksilla ja rikosteknisillä menetelmillä pyritään selvittämään asioita, jotka saattavat johtaa esimerkiksi lentäjän henkilöllisyyden paljastumiseen. Tuhoutuneelle laitteelle on hankala suorittaa tutkimuksia, jos sen osat ovat levinneet ympäristöön. [50] Joskus voi kuitenkin esiintyä tilanteita, joissa on pakko käyttää dronen tuhoavia menetelmiä. Esimerkiksi terrori-iskut ja sotilaalliset hyökkäykset ovat riskitasoltaan erittäin vaarallisia, ja siten ihmisten ja kohteiden suojaaminen menee kaiken muun edelle. Torjuntalaitteet saattavat kuitenkin epäonnistua torjuntatehtävässä, minkä takia tarvitaan vaihtoehtoisia menetelmiä, joilla alue turvataan dronehyökkäyksiltä.

Suomen viranomaisilla on laillinen oikeus puuttua luvattomaan dronetoimintaan. Asiaa koskeva lakimuutos tuli voimaan 18.3.2019, minkä perusteella poliisi saa käyttää teknisiä menetelmiä ja muita voimakeinoja luvattoman dronen pysäyttämiseksi ja sen käytön estämiseksi. Poliisilain luvussa 2 kerrotaan lennokin tai miehittämättömän ilma-aluksen kulkuun puuttumisesta seuraavasti: *"Poliisimiehellä on oikeus ottaa ilmailulain 2 §:n 1 momentin 21 kohdassa tarkoitettu lennokki ja 22 kohdassa tarkoitettu miehittämätön ilmaalus tilapäisesti haltuun, estää sen käyttö tai muutoin puuttua sen kulkuun, jos se on välttämätöntä yleisen järjestyksen ja turvallisuuden ylläpitämiseksi, rikosten ennalta estämiseksi tai jo aloitetun rikoksen keskeyttämiseksi, erityisten valvontakohteiden vartioimiseksi, poliisitehtävän tai merkittävän valtiollisen tapahtuman turvaamiseksi taikka onnettomuuspaikalla suoritettavien toimenpiteiden tai toimenpiteen kohteena olevan henkilön yksityisyyden suojaamiseksi. [44]"* Dronea vastaan käytettävät menetelmät täytyvät olla perusteltuja samalla tavalla kuin muut poliisien käyttämät voimakeinot. Puolustusvoimilla on vastaava oikeus puuttua kasarmialueilla tai harjoitusympäristöissä lentäviin luvattomiin droneihin. [33]

4.1 Radiohäirintä

Radiohäirintä on yleisin torjuntamenetelmä, jolla dronen eteneminen estetään ja pysäytetään [20, 38]. Häirintä kohdistetaan droneen, joka toimii radiovastaanottimena. Tarkoi-

tuksena on häiritä dronen ja radio-ohjaimen välistä digitaalista tietoliikennettä siten, että ohjaimen lähettämiin komentoihin ja radioprotokollatietoihin syntyy virheitä. Häiriösignaalin vaikutuksesta drone ei kykene tulkitsemaan radio-ohjaimen lähettämää signaalia, koska tiedonsiirtovirheiden takia käskyt muuttavat merkitystään tai virheellisyys huomataan. Häiriösignaalin tarkoitus ei ole lähettää dataa, vaan se on täysin satunnaista, mikä näkyy radiospektrissä usein lisääntyneenä kohinana. [20, 50, 53]

Data siirtyy lähettimen ja vastaanottimen välillä paketteina. Jokainen lähetetty paketti sisältää tietyn määrän dataa ja yleensä tarkistussumman. Vastaanotin laskee vastaanotetun datan perusteella uuden tarkistussumman ja vertaa sitä lähettimen tarkistussummaan. Jos nämä summat täsmäävät, saapuva datapaketti hyväksytään. Tämä on yleinen menetelmä tietoliikennetekniikassa, millä varmistetaan, että lähetetty paketti on onnistuneesti siirtynyt vastaanottimelle. Mikäli tarkistussummat eroavat toisistaan, saapuva paketti hylätään, koska tarkistuksen perusteella datan vastaanottamisessa on tapahtunut virhe. [30, 50] Pysäyttävä vaikutus syntyy, kun drone hylkää kaikki saapuvat paketit, minkä seurauksena lentäjä menettää laitteen ohjattavuuden. Häirinnän tehokkuus, joka kohdistuu droneen, riippuu seuraavista tekijöistä:

- Häirintäteho: Häirintälaitteen lähetystehon nostaminen aiheuttaa intensiteetin ja häiriöalueen kasvamisen. [34, 50]
- Etäisyys: Jos häirintälaitteen ja häirittävän kohteen välinen etäisyys kaksinkertaistuu, niin häirintäteho pitää nelinkertaistaa, mikäli häirinnän intensiteetti pidetään vakiona. [34]
- Radiotaajuusalue: Radiohäirinnän täytyy kohdistua dronen käyttämään taajuusalueeseen, muuten häirinnällä ei ole mitään vaikutusta dronen ohjaukseen. [34, 53]

Edellä mainittujen asioiden lisäksi oikean häirintätekniikan valitseminen on tärkeää, jos häirintäteho halutaan mahdollisimman tarkasti kohdistaa tiettyyn kohteeseen. Usein on tarve soveltaa erilaisia häirintätekniikoita riippuen siitä, mitä tietoja saadaan torjuttavasta kohteesta valvontamenetelmien avulla. Alapuolella on listattu erilaisia häirintätekniikoita ja selitetty lyhyesti niiden keskeiset toimintaperiaatteet sekä joitain sovelluskohteita. [22, 34]

- Laajakaistahäirintä: Häirintäteho jakaantuu tasaisesti koko taajuuskaistalle. Kyseessä on yksinkertainen häirintämenetelmä, joka soveltuu tilanteisiin, jossa tarkoituksena on häiritä useita radiolaitteita. [34]
- Kanavahäirintä: Häirintäteho kohdistetaan yksittäiselle kapealle taajuuskanavalle. Menetelmä on käytännössä hyvin heikko, koska suurin osa radiolaitteista käyttää tiedonsiirrossa useampaa eri radiokanavaa. Yksittäisen kanavan häirintä ei ole riittävä estämään radioliikennettä, minkä takia menetelmä usein laajennetaan monikanavahäirinnäksi. [34]
- Monikanavahäirintä: Häirintäteho jaetaan useammalle eri radiokanavalle. Toimii tilanteissa, joissa tunnetaan kaikki häirittävän kohteen käyttämät taajuuskanavat. [34]

- Pyyhkäisyhäirintä: Kapeakaistaisella häirintäsignaalilla pyyhkäistään koko taajuuskaistan yli. Pyyhkäisynopeutta muuttamalla voidaan häirintä kohdistaa tiettyyn laitetyyppiin. Pyyhkäisyhäirinnällä kyetään vaikuttamaan useisiin kohteisiin samanaikaisesti. Käytetään esimerkiksi kaupallisissa häirintälaitteissa [34, 47].
- Älykäs häirintä: Häirintämenetelmä on ohjelmistopohjainen, minkä ansiosta häirintä voidaan kohdistaa esimerkiksi yksittäiseen laitteeseen, mikäli sen tiedonsiirtomenetelmä tunnetaan. Ohjelmiston avulla on helppo dynaamisesti vaihtaa häirintätekniikkaa tilanteen muuttuessa. Käytetään kaupallisissa autonomisissa dronetorjuntajärjestelmissä. [6, 34, 43]

Laajakaista- ja monikanavahäirinnässä suurin osa häirintätehosta kohdistuu aika- ja taajuustasossa sellaisiin alueisiin, joissa sillä hetkellä ei tapahdu radioliikennettä [34]. Tämän takia pyyhkäisyhäirintä ja älykkäät häirintämenetelmät ovat luvattomia dronejen torjunnassa huomattavasti tehokkaampia, jos häirintäteho on vakio riippumatta häirintätekniikasta. Älykästä häirintää hyödyntäen voidaan myös minimoida ulkopuolisiin laitteisiin kohdistuvaa häirintää [43].

