MAANPUOLUSTUSKORKEAKOULU

KYBERELEKTRONISTEN MENETELMIEN SOVELTUVUUS LENNOKKIEN TORJUNTAAN LENTOTUKIKOHDASSA

Pro gradu -tutkielma

Yliluutnantti
Mikko Mäenpää

Sotatieteiden maisterikurssi 8
Ilmasotalinja

Huhtikuu 2019

KYBERELEKTRONISTEN MENETELMIEN SOVELTUVUUS LENNOKKIEN TORJUNTAAN LENTOTUKIKOHDASSA

MAANPUOLUSTUSKORKEAKOULU

Kurssi Sotatieteiden maisterikurssi 8	Linja Ilmasotalinja
Tekijä Yliluutnantti Mikko Mäenpää	
Tutkielman nimi Kyberelektronisten menetelmien soveltuvuus lennokkien torjuntaan lentotukikohdassa	
Oppiaine, johon työ liittyy Sotatekniikka	Säilytyspaikka MPKK:n kurssikirjasto
Aika Huhtikuu 2019	Tekstisivuja 60

TIIVISTELMÄ

Lennokkien määrä lisääntyy jatkuvasti, jolloin todennäköisyys tahattomalle haitan aiheuttamiselle joko sotilas- tai siviili-ilmaukselle kasvaa. Tämän lisäksi on huomioitava mahdollinen tahallinen lentoliikenteen häirintä, tiedustelu tai rikollinen toiminta, joka voi kohdistua lentotukikohtaan. Lainsäädäntö ei vielä anna viranomaisille kovin laajoja oikeuksia lennokintorjuntaan, mutta tilanne on muuttumassa.

Nykyiset lennokintorjuntajärjestelmät luottavat pitkälti joko häirintään tai kybervaikuttamiseen, mutta eivät niiden yhteistoimintaan. Tämän tutkimuksen tarkoituksena on selvittää, mitä etuja yhteistoiminnalla voitaisiin saavuttaa lennokkien torjunnassa lentotukikohdassa. Aihetta on käsitelty sekä lentoturvallisuuden, että operaatioturvallisuuden näkökulmasta.

Pääasiallinen saavutettava etu on lennokin torjunnan hallittavuus, jolloin itse torjunta ei aiheuta suurempaa harmia kuin torjuttava lennokki. Mahdollisia lieveilmiöitä ovat yleisesti käytössä olevien radiotaajuuksien häiriöt, putoavan lennokin aiheuttamat vahingot ja tulipalot.

AVAINSANAT

CEMA, kyber, lennokki, lennokkien torjunta

KYBERELEKTRONISTEN MENETELMIEN SOVELTUVUUS LENNOKKIEN TORJUNTAAN LENTOTUKIKOHDASSA

1. JOHDANTO

Joulukuussa 2018 Lontoon Gatwickin lentokentällä saatiin näköhavaintoja useasta lennokista, minkä johdosta lentotoimina jouduttiin keskeyttämään. Poliisilla ei alkuun vaikuttanut olevan muita toimintavaihtoehtoja kuin käyttää tarkka-ampujia lennokkien metsästämiseen. Yhtään lennokkia ei torjuttu tällä menetelmällä. Ensimmäisen kahden lennokin havaitsemisen jälkeen ei lennokeista saatu enää varmoja havaintoja ja lennokkien olemassaolo kyseenalaistettiin medialle annetuissa lausunnoissa. Poliisin käyttöönottamien torjuntalennokkien uskottiin olleen myöhempien havaintojen aiheuttajia.[12] Lentotoiminta käynnistettiin vasta, kun asevoimat toi Drone Dome -lennokintorjuntajärjestelmän alueelle [102]. Gatwick ja Heathrow hankkivat suorituskyvyltään vastaavat lennokintorjuntajärjestelmät lentotoiminnan turvaamiseksi jatkossa.[12]

Gatwickin tapaus kuvastaa hyvin ongelmia, joita lennokkien torjunnassa on. Ovatko pelkät näköhavainnot luotettavia ja miten erotetaan oma lennokki tunkeutuvasta lennokista? Miten lennokkeja torjutaan turvallisesti ja aiheuttamatta riskiä omalle lentotoiminnalle? Mitä jos lennokkien navigointivalot olisi peitetty?

Sotilasilmailu ei ole immuuni lennokkien aiheuttamalle lentoturvallisuusuhalle. Toisin kuin matkustajakoneella, hävittäjällä ei välttämättä ole mahdollisuutta jäädä maahan odottamaan lennonkin poistumista, vaan ilmaan on päästävä suorittamaan laissa säädettyjä tehtäviä [121, §24; 122, §2, §3]. Sama koskee yhteyskoneita ja helikoptereita, joiden tehtävän keskeytys voi tarkoittaa, että henkeä pelastavaa apua ei saada kohteelle riittävän ajoissa.

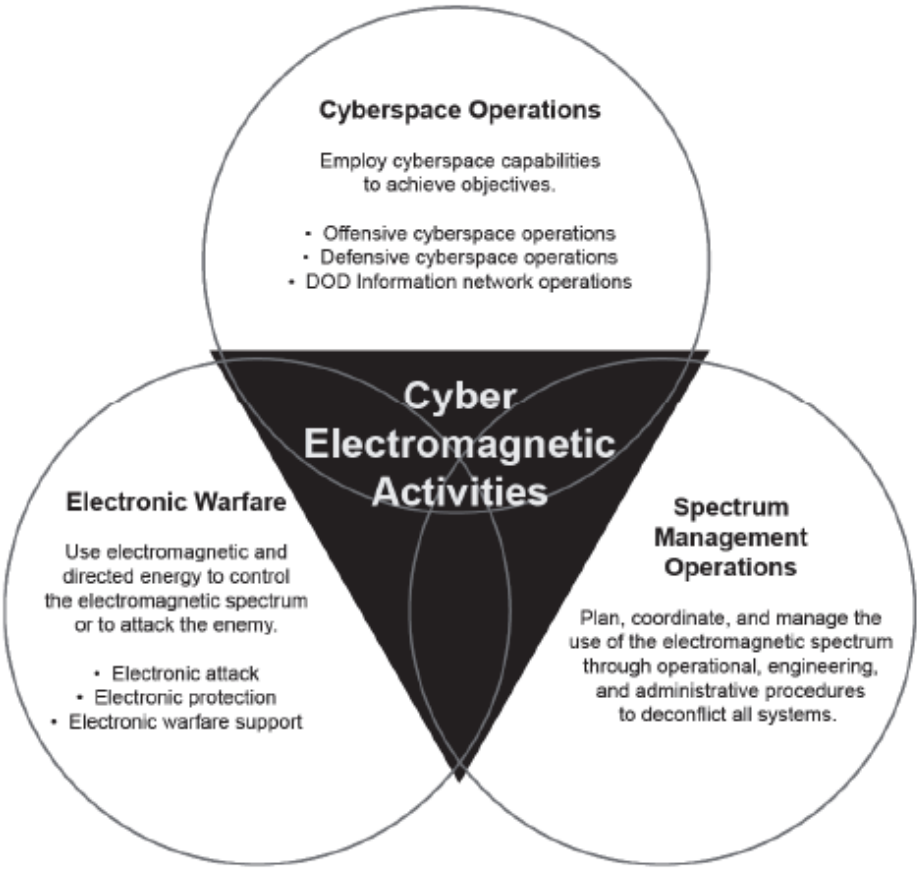
Harrastelija- ja ammattikäyttöön suunnattujen kuvauslennokkien yleistyminen luo uhan operaatio- ja lentoturvallisuudelle. Yleistymistä kuvaa hyvin se, että vuonna 2018 kesäkuun alkuun mennessä lennokeilla tehtyjä ilmailurikkomuksia on ilmoitettu 24, kun vuonna 2017 kokonaismäärä oli vain 17 [6].

Ilmailulain nojalla liikenteen turvallisuusvirasto voi antaa lennokkitoimintaa koskevia määräyksiä [123, §9]. Tämän tutkielman kirjoittamisen aikaan tällainen määräys on M1-32, jossa lennokkien käyttö on rajoitettu 5 kilometrin etäisyydellä kiitotiestä täysin ja muulla lähialueella sekä lentotiedotus- tai radiovyöhykkeellä korkeuden 50 metriä alapuolelle. Jos lennättäminen on suoraan näköyhteyteen perustuvaa näistä rajoituksista voi poiketa ilmailuliikennepalvelun tarjoajan, yleensä paikallisen lennonjohdon, luvalla. Kielto- ja rajoitusalueiden ulkopuolella on toimittava korkeuden 150 metriä alapuolella. Käytettäessä lennokkia näköyhteyden ulkopuolella tai lentotyöhön, on käytöstä tehtävä ilmoitus Liikenteen turvallisuusvirastolle. [104]

Operaatioturvallisuuden näkökulma on huomioitu siten, että kaikki lentotoiminta ml. lennokkitoiminta sotilasalueella on luvanvaraista. Kansainvälisten harjoitusten ja yleisötapahtumien aikana houkutus näiden rajoitusten rikkomiseen kasvaa, jolloin syntyy tarve estää lennokkien toiminta. Ilmailulakia rikkovan ilma-alukseen lentoon on mahdollista puuttua aluevalvontaviranomaisen luvalla. Voimakeinojen käyttäminen lennokkia vastaan on lainsäädännöllisesti haastavaa, sillä aluevalvontalain tarkoittamien huomautuksen ja varoituksen antaminen ilmaaluksen päällikölle [121, §32] ei ole käytännössä mahdollista. Lennokkitoiminnan voidaan joissain tapauksissa tulkita olevan aluevalvontalain tarkoittamaa vihamielistä toimintaa. Esimerkiksi aluevalvontalain §34 momentin 4 tarkoittamaa vieraan valtion tai tunnuksettoman sotilaallisen ryhmän Suomen alueella oleviin, valtakunnan turvallisuuden kannalta tärkeisiin kohteisiin oikeudettomasti kohdistamaa tiedustelua ja elektronista häirintää [121, §34]. Kineettinen vaikuttaminen aiheuttaa kuitenkin uhan tukikohdan rakenteille sekä siellä olevalle materiaalille. Putoava lennokki voi myös aiheuttaa rakennus- tai maastopaloja [78], jotka levitessään uhkaavat tukikohtaa ja lievimmillään aiheuttavat haittaa lentotoiminnalle. Poliisin, Puolustusvoimien ja Rajavartiolaitoksen oikeus torjua lennokkeja on vuoden 2019 keväällä vielä selvityksessä, vaikka lennokkitoiminta joissain tapauksissa aiheuttaa uhan kokonaisvaltaiselle turvallisuudelle. Poliisin oikeutta ottaa lennokki haltuun, estää sen käyttö tai muulla tavoin puuttua sen kulkuun ollaan laajentamassa hallituksen esityksellä 223/2018, joka sisältää niin teknisten- kuin voimakeinojen käyttämisen [124]. Lennokkien käytöstä salakuljetuksessa ja sotilaskohteiden kuvauksessa on jo havaintoja Suomessa. Lisäksi lennokkeja on käytetty terrori-iskussa [107].

1.1. Käsitteet ja määritelmät

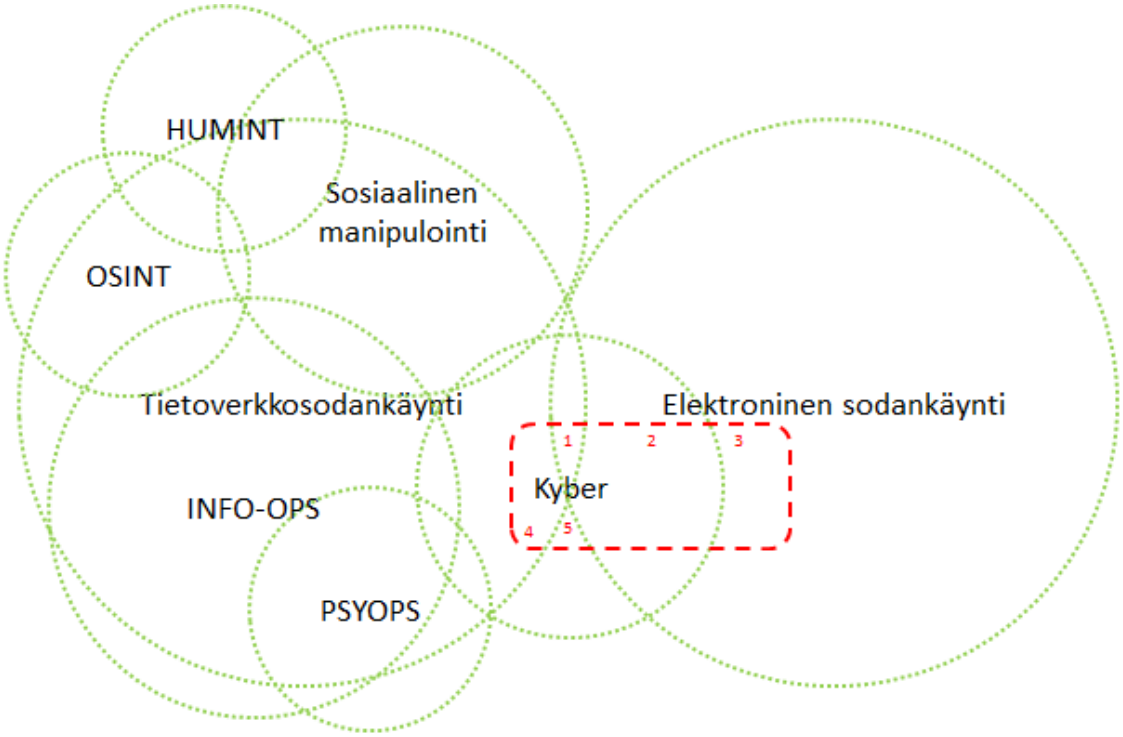
Tutkielman ymmärrettävyyden parantamiseksi on määriteltävä termit kyberelektroniset menetelmät ja lennokin torjunta. Kyberelektronisten menetelmien määrittelemiseksi avataan edelleen termit elektroninen sodankäynti ja kyber.



Kuva 1 Cyber Electromagnetic Activities yhdysvaltalaisen jaon mukaan[115]

”Kyberelektroniset menetelmät” on tässä tutkielmassa käytetty käännös termistä CEMA (Cyber ElectroMagnetic Activities). Yhdysvaltalaisen jaon mukaan tähän kuuluu kolme eri osa-aluetta: elektroninen sodankäynti, kybersodankäynti ja spektrinhallinta [115]. Kuvassa 1 on esitetty, että CEMA on se alue, jossa kaksi tai useampi toiminto toimii yhdessä tukien toista [115]. Suomalaisessa jaottelussa spektrinhallinta on osa elektronista sodankäyntiä [68, s. 26]. Tässä tutkielmassa käsitellään tilannetta, jossa elektronisen sodankäynnin menetelmät ja kybermenetelmät tukevat toisiaan.

”Kyber-” tässä tutkimuksessa tietotekniseen järjestelmään kohdistettu tiedustelu tai vaikuttaminen, joka perustuu tietojärjestelmän loogisen toiminnan epätavanomaiseen hyödyntämiseen. Kortelainen tarkastelee omassa tutkielmassaan termin historiaa laajemmin, mutta liittää siihen myös informaatiosodan käsitteen [67]. Suomen kyberturvallisuusstrategiassa kyber nähdään nimenomaan sanan etuliitteenä, esimerkiksi sanassa kybertoimintaympäristö [101]. Käyttämällä termiä kybertoimintaympäristö voidaan laajentaa perinteisempää tietoverkkosodankäynnin käsitettä tilanteisiin, joissa kohteena oleva tietojärjestelmä ei ole verkossa, tai vaikuttaminen perustuu johonkin muuhun rajapintaan, kuin verkkoliitäntään. Vastavuoroisesti tietoverkkosodankäynnissä on paljon menetelmiä ja tavoitteita, joissa ei tarvitse hyödyntää kybervaikuttamista.



Kuva 2 Tutkimuksen viitekehys

Kuvassa 2 on havainnollistettu tämän tutkimuksen tarkoittaman loogisen kyberin suhdetta tietoverkkosodankäyntiin ja elektroniseen sodankäyntiin. Tietoverkkosodankäynnin alla olevien termien keskinäiset suhteet eivät ole tutkimuksen kannalta oleellisia, vaan kuvan tavoitteena on havainnollistaa niiden suhdetta kyberiin. Tietoverkkosodankäynnin alle on listattu OSINT (open source intelligence, avoimiin lähteisiin perustuva tiedustelu) ja HUMINT(human intelligence, henkilötiedustelu) esimerkeiksi tilanteista, joissa tietoverkossa

tapahtuva tiedustelu ei perustu tietojärjestelmän logiikan epätavanomaiseen hyödyntämiseen. Esimerkiksi OSINTin yhteydessä tapahtuva Facebook-profiilin lukeminen ei ole epätavanomaista, sillä järjestelmä on tarkoitettu nimenomaan siihen tarkoitukseen. INFO-OPS (information operation, informaatio-operaatiot) ja PSYOPS (psychological operations, psykologiset operaatiot) voivat perustua tiedon väärentämiseen käyttäen hyväksi järjestelmän haavoittuvuutta, mutta niissäkin pääosa vaikuttamisesta perustuu edelleen järjestelmän normaaliin toimintaan. Esimerkiksi valheellinen uutisointi ei välttämättä vaadi järjestelmässä olevan tiedon väärentämistä vaan voi perustua tiedon tavanomaiseen syöttämiseen, jonka jälkeen kybervaikuttamisella tieto saatetaan laajemman yleisön tietoon, esimerkiksi käyttämällä Twitter-botteja. INFO-OPSin ohella suureen rooliin tietoverkkosodankäynnissä nousee sosiaalinen manipulointi (social engineering), jossa käytetään hyväksi järjestelmää käyttävän ihmisen luottamusta luotaessa edellytyksiä vaikuttaa järjestelmään. Phising (verkkourkinta) on yleinen sosiaalisen manipuloinnin muoto, jossa kyberkomponentin voi muodostaa sähköpostin lähettäjän väärentäminen.

Kuvaan 2 on lisäksi rajattu punaisella ja numeroitu viisi eri menetelmää, joita tässä tutkimuksessa tarkastellaan:

1. Langattomaan tietoverkkoon kohdistettu kybervaikutus, joka hyödyntää elektronisen sodankäynnin keinoja
2. Langattomasti toimitettava kybervaikutus tai kybervaikutuksella täydennetty elektroninen sodankäynti
3. Puhdas elektroninen sodankäynti
4. Tietoverkossa tapahtuva kybervaikuttaminen
5. Suora kybervaikuttaminen, esimerkiksi usb-median avulla

”Rajapinta” on tässä tutkimuksessa osajärjestelmä, joka mahdollistaa digitaalisen tiedon siirtymisen järjestelmään. Esimerkkejä taktisella tasolla olevista rajapinnoista ovat erinäiset viestivälineet ml. radiot ja puhelimet. Lisäksi kyberille tavanomainen usb-media tai vähemmän tavanomainen suora vaikuttaminen ovat mahdollisia. Suoralla vaikuttamisella tarkoitan järjestelmään rakennettujen rajapintojen ohittamista, esimerkiksi aiheuttamalla häiriö gyroskooppiin tärisyttämällä sen koteloa.

”Elektroninen sodankäynti” (ELSO) on ”sähkömagneettisen spektrin hyväksikäyttöä oman sodankäynnin edistämiseen ja vihollisen sodankäynnin edellytysten heikentämiseen. Sähkömagneettista spektriä hyväksikäyttävät tiedustelu-, valvonta-, johtamis- ja asejärjestelmät eivät sinänsä ole osa elektronista sodankäyntiä. Elektronisesta sodankäynnistä on kyse silloin, kun sähkömagneettisen spektrin avulla pyritään edistämään tai haittaamaan näiden järjestelmien toimintaa tai saamaan niistä tietoja.” [68]

”Lennokin torjunta” on tässä tutkimuksessa toimintaa, jonka tavoitteena on kaapata tai tuhota lennokki tai estää siltä ilmatilan vapaa käyttö. Lennokin torjunnassa käytetty järjestelmä on ”Lennokintorjuntajärjestelmä” (C-UAS, Counter Unmanned Aerial System).

”Lentotukikohta” on tässä tutkimuksessa Ilmavoimien päätukikohta, jossa on normaalioloissa myös siviililentotoimintaa. Tämä rajaa pois tilapäisesti siviililentokentille tai varalaskupaikoille perustettavat tukikohdat. Tukikohdan tarkoituksena huoltaa, aseistaa ja tankata lentokoneita ja tuottaa tämän toiminnan vaatima suoja.