Älykkäässä häirinnässä on mahdollista käyttää apuna full-duplex-tekniikkaa, jonka ansiosta yksittäinen laite kykenee sekä valvomaan dronen radioliikennettä että häiritsemään sitä samanaikaisesti. Valvonta ja häirintä tapahtuu samalla taajuuskaistalla, minkä takia full-duplex-laite häiritsee myös itse itseään. Itseinterferenssin on vaikutus pitää poistaa vastaanotetusta signaalista. [48] Tällä tavoin esimerkiksi autonominen torjuntalaite kykenee seuraamaan taajuushyppelyä käyttävää dronen ohjaussignaalia, jolloin myös suurin osa häirintätehosta kohdistuu juuri tämän dronen ohjaussignaalin. Ajoituksella on suuri merkitys torjunnan onnistumisessa, koska dronen ja ohjauslaitteen käyttämä radiokanava on saattanut vaihtua, jos häirintälaite ei reagoi riittävän nopeasti muutoksiin. [34, 45]

Drone reagoi häirintään samalla tavalla kuin tilanteissa, joissa radioyhteys ohjauslaitteeseen katkeaa. Tyypillisesti drone jää odottamaan yhteyden uudelleen muodostumista ja pyrkii säilyttämään lentokorkeutensa ja sijaintinsa. Dronen lennättämistä on mahdollista jatkaa, mikäli häirintä loppuu tai lentäjä siirtyy lähemmäksi laitetta, jolloin ohjaussignaali vahvistuu. Häirintä ei suoraan aiheuta dronen putomista maahan, vaan drone saattaa itsenäisesti suorittaa hätälaskeutumisen tai palata lähtöpaikkaan GPS-paikannuksen perusteella. Joissain vaiheessa dronen akut kuitenkin tyhjenevät, minkä jälkeen se vajoaa lopulta maahan.

Ohjaussignaalin häiritsemisen lisäksi on perusteltua häiritä myös GPS-signaalia, koska dronet saattavat kyetä radiohäirinnästä huolimatta navigoimaan vielä GPS-koordinaattien avulla. Näin voidaan ainakin osittain torjua automisesti lentäviä droneja, jotka eivät kommunikoi erillisen ohjauslaitteen kanssa. GPS-signaalinhäirintä on suhteellisen helppoa. Esimerkiksi eräässä tutkimuksessa testattiin kaupallisen GPS-häirintälaitteen toimintaa dronen GPS-signaalin häirinnässä. Tutkimuksen tulosten mukaan häirintälaitteen GPS-signaalin häirintäsäde oli n. 200 m, vaikka kyseessä oli hyvin yksinkertainen häirintälaite. Häirintäalueen sisällä dronen diagnostiikka ilmoitti toistuvasti katkenneesta GPS-yhteydestä. [20] GPS-häirintä vaikuttaa aina kaikkiin satelliittipaikannusta käyttäviin lait-

teisiin, minkä takia alueella toimivat omat laitteet menettävät samalla GPS-yhteyden [50].

Droneen kohdistuvaa tahallista häirintää on hankala havaita tai osoittaa todeksi, koska tapahtuneestä häirinnästä ei jää fyysisiä todisteita, eivätkä kaupalliset dronelennokit osaa suoraan ilmoittaa häirinnästä. Lentäjä saattaa saada ilmoituksia, että yhteyssignaali on heikko tai katkennut. Käytännössä häirinnän saattaa huomata myös, jos drone reagoi hitaasti ohjaukseen tai sen lähettämässä kuvasignaalissa ilmenee häiriötä, eikä dronen ja lentäjän välillä sijaitse merkittäviä esteitä tai rajoitteita, jotka saattaisivat selkeästi estää tai vaimentaa signaalia. Joskus edellä kuvatut häiriöt voivat johtua muista tuntemattomista tekijöistä, minkä takia kyseessä ei ole aina aktiivinen radiohäirintä. Esimerkiksi runsas radioliikenne samalla kaistalla tai laitteen omat toimintahäiriöt saattavat vaikuttaa asiaan.

Kaupallisesti on saatavilla ympärisäteileviä taskukokoisia häirintälaitteita, joita myös tavalliset kuluttajat kykenevät tilaamaan ulkomailta, mutta niiden käyttö ja tuonti EU:n alueelle on laitonta. Näiden laitteiden tuottama häirintäteho on kuitenkin olemattoman pieni, minkä takia niiden tehokas häirintäsäde on vain muutaman metrin pituinen. Taskuhäirintälaitteet kykenevät häiritsemään dronen ohjaussignaalia vain lähietäisyydeltä tai sisätiloissa, mutta muuten ne soveltuvat huonosti luvattoman dronen torjuntaan. [20, 38]

Radiohäirinnän suurin ongelma ovat täysin autonomisesti lentävät dronet, jotka hyödyntävät navigoinnissa jotain muuta kuin radio- tai GPS-signaalia. Tämän tyyppisiä droneja vastaan radiohäirintä on hyödytöntä, koska ei ole radioliikennettä, johon radiohäirinnän avulla voitaisiin vaikuttaa [50]. Näin ollen joudutaan turvautumaan muihin torjuntamenetelmiin, joihin tutustutaan tarkemmin luvussa 4.3. Toistaiseksi kaupalliset dronet eivät vielä käytä yleisesti esimerkiksi kuva- tai videopaikannusta, mutta asiasta liittyen on tehty tieteellistä tutkimusta, jolla on osoitettu visuaalinen paikannus täysin mahdolliseksi [56].

4.2 Dronen hakkerointi

Dronen hakkeroinnilla tarkoitetaan tilannetta, jossa poliisi tai jokin muu viranomainen ottaa luvattoman dronen ohjauksen hetkellisesti haltuunsa siten, että alkuperäinen lentäjä menettää dronen ohjattavuuden. Näin on mahdollista estää dronen luvaton lennättäminen ja samalla drone kyetään turvallisesti siirtämään paikkaan, jossa se aiheuttaisi mahdollisimman vähän vaaratilanteita. Tapahtuman jälkeen drone voidaan tarvittaessa palauttaa omistajalleen, jos kyseessä on ollut vahinko, eikä lentäjää ole syytä epäillä rikoksesta. Muussa tapauksessa kaapattuun droneen kohdistetaan esimerkiksi rikostutkinta. Dronen hakkerointi vastaa monelta osin tavallista radiohäirintää. Keskeisin ero näiden kahden torjuntamenetelmän välillä on se, että hakkeroinnissa ei lähetä häiritsevää signaalia, vaan sen tarkoitus on väärentää dronen ohjaussignaali. [30, 53]

Väärennetyn ohjaussignaalin avulla pyritään vaikuttamaan dronen ohjaukseen siten, että drone pääasiassa tottelee kaappaajan lähettämää signaalia. Kaappaaja voi käyttää esimerkiksi normaalia suurempaa lähetystehoa väärennetyssä ohjaussignaalissa, minkä takia drone havaitsee kyseisen signaalin huomattavasti helpommin kuin alkuperäisen

ohjaussignaalin. Kaappauksen onnistumiseen vaikuttaa useampi eri tekijä, minkä takia dronen kaappaaminen ei ole missään nimessä yksinkertainen tehtävä, vaikka se on teoriassa täysin mahdollista. [30]

Toistaiseksi dronen ohjauksessa käytetään useita erilaisia menetelmiä ja tiedonsiirtoprotokollia, minkä vuoksi luvattoman dronen kaappaamiseen tällä hetkellä ei ole olemassa yksittäistä ratkaisua. Tämän takia on tärkeää, että luvaton drone tunnistetaan valvontamenetelmien avulla, koska esimerkiksi mallin perusteella on mahdollista selvittää dronen ohjaukseen liittyviä teknisiä tietoja, joita sitten hyödynnetään laitteen ohjauksen kaappaamisessa. Väärennetyn ohjaussignaalin täytyy täsmälleen vastata alkuperäisen signaalin jokaista ominaisuutta. [30, 40]

Tarkastellaan esimerkiksi tilannetta, jossa kaapattavan dronen ohjaus perustuu taajuushyppelyyn. Ensimmäiseksi pitää selvittää taajuushyppelyn oleelliset ominaisuudet, kuten kanavat, modulaatio, lähetysaika kanavalla, ajoitukset ja hyppelyjärjestys. [50] Näiden tietojen perusteella häirintäsignaali on mahdollista kohdistaa kaappaus yksittäiseen laitteeseen. Toiseksi väärennetyn signaalin pitää sisältää oikean määrän merkkejä ja symboleja siten, että ne muodostavat oikeita ohjauskomentoja. Edellä esitettyjen asioiden perusteella huomataan, että dronen hakkeroinnin onnistuminen riippuu useasta eri tekijästä, minkä takia pienikin virhe voi johtaa kaappauksen epäonnistumiseen. Jos otetaan vielä huomioon alkuperäisessä ohjaussignaalissa mahdollisesti käytettävä satunnaisuus ja salaus, dronen hakkerointi kaikissa tapauksissa ei ole mahdollista [45].

Tutkimuksissa on kuitenkin osoitettu, että dronen hakkerointi on tietyissä tilanteissa täysin mahdollista. Eräs tutkimuksissa käytetty drone on Parrot AR.Drone 2.0 nelikopteri, joka toimii WiFi-ohjauksella. Laite kuuluu halvimpaan dronekategoriaan, minkä lisäksi sitä on mainostettu lapsille soveltuvana leluna. Kyseiseen droneen voidaan kohdistaa erilaisia hakkerointimenetelmiä, jotka hyväksikäyttävät laitteen haavoittuvuuksia. Laite on erityisin helppo kaapata, koska se käyttää salaamatonta tietoliikennettä. [30] Kaappaaja kykenee syöttämään omia komentoja dronen ohjaukseen, vaikka alkuperäinen lentäjä ohjaisi laitetta samaan aikaan. Kaappaaja voi esimerkiksi pakottaa dronen laskeutumaan syöttämällä toistuvasti laskeutumiskomentoja dronen ohjausjärjestelmään. Näin ohjauksen suhteen syntyy kilpailutilanne lentäjän ja kaappaajan välille. Jos oletetaan, että lentäjä haluaa nostaa dronen lentokorkeutta ja kaappaaja yrittää saada dronen laskeutumaan. Mikäli kaappaaja kykenee lähettämään enemmän laskeutumiskomentoja kuin lentäjä nousukomentoja, niin drone lopulta laskeutuu. Laskeutumisnopeus riippuu komentoja lukumäärän suhteesta tietyllä aikavälillä. Esimerkiksi tilanteessa, jossa suhde on tasan 50%, drone pysyisi keskimäärin paikallaan ilmassa. Usein kaappaajalla on selvä etulyöntiasema lentäjään nähden, koska dronen ohjaus ei yleensä käytä maksimitiedonsiirtonopeutta. Näin kaappaaja kykenee lähettämään dronen ohjausjärjestelmään huomattavasti enemmän laskeutumiskomentoja, minkä takia drone tottelee suurimman osan ajasta kaappaajaa. [30]

Teoriassa dronen hakkerointi vaikuttaa erittäin hyvältä ja turvalliselta torjuntamenetelmältä, mutta käytännössä on vaikeaa rakentaa sellainen laite, joka toimisi luotettavasti riippu-

matta dronetyypistä. Mikäli kyseinen tilanne haluttaisiin kuitenkin saavuttaa, niin dronelennokkien ohjaus pitäisi yhtenäistää niin, että kaikki dronet olisivat ohjattavissa esimerkiksi GSM-verkon kautta [37]. Näin ollen dronelentäjät joutuisivat ostamaan SIM-kortin, joka on erikseen rekisteröity droneja varten. Tämän tyyppiseen järjestelmään on mahdollista rakentaa ns. takaportti, jota hyödyntämällä viranomaiset voivat tarvittaessa ottaa luvattomasti lentävät dronet haltuunsa.

4.3 Muita torjuntamenetelmiä

Tutkimustarkoituksessa on suunniteltu torjuntadrone, jota on tarkoitus hyödyntää valvonnassa ja torjunnassa apuvälineenä. Käytännössä se on pienikokoinen dronetorjuntajärjestelmää, jonka merkittävät edut ovat nopeus ja liikkuvuus. Torjuntadrone voidaan rakentaa käyttämällä alustana kaupallista ammattikäyttöön suunniteltua dronea, jonka hyötykuormaksi kiinnitetään erilaisia valvonta- ja häirintälaitteita. Torjuntadronen tärkein tehtävä on valvoa alueella tapahtuvaa dronetoimintaa ja tarvittaessa puuttua luvattomaan toimintaa. Valvontalaitteiden tehtävä on luotettavasti tunnistaa muut dronet, mikä on torjuntadronen toimintavaatimus. Valvontadataa lähetetään maassa sijaitsevaan ohjausasemaan, jossa suoritetaan laskentatehoa vaativa datan prosessointi. Näin torjuntadroneen kiinnitettävien laitteiden määrää on mahdollista vähentää, mikä pienentää kokonaistehonkulutusta ja kasvattaa lentoaikaa. Lisäksi luvattomien dronejen toiminnasta saadaan parempaa tilannetietoa, koska torjuntadrone kykenee esimerkiksi seuraamaan kohdetta vaativassa ympäristössä. Häirintälaitteissa puolestaan voidaan käyttää pienempiä häirintätehoja, koska torjuntadrone pääsee huomattavasti lähemmäksi kohdettaan kuin muut torjuntajärjestelmät. Torjuntadrone saattaa kuitenkin häiritä itse itseään, minkä takia sen on kyettävä toimimaan tarvittaessa autonomisesti. [31]

Autonomisesti lentäviä droneja vastaan radiohäirintä ja hakkerointi ovat täysin hyödyttömiä, minkä takia on tarpeellista tarkastella myös muita mahdollisia torjuntamenetelmiä. Seuraavaksi tutustutaan kahteen vaihtoehtoon, jotka ovat ohjaussensoreiden häirintä ja dronen vahingoittaminen laserin avulla [38]. Autonomiset dronet saavat tietoa ympäristöstään aina jonkin sensorin kautta, minkä perusteella dronen eteneminen on mahdollista pysäyttää häiritsemällä näitä sensoreita. Tällä hetkellä autonomisissa droneissa käytetään kuva- ja videopaikannuksen lisäksi ultraäänipaikannusta [42], mutta niihin vaikuttavia torjuntamenetelmiä ei ehditty tutkia. Teoriassa kaikkiin sensoreihin ja ohjauspiiriin voidaan kohdistaa elektromagneettista häirintää [38].

EMP-generaattori (engl. Electromagnetic Pulse) tuottaa nopeita elektromagneettisia pulsseja, jotka sisältävät huomattavan määrän elektromagneettista energiaa ja aiheuttavat häiriötä elektronisille laitteille [26], minkä takia sitä on mahdollista hyödyntää autonomisten dronejen torjunnassa. Tarkoituksena on elektromagneettisten pulssien avulla aiheuttaa toimintahäiriötä dronen ohjausjärjestelmään ja sensoreihin niin, että drone pysähtyy tai putoaa taivaalta. Menetelmä on tehokas, koska se toimii kaikkia dronetyyppejä vastaan ja yksittäisellä EMP-generaattorilla kyetään vaikuttamaan kaikkiin alueella lentäviin

luvattomiin droneihin samanaikaisesti. Ongelmana on kuitenkin se, että sitä ei voida kohdistaa pelkästään droneihin, vaan se vaikuttaa kaikkiin sähkölaitteisiin samalla tavalla. Esimerkiksi torjunnasta aiheutuu ylimääräistä vahinkoa matkapuhelimille ja kannettavilla tietokoneille. Tämän takia EMP-generaattori ei sovellu siviiliviranomaisten käyttöön, mutta armeija saattaa käyttää sitä terrorismintorjunnassa tai sotatilanteissa. [20]

Toinen esitetty ratkaisu autonomisten dronejen torjuntaan on laser. Sotilaskäytössä laseria on testattu esimerkiksi kranaatinheittimien ja ilma-alusten torjunnassa, mutta kyseistä menetelmää on mahdollista soveltaa myös dronetorjuntaan. Tarkoituksena on kohdistaa suuri tehoinen lasersäde (engl. HEL, High Energy Laser) luvattomasti lentävään droneen. Laserin tuottama lämpö sulattaa dronen muoviosat ja kärventää ohjauspiirin, mikä johtaa lopulta koko laitteen tuhoutumiseen. Torjuntalaserin teho on yleensä useita kilowatteja. Lasertorjuntayksikkö kykenee vaikuttamaan vain yhteen kohteeseen kerrallaan, mutta suuren tehon ansiosta tarvittava vaikutusaika on lyhyt. [46] Dronelennokkien kohdalla jo pienikin potkureihin aiheutettu vaurio saattaa olla riittävä torjunnan kannalta. Laser olisi mahdollista integroida osaksi dronetorjuntajärjestelmää, missä laserosoitinta ohjataan valvontalaitteilta saatavan informaation perusteella. [38] Esimerkiksi Anti-Drone on ilmoittanut, että sen tuotevalikoimasta löytyy dronetorjuntaan soveltuva laserjärjestelmä [4].