1.2. Tutkimustehtävä

Tutkimuksen tavoitteena on selvittää miten kyberelektronisia menetelmiä voidaan käyttää lennokkien torjunnassa. Tämän selvittämiseksi vastataan seuraaviin kysymyksiin lennokkien torjunnan kontekstissa:

1. Miten lentotukikohdan suojaamiseen soveltuvien C-UAS järjestelmien toiminnallisuuksia voi hyödyntää osana kyberelektronista vaikuttamista? Kysymykseen vastataan kirjallisuusselvityksellä.

2. Millaisia elektronisen sodankäynnin keinoja on käytetty soveltuvissa C-UAS järjestelmissä? Kysymykseen vastataan kirjallisuusselvityksellä. Tarkasteluun valitaan kolme kaupallista järjestelmää, jotka poikkeavat toisistaan topologiansa tai toimintatapansa puolesta.
    - AIRFENCE, kybervaikutus ohjaussignaaliin uhkakirjaston perusteella, sekä GNSS ja ohjauslinkin häirintä. Perustuu useaan samanarvoiseen asemaan.[97]
    - Drone Dome, ohjauslinkin häirintä tai elektroninen tuhoaminen laserilla. Monostaattinen.[58]
    - GUARDION, GNSS ja ohjauslinkin häirintä, ohjaus- ja videosignaalin nauhoitus, wlan-disconnect ja elektroninen tuhoaminen HPM-aseella. Koostuu eriarvoisista asemista, joita ohjataan keskitetysti.[69]

3. Millaisia keinoja voidaan käyttää kybervaikuttamisessa, kun kohteena on kaupallinen lennokki tai kauko-ohjattu ilma-alus? Kysymykseen vastataan menetelmätriangulaation avulla, jossa kirjallisuusselvitystä tuetaan kokeilla. Tilannetta tarkastellaan kolmessa eri tapauksessa:
    - Harraste tai urheilukäyttöön tarkoitettu lennokki, jossa ohjauslinkkinä toimii wlan tai bluetooth. Lennokissa ei ole navigaatiojärjestelmää vaan lennättäminen tapahtuu näköyhteyden ja mobiilisovellukseen välitetyn videokuvan perusteella.
    - Vaihtoehtoisesti ammattilaiskäyttöön soveltuva lennokki, jossa ohjaus tapahtuu laitteen mukana toimitettavalla kauko-ohjaimella. Lennokissa on GPS ja se kykenee välittämään paikkatietoa ohjaimeen.
    - Kauko-ohjattu ilma-alus, jossa ohjauslinkkinä toimii XBee. Ilma-aluksessa on sensorifuusiota hyödyntävä navigointi ja se kykenee välittämään paikka- ja tilatietonsa maa-asemalle

1.3. Aiempi tutkimus

Lennokkien aiheuttamaa uhkaa on tutkinut Aki Tornianen Poliisi ammattikorkekorkeakoululle tekemässää opinnäytetyössä ”Drone-uhka - Miehittämättömien lennokkien valvonta ja torjunta”.[103] Opinnäytetyössä on jonkin verran salassa pidettäviä osioita, mutta se antaa hyvän kuvan uhasta ja poliisin toimintavaltuuksista tutkielman kirjoittamishetkellä.

Ilma-alukseen kohdistuvaa kyberuhkaa on tutkinut Antti Kortelainen Maanpuolustukorkeakoulun Sotatekniikan laitokselle laatimassaan pro gradu -tutkielmassa ”Ilma-alukseen kohdistuva kyberuhka”.[67] Kortelasisen tutkielma pohjustaa tässä tutkielmassa tarpeellista ilmailullista näkökulmaa kyberiin, vaikka Kortelainen tutkiikin aihetta miehitettyjen ilma-alusten näkökulmasta.

Lennokkien kyberhaavoittuvuuksia on tutkinut Nils Rodday Twenten yliopistolle tekemässään pro gradu tutkielmassaan ”Exploring security vulnerabilities of unmanned aerial vehicles”. Tutkielman pääpaino on XBee- ja WiFi-haavoittuvuuksien tutkimiessa tietyn lennokkimallin tapauksessa.[93] Roddayn tutkielma paljastaa joidenkin turvallisiksi koettujen ominaisuuksien tuovan vain näennäistä turvallisuutta, sillä niissä on merkittäviä teknisiä haavoittuvuksia. Tämä tutkielma lainaa Roddayn tutkielman rakenteesta ja menetelmistä ja pyrkii arvioimaan hänen menetelmiensä soveltuvuutta osana kyberelektronisia menetelmiä.

Sotilaallisten tutkimusten ja raporttien ulkopuolella ei välttämättä tehdä eroa kyber- ja elektronisen sodankäynnin menetelmien välillä, vaan molemmat mielletään osaksi sähkömagneettisia menetelmiä. Esimerkiksi Le Wang [113] ja Charlampos Kaplanis [61] käsittelevät molemmat omissa tutkielmissaan elektronista häirintää ja langatonta kybervaikuttamista osana vaikuttamista OSI-mallin alempiin kerroksiin tekemättä eroa niiden välille. Erottelu on usein haastavaa, kuten tässäkin tutkielmassa on havaittu, sillä automaattisten järjestelmien häirinnällä saadaan järjestelmän logiikka tuottamaan hyökkääjälle edullinen toiminta.

1.4. Tutkimusmenetelmä ja rakenne

Tässä tutkielmassa käytetty pääasiallinen tutkimusmenetelmä on integroiva kirjallisuuskatsaus. Integroiva kirjallisuuskatsaus on kuvailevan kirjallisuuskatsauksen orientaatio, jossa ilmiötä tarkastellaan mahdollisimman monipuolisesti ilman aineiston systemaattista seulontaa [94].

Tutkielman toisessa pääluvussa käsitellään lennokkien määritelmiä, niiden aiheuttamaa uhkaa ja niiden käyttämiä sensoreita. Luku tukee johdannossa esitettyjä rajauksia ja perustelee miksi lennokkien torjunta on tarpeellista.

Kolmannessa pääluvussa tarkastellaan olemassa olevien kaupallisten C-UAS järjestelmien soveltuvuutta lentotukikohdan suojaamiseen. Kohdetukikohdaksi on valittu Rissalan tukikohta Siilinjärvellä. Tukikohta jakaa kiitotiealueen Kuopion lentoaseman kanssa, jolloin alueella on myös siviililentoliikennettä. Soveltuvuuden arviointi tukee ensimmäiseen alatutkimuskysymykseen vastaamista paljastaen järjestelmien rajoitteita. Lisäksi luku vastaa toiseen alatutkimuskysymykseen.

Neljännessä pääluvussa käsitellään kybervaikuttamista kaupallisiin lennokkeihin. Luvun rakenne noudattaa kolmannen alatutkimuskysymyksen jaottelua. Käsitellyistä ohjauslikeistä XBee:n haavoittuvuuksia on aiemmin tutkittu osana lennokkiin kohdistuvaa kybervaikuttamista. WLAN:in haavoituvuuksia on tutkittu laajasti [113, 61, 109], mutta tutkimuksen osana tunnettujen menetelmien soveltuvuus lennokkeja vastaan varmennetaan kokeellisesti käyttäen kahta eri periaatteella toimivaa lennokkia. XN297LBW-sirun ja sen käyttämän protokollan haavoittuvuuksista ei ole tutkimuksia, mutta sen toimintaa on selvitetty foorumeilla ja GitHubista[92] löytyvässä projektissa. Tässä tutkielmassa selvitetään mahdollisia kybervaikuttamisen menetelmiä hyödyntäen ohjelmoitavaa radiopiiriä ja HackRF-ohjelmistoradiota. Kokeiden tavoitteena on selvittää hyökkäyksen periaatteita, jotta niistä voidaan vetää laajempia johtopäätöksiä tämän tyyppiseen ohjauslinkkiin vaikuttamisesta.

Viidennessä pääluvussa käsitellään elektronisen sodankäynnin ja kybermenetelmien yhteensovittamista toisiaan tukevalla tavalla. Luku on jaettu viiteen eri tavoitteeseen, jotka ovat tiedon kerääminen, kaappaaminen, ilmatilan käytön estäminen, lentoon puuttuminen ja tuhoaminen. Näistä on löydetty tai rakennettu esimerkkitapauksia. Luku vastaa ensimmäiseen alatutkimuskysymykseen.

Kuudennessa pääluvussa kirjataan raportin johtopäätökset, esitetään arvio luotettavuudesta sekä tutkimuskritiikki ja luetellaan tutkielman seurauksena syntyneitä uusia tutkimusongelmia.

1.5. Rajaukset

Tutkimus kartoittaa mahdollisia hyökkäyksellisiä keinoja, joissa yhdistyy sekä kyber-, että ELSO-menetelmiä. Pääasiallinen vaikuttaminen tapahtuu kyberin keinoin, jolloin sitä tuetaan elektronisella tiedustelulla ja vaikuttamisella. ELSO-menetelmät ovat teknisesti niitä, joita on hyödynnetty tutkielmaan valituissa järjestelmissä, mutta niitä voidaan käyttää alkuperäisestä käyttötarkoituksesta poikkeavalla tavalla.

Elektronisen vaikuttamisen keinoihin kuuluvat tässä tutkielmassa sekä kyberaseen toimittaminen, että sen toiminnan edistäminen. Tällaisia keinoja ovat esimerkiksi MitM- (Man in the Middle) ja spoofinghyökkäysten mahdollistaminen heikentämällä alkuperäistä ohjaussignaalia. Elektronisella vaikuttamisella voidaan myös estää vastustajaa reagoimasta kybervaikutukseen estämällä yhteys lennokkiin kokonaan. Näin voidaan estää vastustajaa ohjaamasta ennalta ohjelmoitua reittiä lentävää lennokkia, jos reittiä on onnistuttu muuttamaan kyberin keinoin.

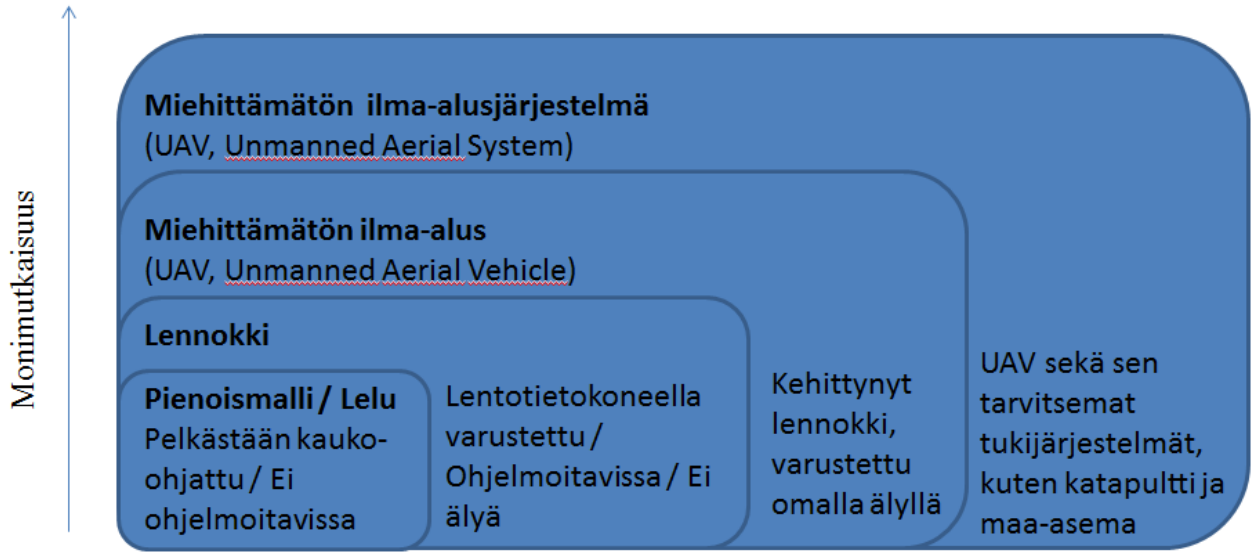
Elektronisen tiedustelun osalta tutkielma on rajattu käsittelemään tilanteita, joissa se hyödyntää kyberiä. Tässä tulee kyseeseen elektroninen maalinosoitus kyberhyökkäyksen seurauksena syntyvään säteilyyn. Myös ohjaus- ja videolinkkien tiedustelu ja nauhoittaminen voi tapahtua elektronisen tiedustelun keinoin.

Tutkimuksen kohteeksi on valittu kaupalliset lennokit, sillä niiden aiheuttamasta uhasta on jo kokemuksia. Sotilaslennokeista on saatavilla huomattavasti vähemmän teknistä tietoa jolloin niiden tutkimisesta saatavat johtopäätökset ovat vaikeammin yleistettävissä kuin kaupallisten lennokkien osalta. Lähdemateriaaliin voi lisäksi liittyä eettisiä ja lainsäädännöllisiä ongelmia. Esimerkiksi kyseeseen voi tulla rikoslain 12. luvun §9 luvaton tiedustelutoiminta tai 32 luvun §1 kätkemisrikos[125]. Lisäksi, varastetun dokumentin tietoja ei välttämättä voi vahvistaa muista lähteistä. Esimerkiksi MQ-9A Reaper-lennokin huolto-ohje, joka maksaisi 150-200$ ja sisältää teknisiä yksityiskohtia [7], on pohjimmiltaan epäluotettava lähde, sillä Yhdysvallat ei ole julkaissut sen sisältämiä tietoja.

2. Lennokki

2.1. Lennokkeja koskevat määritelmät

Lennokki terminä on haastava, sillä se voi tarkoittaa mitä vain paperilennokista miehittämättömään rynnäkkökoneeseen. Tämä skaala jättää lisäksi kokonaan huomioimatta, että merkittävä osa kaupallisista lennokeista on liitteen 1 perusteella koptereita. Englannin kielessä käytetään termiä ”drone” kuvaamaan lennokkeja. Samaa termiä käytetään kuitenkin myös maalla ja vedessä liikkuvista laitteista. Suomenkielessä on käytetty termiä ”drooni” ainakin lennokeista [15]. Puolustusvoimissa käytetään lyhennettä RPAS kuvaamaan miehittämätöntä ilma-alusta, joka voi olla uhka - esimerkiksi lauseessa ”Toimita havaittaessa Puolustusvoimien alueella RPAS”. Koska kyseessä ei todennäköisesti ole miehittämättömän ilma-aluksen kokonaisjärjestelmä, sillä tämä vaatisi myös maa-aseman näkemisen, viitataan lyhenteellä ilmeisesti riittävän monimutkaiseen ilma-alukseen.



Kuva 3 Lennokkien luokittelu monimutkaisuuden perusteella [93]

Lennokkien autonomian astetta pyritään kuvaamaan käyttämällä eriasteisia termejä. Kuvassa 3 esitetty luokittelu on käännökseni Nils Roddayn luokittelusta, joka on vuodelta 2010. Termistö on muuttunut selkeästi, sillä RPA ja RPAS ovat korvanneet UAV ja UAS termit. Kaupalliset lennokit ovat jo nyt lähtökohtaisesti korkeimmalla tasolla, sillä niissä on lentotietokone ja tietty määrä älyä, esimerkiksi NFZ(No Flight Zone)-ominaisuus, joka estää tahattoman toiminnan ilmailun rajoitusalueilla. Olen kääntänyt alkuperäisessä kuvassa olleen termin ”Drone” lennokiksi.

Taulukko 1 lennokkeihin liittyviä keskeisiä käsitteitä

RPA, Remotely Piloted Aircraft, Kauko-ohjattu ilma-alus	Miehittämätön ilma-alus, jota ohjataan kauko-ohjauspaikasta ja käytetään lentotyöhön [104]
RPAS, Remotely Piloted Aircraft System, Kauko-ohjatun ilma-aluksen kokonaisjärjestelmä	Tarkoittaa kauko-ohjattua ilma-alusta, sen kauko-ohjauspaikkoja, tarvittavia ohjaus- ja seurantayhteyksiä ja muita erikseen määrättyjä ilma-aluksen käytön edellyttämän järjestelmän osia [104]
Lennokki	Lentämään tarkoitettu laite, jonka mukana ei ole ohjaajaa ja jota käytetään harraste tai urheilutarkoitukseen pois lukien leluilma-alukset, jotka on suunniteltu käytettäväksi joko yksinomaan tai osaksi alle 14-vuotiaiden lasten leikeissä. [104]
Lentotyö	Ilma-aluksen käyttö erikoistehtäviin [104]

Tässä tutkielmassa käytetään termiä ”lennokki” kuvaamaan kaikkia miehittämättömiä tai vaihtoehtoisesti miehitettyjä ilma-aluksia riippumatta niiden autonomian asteesta. Kyberelektronisten menetelmien kannalta monimutkaisempi järjestelmä mahdollistaa useampia hyökkäysvektoreita. Toisaalta yksinkertaisimmissa järjestelmissä ei välttämättä ole mukana turvallisuusominaisuuksia. Koska rajanveto ei ole aina selkeä ja menetelmien teho perustuu käytettäviin teknologioihin, on mielekkäämpää käyttää termiä lennokki ja jaotella vaikuttamismahdollisuudet teknologioiden mukaan.

Taulukko 2 lennokkien luokittelu lentoteknisten ominaisuuksien perusteella [108]

Lyhenne	Luokitus	Paino (kg)	Kantama (km)	Lentokorkeus (m)	Lentoaika (h)
µ	Micro	<5 / ~0,1**	<10	250	1
Mini	Mini	<20/25/30/150* / 30**	<10	150*	<2
CR	Close Range	25-150	10-30	3 000	2-4
SR	Short Range	50-250	30-70	3 000	3-6
MR	Medium Range	150-500	70-200	5 000	6-10
MRE	MR Endurance	500-1500	>500	8 000	10-18
LADP	Low Alt. Deep Penetration	250-2500	>250	50-9 000	0,5-1
LALE	Low Alt. Long Endurance	15-25	>500	3 000	>24
MALE	Medium Alt. Long Endurance	1000-1500	>500	5/8 000	24-48
HALE	High Alt. Long Endurance	2500-5000	>2000	20 000	24-48
Strato	Stratospheric	>2500	>2000	>20 000	> 48
EXO	Exo-stratospheric	TBD	TBD	>30 500	TBD
UCAV	Unmanned Combat Aerial Vehicle	>1000	+/- 1500	12 000	+/- 2
LET	Lethal	TBD	300	4 000	3-4
DEC	Decoy	150-500	0-500	50 - 5 000	<4

*Kansallisen lainsäädännön mukainen raja [108] Suomessa 25kg [104]

**[18]

Lennokkien luokittelu niiden lentoteknisen suorituskyvyn mukaan antaa oletettua autonomian astetta paremman kuvan mahdollisista vaikuttamiskeinoista. Taulukossa 2 on mustalla viivalla erotettu pelkästään sotilaskäyttöön tarkoitetut lennokit, mutta myös viivan yläpuolella olevia voidaan käyttää eriasteiseen tiedusteluun ja vaikuttamiseen. Tässä tutkielmassa termi ”lennokki” viittaa Micro- ja Mini-luokan lennokkeihin.

2.2. Lennokkien aiheuttama uhka miehitetylle ilma-alukselle

University of Dayton Research Institute julkaisi 13.9.2018 blogikirjoituksen koskien tutkimusta, jossa DJI Phantom 2 törmäytetään Mooney M20 -lentokoneen siipeen noin 206 solmun nopeudella. Törmäys aiheuttaa rakenteellisia vaurioita siiven tukirakenteisiin ja eroaa siten lintutörmäyksestä, jossa vahinko on vain pinnallista. Lintutörmäys aiheuttaa kuitenkin laajemman näkyvän vaurion siiven johtoreunaan. [81] DJI vaati kirjoituksen ja siihen liittyvän videon poistamista, sillä tutkimuksen menetelmiä ei ole julkaistu ja viittasi ASSURE:n tekemään tutkimukseen, jonka tulokset ovat luotettavampia. DJI kritisoi myös epärealistisen korkeaa nopeutta, jolla lennokki törmäytetään pienkoneen siipeen ja syytti tutkimusta pelkoa lietsovaksi.[38]

ASSURE:n tutkimuksessa selvitetään simuloimalla sekä kiinteäsiipisten lennokkien, että nelikopterien aiheuttamaa riskiä ilma-aluksille. Lennokkien mallit perustuivat Precision Hawk Lancaster Hawkeye Mark III ja DJI Phantom 3 -lennokkeihin, joiden massat ovat noin kaksi ja yksi kiloa. Kohdeilma-aluksista on luotu kaksi mallia. Ensimmäinen on geneerinen matkustajakone, joka perustuu Boeing 737 ja Airbus 320 tuoteperheisiin. Toinen malli perustuu Learjet 31A lentokoneeseen ja edustaa tutkimuksessa liikesuihkukonetta. Tulosten perusteella haavoittuvaisimpia kohteita ilma-aluksessa ovat pystyvakaaja ja evä. Moottori kestää törmäyksiä hyvin. Tuulilasille aiheutuva uhka on suurempi kiinteäsiipisten lennokkien osalta. Kiinteäsiipiset lennokit ovat rakenteille vaarallisempia kuin nelikopterit, mutta merkittävästi paloturvallisempia. Rakenteille vaarallisimpia komponentteja ovat akku, kamera ja moottorit, jotka ovat keskimäärin tiheämpiä ja siten painavampia kuin lennokkien rungon osat. Akku aiheuttaa lisäksi merkittävän paloriskin puhjetessaan.[8]

Kaava 1 Kiinteäsiipisen ilma-aluksen lentämiseen vaatima teho

$$P = \frac{1}{2}\rho_{ilma} * {v_{lento}}^3 * A_{siivet} * C_{D_0} + \frac{2 * {m_{ilma-alus}}^2 * g^2}{\rho_{ilma} * v_{lento} * \pi * {L_{siivet}}^2}$$

Kaavasta 1 voidaan laskea teho, jonka kiinteäsiipinen lennokki vaatii pysyäkseen ilmassa. Kaava on avattu tarkemmin liitteessä 4. Käytettäessä parhaita mahdollisia akkuja, joiden tehopainosuhde on noin 260 wattituntia per kilogramma [106], voidaan arvioida lennokin vaatimien akkujen massaa. Esimerkiksi 2 kilogrammaa painava 150 metrin korkeudella toimiva lennokki tarvitsee tämän perusteella noin 91 grammaa akkuja saavuttaakseen tunnin toiminta-ajan, jos sen siipien kärkiväli on metrin ja lentonopeus 15 metriä sekunnissa, mikä on noin 54 kilometriä tunnissa. Tämä on parempi painosuhde kuin nelikopterissa.