5 KAUPALLISET RATKAISUT

Dronelennokkien käytön lisääntyminen on luonut tarpeen valvonta- ja torjuntalaitteiden kehitykselle. Markkinoille on tullut paljon yrityksiä, jotka ovat keskittyneet erityisesti luvattomien dronejen torjuntaan. Kaupallisesti on saatavilla hyvin laaja valikoima erilaisiin tehtäviin soveltuvia valvonta- ja torjuntalaitteita. [9] Tässä luvussa on tarkoitus käsitellä vain kaupallisia tuotteita, jotka soveltuvat siviiliviranomaisten käyttöön, minkä takia tarkastelun ulkopuolella rajataan esimerkiksi sotilastukikohtien suojaamista varten suunnitellut raskaalla aseistuksella varustetut torjuntajärjestelmät.

Yksityishenkilöillä ei ole oikeutta hankkia häirintälaitteita, koska niiden hallussapito ja käyttö on kiellettyä. Tämän takia häirintälaitteita valmistavat yritykset tekevät yhteistyötä vain tiettyjen yritysten, viranomaisten tai armeijan kanssa. Mikä tahansa yritys ei voi kuitenkaan hankkia häirintälaitteita, vaan kyseisen yrityksen toiminta pitää liittyä keskeisesti esimerkiksi vartiointiin tai turvallisuuteen. Valvontalaitteiden kohdalla ei ole samanlaista rajoitteita, joten niiden hankinta on huomattavasti helpompaa. Usein dronetorjuntaan erikoistuneet yritykset tarjoavat useita erilaisia ratkaisuja, joista ostaja voi valita omaan tarkoitukseen soveltuvat laitteistot.

Yritykset kuitenkin kehottavat käyttäjiä tarkastamaan ja päivittämään laitteet säännöllisesti. Fyysisessä tarkastelussa tutkitaan ulkoisia vaurioita laitteen koteloinnissa, johtimissa tai antenneissa. Päivityksillä pidetään huoli siitä, että laitteisto käyttää uusimpia ohjelmistaja ja tietokantoja. [11, 15]

Taulukossa 5.1 on listattu 12 erilaista dronetorjuntaan erikoistunutta yritystä ja niiden toimipisteiden sijainnit, mutta lista on todellisuudessa huomattavasti pitempi. Yritykset ovat valittu siten, että niiden kaupalliset ratkaisut vastaisivat mahdollisimman hyvin aikaisemmissa luvuissa käsiteltyjä valvonta- ja torjuntamenetelmiä sekä muita kandidaatintyön rajauksia. Jokaisella yrityksellä on tuotevalikoimissa useita erilaisia laitteita ja niiden eri versioita, minkä takia ei ole tarpeellista esitellä kaikkia mahdollisia tuotteita, koska saman yrityksen kaupalliset laitteet ovat keskenään hyvin samankaltaisia. Seuraavissa aliluvuissa kaupalliset ratkaisut jaetaan kolmeen eri kategoriaan, jotka ovat valvonta- ja torjuntalaitteet sekä torjuntajärjestelmät. Jokaisessa kategoriassa käsitellään aina muutamia eri yritysten tarjoamia kaupallisia ratkaisuja, jotka ovat suunniteltu samaa tehtävää varten. Kaupallisia tuotteita on tarkoitus vertailla sekä keskenään että tieteellisissä tutkimuksissa esitettyihin menetelmiin ja havaintoihin.

Yritys	Sijainti
Sensofusion	Suomi, Yhdysvallat
Rantelon	Viro
Anti-Drone	Tanska
Blighter Surveillance Systems	Iso-Britannia
Drone Defence	Iso-Britannia
DeTect	Yhdysvallat, Iso-Britannia
Dedrone	Saksa, Yhdysvallat
CTS Technology	Kiina
MCTech	Israel
Department 13	Yhdysvallat
Liteye Systems	Yhdysvallat
DroneShield	Australia

Taulukko 5.1. *Dronevalvontaan ja -torjuntaan erikoistuneita yrityksiä [9]*

Kaupallisia tuotteita on jonkin verran kritisoitu siitä, että ne tarjoavat vain teoreettisia ratkaisuja. Väitetään, että jossain tapauksissa näyttävillä videoilla ja esityksillä yritetään luoda kuva toimivasta järjestelmästä. Tuotteiden tekniset tiedot ovat haettu pääasiassa yritysten verkkosivuilta, minkä takia jotain ominaisuuksia on saatettu liioitella esimerkiksi markkinoinnin tehostamiseksi. [52]

5.1 Valvontalaitteet

Kaupalliset valvontalaitteet perustuvat tällä hetkellä vahvasti radiovalvontaan, jota lähes kaikki markkinoilla olevat valvontalaitteet hyödyntävät. Radiovalvonnan jälkeen seuraavaksi yleisimmät menetelmät ovat optinen valvonta ja tutka. Optisia valvontalaitteita myydään esimerkiksi usein lisävarusteina, jotka voidaan yhdistää valvontajärjestelmään. Akustisia valvontalaitteita ei ole juurikaan markkinoilla, mutta tieteellisen tutkimuksen yhteydessä on rakennettu akustiikkaa hyödyntäviä laitteita ja testattu niiden toimivuutta. Jotkin valvontalaitteita valmistavat yritykset kuitenkin myyvät akustisia sensoreita. [15, 52, 53]

Kuvassa 5.1 on esitetty kolme dronevalvontalaitetta, jotka ovat kaikki eri valmistajien tuotteita. Laitevalmistajat järjestyksessä ovat Dedrone, DeTect ja DroneShield. Laitteet ovat ulkomuodoltaan hyvin samankaltaisia ja ne ovat suunniteltu kestämään vettä ja vaativia olosuhteita. Kuvissa 5.1a ja 5.1b olevat laitteet ovat suhteellisen pieniä, helposti kiinnitettäviä ja ulkoasultaan muistuttavat tavallista sähkölaatikkoa. Molemmat näistä laitteista tunnistavat ja paikantavat dronet radiovalvonnan avulla. Kuvassa 5.1c on DroneSentinel, joka on hieman suurempi modulaarinen yksikkö, mikä mahdollistaa erilaisten valvontalaitteiden helpon kiinnityksen. Kyseisessä yksikössä on kiinnitettynä muun muassa optinen kamera sekä radio- ja tutkavalvontalaitteet. [10, 11, 18]

(a) *RF-300 [10]* ***(b)*** *DroneWatcherRF [11]* ***(c)*** *DroneSentinel [18]*

Kuva 5.1. *Valvontalaitteita*

Laitevalmistajat yleensä ilmoittavat nimelliset valvontaetäisyydet laitteille, minkä yhteydessä on usein myös maininta, että valvontasäde riippuu esimerkiksi dronen kokoluokasta ja valvontaympäristöstä. Dedronen RF-300 valvontayksikön keskimääräinen valvontaetäisyys on noin 1,3 km, minkä sisällä laite kykenee havaitsemaan radio- ja WiFi-ohjattavat dronelennokit [10]. DroneWatcherRF:n valvontasäde on valmistajan mukaan noin 1–3 km ja se kykenee tunnistamaan ja havaitsemaan suurimman osan kaupallisista radio-ohjattavista droneista [11]. DroneSentinelin valmistaja kertoo, että yksikkö tunnistaa ensiksi dronet joko radio- tai tutkavalvonnalla, joiden valvontasäteet ovat 5 km ja 1,5 km. Laitteisto vielä varmistaa havainnot optiikan avulla. Tunnistus suoritetaan joko video- tai infrapunakameralla, jotka kykenevät varmistamaan kohteen noin 1 km tai 380 m etäisyydeltä. [18]

Eri laitevalmistajien verkkosivuilla ja laitteiden datalehdillä esitetyt ominaisuudet vastaavat suhteellisen hyvin muita samankaltaisia tuotteita ja tieteellisten tutkimusten tuloksia, joita on todettu erilaisille valvontamenetelmille. Ainut epäilyttävä asia on DroneSentinelin radiovalvonnan 5 km:n valvontasäde, mikä vaikuttaa hyvin suurelta, jos sitä vertaa tieteellisen tutkimuksen tuloksiin. Asiaa on kuitenkin hankala varmistaa, koska laitteiden tarkat tekniset tiedot ja myyntihinnat eivät ole saatavilla.

5.2 Torjuntalaitteet

Kaupalliset torjuntalaitteet perustuvat radiohäirintään ja ne voidaan jakaa joko kiinteästi asennettuihin tai kannettaviin laitteisiin. Kiinteästi asennetut laitteet ovat yleensä osa suurempaa järjestelmää, joka sisältää sekä valvonta- että torjuntayksiköt. Kannettavat laitteet ovat joko ympärisäteileviä tai suuntaavia, jotka muistuttavat ulkoasultaan esimerkiksi kivääriä tai salkkua. Suunta-antennin avulla saavutetaan parempi häirinnän tehokkuus kohdetta vastaan, koska häirintäsignaali kohdistuu lähes kokonaisuudessaan antennin

(a) *Drone Jamming Gun [47]* ***(b)*** *DroneGun Tactical [17]* ***(c)*** *Paladyne E1000MP [15]*

Kuva 5.2. *Torjuntalaitteita*

suuntaan. Suuntaavat häirintälaitteet eivät kuitenkaan ole täysin ideaalisia, vaan ne säteilevät myös jonkin verran taakse ja sivuille. Säteilykuvion takia myös muut ympäröivät laitteet saattavat altistua häirinnälle, vaikka ne eivät olisi varsinaisena kohteena.

Kuvassa 5.2 on esitetty kolme erilaista kannettavaa häirintälaitetta, joista 5.2a ja 5.2b muistuttavat kivääriä, joka on varustettu suunta-antennilla ja 5.2c on ympärisäteilevä salkun muotoinen häirintälaite. Salkkuratkaisu on ulkoasultaan neutraali, eikä se aiheuta ylimääräistä huomiota esimerkiksi yleisellä paikalla. Laitteiden valmistajat järjestyksessä ovat Rantelon, DroneShield ja DroneDefence. Jokaisen valmistajan laite kykenee häiritsemään useita droneohjaukselle tyyppillisiä taajuusalueita sekä satelliittipaikannukseen perustuvaa GPS-signaalia. Rantelonin ratkaisu on huomattavasti kevyempi verrattuna kahteen muuhun häirintälaitteeseen, koska se painaa vain 2 kg. DroneGun Tactical ja Paladyne E1000MP painavat noin 7 kg ja 10 kg. Lisäksi Paladyne E1000MP on mahdollista aktivoida etäältä, mutta samanlaista ominaisuutta ei löydy kahdesta muusta häirintälaitteesta. [15, 17, 47]

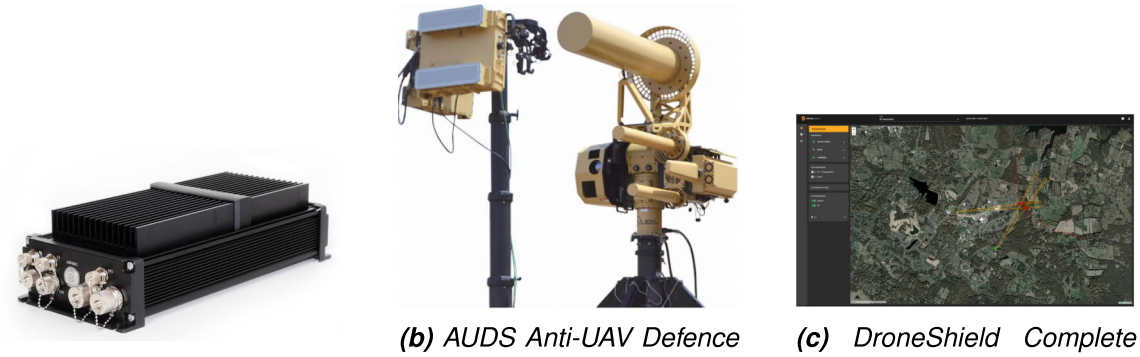
Yritysten mukaan kaikki laitteet ovat helppokäyttöisiä, eikä käyttö vaadi erikoiskoulutusta. Laitteet ovat valmiina toimintaan vain muutaman napin painalluksen jälkeen, minkä ansiosta laitteilla voidaan nopeasti vastata havaittuun droneuhkaan. Rantelonin ja Dronedefencen laitteiden tehokas toimintasäde on noin 1 km. DroneShieldin häirintälaitteelle toimintasäteeksi on ilmoitettu 1–2 km. Kaikkien häirintälaitteiden toimintasäde on suurin piirtein sama, vaikka kyseessä on kolme hieman erilaista ratkaisua. [15, 17, 47]

Kaikista kolmesta laitevalmistajasta ainoastaan Rantelon on ilmoittanut heidän laitteensa käyttämän häirintätekniikan, joka on pyyhkäisyhäirintä [47]. Muiden laitteiden häirintätekniikasta ei ole tällä hetkellä varmaa tietoa, mutta todennäköisesti ne hyödyntävät myös jotain saman tyyppistä menetelmää. Yleisesti häirintälaitteiden teknisistä ratkaisuista on hyvin vähän tietoa julkisesti saatavilla.

5.3 Torjuntajärjestelmät

Kaupalliset torjuntajärjestelmät ovat kokonaisratkaisuja, jotka koostuvat usein kiinteästi asennetuista valvonta- ja torjuntalaitteista. Näiden fyysisten laitteiden lisäksi järjestel-

mään kuuluu erilaisia ohjelmistoja, jotka takaavat järjestelmän eri osien keskenäisen toiminnan. Järjestelmän käyttäjää varten on luotu helppokäyttöinen käyttöliittymä, joka esittää havaitut dronet reaaliajassa kartalla, kirjaa havainnot muistiin myöhempää tarkastelua varten ja tarvittaessa lähettää ilmoitukset havainnoista esimerkiksi tekstiviestillä tai sähköpostilla. Järjestelmät kykenevät suorittamaan dronevalvontaa autonomisesti. Torjuntayksiköitä voidaan operoida joko manuaalisesti tai asettaa ne automaattitilaan, jolloin järjestelmä itsenäisesti ohjaa häirintälaitteita saapuvien valvontatietojen perusteella. Yhdessä nämä kaikki muodostavat tehokkaan kokonaisratkaisun, joka kykenee torjumaan lähes kaikki luvattomien dronejen aiheuttamat uhkatilanteet. Torjuntajärjestelmät soveltuvat osaksi lentokenttien, vankiloiden, energialaitosten, varuskuntien ja tärkeiden valtion rakennusten turvallisuusratkaisuja.



(a) *AIRFENCE [52]*

(b) *AUDS Anti-UAV Defence System [6]*

(c) *DroneShield Complete [19]*

Kuva 5.3. *Dronetorjuntajärjestelmiä*

Kuvassa 5.3 on esitetty joitain kaupallisten torjuntajärjestelmien keskeisiä laitteita ja ohjelmistoja. Torjuntajärjestelmät ovat suuria kokonaisuuksia, minkä takia kaikkia järjestelmän osia on hankala esittää yhdessä kuvassa. Kohdassa 5.3a on suomalaisen Sensofusionin kehittämä Airfence-järjestelmä, jonka tekniikka syntyi osana sotilasprojektia, jossa kartoitettiin miehittämättömien ilma-alusten aiheuttamia uhkia. Sensofusion tekee yhteistyötä muun muassa Suomen puolustusvoimien ja Yhdysvaltain ilmailuhallinto FAA:n kanssa. Yhteistyön ansiosta yhtiö on päässyt testaamaan laitteitaan Yhdysvaltojen lentokentille, jossa luvattomat dronet ovat huomattavasti suurempi uhka kuin Suomessa tällä hetkellä. Tämän lisäksi tekniikkaa on testattu Euroopassa viranomaiskäytössä. [41, 52]

Markkinoilta löytyy tällä hetkellä Airfence 6.0, joka on järjestelmän uusin versio. Järjestelmä hyödyntää ainoastaan radiovalvontaa ja -häirintää, mutta kykenee verkkosivujen mukaan saavuttamaan jopa 10 km valvontasäteen. Näin suuri valvontasäde vaikuttaa epätodelliselta. Toisaalta kyseessä on yhtiö, joka on alansa suurimpia toimijoita ja vaikuttaa luotettavalta. Verkkosivujen mukaan järjestelmä hyödyntää ohjelmistopohjaisia radioita, jotka ovat yhdistetty graafiseen käyttöliittymään. [52]

Kuvassa 5.3b on AUDS Anti-UAV torjuntajärjestelmä, joka on kehitetty kolmen yrityksen yhteistyön tuloksena. Blighter Surveillence System tarjoaa järjestelmän tutkavalvontalaitteen, jonka valvontaetäisyys on datalehden mukaan 10 km. Järjestelmän optiikka on Chess Dynamicsin tuottama, millä ohjataan radiohärintää suorittavia suunta-antenneja.