Kaava 2 Helikopterin leijumiseen vaadittava teho

$$P = \frac{{m_{ilma-alus}}^{1,5} * g^{1,5}}{\sqrt{2\rho * A_{roottori}}}$$

Esimerkiksi noin puoli kiloa painavan JJPRO HAX3 nelikopterin akku painaa koteloineen mittauksen perusteella 106 grammaa. Sen toiminta-aika on parhaimmillaan 17 minuuttia[59]. Vastaavasti ASSURE:n mallissa käytetyn noin kilon painoisen Phantom 3 nelikopterin akku painaa 363 grammaa ilman koteloa, eli nelikopterinkin tapauksessa painon kaksinkertaistuminen vaatii noin kolme kertaa enemmän akkuja. Tämä vastaa kaavassa 2 esitettyä leijumisen vaatimaa tehoa, jossa painon eksponentti on 1,5, jolloin kaksi kertaa painavampi ilma-alus vaatii 2,8 kertaa enemmän tehoa leijumiseen. Myös tämä kaava on avattu tarkemmin liitteessä 4. Phantom 3:n käytännön toiminta-aika on parhaimmillaan 25 minuuttia [phanom3, s. 6], mikä on noin 47% pitempi lentoaika, kuin puolet kevyemmällä HAX3-lennokilla. Kun otetaan huomioon sekä suurempi paino, että lentoaika, olisi saman laatuisen akun painosuhde oltava 4,27. Tällöin, HAX3 akun painoksi ilman koteloa tulisi 85 grammaa. 106 gramman akkukokoonpanosta kotelon paino olisi tällöin 21 grammaa, mikä vaikuttaa korkealta, vaikka kotelossa on mukana myös elektroniikkaa. Muita tehoon vaikuttavia tekijöitä ovat roottorin koko ja muotoilu, sekä mahdolliset lennokin sisäiset tehohäviöt. Näistä kaavassa 2 on huomioitu vain roottorien tehollinen kokonaispinta-ala.

Vaikka nelikopterin painavampi akku aiheuttaa isomman vaaran ilma-aluksille sekä massansa että paloriskinsä seurauksena, on vähentää nelikopterin rajallisempi toiminta-aika uhan kestoa. Riskeistä huolimatta yhtään ilma-alusta ei ole tuhoutunut törmäyksessä nelikopterin kanssa eikä niistä johtuvat lennon keskeytykset ole tutkimuksen tekohetkellä vielä johtaneet vakaviin onnettomuuksiin. Kiinteäsiipisten lennokkien törmäyksiä ei ole tutkimuksen tekohetkellä uutisoitu lainkaan.

Yhdistettynä siihen, että kiinteäsiipinen lennokki aiheuttaa isomman riskin ilma-aluksen rakenteille, pitemmällä toiminta-ajalla varustettu kiinteäsiipinen lennokki vaikuttaa tehokkaammalta työkalulta lentotoiminnan häirintään.

Kauko-ohjatut järjestelmät aiheuttavat luonteensa vuoksi uhan myös elektronisessa toimintaympäristössä. Euroopan talousalueella myytävien lennokkien on täytettävä Euroopan Unionin EMC-direktiivin vaatimukset, sekä oltava Kansainvälisen Televiestintäliiton (ITU, Intenational Telecommunication Union) yleissopimuksen mukainen [45]. Tästä syystä Kaupallisten lennokkien käyttämät taajuudet eivät lähtökohtaisesti aiheuta häiriötä ilmailussa käytettäville taajuuksille. ITUn yleissopimuksessa ilmailulle on tarkoituksella varattu erilliset taajuudet kaupallisista telelaitteista, jotta lentoturvallisuus ei vaarantuisi [55].

Taajuusalue	Käyttötarkoitus
Alle 30MHz	AMS (Aeronautical Mobile Service), NDB(Nondirectional Beacon)
108 – 117.975 MHz	ILS(Instrumental Landing System), VOR(VHF Omnidirectional Radar), GBAS(GNSS Ground-Based Augmentation System)
117.975 – 137 MHz	AMS (mm. lennonjohto), Ilmailun hätätaajuus (121,5Mhz)
960 – 1 215 MHz	DME (Diretion Meassurement Equment)
5 030.4 – 5 150.0 MHz	MLS (Microwave Landing System)

Ilmailussa käytettävät taajuudet [55]

2.3. Lennokkien aiheuttama uhka operaatioturvallisuudelle

Operaatioturvallisuus on prosessi, jossa tunnistetaan kriittinen informaatio ja analysoidaan omaa toimintaa. Operaatioturvallisuus kiistää vastustajalta kriittisen informaation ja mahdollisuuden arvioida toimintaa ja sen tavoitteita indikaattoreiden perusteella.[116] Koska kyseessä on nimenomaan informaation suojaus, määritelmään ei voida liittää suorituskykyjä tai infrastruktuuria, kuten esimerkiksi ilmaoperaation tarvitsema kiitotie.

Samuli Pietiläinen tekee pro gradu tutkielmaa taktiikan laitokselle multikoptereiden aiheuttamasta uhasta lentotukikohdalle. Alustavien tulosten perusteella voidaan todeta, että multikopterit aiheuttavat uhan myös operaatioturvallisuudelle. Pietiläisen tutkielman turvaluokka on ”käyttö rajoitettu”.[90] Tulosten tarkempi avaaminen ei siksi ole tämän tutkimuksen käytettävyyden kannalta mielekästä.

2.4. Sensorit ja niiden fuusio lennokeissa

Sensorifuusio mahdollistaa lennokin turvallisen käyttämisen. Nelikopterin leijunta edellyttää, että roottorit vetävät täsmälleen siihen vaikuttavia voimia vastaan, muutoin nelikopteri ei pysy paikallaan. Painovoiman lisäksi tuuli ja roottorien aiheuttamat pyörteet voivat aiheuttaa leijuntaa haittaavan voiman. Kiinteäsiipisten lennokkien osalta lennokin asento vaikuttaa siipien luomaan nosteeseen ja ohjauspintojen vaikuttavuuteen. Esimerkiksi siipien kohtauskulma vaikuttaa siivekkeiden toimintaan, jolloin kohtauskulman kasvaessa riittävästi kallistuksen muuttaminen hidastuu.

Liitteen 1 lennokeista kaikista laajin sensoripaketti on Autel Robotics EVO:ssa, jossa hyödynnetään barometria, kiihtyvyysantureita, gyroskooppeja, elektronista kompassia, optisia sensoreita ja akustisia sensoreita. Lisäksi siinä on sekä GPS, että GLONASS vastaanotin jolloin sensorifuusiossa voidaan periaatteessa hyödyntää useampaa satelliittipaikannusjärjestelmää. Lennokeissa käytetyt anturit ovat todennäköisesti MEMS-antureita (Micromechanical systems) niiden edullisen hinnan ja pienen koon vuoksi.

Yhdistelemällä sensorien tuottamaa tietoa ja suodattamalla mittauksia saadaan lennokista parempaa tila- ja paikkatietoa. Tämä myös lisää häiriönkestävyyttä, jos esimerkiksi GNSS-paikannusta ei ole käytettävissä, mutta lennokin on kuitenkin säilytettävä vakautensa.

Tarkkaa paikkatietoa yhdistettynä kuviin voidaan käyttää kohteen kartoittamiseen tai jopa 3D-mallintamisen. Tähän on olemassa pilvipohjainen ratkaisu, jolloin lennokin järjestelmiä käytetään automatisoidusti datan keräämiseen ja varsinainen kartoitus tai mallintaminen tapahtuu pilvessä.[126; 127]

2.4.1. Barometri

Barometri mittaa lennokkiin kohdistuvaa ilmanpainetta. Koska ilmanpaine vähenee ennustettavalla tavalla korkeuden kasvaessa, voidaan barometrilla mitata korkeuden eroa lähtötilanteeseen. MEMS-barometrin toiminta perustuu joko piestoresisitiiviseen materiaaliin tai kapasitanssin muutokseen. Molemmissa tapauksissa mitataan ulkoisen paineen aiheuttamaa muodonmuutosta sähköä johtavaan kalvoon, joka sulkee joko tyhjiön tai vertailupaineessa, esimerkiksi vakiopaine, olevan kammion. Lämpötila vaikuttaa sensorin toimintaan muuttaen kalvon sähkönjohtavuutta ja vertailupaineessa olevan kaasun tilavuutta. Tämän vuoksi sensori on kalibroitava eri lämpötiloihin ja sen mittaustulosta korjattava lämpötilan mukaisesti. [14] Normaalipaine merenpinnan tasolla on noin 1013 hehtopaskalia, mutta käytännössä ilmanpaine voi vaihdella 37 hehtopaskalia molempiin suuntiin. Merenpinnan tasolla suuremmat vaihtelut ovat poikkeuksellisia. Matalilla korkeuksilla yhden hehtopaskalin muutos vastaa noin 8 metrin muutosta korkeudessa.

2.4.2. Kiihtyvyysanturi

Kiihtyvyysanturi on jouseen kiinnitetty tunnettu massa, joka on kapasitaattorin kantojen välissä, massan inertia jousivoimaa vastaan on seurausta newtonin ensimmäisestä laista ja sijainnin muuttuminen muuttaa kapasitaattorin ominaisuuksia. Vaihtoehtoisesti liike voidaan mitata pietsoresistiivisesti. Tällöin jousessa on oltava pietsoresistiivistä materiaalia, jonka resistiivisyys muuttuu jousen muuttaessa muotoaan. Resonanssin vähentämiseksi massa on yleensä öljyssä tai kaasussa. [64]

2.4.3. Gyroskooppi

Perinteisessä gyroskoopissa pyörivä massa on akseloitu niin, että sillä on kolme vapausastetta. Tällöin se kykenee säilyttämään pyörimisliikkeen, vaikka gyroskoopin alustan tila muuttuisi. Tämän kaltainen laite on altis mekaaniselle kulumiselle jonka vuoksi nykyaikaisemmat gyroskoopit ovat optisia. [64]

Optisten gyroskooppien tapauksessa vaihtoehtoina ovat laser-gyroskooppi ja kuituoptinen gyroskooppi. Lasergyroskoopissa mitataan kahden vastakkaisen lasersäteen erotusta ja kuituoptiset valon kulkua eri suuntiin kuitusilmukassa. Optiset gyroskoopit ovat kuitenkin edelleen suurikokoisia ja kalliita. [64, s. 13]

MEMS-gyroskooppi on kaikista yleisin gyroskooppi johtuen sen pienestä koosta ja edullisesta hinnasta. Sen toiminta perustuu edestakaisin värähtelevän massaan, jolloin coriolisvoima virittää resonanssin kohtisuoraan värähtelyn suuntaan nähden, jos kulmataajuus nousee värähtelyn suunnassa. Korkeampi värähtelyn amplitudi parantaa mittaustarkkuutta. Lämpötila vaikuttaa mittaukseen, jolloin anturi on kalibroitava eri lämpötiloille ja tämä on huomioitava mittauksien tulkinnassa.[64]

2.4.1. Elektroninen kompassi

Elektronisen kompassin toiminta perustuu Maan magneettikentän suunnan mittaamiseen. Magnetometri on laite, jolla voidaan mitata magneettikentän voimakkuutta tai magneettivuon tiheyttä. Magnetometri voi perustua Hall-ilmiöön tai magnetoresistiiviseen materiaaliin. Näiden kahden tyypin lisäksi on olemassa erinäisiä käämeihin perustuvia antureita magneettikentän mittaamiseen. Näistä mainittakoon pyörivä käämi, magnetoinduktiivinen anturi ja fluxgate-magnetometri.

Hall-ilmiöön perustuvassa anturissa levyn muotoisen virtajohtimen ollessa kohtisuoraan magneettikenttään nähden, syntyy levyn reunojen välille jännite. Tämän niin kutsutun Hall-jännitteen suuruus riippuu sekä magneettivuon tiheydestä että levyn muotoisessa johtimessa kulkevan virran suuruudesta.[80, s. 14]

Magentoresistanssiin perustuvassa anturissa johtimen resistanssi muuttuu siihen vaikuttavan magneettikentän vaikutuksesta. Resistanssin mittaaminen on suhteellisen helppoa, jolloin anturi on pienikokoinen ja edullinen. [71, s.12]

Pyörivään käämiin indusoituu sinimuotoinen jännite. Käämin ei varsinaisesti tarvitse pyörähtää kokonaista kierrosta, vaan riittää, että se värähtelee. Indusoituva jännite on verrannollinen magneettikentän voimakkuuteen. [71, s.11]

Magnetoinduktiivisessa anturissa ferromagneettisella sydämellä varustettuun käämi liitetään osaksi oskillaattoripiiriä. Koska ulkoinen magneettikenttä muuttaa sydämen permeabiliteettia, muuttuu kelan induktanssi magneettikentän muuttuessa. Tämä voidaan mitata oskillaattoripiirin taajuuden muutoksesta.[71, s. 13]

Fluxgate-anturissa kahdella käämillä on yhteinen sydän. Sisempään käämiin johdetaan sinimuotoinen virta, jolloin sen herätesignaali indusoituu ulompaan kelaan säröytyneenä. Säröytymisen epäsymmetrisyydestä voidaan päätellä magneettikentän voimakkuus ja suunta. [71, s.13]

2.4.2. Optiset sensorit

Optiset sensorit voidaan jakaa passiivisiin ja aktiivisiin sensoreihin. Passiivisia sensoreita ovat esimerkiksi kamerat ja valoisuussensorit. Aktiivisia sensoreita ovat ensimerkiksi laserkeilain ja infrapunaestesensori.

Kamera on suhteellisen monipuolinen sensori. Ihminen kykenee kameran kuvan perusteella arviomaan lennokin asentoa ja jopa lentosuuntaa. Yhdistettynä konenäköön lennokin välittämän videon perusteella voidaan ehkäistä lennonkin törmääminen paikallaan oleviin tai liikkuviin esteisiin [74]. Liitteen 1 perusteella alaspäin katsova kamera on suhteellisen yleinen sensori leijumisen vakauttamiseen ja tarkkuuslaskeutumiseen. Kameran tuottaman tiedon hyvyyttä voidaan arvioida valoisuussensorilla, jolloin esimerkiksi konenäköalgoritmi voidaan kytkeä pois käytöstä valoisuuden tippuessa liian alas. Lisäksi valoisuuden mittaaminen on oleellista kameran valotuksen säätämiseksi.

Laserkeilainta voidaan käyttää etäisyyden mittaamiseen esteistä ja maasta. Tämä toimii erityisen hyvin rakennetuissa ympäristöissä, joissa voidaan olettaa esimerkiksi suorat seinät. Lisäksi laserilla voidaan joissain tilanteissa mitata kuljettua matkaa. [96]

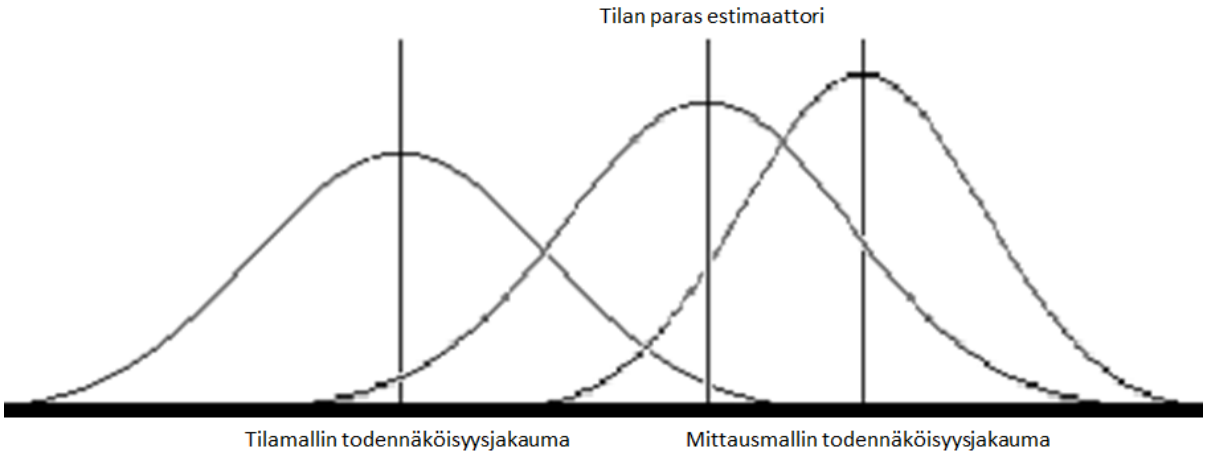
Infrapunaestesensori voidaan ajatella matalan resoluution laserkeilaimeksi. Sensorin tyypistä riippuen se voi mitata vain etäisyyttä maahan tai muodostaa 3D kuvan esteestä sen väistämiseksi [33].

2.4.3. Akustiset sensorit

Ultraäänisensori vaikuttaa liitteen 1 perusteella olevan yleinen korkeuden mittaamisessa käytettävä sensori. Ultraäänisensori voi perustua joko kulkuajan mittaamiseen tai signaalin heikkenemiseen ilmakehän vaikutuksesta[52]. Äänen nopeus vaihtelee vallitsevan paineen, kosteuden ja lämpötilan mukaan enemmän, kuin sähkömagneettisen säteilyn osalta, jolloin tarkkuutta vaativissa tilanteissa sensori on syytä kalibroida[52].

2.4.4. Kalman-suodin

Käytettäessä useampaa sensoria saadaan enemmän mittauksia kuin yksikäsitteiseen paikkaratkaisuun tarvitaan. Tällöin voidaan käyttää suodattimia, kuten Kalman-suodin. Se tuottaa parhaan lineaarisen harhattoman estimaattorin mitattavan systeemin tilalle. Suodin tosin olettaa, että sekä prosessin dynamiikan tilamalli että mittausmalli ovat lineaarisia ja niihin liittyvät alkuehto sekä kohinat ovat normaalijakautuneita. Prosessin dynamiikalla tarkoitetaan prosessin muutosta ajan kuluessa. Tilan paras estimaattori löydetään käyttämällä ehdollisen odotusarvon funktiota. [5]. Ehdollisen odotusarvon muodostamisen periaate on esitetty kuvassa 4.



Kuva 4 Kalman-suotimen tuottaman tilan estimaattorin periaate

Useimmiten systeemi ei ole lineaarinen, jolloin sille ole välttämättä analyyttistä ratkaisua. Muutenkin analyyttinen ratkaisu voi olla monimutkainen ja hidas laskea. Vaihtoehtoisesti systeemi voidaan ratkaista iteratiivisesti. Näille ratkaisutavoille on olemassa omia niin kutsuttuja laajennettuja Kalman-suotimia. [5]

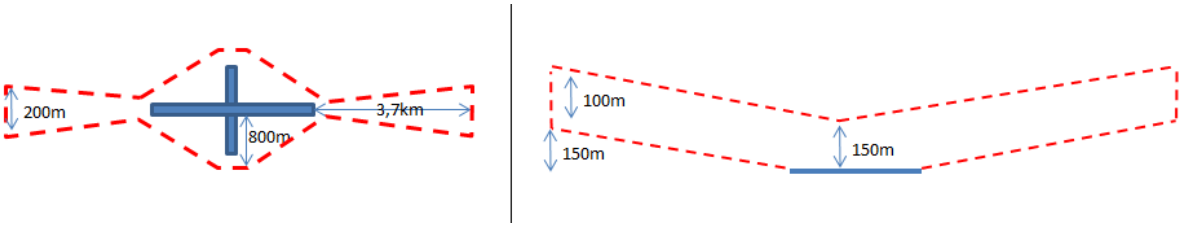
Mallien muokkaamisen sijaan on mahdollista sovittaa tuloksia normaalijakaumaan. Tällöin kyseeseen tulevat hajustamaton Kalman-suodin tai Hiukkassuodin. Hajustamaton perustuu kiinteisiin pisteisiin, joilla arvioidaan jakauman odotusarvoa ja kovarianssia. Hiukkassuodin on kuten hajustamaton, mutta kiinteiden pisteiden sijaan perustuu ”hiukkasiin”, jotka luodaan Monte Carlon menetelmällä ja sovitetaan todennäköisyysjakaumaksi.[62].