Häirintälaitteet ovat puolestaan Enterprice Control Systems Ltd:n tekniikkaa, joka käyttää älykästä radiohäirintää. [6]

Kuvassa 5.3c on DroneShieldin Complete-järjestelmän käyttöliittymä, jossa on aluekartta keskellä ja vasemmassa reunassa on valikko erilaisia asetuksia varten. Käyttöliittymä on hyödyllinen esimerkiksi dronehavaintojen analysoinnissa. Torjuntajärjestelmän valvontayksikkö on aikaisemmin kuvassa 5.1c oleva DroneSentinel. Samaan metallirunkoon kiinnitetään myös radiohäirintälaitteet, joiden häirintäsäteeksi on esitetty yrityksen verkkosivuilla 1,5 km. [19]

Eri torjuntajärjestelmien vertailussa huomataan, että toimivan kokonaisuuden voi rakentaa monella eri tavalla muodostamalla erilaisia valvonta- ja häirintälaitekombinaatioita. Erityisesti älykkään häirinnän ja ohjelmistopohjaisten radioiden merkitys korostui kokonaisratkaisujen tarkastelussa, mitkä ovat todettu tehokkaiksi häirintätekniikoiksi luvattomien dronejen torjunnassa [43].

6 YHTEENVETO

Työssä tutustuttiin ensimmäiseksi dronelennokkien tekniikkaan ja käyttökohteisiin. Tekniikan ymmärtäminen on tärkeä osa aihetta, koska jokainen valvonta- ja torjuntamenetelmän toiminta perustuu jollain tavalla dronejen teknisiin ratkaisuihin. Markkinoilla on suuri määrä erilaisia droneja, mikä on aiheuttanut haasteita luvattomien dronejen torjunnassa. Aikaisemmin dronet olivat pääasiassa harrastekäyttäjien suosiossa, mutta nyt ne ovat yleistyneet myös ammatti-, viranomais- ja tutkimuskäytössä. Dronelennokkien kehitys on mennyt nopeasti eteenpäin, koska tekniikka on yleistynyt ja komponenttien hinnat ovat laskeneet. Droneista tehdään jatkuvasti sekä tieteellistä tutkimusta että kaupallista tuotekehitystä.

Työn aihe on ajankohtainen, mikä todettiin, kun tarkasteltiin erilaisia vaara- ja uhkatilanteita. Suomessa on toistaiseksi vältytty droneiskuilta, mutta luvatonta käyttö on selvästi lisääntynyt myös kotimaassa. Traficomin mukaan dronet ovat vuoden 2018 huolestuttavin ilmailuturvallisuustrendi. Varsinkin ulkomailla luvattomat dronet ovat olleet suuri ongelma, koska niitä on suhteellisen helppo hyödyntää rikoksentekovälineenä. Kriittisiä kohteita ovat esimerkiksi lentokentät, voimalaitokset, vankilat, rajavyöhykkeet ja valtion rakennukset.

Työssä käsiteltiin neljää erilaista valvontamenetelmää, jotka perustuvat akustiikkaan, optiikkaan, radiotekniikkaan ja tutkaan. Jokaisella valvontamenetelmällä on oma toimintaperiaate, minkä takia ne erovat toisistaan. Suurimmat erot menetelmien välillä syntyvät, kun vertaillaan valvontasäteitä keskenään. Toimintaympäristöt vaikuttavat olennaisesti valvontamenetelmien toimintaa, minkä takia niiden vaikutukset pitää huomioida valvontalaitteiden ja -järjestelmien valinnassa.

Dronevalvonnassa tietokannoilla on suuri merkitys eri dronetyyppien tunnistuksessa. Koneoppimisen avulla järjestelmälle opetetaan dronejen ainutlaatuisia ominaisuuksia, kuten äänisignaaleja, ulkoisia rakenteita, radioprotokollatietoja ja mikro-Doppler-jälkiä. Eri sensoreista saatavia valvontatietoja yhdistelemällä lähes kaikki dronet ovat tunnistettavissa. Tämän ansiosta dronevalvonta on mahdollista toteuttaa täysin autonomisesti, mikä on kustannustehokasta. Yritykset joutuvat kuitenkin jatkuvasti päivittämään tietokantojaan, kun uusia droneja tulee markkinoille. Valvontalaitteiden omistajalla on vastuu päivittää ohjelmistot ja huoltaa laitteet säännöllisesti, mikä on tärkeä osa tehokasta ja onnistunutta dronevalvontaa.

Tällä hetkellä lähes kaikki kaupalliset torjuntalaitteet käyttävät pääasiassa radiohäirintää,

eikä muita siviiliviranomaisille soveltuvia teknisiä menetelmiä toistaiseksi tunneta. Dronen hakkerointi on edistyneempi versio radiohäirinnästä, mutta sen soveltaminen käytännössä on haasteellista. Sotilaskäytössä on testattu esimerkiksi elektromagneettista häirintää ja laseria, mutta näiden menetelmien käytöstä aiheutuu häiriötä ja ylimääräisiä vahinkoa ulkopuolisille sähkölaitteille, minkä takia ne eivät sovellu siviiliviranomaisten käyttöön.

Toistaiseksi dronet ovat olleet valvonta- ja torjuntamenetelmien kehitystä edellä, vaikka markkinoilla on runsaasti luvattomien dronejen torjuntaan erikoistuneita yrityksiä. Valvontalaitemarkkinoilla radiovalvonta on ehdottomasti käytetyin valvontamenetelmä, minkä jälkeen optinen ja tutkavalvonta ovat tasavahvassa asemassa. Akustista valvontaa hyödynnetään kaikista vähiten, mikä johtuu sen rajoittuneesta valvontasäteestä. Yritykset ovat pitkään testanneet ja kehittäneet laitteistoja ja järjestelmiä, minkä perusteella on todennäköistä, että valvonta- ja torjuntalaitteiden asentaminen aloitetaan lähiaikoina.

Autonomiset dronet ovat aiheuttaneet uudenlaisen ongelman luvattomien dronejen torjunnassa, koska ne eivät muodosta radioyhteyttä ohjausasemaan. Tämän takia radioliikenteen kuuntelu passiivisen radiovalvonnan avulla ei ole mahdollista, eikä niitä voida torjua radiohäirinnällä. Autonomisen dronen havaitseminen on kuitenkin mahdollista kaikilla muilla valvontamenetelmillä. GPS-häirintä toimii ainoastaan tapauksissa, joissa dronet suunnistavat satelliittipaikannuksen avulla. Todellisuudessa autonomiset dronet käyttävät satelliittipaikannuksen rinnalla esimerkiksi visuaalista paikannusta, minkä takia aihe vaatii jatkotutkimusta.

Työssä tarkastellaan yksittäisen dronen havaitsemiseen ja torjuntaan soveltuvia menetelmiä, mutta uusia haasteita esiintyy, jos kyseessä on luvaton droneparvi. Valvontalaitteiden pitää osata yhdistää antureista saatava data yksittäiseen droneen, koska niiden on kyettävä tunnistamaan ja seuraamaan useita kohteita samanaikasesti. Parvessa lentävät dronet kommikoivat myös jollain tavalla keskenään, mikä estää niitä törmäämästä toisiinsa. Samalla se on kokonaan uusi ominaisuus, jota voidaan hyödyntää dronejen havaitsemisessa. Torjuntamenetelmien kohdalla todettiin, niillä on mahdollista vaikuttaa useisiin kohteisiin yhtä aikaa. Lisäksi useimmat yritykset ovat ilmoittaneet, että heidän laitteet soveltuvat myös droneparvien torjuntaan.