Käytettyjen menetelmien perusteella voidaan olettaa, että yleisesti menetelmät on yllä esitelty laskentanopeuden näkökulmasta laskevassa järjestyksessä. Kuitenkin on huomioitava, että useimmissa tilanteissa on pakko käyttää laskennallisesti raskaampaa suodinta. Toisaalta tulosten sovittaminen voi olla mallin muokkaamista tehokkaampaa, jos malli on erityisen monimutkainen tai tulokset ovat helposti sovitettavissa.

Laskennan raskaus voi rajoittaa suotimien käyttöä lennokeissa, sillä tehokkaammat prosessorit käyttävät usein enemmän virtaa. Tällöin rajallinen akkukapasiteetti voi olla houkuttelevampaa suunnata itse lentämisen vaatimaan tehontuottoon ja käyttää sensorifuusiossa yksinkertaisempia malleja.

3. Lennokkien torjunnassa käytettävien järjestelmien esittely

Tässä luvussa esitellään kolme järjestelmää joiden topologia tai toimintatavat eroavat toisistaan. Tavoitteena on arvioida järjestelmien soveltuvuutta Rissalan tukikohdan suojaamiseen tutkimuksen tarkoitukseen luodun riskianalyysin perusteella. Rissalan tukikohta jakaa kiitotiealueen Kuopion lentoaseman kanssa.



Kuva 5 Rissalan tukikohdan suojattava alue (ei mittakaavassa)

Kuvassa 5 on esitetty tässä luvussa käytettävä tukikohdan suojattava alue. Kuopion ILS-lähestymisessä käytettävä liukukulma on 3 astetta[4], mikä tarkoittaa, että enintään 150 metrin korkeudella toimiva lennokki on vaarallinen kiitotien jatkeella aina noin 3,7 kilometriin asti. Liukukulman on laskettu korjausvaraa korkeussuunnassa noin 0,7 astetta, sekä sivuttaissuunnassa noin 1,4 astetta. Kuvassa näkyvä poikkikiitotie on helikopterikäytössä ja niiden käyttämien sääsuojien takia sille ei ole turvallista laskeutua kiinteäsiipisellä koneella. Tämän vuoksi sille ei tarvitse huomioida liukupolkua. Kuopion aidatun kiitotiealueen ympärysmitta on noin 8 kilometriä. Tässä luvussa oletetaan, että kaikki sotilaslentotoiminnan käyttämä infrastruktuuri on tämän aidatun kiitotiealueen sisällä, jolloin operaatioturvallisuuden suojaamiseksi riittää, että lennokkitoimintaan kyetään vaikuttamaan aidatulla kiitotiealueella.

3.1. Airfence

Sensofusionin Airfence järjestelmän toiminta perustuu lennokkien käyttämien taajuuksien passiiviseen seurantaan. Havaitessaan lennokin järjestelmä kykenee paikantamaan ja seuraamaan taajuusalueella 80MHz - 6GHz toimivaa lennokkia sekä tarvittaessa puuttumaan sen lentoon. Havaitsemisetäisyys voi olla jopa 10 km. Lentoon puuttuminen tapahtuu joidenkin lennokkien osalta ohjaamalla lennokki laskuun. Tämä ominaisuus ei välttämättä vaadi käyttäjän toimenpiteitä vaan järjestelmä voi aloittaa vastatoimet automaattisesti. Järjestelmä kykenee myös häiritsemään ainakin 2,4GHz taajuusalueella toimivia lennokkeja. Järjestelmän käyttöliittymä on web-pohjainen ja sen asemilla on tästä syystä oltava jatkuva yhteys internetiin. Järjestelmässä on käytössä mobiili-ilmoitukset, jotka pitävät käyttäjän tietoisena järjestelmän havainnoista ja toimenpiteistä.[97]

Kuva 6 AirFence yksikkö [98]

Airfence on käytössä muun muassa Yhdysvaltojen merijalkaväellä, sekä FAA:lla (Federal Aviation Administration). Näistä jälkimmäinen käyttää järjestelmää lentokenttien suojaamiseen. Eurooppalaisista käyttäjistä mainittakoon Nordic unmanned.[98]

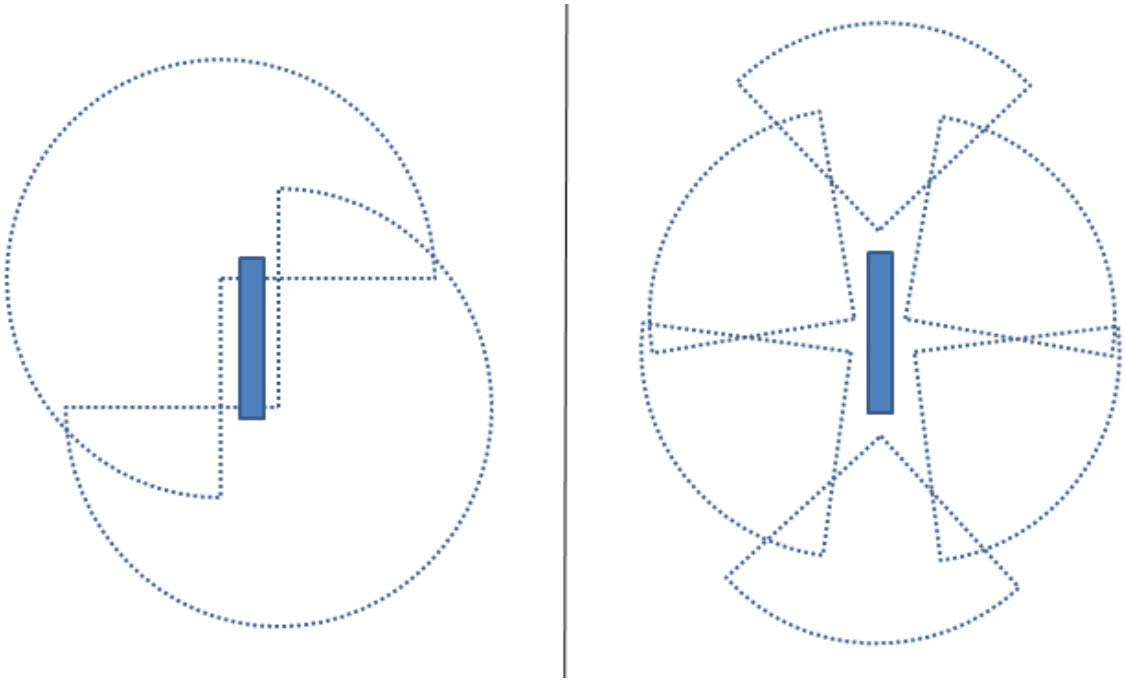
Yhdysvaltalainen Department 13 on kehittänyt vastaavan järjestelmän nimellä MESMER, joka perustuu ohjauslinkin kaappaamiseen ilman häirintää. Sen kaappaus perustuu ohjauspakettien prioriteetin manipulointiin, jossa ohjaimen paketit jäävät alemmalle prioriteetille ja MESMER saa täyden hallinnan. AirFencen tavoin tämän ominaisuuden toiminta perustuu tunnettuihin lennokkimalleihin, jolloin järjestelmän ohjelmistoa on päivitettävä jatkuvasti uusien lennokkien tullessa markkinoille. MESMER:in kantama käytettäessä 2,4GHz taajuutta on 4 kilometriä. AirFencestä poiketen, se kykenee käyttämään myös korkeampaa 5GHz ja alempia 430-435MHz sekä 902-928MHz ISM-taajuuksia.[19]

3.2. Drone Dome

Rafael Andvanced Defense Systemsin Drone Dome -järjestelmä etsii lennokkeja käyttäen aktiivista RADA Innovative Defense Electronicsin RPS-42 pMHR monitoimitutkaa, joka kykenee valvomaan 90 asteen sektorin. Neljällä tutkalla saadaan aikaan 360 asteen valvonta. RPS-42 on S-alueella toimiva AESA-tutka, joka kykenee havaitsemaan lentokoneen 50 kilometrin päästä ja lennokin tyyppillisesti 3,5-10 kilometrin päästä riippuen lennokin tutkapoikkipinta-alasta. Lennokkien tunnistaminen tapahtuu Controp MEOS elektro-optisella/infrapuna (EO/IR) valvontayksiköllä ja Netline NetSense Wideband -valvontasensorilla. NetSense Wideband kykenee valvomaan taajuusaluetta 20MHz-6Ghz. [58]

Kuva 7 DroneDome-asema [58]

Järjestelmän vaikuttaminen koostuu elektronisesta häirinnästä ja tuhoamisesta. Häirintä toteutetaan C-Guard RD-häirintämoduulilla, joka kykenee häiritsemään VHF- ja UHF-taajuuksia jopa 400 watin teholla. Tuhoaminen toteutetaan Rafaelin Lite Beam -laserilla, jonka kantama on noin 2 kilometriä. Laser tähdätään käyttäen Controp MEOS-yksikköä, jonka sensorit on asennettu samaan koteloon laserin kanssa.[58] Saman tyylistä tähtäysratkaisua on käytetty myös pakettiauton kokoisessa Silent Hunter-laserissa, jonka kantama on noin 4 kilometriä. [48] Laserin kantaman lisääminen vaikuttaa lisäävän järjestelmän kokoa merkittävästi.



Kuva 8 DroneDome tutkien kantamat eri topologioilla

DroneDome järjestelmän asemille mahdollista topologiaa ohjaa eniten tutkan rajallinen 90 asteen sektori. Kuvassa 8 on tämä rajallinen sektori huomioiden kaksi eri vaihtoehtoa, jolla asemat voisi sijoitella, jos halutaan suojata sekä kiitotiealue, että kiitotien jatke kolmeen kilometriin asti. Ensimmäinen vaihtoehto on järjestää asemat kahdeksi ryppääksi, jossa kummassakin on kolme asemaa. Tämä vaihtoehto minimoi valvonnan katveet, mutta samalla rajoittaa efektorien käyttöä. Koska kyseessä on modulaarinen järjestelmä, voisi näihin ryppäisiin sijoittaa yhden täydellisen aseman ja kaksi asemaa, joissa on vain tutka ja NetSense sensori. Näin asemien laserit tähtäysjärjestelmineen ja C-Guard-häirintämoduulit olisi mahdollista sijoittaa esimerkiksi suojaamaan kiitotien jatketta. Toisessa vaihtoehdossa tasa-arvoiset asema on sijoitettu erilleen toisistaan. Tämä lisää katveita, mutta mahdollistaa kaikille asemille tehokkaan vaikuttamisen ilman, että niiden moduuleja tarvitsee sijoittaa erilleen. Lisäksi kiitotien lähistölle muodostuvat katveet ovat valvottavissa asemien elektro-optisilla sensoreilla.

3.3. GUARDION

Rohde&Schwarzin, ESG:n(ESG Elektroniksystem- und Logistik-GmbH) ja Diehlin yhteistyössä kehittämä GUARDION on modulaarinen lennokintorjuntajärjestelmä, joka koostuu sensoreista, efektoreista ja johtamisjärjestelmästä. Alkuvaiheen havaitseminen perustuu perävaunuasenteiseen aktiiviseen valvontatutkaan, joka kykenee valvomaan yksinään 360 asteen sektorin. Muita sensoreita ovat akustinen sensori, elektro-optinen/infrapuna-kamera ja ARDRONIS-järjestelmästä kehitetyt sensorit. [69] ARDRONIS-järjestelmä kykenee havaitsemaan, suuntimaan ja tunnistamaan 400 MHz - 5.8 GHz - taajuusalueella toimivan lennokin sen ohjaussignaalin rakenteen perusteella [57]. GUARDION-järjestelmän efektorit ovat WiFi-disconnect -osajärjestelmä, GNSS- ja ISM-häirintälähettimet, sekä HPEM(High Powered Electromagnetic)-osajärjestelmä. HPEM-osajärjestelmä tuottaa voimakkaan sähkömagneettisen pulssin, joka indusoi lamauttavat jännitteen kohdejärjestelmään. Järjestelmää ohjataan TARANIS-johtamisjärjestelmällä, joka esittää tilannekuvaa ja ohjaa efektoreita. Järjestelmään on mahdollista saada mobiili-ilmoitukset, jotka ilmoittavat positiolta poistuneille operaattoreille mahdollista lennokkihavainnoista.[69]

Kuva 9 Guardion-järjestelmä ilman ARDRONIS-asemia [69]

Lentoasemilla on käytöstä poistettuja TAR-tutka-asemia (Terminal Area Radar, lähestymisalueen tutka), joihin sijoitettu GUARDION-järjestelmän tutka kykenisi valvomaan lähialuetta tehokkaasti. Useamman tutkan sijoittaminen alueelle ei ole kannattavaa, sillä ne voivat häiritä toisiaan ja järjestelmän kuvauksessa ei mainita, että johtamisjärjestelmä kykenisi käsittelemään kahden tutkan tietoja. Yhden tutkan tapauksessa kiitotien jatkeita on mahdollisesti valvottava muilla keinoilla, sillä lennokkien pieni tutkapoikkipinta-ala voi lyhentää havaintoetäisyyttä liikaa. Jos molemmille jatkeille sijoitettaisiin kolme ADRONIS-asemaa, saataisiin jatkeet valvottua ja niissä oleviin lennokkeihin vaikutettua. ISM- ja mahdollisesti GNSS-häirintälähettimet riittävät todennäköisesti kiitotiealueen suojaamiseen.

3.4. Yhteenveto järjestelmistä ja matemaattinen tarkastelu

Lennokit aiheuttavat uhan sekä lento- että operaatioturvallisuudelle. Lentoturvallisuuden näkökulmasta mikään tarkastelluista järjestelmistä ei sovellu erityisen hyvin kiitotien jatkeiden suojaamiseen Trafin määrittämään viiteen kilometriin asti. Operaatioturvallisuuden näkökulmasta suojattava alue on pienempi ja siihen jokainen järjestelmä soveltuu. Järjestelmien hinnoista ei ole julkisuudessa tietoa, mutta ottaen huomioon käytetyt teknologiat ja järjestelmien monimutkaisuus, ne on todennäköisesti esitelty nousevassa kustannusjärjestyksessä.

Esiteltyjen järjestelmien elektroniset sensorit vaikuttavat suorituskyvyltään poikkeuksellisen huonoilta suhteessa AirFencen ilmoittamaan 10 kilometrin havaintoetäisyyteen, joka toteutuessaan riittäisi hyvin lentoaseman lähialueen valvontaan. Kuinka herkkä antennin pitäisi olla, jotta se havaitsisi WiFi-kanavalla 100 (5500MHz) toimivan lennokin edes kolmen kilometrin päästä?

Kaava 3 vapaan tilan vaimennus

$$L_f = 32{,}4 + 20 \cdot \log(f_{MHz}) + 20 \cdot \log(R_{km})$$

Vapaan tilan vaimennuksen kaavasta kyseisen tilanteen vaimennus olisi noin 121 desibeliä. Jos lennokin lähettimen teho on 100 milliwattia (20dBm), niin vastaanottimelle saapuva teho on noin 0,1 pikowattia (-100dBm). Tyyppillisen WiFi-tukiaseman herkkyys on -96dBm [113], jolloin se kykenisi havaitsemaan kyseisen lennokin noin kolmen kilometrin päästä. Ei ole epärealistista olettaa, ettei elektronisen tiedustelun sensoreilla päästäisi pitempiin etäisyyksiin. AirFencen ilmoittama 10 kilometrin havaintoetäisyys vaatisi kanavalla 1(2412MHz) olevalle lennokille vastaavan herkkyyden, sillä vaimennus olisi tässä tapauksessa noin 120 desibeliä. Käytännössä kuitenkin sallittu lähetysteho riippuu taajuusalueesta, jolloin ei ole järkevä yleistää laskuissa käytettyä tehoa (20dBm) kaikille sallituille taajuuksille.

Lennokkien lähettimen toiminta voidaan Liikenne- ja viestintäviraston määräyksen 15 mukaisesti nähdä joko yleisenä lyhyen kantaman radiolähettimenä (10§) tai laajakaistaiset datasiirtolaitteena mukaan lukien langattomat lähiverkot (13§). [72] Yleisen lyhyen kantaman radiolähettimen osalta tehot ovat:

- ”2400,000–2483,500 MHz Efektiivinen säteilyteho ≤ 10 mW EIRP” [72]
- ”5725–5875 MHz Efektiivinen säteilyteho ≤ 25 mW EIRP” [72]

Desibeleinä tehot ovat noin ≤10dBm ja ≤13,98dBm.

Transmitter Power (EIRP)	2.4 GHz FCC: ≤26 dBm; CE: ≤20 dBm; SRRC: ≤20 dBm 5.2 GHz FCC: ≤23 dBm 5.8 GHz FCC: ≤23 dBm; CE ≤13 dBm; SRRC: ≤23 dBm

Kuva 10 Mavic 2 Pro käyttöohjeen ilmoittamat säteilytehot [25]

Tehoista ainoastaan 5,8GHz alueella oleva vastaa kuvan 5 Mavic 2 Pron tehoa Euroopan alueella (CE, Conformité Européenne), mutta 2,4GHz alueen teho on merkittävästi suurempi kuin lyhyen kantaman radiolähettimelle on sallittu. Voidaan olettaa, että tällä taajuusalueella sovelletaan 13§ tarkoittamille datansiirtolaitteille asetettuja rajoja, jotka ovat:

- ”2400,000–2483,500 MHz Efektiivinen säteilyteho ≤100 mW EIRP. Käyttö on sallittu myös ilmassa olevassa ilma-aluksessa tai muussa ilmailuun käytettävässä laitteessa.” [72]
- ”5150,000–5250,000 MHz Efektiivinen säteilyteho ≤ 200 mW EIRP, lähetteen spektrin tehotiheys oltava ≤ 10 mW/1 MHz EIRP. Saa käyttää ainoastaan sisätiloissa.” [72]
- ”5250,000–5350,000 MHz Efektiivinen säteilyteho ≤ 200 mW EIRP, lähetteen spektrin tehotiheys oltava ≤ 10 mW/1 MHz EIRP. Saa käyttää ainoastaan sisätiloissa.” [72]
- ”5470,000–5725,000 MHz Efektiivinen säteilyteho ≤ 1 W EIRP, lähetteen spektrin tehotiheys oltava ≤ 50 mW/ 1 MHz EIRP. Käyttö on sallittu myös ilmassa olevassa ilma-aluksessa tai muussa ilmailuun käytettävässä laitteessa.” [72]

Langattomille lähiverkoille sallittu taajuusalue siis päättyy 5725MHz ja kuvassa 5 näkyvä 5,2GHz taajuusalue on sallittu käytettäväksi ainoastaan sisätiloissa. 5725-5850MHz taajuusalue on sallittu 14§ tarkoittamille kiinteille laajakaistaisille tiedonsiirtolaitteille enintään 4 watin teholla EIRP[72]. ECC.n suositus ECC/REC/(06)04 (USE OF THE BAND 5725-5875 MHz FOR BROADBAND FIXED WIRELESS ACCESS(BFWA)) määrittelee kiinteän laajakaistaisen tiedonsiirtolaitteen tarkoitetuksi sekä sisä- että ulkokäyttöön. Se on kuitenkin pääasiallisesti tarkoitettu käytettäväksi määritellyllä kiinteällä alueella.[47] Paras mahdollinen kantama on siis oletettavasti saavutettavissa käyttämällä matalinta ulkokäyttöön sallittua 5GHz taajuusalueen kanava 1 watin teholla. Koska tehotiheys on 50 milliwattia megahertsille, kaistanleveyden on oltava 20MHz, jotta teho on sallittu. Tällöin käytetyn kanavan keskitaajuudeksi muodostuu 5480MHz, jolloin vapaan tilan vaimennuksen kaavasta saadaan noin 97dBm teho vastaanottimella kymmenen kilometrin päässä. Huonoin mahdollinen tilanne on taas 5,8GHz taajuusalueella käytettäessä 25 milliwatin lähetystehoa, jolloin vastaanottimelle saadaan noin 97dBm teho vasta 1,6 kilometrin päässä.

Matemaattisen tarkastelun perusteella voidaan päätellä, että Airfencen ilmoittama havaintoetäisyys on teoriassa mahdollinen tietyissä tapauksissa. Toisaalta huonoin mahdollinen tilanne on teoriassa yli kaksi kilometriä alle turvallisen liukukäytävän vaatiman 3,7 kilometriä. Tällöin tutkien kantamat alkavat mahdollisesti olemaan kilpailukykyisiä, sillä esimerkiksi DroneDomen ilmoitettu tutkan kantama on huonoimmillaankin 3,5 kilometriä.

Kaava 4 Tutkayhtälö

$$P_{rx} = \frac{P_{tx} G^2 \lambda^2 \sigma_m}{(4\pi)^3 R^4}$$

Tutkayhtälöstä näemme, että etäisyyden kasvattaminen vähentää vastaanotettua tehoa nopeasti. Vastaavasti antennivahvistuksen ja aallonpituuden kasvattamien lisäävät vastaanotettua tehoa. 3,2 kilometrin havaintoetäisyys ja luotettava tutkaseurannan muodostaminen 2 kilometrin etäisyydeltä ovat mahdollisia X-alueen tutkalla, kun kohteena on lennokki[128]. Drone-Domessa olevan S-alueen tutkan aallonpituus on ainakin kaksi kertaa suurempi, jolloin havaintoetäisyys voisi kasvaa vähintään noin 41% ja parhaimmillaan noin 145%. Näin ollen, jos 3,2 kilometrin havaintoetäisyys kasvaa 145%, saataisin noin 7,8 kilometrin havaintoetäisyys. Matalamman taajuuden käyttäminen kuitenkin pienentää lennokkien tutkapoikkipinta-alaa[Li], jolloin käytännössä havaintoetäisyys ei kasva näin merkittävästi tai se voi jopa pienentyä. Vertailtaessa 12–15 ja 3–6 GHz taajuusalueilla mitattuja tuloksia, alempi taajuus pienentää tutkapoikkipinta-alaa noin 10 desibeliä, mikä tarkoittaa neliömetreinä kymmenkertaista pienentymistä[129]. [128] mittattu lennokki oli Phantom 2. [129] mitatuista lennokeista Phantom 4 oli tutkapoikkipinta-alaltaan keksikokoinen, vaikka se oli kooltaan pienin. Lennokin malli vaikutti tutkapoikkipinta-alaan jopa 11 desibelin verran [129]. Koska ulkoisista mitoista ei voi luotettavasti arvioida lennokin tutkapoikkipinta-alaa, eivät Phantom 2 ja Phantom 4 ole välttämättä vertailukelpoisia.

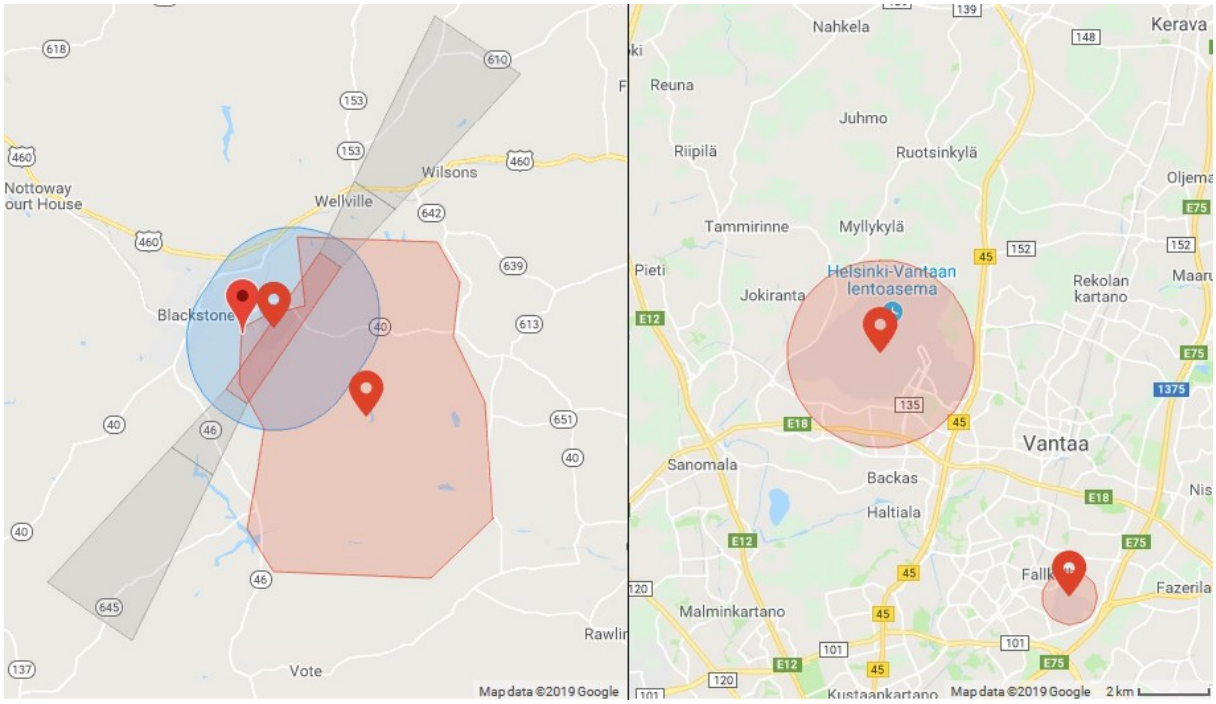
Drone Dome tutkan osalta ilmoitettu tyypillinen havaintoetäisyys voi pitää paikkansa, vaikka lennokkien tutkapoikkipinta-aloissa on merkittäviä eroja, jolloin käytännön havaintoetäisyys voi vaihdella. Olettaen, että paras tilanne on 10 kilometrin etäisyys, jolloin on helposti laskettavissa, että 10 kertaa pienemmälle maalille se on noin 5,6 kilometriä. Tämä on kuitenkin edelleen aiemmin ilmoitetun 3,5-10 kilometrin tyypillisen havaintoetäisyyden sisällä.

Lennokin vastaanotin on houkutteleva kohde elektroniselle tuhoamiselle, sillä sen toiminta perustuu radiosäteilyn muuntamiseen sähkövirraksi. Kohteena olevien piirien tuhoutuminen on seurausta siitä, että piiriin indusoidaan suurempi teho, mitä piiri on suunniteltu kestämään. 1 watin tehoa voidaan pitää varmana rajana, jonka jälkeen vastaanottimen puolijohdekomponentit vaurioituvat puolijohteessa käytetyn metallien siirtyessä. [130] Huomioitavaa on, että mikrosirut vaikuttavat olevan merkittävästi tätä herkempiä, esimerkiksi nRF24L01 (normaali teho 60mW)[131] ja XN297 (normaali teho 50mW)[82]. Toimintatehon ylittäminen saattaa aiheuttaa pysyvän vaurion mikrosiruun[131].

Vapaan tilan vaimennus on merkittävä osa tehohäviötä, mutta on huomioitava myös polarisaatiosta seuraava vaimennus, antennin aiheuttama vahvistus, antennin ja vastaanottimen välinen vaimennus sekä radioaaltojen heijastumisesta seuraava vahvistus. Riittävän voimakkaalla teholla pulssin pituudeksi riittää muutamia mikrosekunteja. [130] Vapaan tilan vaimennuksen kaavalla voidaan arvioida, että 60mW kestävän vastaanottimen maksimiteho saadaan ylitettyä 100 metrin päässä vasta kun lähettimen teho on noin 10MW. Tämä on suhteellisen suuri teho, sillä esimerkiksi BUK-M1 ilmatorjuntajärjestelmässä käytetty maalinosoitustutka toimii 2kW teholla maaliosoitusmoodissa[66].HPEM-järjestelmissä huipputeho voi kuitenkin hetkellisesti nousta korkeammaksi. Esimerkiksi 350MHz taajuudella toimiva HPEMcase, jonka säteilyn huipputeho on 365MW[111]. Tällä teholla ja taajuudella lähetetty pulssi on vielä noin 1,3 kilometrin päässä vastaanotettavissa 1W teholla, jolloin vastaanottimen puolijohdekomponenttien voidaan olettaa vaurioituvan. Huomioitavaa on kuitenkin, että taajuus on matalampi kuin useimpien lennokkien käyttämät taajuudet, jolloin [130] perusteella vastaanotin on voitu suojata esimerkiksi taajuusleikkurilla.

4. Kybervaikuttaminen kaupallisiin lennokkeihin ja niiden ohjausjärjestelmiin

Tässä luvussa tarkastellaan tunnettuja kybervaikuttamisen keinoja, joita voidaan hyödyntää toimittaessa kaupallisia lennokkeja vastaan. Kaupallinen lennokki on houkutteleva vaihtoehto täydentämään lentotukikohtaan kohdistuvaa tiedustelua. Niiden maahantuominen tai hankkiminen paikanpäällä ei ole epäilyttävää, mutta niiden suorituskyky riittää hyvin lähialueen tiedusteluun. Kaupallisten lennokkien käyttöä kiinteää lentotukikohtaa vastaan rajoittaa osaan ohjelmoitu NFZ-ominaisuus, joka estää niiden käyttämisen rajoitusalueilla[65].



Kuva 11 Blackstone ja Helsinki-Vantaa GEO zonet [39]

Kuvassa 11 on kuvankaappaus DJI:n geomap sivulta, jossa on näkyvissä DJI:n käyttämät NFZ-rajoitusalueet. Vasemmalla on Blackstonen sotilaslentokentän, sekä Fort Picketin varuskunta-alueen rajoitukset. Vertailun vuoksi kuvassa on oikealla myös samalla mittakaavalla Helsinki-Vantaa ja Malmin lentokenttien rajoitukset. Koska suomessa lennokkitoiminta on kielletty 5 kilometrin säteellä kiitotiestä[104], alueiden tulisi olla merkittävästi isompia. Harmaalla olevat alueet ovat korkeusrajoitettuja, sininen alue vaatii käyttäjän hyväksynnän ja punaisella alueella lentäminen on estetty[39]. Tämä ominaisuus on kuitenkin mahdollista kiertää. Esimerkiksi DJI tarjoaa mahdollisuutta ominaisuuden pois kytkemiselle, jos lennokin omistajalla on esittää tarvittavat viranomaisluvat lentotoimintaan rajoitusalueilla. DJI:n rajoituskartta ei ole myöskään kovin kattava, sillä vaikka Rovaniemen ja Pirkkalan lentokentillä on rajoitusalue, niin Halli, Tikkakoski ja Rissala eivät ole rajoitettuja[39].

Lisäksi lennokki on mahdollista ”jailbreakata” jolloin lennokkiin asennetaan virallisen päivityksen sijaan muokattu päivitys. Käytännössä tämä ei eroa älypuhelimista tutuista ”jailreak” tai ”root” -muokkauksista, mutta lennokkien osalta ei ole vielä muodostunut yhtä laajaa harrastelijayhteisöä. Lisäksi lennokkivalmistajien on helpompi perutella tämän kaltaisten muokkausten estämistä lentoturvallisuuden lisäämiseksi[65]. DJI tarjoaa palkkioita niille, jotka paljastavat haavoittuvuuksia sen lennokeissa. Esimerkiksi NFZ-rajoituksen ohittamisesta voi saada 500-1000 dollarin palkkion.[40]

4.1. Harraste- ja urheilulennokit

Harraste- ja urheilulennokilla tarkoitetaan tässä tutkimuksessa Trafin määräyksen mukaisesti:

”lentämään tarkoitettua laitetta, jonka mukana ei ole ohjaajaa ja jota käytetään harraste- tai urheilutarkoitukseen pois lukien leluilma-alukset, jotka on suunniteltu tai tarkoitettu käytettäväksi joko yksinomaan tai osaksi alle 14-vuotiaiden lasten leikeissä; ”[104]

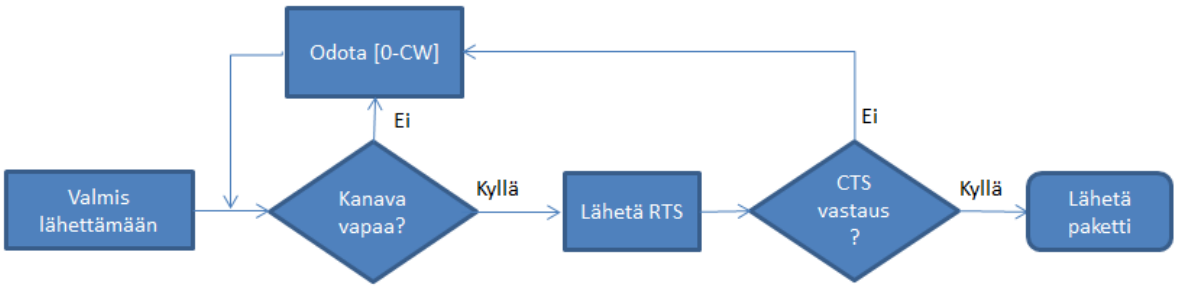
Näissä ohjauslinkkinä toimii yleensä WLAN tai Bluetooth, jolla saavutetaan yhteensopivuus käyttäjän älylaitteen kanssa. Vaikka myös muut ohjauslinkit, kuten ZigBee, Skyartec tai Flysky, soveltuisivat Trafin määritelmän mukaiseen urheilu- tai urheilukäyttöön, jätän ne tässä alaluvussa käsittelemättä, koska ne eivät toistaiseksi ole yhteensopivia älylaitteiden kanssa. Näistä ZigBee tosin on yleistynyt esimerkiksi älyvalaisin ja IoT-käytössä, joten se mahdollisesti tulee osaksi joidenkin älylaitteiden yhteysvaihtoehtoja tulevaisuudessa.

4.1.1. 802.11 WLAN

Siviilimarkkinoille on paljon lennokkeja, joita ohjataan älypuhelimen tai tabletin kautta, tai niitä hyödynnetään osana järjestelmää. Aiemmin esitellyt Guardion ja Airfence hyödyntävät järjestelmissään 802.11-standardin mukaisten WLANien toimintaan liittyviä haavoittuvuuksia. 802.11:sta on useita eri versioita, joiden erottelussa käytetään joko yhtä tai kahta kirjainta. Wi-Fi on taas kaupallinen brändi. Sen yhteydessä käytetään numeroita, esimerkiksi Wi-Fi5, joka myönnetään laitteille, joissa käytetään 802.11ac-standartin mukaista protokollaa. Merkintä 802.11X tarkoittaa yleisesti 802.11-standardin mukaisia WLANeja, kun taas 802.11ax on tarkasti määritelty tietyksi standardiksi, eli ei siis kaikki 802.11a-sarjan standartit. Koska pieni x-kirjain on otettu mukaan standarteissa käytettäviin kirjaimiin, ei tässä tutkielmassa käytä 802.11X merkintää.

IEEE 802.11-standardin mukaisissa wlaneissa törmäyksiä pyritään rajoittamaan MAC(Media Access Control)-kerroksen RTS(Request To Send)- ja CTS(Clear To Send)-kehyksillä. Käytännössä lähettäjä ilmoittaa vastaanottajalle aikovansa aloittaa lähetteen (RTS). Ollessan vapaa vastaanottaja ilmoittaa tästä(CTS). CTS-kehys myös estää muita verkon jäseniä aloittamasta lähetystä ennen kuin RTS:n lähettänyt lopettaa omansa.[99]. Näiden kehysten käyttöä rajoitetaan käyttämällä satunnaislukua, joka valitaan väliltä 0-CW, jossa CW (Connection Window) on yhteysikkunan laitekohtainen koko. Käyttämällä tarkoituksella pienempiä yhteysikkunoita voidaan verkosta saada omaan käyttöön isompi osuus tarjolla olevasta kaistasta. [70] Kehyksiä voidaan myös käyttää tavanomaisempaan liikenteen häirintään, jos hyökkääjä ei tarvitse verkkoa omaan käyttöönsä.

Toinen törmäyksien vähentämiseen käytetty menetelmä on CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance), jossa kanavaa kuunnellaan ennen lähettämistä. Jos kanava on käytössä, odotetaan sen vapautumista. Kun kanava havaitaan vapaaksi, odotetaan satunnainen aika ennen lähettämistä.[61, 113] Tämä toiminnallisuus liittyy oleellisesti RTS/CTS-kehysten käyttämän CW-arvon käyttöön. Kuvassa 12 on havainnollistettu koko varmistusketju.



Kuva 12 CDMA/CA RTS/CTS vuokaavio

WLAN-liikenne on siirtotiensä vuoksi helposti salakuunneltavissa. Salaamalla datakehykset saavutetaan jonkin asteinen suoja, mutta tätä varten laitteen pitää vaihtaa salausavain tukiaseman kanssa. Tämän vuoksi kaikkia langattoman liikenteen sanomia ei ole käytännöllistä suojata, koska verkkoon liittyessä laitteella ei ole epäsymmetrisen salauksen kautta saatavaa salausavainta. Ennen avainten vaihtoa laitteen tulee löytää tukiasema ja liittyä siihen - myöskään näitä sanomia ei voi salata. Datakehysten salaaminen ei suojaa toistohyökkäyksiltä, sillä otsikkokehykset ovat edelleen salaamattomia.[17] Oheisessa taulukossa on listattu hallintasanomia, joiden käyttö hyökkäyksissä kuvataan myöhemmin tässä tutkielmassa.

Taulukko 3 kyberille otolliset hallintasanomat

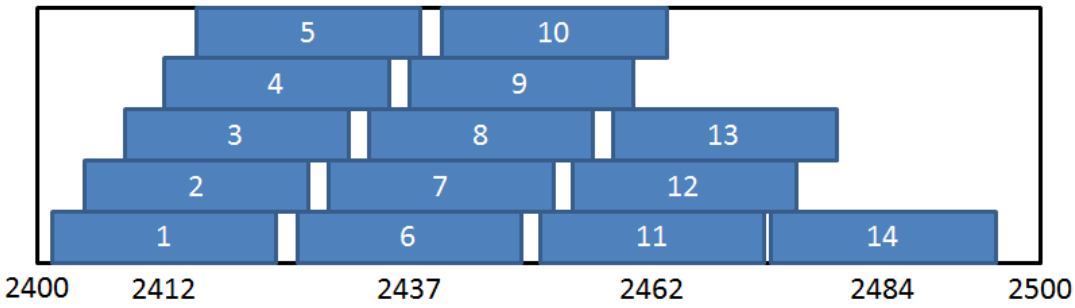
Beacon and probe request/response	Majakka ja palvelukykyjen sanomat	Tukiasema ilmoittaa olemassaolonsa, SSID:nsä ja tarjoamansa palvelun laadun
Authentication / Deatuhentication	Tunnistautuminen ja tunnistautumisen purku	Epäsymmetrisen salauksen perustaminen ja sen purkaminen. Sanomiin vastataan symmetrisesti, jotta osapuolet käyttävät samaa salausta.
Association / Disassociation	Tukiasemaan liittyminen ja poistuminen	Pyyntö muodostaa tai purkaa yhteys
Spectrum management action	Spektrin hallinta	Taajuden ja kanavan muutokset

Kaikkia taulukon 3 hallintasanomia voi käyttää DoS-hyökkyksessä (Denial of Service, palvelunestohyökkäys). Esimerkiksi disassocistion tai deauthentication-sanomia voidaan pommittaa toistuvasti ohjaimeen, jolloin ohjain joutuu toistuvasti reagoimaan muodostamalla tai salaamalla yhteyden uudestaan. Käytännössä sanoma voidaan lähettää riittävän usein, että lennokin ohjaaminen muuttuu mahdottomaksi. Ohjauksen lisäksi lennokki ei kykene välittämä kuva- tai videodataa.

802.11w-version myötä hallintasanomien käyttö hyökkäyksissä on vaikeutunut hallintasanomiin lisättävien toistohyökkäys ja spoofing-suojausten seurauksena[17]. Luultavasti suuressa osassa lennokkeja tullaan pysymään vielä vähemmän suojatuissa versioissa. Tämä on pääosin seurausta tarpeesta säilyttää yhteensopivuus kuluttajien vanhempien päätelaitteiden kanssa ja näin saavuttaa laajempi asiakaskunta. Jos ja kun paremmin suojattujen laitteiden kysyntä kasvaa joko kyberkiusanteon tai rikollisuuden seurauksena, muuttuu näiden hallintasanomien käyttö vaikeammaksi. Tätä oletusta tukee, että Wi-Fi allianssi on parantanut hallintasanomien suojausta WPA3 julkaisun myötä[114].