LÄHTEET

[1] Amazon. *DIY Mini RC Toy Quadcopter Battle Drone Set Building Kit With FPV HD Camera RTF Helicopter For Kids with Extra Battery and Battery for Remote Controller*. URL: https://www.amazon.com/Quadcopter-Building-Helicopter-Battery-Controller/dp/B071YLD2NJ?ref_=fsclp_pl_dp_3 (viitattu 04. 05. 2019).

[2] Amazon. *First prime air delivery*. URL: https://www.amazon.com/b?node=8037720011 (viitattu 09. 03. 2019).

[3] Amazon. *Top Race DIY Drone Building Blocks 2.4GHz Remote Control Drone, Build it Yourself and Fly, 54 Pieces (TR-D5) for Ages 14+*. URL: https://www.amazon.com/Top-Race-Building-Control-Yourself/dp/B071ZZJ5L1?ref_=fsclp_pl_dp_4 (viitattu 04. 05. 2019).

[4] ANTIDRONE. *Long-range counter-UAV system*. URL: https://anti-drone.eu/solutions/special-response-vehicle.html (viitattu 18. 05. 2019).

[5] S. Basak ja B. Scheers. Passive radio system for real-time drone detection and DoA estimation. *2018 International Conference on Military Communications and Information Systems (ICMCIS)*. Toukokuu 2018, 1–6. DOI: 10.1109/ICMCIS.2018.8398721.

[6] Blighter Surveillance Systems. *AUDS Anti-UAV Defence System*. URL: http://www.blighter.com/products/auds-anti-uav-defence-system.html (viitattu 18. 05. 2019).

[7] Boomspeaker. *Noise level chart: Decibel levels of common sounds with examples*. URL: https://boomspeaker.com/noise-level-chart-db-level-chart/ (viitattu 09. 04. 2019).

[8] W. Budiharto, A. A. S. Gunawan, J. S. Suroso, A. Chowanda, A. Patrik ja G. Utama. Fast Object Detection for Quadcopter Drone Using Deep Learning. *2018 3rd International Conference on Computer and Communication Systems (ICCCS)*. Huhtikuu 2018, 192–195. DOI: 10.1109/CCOMS.2018.8463284.

[9] J. Carlini. *The Anti-Drone Revolution: 22 Companies Building Killer Drone Tech Today*. URL: https://mag.dronesx.com/anti-drone-revolution-companies-building-killer-drone-tech/ (viitattu 18. 05. 2019).

[10] Dedrone. *RF-300 Datasheet*. URL: %5C%5C%20https://assets.website-files.com/58fa92301759990d60953ccf/5a981fc9d790df0001e798f7_dedrone-datasheet-rf-300-en.pdf.

[11] DeTech. *Drone Detection & Defense Systems - DroneWatcherRF*. URL: https://detect-inc.com/drone-detection-defense-systems/ (viitattu 18. 05. 2019).

[12] DJI. *FLY SAFE GEO ZONE MAP*. URL: https://www.dji.com/fi/flysafe/geo-map (viitattu 09. 04. 2019).

[13] DJI. *Inspire 2 User Manual v1.0*. URL: https://dl.djicdn.com/downloads/inspire_2/INSPIRE+2+User+Manual+.pdf (viitattu 09. 03. 2019).

[14] DJI. *Mavic Air User Manual v1.0*. URL: https://dl.djicdn.com/downloads/Mavic%20Air/Mavic%20Air%20User%20Manual%20v1.0.pdf (viitattu 09. 03. 2019).

[15] DroneDefence. *Paladyne E1000MP*. URL: https://www.dronedefence.co.uk/products/paladyne-e1000mp/ (viitattu 18. 05. 2019).

[16] Droneinfo. *Lennokkien lennättämisen ABC*. URL: https://www.droneinfo.fi/fi (viitattu 09. 03. 2019).

[17] DroneShield. *DroneGun Tactical - Highly Effective, Portable Drone Countermeasure*. URL: https://www.droneshield.com/dronegun-tactical (viitattu 18. 05. 2019).

[18] DroneShield. *DroneSentinel*. URL: https://www.droneshield.com/sentinel (viitattu 18. 05. 2019).

[19] DroneShield. *DroneShield Complete*. https://www.droneshield.com/droneshield-complete. (Viitattu 18. 05. 2019).

[20] J. Farlik, M. Kratky ja J. Casar. Detectability and jamming of small UAVs by commercially available low-cost means. *2016 International Conference on Communications (COMM)*. Kesäkuu 2016, 327–330. DOI: 10.1109/ICComm.2016.7528287.

[21] D. Floreano ja R. J. Wood. Science, technology and the future of small autonomous drones. Nature Publishing Group, 2015, 460–466. DOI: 10.1038/nature14542. URL: https://doi.org/10.1038/nature14542.

[22] I. Guvenc, F. Koohifar, S. Singh, M. L. Sichitiu ja D. Matolak. Detection, Tracking, and Interdiction for Amateur Drones. *IEEE Communications Magazine* 56.4 (huhtikuu 2018), 75–81. ISSN: 0163-6804. DOI: 10.1109/MCOM.2018.1700455.

[23] J. P. Hansen, A. Alapetite, I. S. MacKenzie ja E. Møllenbach. The Use of Gaze to Control Drones. *Proceedings of the Symposium on Eye Tracking Research and Applications*. ETRA '14. Safety Harbor, Florida: ACM, 2014, 27–34. ISBN: 978-1-4503-2751-0. DOI: 10.1145/2578153.2578156. URL: http://doi.acm.org/10.1145/2578153.2578156.

[24] R. I. A. Harmanny, J. J. M. de Wit ja G. P. Cabic. Radar micro-Doppler feature extraction using the spectrogram and the cepstrogram. *2014 11th European Radar Conference*. Lokakuu 2014, 165–168. DOI: 10.1109/EuRAD.2014.6991233.

[25] N. Help. *Noise Level Chart*. URL: https://www.noisehelp.com/noise-level-chart.html (viitattu 09. 04. 2019).

[26] G. Heyno, H. Diethard ja K. Dietrich. *Emp generator*. US4845378A. URL: https://patents.google.com/patent/US4845378A/en.

[27] F. Hoffmann, M. Ritchie, F. Fioranelli, A. Charlish ja H. Griffiths. Micro-Doppler based detection and tracking of UAVs with multistatic radar. *2016 IEEE Radar Conference (RadarConf)*. Toukokuu 2016, 1–6. DOI: 10.1109/RADAR.2016.7485236.

[28] IEC infrared systems. *Banshee*. URL: http://www.iecinfrared.com/products/integrated-systems/banshee/ (viitattu 18. 05. 2019).

[29] B. Insider. *Drone market shows positive outlook with strong industry growth and trends*. URL: https://www.businessinsider.com/drone-industry-analysis-market-trends-growth-forecasts-2017-7?r=US&IR=T&IR=T (viitattu 19. 03. 2019).

[30] R. C. Johann-Sebastian Pleban Ricardo Band. *Hacking and securing the AR.Drone 2.0 quadcopter: investigations for improving the security of a toy*. 2014. DOI: 10.1117/12.2044868. URL: https://doi.org/10.1117/12.2044868.

[31] Z. Kaleem ja M. H. Rehmani. Amateur Drone Monitoring: State-of-the-Art Architectures, Key Enabling Technologies, and Future Research Directions. *IEEE Wireless Communications* 25.2 (huhtikuu 2018), 150–159. ISSN: 1536-1284. DOI: 10.1109/MWC.2018.1700152.

[32] M.-L. Kämppi. *Rajavartiolaitos innostui kameralennokeista – drone halutaan käyttöön jokaiselle partiolle*. URL: https://yle.fi/uutiset/3-10531225 (viitattu 19. 03. 2019).

[33] Lentoposti. *Presidentti vahvisti poliisille oikeudet puuttua drone-toimintaan teknisin ja voimakeinoin*. URL: https://www.lentoposti.fi/uutiset/presidentti_vahvisti_poliisille_oikeudet_puuttua_drone_toimintaan_teknisin_ja_voimakeinoin (viitattu 06. 04. 2019).