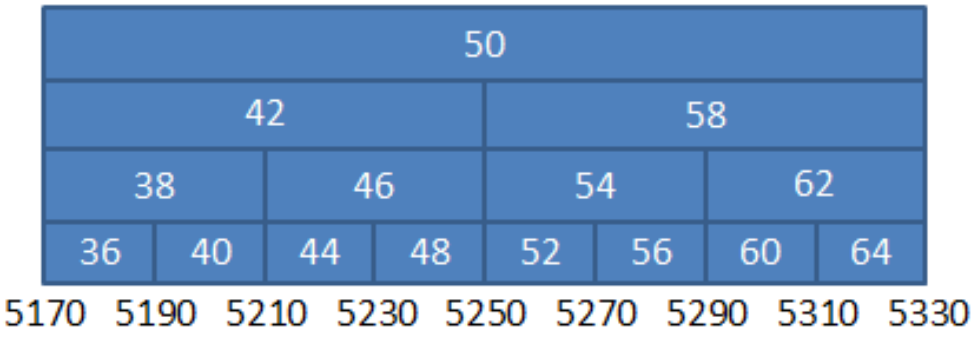
4.1.2. WLAN-taajuudet

Yleisesti käytössä olevista WLAN-taajuusalueista käytetään merkintöjä 2,4GHz ja 5GHz[61] tai 2.4G ja 5G[113]. 2,4GHz toimii 2,4GHz-2,5GHz ISM-taajuusalueella. Käytännössä WLAN-kanavien varaamien taajuuksien alaraja 2401MHz ja yläraja2495MHz. Taajuusalue on jaettu 2,4GHz WLANeissa 5MHz välein 22MHz kanaviin, joita on yhteensä 14. Viimeinen kanava on poikkeuksellisesti 12MHz välillä. Käytännössä taajuusalueella on enintään neljä kanavaa, jotka eivät häiritse toisiaan 1, 6, 11 ja 14. Näitä kutsutaan häiriöttömiksi kanaviksi.



Kuva 13 2,4GHz WLAN-kanavat ja häiriöttömien kavavien keskitaajuudet Mhz [WLAN_MAC_PHY]

5GHz WLANit käyttävät viittä eri kaistanleveyttä jotka ovat 10, 20, 40 80 ja 160MHz. Koska kaistanleveydet ovat toistensa monikertoja ja pääosa kanavista on lähtökohtaisesti 20MHz kaistanleveydellä, voidaan kanavien taajuusalueita yhdistelemällä saada käyttöön isompi määrä kanavia. Saman levyiset kaistat eivät ole päällekkäin kuten 2,4GHz WLANeissa.



Kuva 14 Eräiden 5GHz WLAN-kanavien numerointi ja taajuusvälit MHz

4.1.3. Bluetooth

Käyttämällä Bluetoothia lennokin ohjaamiseen voidaan hyödyntää olemassa olemia Bluetooth peliohjaimia, kuten Wii- tai Xbox-ohjaimet. Kuitenkin esimerkiksi DJI Tello tapauksessa itse lennokissa ei ole Bluetoothia, vaan ohjaimella ohjataan älypuhelimessa olevaa sovellusta josta on wlan-yhteys lennokkiin. Bluetoothilla varustettuja lennokkeja on mahdollista rakentaa käyttämällä Arduino-mikrokontrolleria ja MultiWii-sovellusta [79]. DJI Phantom 2 lennokissa on kolme eri langatonta yhteyttä, joista yksi on Bluetooth[30].

Bluetooth on WLANin tavoin haavoittuvainen DoS-hyökkäyksille. Kopioimalla isäntälaitteen BD_ADDR (Bluetooth device adress) hyökkääjän hallussa olevaan laiteeseen, vastaa tämä laite isäntälaitteelle osoitettuihin kyselyihin. Koska myös isäntälaite vastaa kyselyyn, vastaussignaalit häiritsevät toisiaan jolloin kyselyn vastausta ei voi tulkita. [132] Bluetooth käyttää salauksessaan 7-16 oktetin (56-128bittiä) avaimia. Salaus on vapaaehtoinen. [13] Lyhyet avaimet on mahdollista arvata ja tarvittaessa ne voi kuunnella avainten vaihdossa. [132]

Bluetooth käyttää 2,4 GHz ISM-taajuusaluetta[13].

4.1.4. Ohjauslinkin käytön estäminen

Ohjauslinkin käytön estämien DoS-hyökkäyksellä on suhteellisen yksinkertainen menetelmä lennokkien torjuntaan ja muistuttaa periaatteeltaan tavanomaista elektronista häirintää. Kanavan käyttöä voi häiritä neljällä pääasiallisella tavalla[61, 113]:

1. Jatkuva häirintä, jossa kanavalle lähetettään satunnaista dataa välittämättä sen rakenteesta

2. Looginen häirintä, jossa kanavalle lähetetään jatkuvasti oikein muotoiltuja paketteja, jotka sisältävät hyödytöntä dataa

3. Satunnainen häirintä, jossa menetelmää 1 tai 2 käytetään satunnaisina ajanhetkinä, jolloin virrankulutus on alhaisempi, mutta kanavaa saatetaan häiritä myös silloin, kun sillä ei ole liikennettä

4. Reaktiivinen häirintä, jossa menetelmää 1 tai 2 käytetään kun kanavalla havaitaan liikennettä jolloin virrankulutus on myös alhaisempi ja häirintä on vaikeampi havaita

Näistä menetelmä 2 on paras, sillä se estää kanavan käytön täysin. Menetelmien 3 ja 4 tehokkuus laskee etäisyyden kasvaessa merkittävästi, vaikka myös menetelmä 4 voi estää kanavan käytön täysin lyhyillä etäisyyksillä. Myös menetelmän 1 tehokkuus laskee etäisyyden kasvaessa, mutta se on edelleen suhteellisen tehokas.[61, s. 30]

Lennokin toimiessa tukiasemana tulee myös kyseeseen joko association tai authentication-pyyntöjen jatkuva lähettäminen (association ja authenticaton flood -hyökkäykset). Tukiasema tallentaa authentication-pyynnöt tauluun, jolloin lähettämällä tuhansia pyyntöjä satunnaisesti vaihtuvilla mac-osoitteilla taulu voidaan täyttää. Tämä johtaa siihen, että tukiasema ei enää pysty vastaanottamaan uusia pyyntöjä tai se voi jopa alkaa tyhjentää vanhoja pyyntöjä. Pahimmillaan tukiasema voi resetoitua.[61, s. 36] Association-pyyntöjen väärinkäyttäminen perustuu samaan ilmiöön, mutta sitä vastaan on kehitetty suojakeinoja perustuen pakettien sarjanumeroiden seurantaan.[61, 113] Liitteessä 3 on kuvattu käytännössä miten DoS-hyökkäyksiä on mahdollista toteuttaa WLAN-linkillä ohjattavaan lennokkiin. Authentication flood ei vaikuta toimivan ainakaan liitteen kokeessa käytettyyn TELLO-lennokkiin. Lennokki on mahdollisesti ohjelmoitu hyväksymään vain yksi yhteys kerrallaan, jolloin sillä ei ole tarvetta ylläpitää taulua yhteyspyynnöistä.

4.1.5. Ohjauslinkin kaappaaminen

Ohjaimen linkin kaappaaminen tapahtuu luomalla tukiasema, jonka SSID ja MAC-osoite on sama kuin lennokilla, mutta joka käyttää eri kanavaa tai samaa kanavaa joka näkyy kohdelaitteelle voimakkaampana. Tämän jälkeen ohjaimelle lähetetään väärennetty deauthentication sanoma, jolloin ohjain katkaisee yhteyden hetkellisesti. Tällöin ohjain yrittää liittyä voimakkaimmin kuuluvaan tunnettuun verkkoon. Koska hyökkääjän tukiaseman SSID ja MAC ovat nyt samat kuin lennokilla, ohjain olettaa hyökkääjän verkon olevan tunnettu. Ratkaisevaksi parametriksi jää verkon voimakkuus ohjaimen päässä, johon voidaan vaikuttaa käyttämällä suuntaavaa antennia tai lisäämällä tukiaseman lähetystehoa. Vaihtoehtoisesti kohdistamalla häirintää tukiasemana toimivan lennokin suuntaan saadaan se hiljennettyä.[109]

Lennokin näkökulmasta ohjauslinkki katoaa yllättäen ja se alkaa suorittaa asiaankuuluvia toimenpiteitä, jotka harraste- ja urheilulennokeilla rajoittuvat käytännössä leijumiseen ja laskeutumiseen. Vaihtoehtoisesti hyökkäyksessä voidaan luoda myös valeohjain, joka yhdistetään lennokkiin. Jos lennokki sallii vain yhden yhteyden kerrallaan, on alkuperäinen ohjain irrotettava verkosta käyttämällä disassociation- tai deauthentication-sanomaa, jolloin hyökkääjä voi ehtiä varata yhteyden ennen kuin ohjain palaa verkkoon.

Deauthentication-sanoman väärinkäyttöön perustuva hyökäys on suhteellisen yksinkertainen automatisoida. Esimerkikksi Perl- ja NodeJS-skripteillä kirjoitettu SkyJack ohjelmisto on alun perin tehty katkaisemaan automaattisesti Parrot SA:n valmistamien lennokkien yhteys ohjaimeen ja luomaan uusi yhteys lennokkiin, ennen kuin ohjain ehtii palata verkkoon. Se käyttää hyväkseen aircrack-ng ohjelmistopakettia. Aircrack-ng koostuu useasta eri työkalusta ja sen käytöstä on esimerkki liitteessä 3. Ohjelmistopaketti sisältää myös työkalun nimeltä aircrack-ng, jota käytetään salauksen murtamiseen. Itse SkyJack ohjelmisto vain automatisoi komennot ja sisältää listan kohteena olevista MAC-osoitteista.[60] Tässä tapauksessa IEEE:n julkaisemat Parrotille rekisteröidyt 90:3A:E6, A0:14:3D, 00:26:7E, 00:12:1C ja 90:03:B7-avaruudet[56]. Kaikki nämä eivät ole välttämättä lennokkikäytössä, mutta listan käyttäminen vähentää kuitenkin arvauksia, jos alueella on useampi WLAN. Yhteyden katkaisemisen jälkeen SkyJack imitoi ohjaimen ohjaussanomia saaden lennokin lentämään kuvion ja laskeutumaan sen jälkeen [60]. Koska ohjaussignaalien imitointi on toteutettu NodeJS:llä, joka on tulkattava kieli, voidaan lennettävä kuvio muokata helposti halutunlaiseksi tai jättää kokonaan pois.

SkyJack ei yritä murtaa kohdeverkon salausta, vaikka Perl-skriptissä on määritelty tähän vaadittava aircrack-ng -työkalu[60]. AR Drone 2.0 ei käytä mitään salausta, mutta esimerkiksi Ryze TELLO voi käyttää WPA2 PSK-suojausta. Tämän tyyppinen suojaus on yleinen WiFi-verkoissa ja sen purkamiseen on tunnettuja ratkaisuja.

WPA ja WPA2 käyttävät istuntokohtaista avainta (PTK, Paiwise Temporal Key) liikenteen salaamiseen. PTK koostuu kuudesta tekijästä:

1. Tukiaseman MAC-osoite (lennokki)
2. Asiakkaan MAC-osoite (ohjain)
3. Tukiaseman ESSID
4. ANonce (tukiaseman satunnaisluku)
5. SNonce (asiakkaan satunnaisluku)
6. Salainen avain (PSK, Pre Shared Key), joka on tukiaseman ja asiakkaan tiedossa

Kohdat 1 ja 2 ovat löydettävisä käyttäen airomon-ng -työkalua. Tällöin voidaan löytää myös ESSID, mutta se voi olla myös piilotettu. Piilotetun ESSID:n voi murtaa bruteforce-menetelmää käyttäen mdk3-työkalua. ESSID:n pituus on maksimissaan 32 bittiä[113]. Vaihtoehtoisesti, koska ESSID on mukana asiakaan probe requestissa, voidaan se salakuunnella. [113]

WPA-kättely on neliosainen ja se alkaa tukiaseman lähettäessä ANonce:n asiakkaalle, jolloin asiakas laskee tukiaseman antamalle IE:lle (Information Element) ja omalle SNonce:lle MIC-arvon (Message Integrity Code) käyttäen omaa SNonce-arvoaan sekä käyttäjän syöttämää salaista avainta. Tämän jälkeen asiakas lähettää SNoncen, IE:n ja MIC:n tukiasemalle, joka laskee oman MIC:n käyttäen tietämiään arvoja, sekä juuri saatua SNonce-arvoa. Näin tukiasema voi varmistua, että asiakkaaseen syötetty salainen avain on oikein. Jos avain oikein, tukiasema lähettää GTK:n (Group Temporal Key) ja siihen liittyvät IE:t, joista on laskettu MIC. Asiakas tarkastaa nämä ja jos MIC täsmää, asiakas päättä kättelyn lähettämällä ACK-sanoman ja siitä lasketun MIC:n.[110]

Koska ANonce ja SNonce on helppo salakuunnella kättelyn aikana, ainoa tuntematon tekijä on PSK, sillä sitä ei missään kohtaa siirretä. Se on kuitenkin mahdollista päätellä, sillä PTK:n muodostumistapa tunnetaan. Tällöin PTK pitää muodostaa käyttäen arvattua avainta, joka on 128 bittiä pitkä[61]. Tarvittavien arvauksien määrää voidaan yrittää vähentää käyttämällä sanakirjahyökkäystä. 2013 kotitietokoneella voitiin luoda jopa 10 000 PTK:ta sekunnissa, jos laskennassa käytetään näytönohjainta.[113] 2016 vastaava luku oli jo 200 000 [61]. Avaimen oikeellisuus on mahdollista tarkastaa generoimalla MIC-arvoja ja vertaamalla niitä kaapattuihin arvoihin.

Satunnaisten arvausten sijaan voidaan myös käyttää esimerkiksi Beck & Tews -hyökkäystä, joka perustuu ARP-vastausten kuuntelemiseen ja virheilmoitusten väärinkäyttöön. Tällä menetelmällä salaus on mahdollista purkaa 12-15 minuutissa. [89] Tämä on merkittävästi nopeampi menetelmä, jos salainen avain ei ole altis sanakirjahyökkäyksille. Tässä tapauksessa satunnainen arvaaminen voi pahimmillaan viedä vuosia.

4.1.6. Videolinkki

Lennokin videolinkki voidaan toteuttaa erillisellä kanavalla kuin millä ohjaaminen tapahtuu. Puhtaasti sovelluksella ohjattavat niin sanotut selfie-lennokit (eng. selfie drone), joita ohjataan WLANin yli käyttävät yleensä samaa kanavaa sekä videokuvan välittämiseen, että ohjaamiseen. Linkkien toimintaa on taulukoitu liitteessä 2.

Käytettäessä erillistä kanavaa, videokuvan salaaminen ei ole ensiarvoisen tärkeää, sillä sen hyödyntäminen kopteria toimittaessa kopteria vastaan on haastavaa. Vaikka sen perustella voidaankin suunnata valvontaa, niin suunnattu vaikuttaminen tarvitsee kuitenkin erillisen maalinosoituksen. Reaaliaikainen videolinkki mahdollistaa lennokin ohjaamisen erilleen esteistä, sekä kuvatiedustelun suuntaamisen ja sen hyödyntämisen, vaikka lennokki tuhottaisiinkin.

Kuva 15 JJPRO HAX -kopterin RTSO-kättelyn alku

RTSP (Real Time Streaming Protocol) käyttö vähentää asiakasohjelmistoon tarvittavaa ohjelmointia, sillä sille on tarjolla valmiita kirjastoja. Kuvan 15 tapauksessa lennokki toimii RTSP-palvelimena, johon sovellus ottaa yhteyden. Käytettävät arvot on helppo arvata, sillä 554 on RTSP-vakioportti[16] ja IP 192.168.-osoiteavaruus on varattu sisäverkoille. Tässä tapauksessa lennokin videolinkkiin on mahdollista päästä käsiksi ilman, että tästä tulee mitään indikaatiota lennokin ohjaajalle.

Palvelimen löytäminen mahdollistaa palvelimen ylikuormittamisen, joka voi vaikuttaa myös lentoa ohjaaviin järjestelmiin. Vaihtoehtoisesti toisto voidaan keskeyttää käyttämällä PAUSE-sanomaa tai ohjaamalla lennokin ohjaajan striimi väärälle pavelimelle käyttämällä REDIRECT-sanomaa. Väärä palvelin voi esimerkiksi toistaa lennokilta aiemmin nauhoitettua videokuvaa, jolloin ohjaajan näkökulmasta lennokki ei enää vastaa ohjauskomentoihin, vaikka videolinkki vaikuttaisi toimivan.

Asiakasohjelmiston kautta voidaan soluttaa laitteeseen haitallista koodia käyttämällä SET_PARAMETER-sanomaa. Sama toimii myös palvelimen päässä. [76] Käytännössä laitteen tyyppi ja mahdolliset haavoittuvuudet on löydettävä salassa, sillä turvallisuusaukkoja tukitaan jatkuvasti.

Videolinkkiä on mahdollista häiritä myös käyttämällä hyväksi ohjaajan päätelaitteen mahdollisia avoimia rajapintoja. Esimerkiksi voidaan väärentää ilmoituspalvelimen push-sanomia, jolloin kohdelaite saa toistuvia ilmoituksia. Näihin sanomiin on edelleen mahdollista soluttaa haitallista koodia, joka haittaa laitteen käyttöä tai tekee sen käyttökelvottomaksi.

4.2. Vaihtoehtoisesti ammattilaiskäyttöön soveltuvat lennokit

Tässä tutkielmassa vaihtoehtoisesti ammattilaiskäyttöön soveltuvat lennokit noudattavat samaa määritelmää kuin aiemmin mainittu urheilu ja harrastekäyttöön soveltuva lennokki. Niissä on kuitenkin erillinen ohjain, joka on varta vasten kyseiselle lennokille, sekä kyky käyttää satelliittipaikannusta. Tämä määritelmä pois sulkee esimerkiksi DJI Spark[33] ja Parrot ANAFI[84] nelikopterit, sillä vaikka niissä on erillinen ohjain, niiden ohjaus ja videolinkkinä toimii wlan.

Ohjaus- ja videolinkit ovat useimmiten wlanin käyttämillä taajuuksilla. Esimerkiksi DJI:n Lightbridge ja Ocusync käyttävät näitä taajuuksia. Näistä Ocusync toimii myös joillain olemassa olevista tele-siruista, kuten LC1813. DJI ilmoittaa omilla sivuillaan näiden linkkien olevan ainakin videolinkkejä, mutta ei ota kanta ohjauslinkkiin. DJI Matrice 100 käyttöohjeessa mainitaan, että Lightbridge on sekä ohjaus-, että videolinkki[32]. Ainakin Lightbridgessä on parannettu linkin salausta firmware päivityksellä 07.04.2016, eli oletettavasti se on ollut aikaisemmin haavoittuvainen[37].

4.2.1. Ohjauslinkki XN297LBW-sirulla

Panchip XN297LBW -sirun valinta perustuu siihen, että tutkijalla on tutkimusta tehdessä ollut käytössä kaksi tätä sirua käyttävää nelikopteria. Siru on ilmeisesti kopio NRF24L01+ -sirusta, josta on myös muita kopioita, ainakin RFM73, RFM75 ja LCX24G[92]. NRF24L01+ on mahdollista ohjelmoida kommunikoimaan näiden sirujen kanssa[92], jolloin siten sitä voisi mahdollisesti käyttää kaappariohjaimessa.

XN297L-siru toimii 2,400-2,483GHz taajuusalueella. Liikennöinti tapahtuu SPI (Serial Peripheal Interface)-väylän kautta. Radioliikenne on taajuusmoduloitu käyttäen GFSK:ta(Gaussian frequency shift keying) käyttäen neljä bittistä avainta (arvot väliltä 0000-1111). Sirussa on sisäänrakennettu RSSI(received signal strength indicator). Vastaanottoherkkyys riippuu käytettävästä lähetysnopeudesta -93dBm 250kbps -nopeudelle, -87dBm 1Mbps-nopeudelle ja -83dBm 2Mps-nopeudelle. Lähetysteho on enimmillään 13dBm, mutta käytännössä 2dBm. SPI:n ohjeformaatti tukee lähettämistä kuittausvaateella (ACK acknowledgement) tai ilman. Siru tukee lähetysten koodijakokanavointia.[82] Kaksi viimeistä kirjainta B ja W kertovat sirun version ja muodon, tässä tapauksessa SOP8.[83]. SOP8 sirussa on kahdeksan pinniä. Muita vaihtoehtoja olisi 16 pininen SOP16 ja 20 pinninen QFN.[82]

Sirun toiminta muistuttaa Bluetoothin toimintaa, eli on mahdollista, että se on altis samantyyppisille DoS-hyökkäyksille.

4.2.2. Ohjauslinkin kaappaaminen

Panchip XN297L-sirujen välisen radioliikenteen purkaminen on kolmivaiheinen. Ensin pitää löytää käytetyt kanavat, arvata GFSK-avain ja sen jälkeen tarvittaessa koodijakokanavoinnin avain. Tätä tutkimusta varten mitatut kahden eri valmistajan ohjaimien käyttämät taajuudet vaikuttivat pysyvän vakioina käynnistyskertojen välillä. Molempien osalta oli löydettävissä neljä eri kanavaa joidenka kaistanleveys oli sunnilleen 2MHz. Tämä vastaa 2Mbps siirtonopeuden käyttämää kaistanleveyttä, jolloin kanavien minimiväli on 2 MHz[82]. Kanavaväli voi kuitenkin olla suurempi ja toisen ohjaimen osalta yhden kanavan keskitaajuus oli pariton. Molempien ohjaimien osalta keskitaajuudet kuitenkin osuivat megahertseille. Tämä vähentää tarvittavien arvausten määrää, sillä sirun käyttämä taajuusalueella on 84 mahdollista kanavaa, jos lasketaan myös 2400MHz ja 2083MHz kanavat.

Kun taajuudet on löydetty ja ohjauslinkki tunnistettu, itse lähetteiden purkaminen on mahdollista automatisoida. SkyJack ohjelmistosta on olemassa versio, joka murtaa automaattisesti 3DR-lennokeissa käytetyn ohjauslinkin taajuushypytyksen. Alkuperäisessä SkyJack kokoonpanossa käytetyn WLAN-radion sijaan se käyttää TI CC1111-sirua, joka on ohjelmoitavaaradiosiru.[60]

Vastaava toteutus löytyy pienoismalleissa käytettävää DSMX-radioita vastaan suunnitellusta Icarus-laitteesta. Icarus on DSMX-ohjaimeen asennettava laite, joka tunnistaa yhteensopivan lennokin ja murtaa sen ohjauslinkin bruteforce-menetelmällä. Lisäksi laite hyödyntää kehysten ajastukseen liittyvää haavoittuvuutta, jolla kaappariohjaimen paketit tulkitaan ennen alkuperäisen ohjaimen paketit. Näin lennokki saadaan hylkäämään alkuperäisen ohjaimen komennot ja se on täysin kaappariohjaimen hallinnassa.[49]

Tässä tutkimuksessa yritettiin löytää vastaava toteutus käytettäväksi XN297L-siruja vastaan. Huolimatta löydetyistä taajuuksista [92] lähdekoodista muokattu ja käännetty ohjelma ei vastaanottanut yhtään pakettia käytettäessä NRF24L01+-sirua. Alkuperäinen lähdekoodi oli tarkoitettu Arduino-alustalle ja se muokattiin tätä tutkimusta varten yhteensopivaksi Raspberry Pi 2+ B -pienoistietokoneen kanssa käyttäen [43] esimerkin mukaista suoraa rekisterilukua GPIO-pinnien (general purpose input/output) tilan käsittelyyn. Ongelmaksi muodostuivat, ettei sirun toimintaa voitu varmistaa ja sirun suuri 64 bitin osoiteavaruus. Tulosten perusteella osoitteen satunnainen arvaaminen ei ole kovin tehokas tapa kaapata liikennettä johtuen osoiteavaruuden koosta.

4.2.3. GNSS-häirintä

Lennokki voi hyödyntää satelliittijärjestelmää sekä oman paikkansa, että ajan selvittämiseen. Satelliitin taajuuden häiritseminen on helppoa suurien etäisyyksien johdosta, mutta höytysanomien väärentämisellä lennokkiin voidaan vaikuttaa hallitummin.

Sijainnin, erityisesti korkeustiedon, väärentäminen on hyvä keino pakottaa lennokki pois toiminta-alueelta tai laskuun. Iran väittää käyttäneensä GPS-korkeustiedon väärentämistä pakotettuaan Yhdysvaltojen RQ-170 lennokin laskeutumaan hallitsemalleen aavikolle[100].

Lentoturvallisuuden näkökulmasta satelliittinavigoinnin häiritseminen on ongelmallista, sillä myös miehitetyt ilma-alukset käyttävät sitä. Miehitetylle ilma-alukselle on kuitenkin helpompaa luopua satelliittinavigoinnin käytöstä ja siirtyä käyttämään esimerkiksi lentopaikan mittarilähestymispalveluita ja omaa paine-, sekä radiokorkeamittaristoaan.

Osaa kaupallisista lennokeista ei voi lennättää, jos lennokki ei saa yhteyttä riittävään määrään satelliitteja. Häiriöihin on varauduttu mahdollistamalla useamman satelliittijärjestelmän käyttö (esimerkiksi GPS ja GLONASS). Lisäksi esimerkiksi Mavic Prossa on käytetty myös hahmon tunnistavaa kameraa ja ultraäänisensoreita vaihtoehtona satelliittipaikannuksen käytölle[25].

Jos satelliittijärjestelmien signaali katkeaa lennon aikana, lennokki siirtyy failsafe-tilaan ja on mahdollista, että lennokki toimii jollain seuraavista tavoista:

- jää paikalleen kunnes signaali palaa
- sammuttaa moottori ja putoaa autorotaation varassa
- laskeutuu välittömästi turvallisella nopeudella
- nostaa korkeutta kunnes signaali palaa
- palaa kohti lähtöpistettä varajärjestelmän, esimerkiksi elektronisen kompassin avulla
- palaa lähtöpisteelle käyttäen seuraten lennon aikana nauhoitettua maastokarttaa
- hakeutuu kohti ohjaimen signaalia

Lennokkien autonomisessa toiminnassa on tasapainoiltava turvallisuuden ja järjestelmän selviytymisen välillä. Turvallisuuden näkökulmasta lennokki voi tehdä toimenpiteitä suhteellisen korkealla, kunnes akun varaus laskee niin alas, että on laskeuduttava. Toisaalta lennokkia ei ole välttämättä turvallista ohjata ilman tarkkaa paikannusta, jolloin autonomian tulisi pakottaa lennokki laskuun riippumatta käyttäjän eduista. Lennokin käyttäjälle on luonnollisesti edullista, että lennokki palaa käyttökunnossa takaisin.

Liitteessä 1 on listattu lennokkikohtaisia eroja. Pääasiallinen toiminta vaikuttaa olevan, että lennokki jää odottamaan GNSS-yhteyden palaamista ollessaan edelleen ohjattavissa. Muutamassa tapauksessa lennokki laskeutuu välittömästi hallitusti. Monipuolisia sensorijärjestelmiä ei käytetä hyväksi muuta kuin aivan laskeutumisen viimehetkillä, jolloin vältetään laskeutuminen epätasaiselle alustalle. Kolmannen osapuolen ohjelmistojen käyttö lennokeissa mahdollistaa räätälöidymmän fail-safe tilan.

Yksi mahdollinen ohjaimen suuntaan hakeutumisen toteutus olisi käyttää ohjelmoitavaa TELLO-lennokkia, johon ohjelmoidaan paluutoiminto hakeutuman ohjaavaan älylaitteeseen. Telloa ohjataan käyttäen WiFi-yhteyttä ja sen RSSI-arvoja voidaan käyttää karkeasti ohjaimen suunnan löytämiseen, sillä tätä tutkimusta varten tehtyjen testien perusteella RSSI on suurin kun lennokin kamera on poispäin ohjaimesta ja pienenee kunnes kamera on kohti ohjainta. Tämä ei luonnollisesti toimi yhtä hyvin reaalimaailman tilanteissa, joissa fail-safe todennäköisesti aktivoituisi, sillä häiriöt ja heijastukset voivat vääristää RSSI-arvoja.

4.3. RPA - Miehittämätön ilma-alus

Tässä tutkielmassa miehittämätön ilma-alus on, Trafin määritelmää:

”kauko-ohjatulla ilma-aluksella (Remotely Piloted Aircraft, RPA) miehittämätöntä ilma-alusta, jota ohjataan kauko-ohjauspaikasta ja käytetään lentotyöhön;”[104]

mukaillen, lentotyöhön tarkoitettu lennokki. Trafin määritelmässä poiketen tässä tutkielmassa käsitelty RPA on varta vasten lentotyöhön suunniteltu ja sitä ei voi hintansa tai ominaisuuksiensa puolesta ajatella tarkoitetuksi harraste- tai urheilukäyttöön.

4.3.1. XBee

XBee on Digi Internationalin tuoteperhe, jonka sirut pohjautuvat IEEE 802.15.4 -standartiin. Osaan siruista on mahdollista asentaa ZigBee, mutta silloin XBee toiminnallisuudet menetetään.[93] Digi International tarjoaa myös Xbee-siruja, joihin on esiasennettu Zigbee. Toinen tarjottu mesh-verkkoratkaisu on DigiMesh, jossa ZigBeestä poiketen kaikki solmut ovat saman arvoisia.[24]

Roddayn tutkimuksessa tarkastellaan XBee868LP-sirua. Siruun on mahdollista ohjelmoida kaksi eri osoitetta (Device High Address ja Device Low Address). Molemmat voivat saada arvon välitä 0x00000000-0xFFFFFFFF, eli kyseessä on 32 bitin osoite. XBee-verkko ei perustu siihen, että lennokki toimisi tukiasemana, kuten WLANin tapauksessa, vaan kybervaikuttamisen mahdollistamiseksi kohteen osoite tulee arvata. Kaksi 32 bittistä osoitetta tarkoittaa pahimmillaan noin 15,4 *10^25 arvauskertaa. Tämä ei ole erityisen paljon, mutta koska siru käyttää EEPROM-muistia (Electronically Erasable Programmable Read-Only Memory), jonka uudelleenkirjoitussyklit loppuvat kesken ennen kuin kaikki osoitteet on voitu testata. Sirun toiminnan emulointi on myös haastavaa, sillä sen firmware on salattu. Käytännössä osoitteiden arvaaminen ”Brute Force”-menetelmällä ei siis ole kannattavaa, vaikka Device High Address on sirun tapauksessa aina 0x00113A200. Ratkaisun ongelmaan tuo kuitenkin XCTU-sovelluksen ”Node Discovery”-ominaisuuden käyttämä broadcast-paketti. Verkon jokainen solu (siru) kuittaa aina paketin omalla osoitteellaan riippumatta siitä, onko paketti lähetetty suoraan solun osoitteeseen, vai broadcastilla.[93]

XBee-PRO 900HP-sirun käyttöohjeessa mainitaan, että osoitteet tulevat IEEE:ltä ja osoite 0x00113A200 on Digi-laitteen tunniste. Device High Address ja Device Low Address termit on vaihdettu Serial Nuber High ja Serial Number Low termeihin, mutta ne ovat edelleen 32 bittisiä. Sirun osoitetta ei ole välttämättä mahdollista päätellä broadcast-paketilla. [20] Vastaava Digi-laitteen tunniste on havaittavissa myös 868LP-sirun seuraajan XBeeSX868RF-sirun käyttöohjeessa, jonka kaikissa esimerkeissä on sama Serial Number High. Lisäksi tässä sirussa on edelleen Roddayn haavoittuvuus broadcast-paketin käytölle.[21]

Sirujen numerointi kuvaa niiden käyttämiä taajuuksia. 900HP:n taajuusalue on 902-928MHz ja se on jaettu kanaviin häiriöiden ehkäisemiseksi[22]. Käyttämällä dipoliantenneja saadaan jopa 15,5 kilometrin kantama[22]. 868LP:n taajuusalue on 863-870MHz. Teoreettinen kantama käyttämällä vahvistavia antenneja on 14,5 kilometriä. [23]

4.3.2. Sensorifuusioon perustuva navigointi

Usean sensorin mittauksen yhdistäminen mahdollistaa tarkemman paikkatiedon lisäksi paremman häiriönsiedon. MEMS-gyroskoopissa voi esiintyä liukumaa, jota voidaan tarvittaessa korjata käyttämällä kiihtyvyysanturien mittauksia[64, s. 26]. Kiihtyvyysantureille häiriötä aiheuttaa mekaaninen kohina[64, s. 26]. Häiriöiden aiheuttamien mittausvirheiden aiheuttama kokonaisvirhe paikkatiedossa kumuloituu ajan myötä, minkä johdosta pelkästään inertianavigointiin ei välttämättä voi luottaa. Tämän takia paikkatieto on syytä tarkistaa aika-ajoin käyttämällä satelliitinjärjestelmää.

Kybervaikutuksen kohdistaminen tällaiseen järjestelmään voi olla haastavaa, sillä järjestelmä voi lopettaa jonkin sensorin käytön siinä olevan virheen kasvaessa liian suureksi ilman, että se menettää täysin kykyä paikantaa itsensä.

5. Lennokkien torjuminen kyberelektronisilla menetelmillä

Tässä luvussa selvitetään mitä kyberelektronisia menetelmiä (CEMA) olisi mahdollista käyttää lennokkeja vastaan. Luvussa tehdään yhteenvetoa ja johtopäätöksiä perustuen aiemmin tässä tutkielmassa esitettyyn teoriaan.

5.1. Tiedon kerääminen

Tiedon keräämisellä tarkoitetaan tässä tutkielmassa tilannetta, jossa lennokki saatetaan kybervaikuttamisen keinoin alttiiksi elektroniselle tiedustelulle tai elektronisella tiedustelulla mahdollistetaan kybervaikuttaminen.

AirFencen käyttämä kolmiomittaukseen perustuva paikantaminen on esimerkki tilanteesta, jossa hyödynnetään sekä elektronista tiedustelua, että kybertiedustelua lennokin sijainnin ja mallin tunnistamiseen. Tämän tiedon perusteella järjestelmä osaa aloittaa soveltuvat vastatoimet. Lennokin tunnistamisen osalta kybertiedustelu on ehkä huono termi, sillä kyseessä on passiivinen taajuuksien valvonta ja lennokin tunnistaminen perustunee Mac-osoiteavaruuksiin ja käytettyyn protokollaan.

Jos lennokki on ohjelmoitu lentämään tiettyä reittiä radiohiljaisuudessa voi siihen yrittää vaikuttaa arvaamalla sen kuuntelema taajuus ja protokolla. WLAN-verkkojen tapauksessa voidaan lähettää ARP-kyselyjä, jolloin lennokki vastaa kyselyyn, jos IP-osoite on oikea. XBee-verkoissa voidaan lähettää broadcastilla Node Discovery-paketti, johon kaikki kyseisessä verkossa olevat sirut vastaavat. On epätodennäköistä, että alueelta olisi mahdollista löytää aiemmin havaitsematon lennokki, joka on ohjelmoitu toimimaan radiohiljaisuudessa, satunnaisilla arvauksilla. Pikemminkin tällaista menetelmää voisi käyttää, kun alueella on havaittu, esimerkiksi valvontakameralla tai näköhavainnon perusteella, joku tietyn mallinen lennokki ja siitä ei ole vielä elektronista havaintoa. Tällöin yhteyden parametrien arvaaminen helpottuisi ja lennokki olisi mahdollista saada säteilemään ja siten paljastamaan oman sijaintinsa.

Varsinaisen havaitsemisen sijaan todennäköisempi käyttötapa olisi signaali ja mittaustiedustelun tukeminen. Jos lennokissa on erillinen ohjaus- ja datalinkki, mutta datalinkki ei ole päällä, voidaan se yrittää käynnistää ohjauslinkin yli. Tällöin datalinkin liikennettä voidaan nauhoittaa myöhempää purkamista varten. Vastaavasti, jos lennokissa on häirintälähetin, niin voi sen toimintaan, kuten moodit ja teho, yrittää vaikuttaa ohjauslinkillä, jolloin häirintälähettimen suorituskyvystä saadaan kerättyä tietoa.

Kybervaikuttaminen luvussa 3.2 käsiteltäviin ohjauslinkkein ei ole mahdollista ilman, että signaalia nauhoitetaan ja päätelaitteiden käyttämät avaimet puretaan. Elektronisen tiedustelun tuki on välttämätön, jos halutaan suunnata kybervaikutusta tällaiseen järjestelmään. Käytännössä lennokkien käyttämiä protokollia kannattaa kerätä valmiiksi, jolloin purkamiseen voidaan käyttää kohdennettuja arvauksia. Jos tiedetään, että protokolla käyttää aina 16 tai 32 bittistä avainta, niin on turhaa kokeilla minkään muun pituisia. Tämä vähentää arvauksien määrää noin puoleen.

5.2. Kaappaaminen

Kaappaamisella tarkoitetaan tässä tutkielmassa tilannetta, jossa kybervaikuttamisella onnistutaan väärentämään lennokkien ohjaussignaaleja riittävästi, että lennokki on ohjattavissa puolustajalle edullisella tavalla esimerkiksi pakottamalla se laskuun tai törmäyttämällä se esteeseen.

Tammikuun 5. ja 6. päivän välisenä yönä 2018 Venäjä tuhosi ilmatorjunnalla seitsemän ja pakotti laskuun kuusi terroristien käyttämää lennokkia. Näistä kuudesta kolme tuhoutui niihin kiinnitettyjen pommien räjähtäessä. Lennokit olivat iskemässä Syyrian Latakian lähistöllä sijaitsevaan Khmeimimin lentotukikohtaan. Niihin oli ohjelmoitu kohteita tukikohdan sisällä ja ne oli varustettu videokameralla. [107] Lennokit lensivät aluksi esiohjelmoitua reittiä, mutta kohdatessaan häirintää ne vaihtoivat kauko-ohjaukseen. Venäjän varapuolustusministerin Alexander Fominin mukaan kauko-ohjaus toteutettiin Yhdysvaltojen alueelle lähettämästä Poseidon-8 tiedustelukoneesta käsin.[105] Riippumatta siitä kuinka uskottavina Venäjän puolustusministeriön edustajien lausuntoja pitää, kuvastaa tämä operaatio Venäläisestä näkökulmasta uskottavaa lennokkeja vastaan suunnattua CEMA-operaatiota osana tukikohdan ilmatorjuntaa.

Operaatiossa lennokit saatiin fail-safe -tilaan elektronisella vaikuttamisella, jolloin niihin oli mahdollisuus kohdistaa kybervaikutusta. Koska kauko-ohjaus oli edelleen mahdollista, häirintä kohdistettiin todennäköisesti lennokkien satelliittinavigointiin. Lennokin oli jollain tapaa joko tunnistettava itse häirintä tai se vaihtoi kauko-ohjaukseen joko satelliittiyhteyden menettämisen tai saavutetun reittipisteen perusteella. Häirinnän tunnistamista puoltaa tieto, että Venäläisillä on kyky harhauttavaan GPS-häirintään, jollaista Iran käytti Yhdysvaltalaista tiedustelulennokkia vastaan. Tässä tapauksessa satelliittiyhteyttä ei olisi näennäisesti missään kohtaa menetetty, eli kyseessä ei olisi tavanomainen fail-safe. Vaihtoehtoisesti lennokkien kauko-ohjauspaikka tunnisti häirinnän ja käski lennokkia luopumaan ennalta ohjelmoitujen reittipisteiden seurannasta ja alkaa noudattaa kauko-ohjausta. Tavanomaisen peittävän häirinnän käyttöä puoltaisi, jos Venäläiset olisivat tunnistaneet kyseessä olevan aseistetut lennokit ja riskianalyysin perusteella eivät halunneet niiden laskeutuvan sen hetkisellä lentosuunnalla. Se, että lennokit vaihtoivat kauko-ohjattuun tilaan jonkin tietyn pisteen perusteella, ei ole kovin todennäköistä, koska lennokkeihin oli ohjelmoitu maalipisteitä.

Elektroninen vaikuttaminen oli tärkeää operaation onnistumisen kannalta, sillä ennen sitä kauko-ohjauksesta ei ilmeisesti ollut viitteitä. Ohjaussignaali olisi tässä tapauksessa ollut tunnistettavissa uutena signaalina, joka ilmaantuu reaktiona häirintään. Signaali on todennäköisesti ISM-taajuusalueella, sillä siihen soveltuvia lähetin- ja vastaanotinsiruja on helposti saatavilla. Jos up- ja downlink käyttivät samaa taajuutta ja protokollaa, lennokkien lähettämien signaalien purkaminen auttaa ohjauslinkin väärentämisessä. Elektronista vaikuttamista käytettiin mahdollisesti myös kauko-ohjauspaikan signaalien häiritsemiseen, jolloin kauko-ohjauspaikalla ei ollut mahdollisuuksia korjata lennokin korkeutta. Vain puolet lennokeista tuhoutui laskeutumisen yhteydessä, mikä viittaa siihen, että lennokit olivat täysin Venäläisten hallinnassa.