[34] M. Lichtman, J. D. Poston, S. Amuru, C. Shahriar, T. C. Clancy, R. M. Buehrer ja J. H. Reed. A communications jamming taxonomy. *IEEE Security Privacy* 14.1 (tammikuu 2016), 47–54. ISSN: 1540-7993. DOI: 10.1109/MSP.2016.13.

[35] P. Liesmäki. *Poliisi hankkii kymmeniä uusia droneja tänä vuonna – Raahessa ilmaalus löysi eksyneen sienestäjän*. URL: https://www.maaseuduntulevaisuus.fi/tiede-tekniikka/artikkeli-1.307175 (viitattu 19. 03. 2019).

[36] T. Luna. *Ultimate DJI sound comparison!* URL: https://www.wetalkuav.com/ultimate-dji-sound-test/2/ (viitattu 09. 04. 2019).

[37] S. Mandal, K. Maheta, V. Kumar ja M. S. Prasad. Control of UAV Using GSM Technology. *Proceedings of the International Conference on Modern Research in Aerospace Engineering*. Toim. S. Singh, P. Raj ja S. Tambe. Singapore: Springer Singapore, 2018, 77–85. ISBN: 978-981-10-5849-3.

[38] T. Multerer, A. Ganis, U. Prechtel, E. Miralles, A. Meusling, J. Mietzner, M. Vossiek, M. Loghi ja V. Ziegler. Low-cost jamming system against small drones using a 3D MIMO radar based tracking. *2017 European Radar Conference (EURAD)*. Lokakuu 2017, 299–302. DOI: 10.23919/EURAD.2017.8249206.

[39] Multitronic. *DJI Inspire 2 without camera*. URL: https://www.multitronic.fi/fi/products/1524943/dji-inspire-2-without-camera (viitattu 19. 03. 2019).

[40] P. Nguyen, M. Ravindranatha, A. Nguyen, R. Han ja T. Vu. Investigating Cost-effective RF-based Detection of Drones. *Proceedings of the 2Nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use*. DroNet '16. Singapore, Singapore: ACM, 2016, 17–22. ISBN: 978-1-4503-4405-0. DOI: 10.1145/2935620.2935632. URL: http://doi.acm.org/10.1145/2935620.2935632.

[41] T. Ovaskainen. *Suomalaisyhtiö pääsee kokeiluun USA:n lentokentille – torjuu UAV-kopterien riskejä, "kykenee haltuunottoon"*. 2016. URL: https://www.uusisuomi.

fi/kotimaa/195452-suomalaisyhtio-sensofusion-paasee-kokeiluun-usan-lentokentille-torjuu-uav-kopterien (viitattu 04. 06. 2019).

[42] J. A. Paredes, F. J. Álvarez, T. Aguilera ja J. M. Villadangos. 3D Indoor Positioning of UAVs with Spread Spectrum Ultrasound and Time-of-Flight Cameras. *Sensors* 18.1 (2018). ISSN: 1424-8220. DOI: 10.3390/s18010089. URL: https://www.mdpi.com/1424-8220/18/1/89.

[43] K. Pärlin, M. M. Alam ja Y. Le Moullec. Jamming of UAV remote control systems using software defined radio. *2018 International Conference on Military Communications and Information Systems (ICMCIS)*. Toukokuu 2018, 1–6. DOI: 10.1109/ICMCIS.2018.8398711.

[44] Poliisilaki. *11 § - Lennokin tai miehittämättömän ilma-aluksen kulkuun puuttuminen*. URL: https://www.finlex.fi/fi/laki/ajantasa/2011/20110872#L2P11a (viitattu 18. 05. 2019).

[45] P. Popovski, H. Yomo ja R. Prasad. Strategies for adaptive frequency hopping in the unlicensed bands. *IEEE Wireless Communications* 13.6 (joulukuu 2006), 60–67. ISSN: 1536-1284. DOI: 10.1109/MWC.2006.275200.

[46] M. Prigg. *A 'death ray' for all seasons: Boeing reveals drone-killing laser weapon can target craft through fog, wind and rain - and it's all done with an Xbox controller*. 2014. URL: https://www.dailymail.co.uk/sciencetech/article-2757171/Boeing-reveals-death-ray-drone-killing-laser-weapon-target-craft-fog-wind-Xbox-controller.html (viitattu 04. 06. 2019).

[47] Rantelon. *Drone Jamming Gun PJ-2458*. URL: https://rantelon.ee/wp-content/uploads/2019/05/PJ-2458.pdf (viitattu 18. 05. 2019).

[48] T. Riihonen, D. Korpi, M. Turunen ja M. Valkama. Full-duplex radio technology for simultaneously detecting and preventing improvised explosive device activation. *2018 International Conference on Military Communications and Information Systems (ICMCIS)*. Toukokuu 2018, 1–4. DOI: 10.1109/ICMCIS.2018.8398707.

[49] Robota. *Hobbyist Drones vs. Commercial/Research Drones: How to Tell the Difference*.
http://www.robota.us/how-to/hobbyist-drones-vs-commercialresearch-drones-tell-difference/. (Viitattu 04. 05. 2019).

[50] Rohde & Schwarz GmbH & Co KG. *Protecting the Sky: Signal Monitoring of Radio Controlled Civilian Unmanned Aerial Vehicles and Possible Countermeasures*. URL: https://www.scribd.com/doc/315420957/Protecting-the-Sky (viitattu 18. 05. 2019).

[51] F. Sauer ja N. Schörnig. Killer drones: The 'silver bullet' of democratic warfare? *Security Dialogue* 43.4 (2012), 363–380. DOI: 10.1177/0967010612450207. eprint: https://doi.org/10.1177/0967010612450207. URL: https://doi.org/10.1177/0967010612450207.

[52] Sensofusion. *AIRFENCE*. https://www.sensofusion.com. (Viitattu 18. 05. 2019).

[53] X. Shi, C. Yang, W. Xie, C. Liang, Z. Shi ja J. Chen. Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges. *IEEE*

Communications Magazine 56.4 (huhtikuu 2018), 68–74. ISSN: 0163-6804. DOI: 10.1109/MCOM.2018.1700430. (Viitattu 16. 03. 2019).

[54] M. Skara. *Brittiministeri lennokkihyökkäyksestä Gatwickin lentokentälle: Tämä on uudenlainen uhka, johon on varauduttava*. URL: https://yle.fi/uutiset/3-10567610 (viitattu 08. 03. 2019).

[55] K. Smith. *DRONE RACING: WHAT IS IT?* URL: https://myfirstdrone.com/blog/drone-racing-what-is-it (viitattu 18. 05. 2019).

[56] N. Smolyanskiy, A. Kamenev, J. Smith ja S. Birchfield. Toward Low-Flying Autonomous MAV Trail Navigation using Deep Neural Networks for Environmental Awareness. *CoRR* abs/1705.02550 (2017). arXiv: 1705.02550. URL: http://arxiv.org/abs/1705.02550.

[57] U. S. Technology. *Battery Management Systems BMS & Battery Packs*. https://www.unmannedsystemstechnology.com/category/supplier-directory/propulsion-power/battery-management-systems-bms-battery-packs/. (Viitattu 09. 03. 2019).

[58] Traficom. *Kauko-ohjattujen lennokkien ja ilma-alusten (UAS/RPAS/Drone) taajuudet ja radiolupa-asiat*. URL: https://www.traficom.fi/fi/liikenne/ilmailu/kauko-ohjattujen-lennokkien-ja-ilma-alusten-uasrpasdrone-taajuudet-ja-radiolupa (viitattu 10. 03. 2019).

[59] Traficom. *Radiotaajuusmääräys 4*. URL: https://www.finlex.fi/data/normit/44839/Radiotaajuusmaarays_M4Y-FI.pdf (viitattu 09. 04. 2019).

[60] *Venezuelan presidenttiä vastaan hyökättiin räjähdelennokeilla – "Tämä oli salamurhayritys"*. https://www.is.fi/ulkomaat/art-2000005780629.html. 5. elokuuta 2018. (Viitattu 08. 03. 2019).

[61] Verkkokauppa. *DJI Mavic Air -nelikopteri, Onyx Black*. https://www.verkkokauppa.com/fi/product/28020/. (Viitattu 19. 03. 2019).

[62] D. Waldstein. *Drone Crash Interrupts Match*. Syyskuu 2015. URL: https://www.nytimes.com/live/us-open-results/drone-crash-interrupts-match/ (viitattu 09. 04. 2019).