WLAN-yhteyden kaltaisissa ohjauslinkeissä, jossa on käytössä useampi kanava, kybervaikutuksen tehostaminen häirinnällä toteutetaan häiritsemällä alkuperäistä kanavaa ja lähettämällä väärennettyä liikennettä toisella kanavalla. Tätä vaikutusta voidaan edelleen tehostaa häiritsemällä kaikkia muita kanavia, jolloin kauko-ohjauspaikalla on haastavampaa palauttaa yhteyttä kanavaa vaihtamalla.[77] Kaikkien WLAN kanavien häirintää helpottaa se, että niissä käytetään julkistettuja taajuuksia ja koodijakokanavoinnin avaimia. Tämän tyyppisten verkkojen häirintä poikkeaa perinteisestä häirinnästä siten, että myös lähettäjää voi häiritä.

Käyttämällä älykästä häirintää, kanavaa voidaan häiritä aina, kun havaitaan kauko-ohjauspaikan liikennettä, joka on tunnistettavissa otsikkokehyksestä. Ilmiö on vastaava kuin aiemmin esitelty bluetooth DoS-hyökkäys, jossa isäntälaitteen osoitteen väärentämisellä saatiin aikaan päällekkäisiä signaaleja. Vastaavasti kaikki lennokin vastaanottokuittaukset voi häiritä, jolloin ohjauspaikka joutuu lähettämään paketteja uudelleen. Jos verkossa käytetään protokollaa, joka ei edellytä vastaanottokuittauksia, kuten UDP tai RTSP, voidaan verkkoa häiritä aina kun hyökkääjä ei lähetä, jolloin MAC-protokollaa noudattava kauko-ohjauspaikka ei missään kohtaa pysty lähettämään, sillä se odottaa kanavan vapautumista. [109] Nämä menetelmät edellyttävät, että ohjaimen signaali on havaittavissa.

Koska MAC-protokollan CW-arvo ehkäise päällekkäisiä lähetteitä normaalissa toiminnassa ja hyökkääjän voidaan olettaa käyttävän sitä virheellisesti, ei ohjausasema todennäköisesti onnistu häiritsemään omilla lähetteillään hyökkääjän lähetteitä. Jos ohjauspaikan suunta saadaan pääteltyä ja häiritä kyetään suuntaamaan siihen ilman, että lennokkia häiritään, ohjausaseman näkökulmasta kanava on tukossa, jolloin se odottaa lähetysvuoroaan. Tässä tapauksessa häirintä voi olla jatkuvaa. Häirinnän tehokkuutta voi parantaa käyttämällä oikein muodostettuja paketteja, mutta myös satunnainen kohina vaikeuttaa ohjausaseman toimintaa merkittävästi.

Kuva 16 Elektoninen vaikuttaminen mesh-verkon solmukohtaan

XBeessä käytettävät DigiMesh- ja ZigBee-protokollat mahdollistavat ohjauslinkin muodostamisen käyttäen mesh-verkkoa. Näin saavutetaan pitempi kantama, mutta verkkoon saattaa muodostua haavoittuvia solmukohtia. Vastaava tilanne voi syntyä, jos WLAN-ohjauslinkin kantamaa lisätään käyttämällä WLAN-toistinta, kuten [51] tapauksessa. Suuntaamalla elektroninen vaikuttaminen tällaiseen solmukohtaan, voidaan katkaista lennokkien yhteys kauko-ohjauspaikkaan. Tämän jälkeen ohjauslinkin kaappaaminen ei vaadi enää kanavan vaihtamista, sillä kauko-ohjauspaikka on kaapattavien lennokkien näkökulmasta hiljentynyt. Tällöin niille voi lähettää alkuperäisellä kanavalla ohjauskomentoja ilman, että syntyy kilpailutilannetta tai signaalien keskinäistä häiriötä.

5.3. Ilmatilan käytön estäminen

Ilmatilan käytön estämisellä tarkoitetaan tässä tutkielmassa tilannetta, jossa vaikuttamisella saadaan aikaan tilanne, jossa lennokin ohjaaminen alueella muuttuu mahdottomaksi. Tämä menetelmä on helpompi automatisoida eikä lennokille tarvitse määritellä laskeutumisaluetta. Lisäksi vältytään hallitsemattomassa laskeutumisessa tuhoutuneeseen lennokkiin kohdistuvilta korvausvaatimuksilta.

Kaupallisissa lennokeissa saattaa olla tietyllä komennolla aktivoitava RTH (Return To Home)-toiminto, joka saa lennonkin palaamaan joko reittiä noudattaen, tai lyhyintä tietä lähtöpaikalleen. Teknisesti tämän toiminnallisuuden hyväksikäyttäminen tapahtuu kuten AirFencen laskunpakottamisen tapauksessa, eli tunnistamalla lennokki ja lähettämällä asiaankuuluva komento. On mahdollista, että lennokin ohjaaja tunnistaa tilanteen ja palauttaa lennokin takaisin hallintaansa. Tämän estämiseksi lennokin ohjauslinkkiä tulee häiritä välittömästi RTH-komennon lähettämisen jälkeen.

Jos maali tunnistetaan lennokiksi, jonka fail-safe joko GNSS- tai ohjausyhteyden menettämisen jälkeen on palata kohti lähtöpaikkaa, voidaan lennokki saada poistumaan alueella pelkällä elektronisella vaikuttamisella. Tällöin kyber-komponenttina on tarvittaessa maalin tunnistaminen. Maalin tunnistaminen on oleellista, jos halutaan varmistaa, että lennokin fail-safe ei ole välitön laskeutuminen, paikalleen jääminen kunnes akun varaus pakottaa laskeutumaan tai lennokki putoaa akun tyhjennyttyä.

Estesensoreilla varustetuille lennokeille voi olla mahdollista luoda valemaaleja. Yksinkertainen esimerkki olisi alaspäin suunnatun optisen tai akustisen sensorin häirintä niin, että lennokki luulee olevansa lähellä pintaa ja joko nostaa korkeutta tai ainakin estää korkeuden vähentämisen. Sensorifuusion käyttäminen lennokissa ei merkittävästi vähennä tämän menettelemän tehoa, sillä korkeutta esteistä ei voi mitata suurimmalla osalla lennokeissa tyypillisesti olevista sensoreista, kuten barometrilla, joka mittaa vain korkeutta suhteessa lähtöpaikkaan.

Lennokin kameran häikäiseminen on ainakin teoriassa mahdollista, mutta kameran havaitseminen ja tunnistaminen muista heijastavista kohteista on haastavaa. Häikäisemällä voidaan suojata yksittäisiä kohteita, sillä järjestelmällä pitää olla näköyhteys kameran CCD-kennoon. Häikäiseminen tekee kameran kuvista ja videosta käyttökelvottoman, mutta ei vahingoita kameran käyttäjää.[91] Käyttämällä lasershow teholuokan lasereita voidaan kameran sensoria vahingoittaa pysyvästi[73]. Häikäisemisen itsessään ei sinänsä sisällä tämän tutkielman tarkoittamaa kyber-elementtiä, sillä valotuksen säätäminen ja kohteen ylivalottuminen ovat osa kameran tavanomaista toimintaa. Tulevaisuudessa kameroissa saattaa olla kuvaamisen estävä suojatoiminto [theatlantic], jota on ehkä mahdollista käyttää väärin.

5.4. Lentoon puuttuminen

Lentoon puutumisella tarkoitetaan tässä tutkielmassa tilannetta, jossa kybervaikuttamisella vaikeutetaan lennokin käyttämään reittiin ilman, että ohjaussignaalia onnistutaan kaappaamaan. Tämän menetelmän tavoitteena on estää lennokin tehtävän suorittaminen ja lennokin tuleva käyttö pakottamalla se laskeutumaan.

Jos lennokki lentää GNSS-navigoinnin varassa, voidaan se pakottaa laskeutumaan väärentämällä korkeustietoa. Ohjaajan on kuitenkin mahdollista havaita tällainen häirintä ja joko kytkeä satelliittinavigointi pois, tai korjata korkeutta aktiivisesti. Kuten kaappaustilanteessa, lennokki saattaa lentää ennalta ohjelmoituja reittipisteitä pitkin, jolloin ohjaussignaali paljastuu vasta häirintätilanteessa. Jos ohjaussignaali saadaan häirittyä nopeammin kuin sillä saadaan korjattua virheellinen korkeuden muutos, saadaan lennokki törmäytettyä maahan.

Lennokin NFZ-ominaisuus ei välttämättä ole poiskytketty, vaikka se toimiikin lentoaseman läheisyydessä. Tämä johtuu siitä, että läheskään kaikkia lentopaikkoja ei ole listattu rajoitusalueeksi. Väärentämällä GNSS-paikkatieto varmaan lentokieltoalueeseen, kuten Helsinki-Vantaa tai Washington DC, voidaan lennokki saada laskeutumaan NFZ-ominaisuuden avulla. Tässä tilanteessa ei välttämättä ole tarpeen häiritä ohjaussignaalia, mutta tällöin riskinä on, että laskeutuminen voidaan keskeyttää.

Joissain lennokeissa on hätälaskeutumistoiminto, jota voidaan käyttää samalla tavalla kuin aiemmin mainittua RTH-toimintoa. Visuo-lennokin hätälaskeutuminen sammuttaa kopterin ja se laskeutuu autorotaation varassa[112]. Tällöin ohjauslinkkiä ei tarvitse häiritä, sillä laskeutumista ei enää voi keskeyttää. Jos hätälaskeutuminen suoritetaan sensorien varassa, on lennokissa edelleen virta, jolloin ohjauslinkkiä on tarpeen häiritä. Laskeutumissensorit ovat usein optisia tai akustisia, jolloin niiden häirintä ei välttämättä ole mahdollista kovin suurilla etäisyyksillä. Niiden häirinnällä voitaisiin varmistaa lennokin laskeutuminen myös sille epäotolliselle alustalle, jolloin vältettäisiin lennokin jääminen leijumaan ja odottamaan ohjaimen lupaa laskeutua epätasaiselle alustalle.

5.5. Tuhoaminen

Tuhoamisella tarkoitetaan tässä tutkielmassa tilannetta, jossa lennokki tuhotaan tarkoituksellisesti käyttämällä joko elektronista tuhoamista tai pakottamalla se putoamaan korkealta. Menetelmän etuna on se, että lennokki saadaan nopeasti poistettua pysyvästi käytöstä ilman, että sitä on tarpeen täysin kaapata.

Elektronisessa tuhoamisessa käytettävien Laser- ja HPEM-aseiden kantama on rajallinen, jolloin lennokki voidaan pitää tai saattaa niiden ulottuville käyttäen jotain aiemmin tässä luvussa esiteltyä keinoa. Esimerkiksi tilanteessa, jossa lennokki lentää aseen alakatveessa, voidaan se pakottaa nostamaan korkeutta joko aktivoimalla lennokin RTH tai saattamalla lennokki korkeuden nostoa vaativaan fail-safe tilaan.

Pudottamalla lennokki korkealta saadaan lennokkiin todennäköisesti aiheutettua lamauttavaa vahinkoa, sillä autorotaatio vaikuttaa liitteessä 1 käsiteltyjen lennokkien käyttöohjeiden sisältämien varoitusten perusteella harvinaiselta. Tämä voi osin johtua lennokkien suuresta massasta suhteessa niiden roottorien pinta-alaan ja osin roottoreiden lukitustoiminnosta.

Hyväksikäyttämällä lennokkien hätäseis ominaisuutta, voidaan lennokki saada putoamaan korkealta. Tässä tapauksessa alkuperäisen ohjaimen signaali on todennäköisesti saatava estettyä joko elektronisella tai kybervaikuttamisella, sillä hätäseis vaatii joissain tapauksissa pitkän ohjauskomennon, jolloin alkuperäinen ohjain voi estää komennon suorittamisen.

Kriittisen virheen aiheuttaminen lentotietokoneeseen käyttämällä hyväksi haittakoodin syöttämistä esimerkiksi videonsiirtoprotokollan kautta, aiheuttaa ainakin Mavic Pron osalta moottorien hätäseis toiminnon, kun taas GoPro Karma yrittää laskeutua virheestä huolimatta. Jos hyväksikäytettävä kriittinen virhe vaatii tietyn lentomoodin ,voidaan kybervaikutusta joutua tukemaan häirinnällä. Esimerkiksi Mavicin tapauksessa ATTI, on GNSS-signaali katkaistava häirinnällä ennen kuin haittakoodi syötettään. Tällöin lennokki vaihtaa automaattisesti ATTI-moodiin eikä ohjaajalla ole käytännössä mahdollisuutta vaihtaa moodia takaisin, sillä lennokki tunnistaa GNSS-signaalin puuttumisen.

6. Johtopäätökset

Kyberelektroninen vaikuttaminen tekee lennokkien torjunnasta hallittavampaa. Lennokkien torjunta voi aiheuttaa suuremman ongelman, kuin itse lennokki, aiheuttaen häiriöitä lennonvarmistuslaitteisiin, miehitetyille ilma-aluksille ja ympäröivälle yhteiskunnalle. Alueelle kuulumattoman lennokin luotettava tunnistaminen, paikantaminen ja asteittaiset vastatoimet vähentävät näitä riskejä.

Elektroninen häirintä on erityisen tehokas vastatoimi, sillä CDMA/CA menetelmää käyttävissä verkoissa ei ole väliä häiritäänkö ohjainta vai lennokkia. Häirintä ei ole myöskään tässä tapauksessa välttämättä tehokilpailu, vaan se voi olla kybervaikuttamisen keino. Pelkän taajuuden perusteella häirintää ei kuitenkaan kannata aloittaa, sillä lennokit reagoivat eri tavalla häirintään. Pahimmillaan lennokki voi lähteä ajelehtimaan ja pudotessaan vahingoittaa henkilöitä tai materiaalia. Kesäaikaan myös maasto- ja metsäpalojen riskiä on syytä arvioida.

Lennokkien käyttämien taajuuksien ja protokollien kirjo on laaja. Kybervaikuttaminen aiemmin tuntemattomaan lennokin ohjauslinkkiin on haastavaa, sillä salauksen purkaminen vaatii aina jonkin lähtökohdan. Satunnaista arvailua vaikeuttaa, että salauksia voidaan käyttää useampaa päällekkäin, mikä kasvattaa vaadittavien arvausten määrää nopeasti. Tämän vuoksi on ylläpidettävä uhkakirjastoa, johon kerätään jo ennen lennokin muodostumista ongelmaksi tietoa linkin toiminnasta ja mahdollisista haavoittuvuuksista. Kybervaikuttaminen ei voi olla ainoa vastatoimi suojattaessa kriittisiä kohteita.

Kybervaikuttamista vaikeuttavat pahantahtoiset kybervaikuttajat. Lennokkien valmistajat joutuvat päivittämään omia järjestelmiään, jolloin myös mahdollisesti päivitettävän Poliisilain suoma laillinen kybervaikuttaminen vaikeutuu mahdollisten haavoittuvuuksien vähentyessä. Lennokkeihin on mahdollista ohjelmoida suoja-alueita, joilla lentäminen ei ole mahdollista. Tätä kuitenkin vaikeuttaa valmistajien tietokantojen vajavaisuus ja mahdolliset tavat, joilla suojaominaisuuksia voi kiertää. Asiakkaat haluavat lennokkeja, joilla voi lentää tarvittaessa myös sisällä ilman GNSS-signaalia. Myöskään ulkona lentämistä ei haluta rajoittaa liiaksi.

Osa lennokkivalmistajista tuottaa myös ohjauslinkkien protokollat, jolloin niistä ei ole saatavilla helposti kattavaa tietoa. Security through obscurity lähestyminen toimii jonkin aikaa, mutta mahdollistaa nollapäivähyökkäysten keräämisen. Palkkioiden maksaminen virheitä löytäville hakkereille ja yhtiöön palkattujen hakkereiden käyttö lieventää ongelmaa.

Monikäyttöiset protokollat, kuten 802.11 ja 802.15 soveltuvat käytettäväksi myös lennokeissa. Niissä olevat haavoittuvuudet löytyvät nopeasti, koska ne ovat laajasti käytössä. Näiden nollapäivähaavoittuvuudet ovat sen takia arvokkaampia ja millään yksittäisellä valmistajalla ei ole välttämättä mahdollisuutta maksaa riittävän suurta palkkiota, että niitä ei myytäisi mieluummin rikollisille tai haavoittuvuuksia välittäville yrityksille. Esimerkiksi Zerodium voi maksaa jopa 100 000$ WiFi:stä löydetystä nollapäivästä[134].

Wi-Fi WPA3 tekee 802.11 protokollasta todella varteenotettavan kilpailijan valmistajien omille protokollille. Pääosa tässä tutkielmassa esitellyistä kybervaikuttamisen keinoista perustuu nimenomaan salaamattomien hallintakehysten väärinkäyttöön. Jos alkuperäistä verkon muodostumista ei onnistuta kuuntelemaan, keinot rajoittuvat käytännössä ohjauslinkin toiminnan vaikeuttamiseen käyttämällä hyväksi MAC-tason haavoittuvuuksia.

Olemassa olevien järjestelmien suorituskyky ei ole riittävä, että lentotoiminta saataisiin luotettavasti suojattua lentokentän alueelta käsin. Kiitotien jatkeilla toimivat lennokit ovat merkittävästi suurempi uhka lentotoiminnalle kuin lentokentän päällä olevat. Tämä johtuu suuremmista tilannenopeuksista mahdollisten törmäyksien sattuessa. Operaatioturvallisuuden näkökulmasta tilanne on käänteinen. Jos lennokkiin vaikutetaan protokollalla, joka edellyttää kaksisuuntaista yhteyttä, nousee lennokin teho rajoittavaksi tekijäksi. Elektronisella vaikuttamisella ei ole tätä rajoitusta, jolloin se kannattaa säilyttää osana lennokintorjuntajärjestelminä muutoinkin, kuin pelkästään kyberiä tukevana osana.

Mikrokontrollereiden ja pienoistietokoneiden ympärille rakentunut kehittäjäyhteisö on tehnyt kehittyneiden omatekoisten lennokkien valmistamisesta helppoa. Kyberelektronista torjuntaa vaikeuttaa se, että vaikka taajuuksien käytöstä on viestintäviraston määräys[72], tällaisten lennokkien käyttämät taajuudet ja lähetystehot eivät välttämättä noudata sitä. Vaikka ohjauslinkissä käytetty siru onnistuttaisiin tunnistamaan, sen ohjauslinkin komennot voivat olla tuntemattomia. Jos lennokki on tehty varta vasten kiertämään vastatoimia, ei sen ohjauslinkki välttämättä edes ole päällä. Tällöin mahdollisia vastatoimia on GNSS-häirintä, elektroninen tuhoaminen tai kineettinen tuhoaminen.

Sekä kaupalliset toimijat, että harrastelijat luovat kaupallisiin lennokkeihin omia ohjelmistojaan. Näin olemassa olevan rungon aerodynaamista ja sähköteknistä suorituskykyä ei tarvitse kehittää itse, vaan voidaan hyödyntää mahdollisesti miljoonien arvoinen tuotekehitys, jonka esimerkiksi DJI on tehnyt. Osa lennokeista on jopa varta vasten tehty jollain asteella kehitysalustaksi, jolloin mahdollinen firmwaren salaaminen tai muut suojakeinot eivät muodostu ongelmaksi.

6.1. Luotettavuus

Luvussa 3 sekä liitteissä 1 ja 2 on käytetty lähteenä valmistajien antamia tietoja, jolloin ilmoitetut ominaisuudet eivät välttämättä toteudu käytännössä, vaan ne ovat mahdollisia vain laboratorio-olosuhteissa tai jopa pelkästään teoriassa. Luvussa 3 toteutettu matemaattinen tarkastelu tukee tätä olettamusta.

Luvussa 4 esitelty teoria on pyritty varmentamaan kokeellisesti. XBee:n osalta kokeellisessa varmentamisessa on luotettu toiseen tutkimukseen, mutta siinä esitetyt havainnot ovat linjassa valmistajan ilmoittamien tietojen kanssa.

Tutkimuksen kannalta keskeisiä kybermenetelmiä on onnistuttu tutkimaan useasta lähteestä ja WLAN:in osalta varmentamaan kokeellisesti. Vaihtoehtoisesti ammattilaiskäyttöön soveltuvien lennokkien osalta tarkasteluun valitun XN297L-sirun toimintaa ei kyetty luotettavasti tutkimaan, sillä yhtään pakettia ei onnistuttu kaappaamaan. Tätä koetta edeltävä ohjaimien taajuuksien kartoitus on sen sijaan luotettava, sillä niitä onnistuttiin toistuvasti nauhoittamaan vaikka ohjaimista poistettiin mittausten välissä paristot muistin tyhjentymisen varmistamiseksi.

Luvussa 5 pääosa sisällöstä perustuu aiemmista luvuista vedettyihin johtopäätöksiin. Kaappaamisesta on esitetty esimerkki, mutta sekin perustuu vain yhden organisaation lähteisiin, jolloin annettuja tietoja ei kyetä varmistamaan muista lähteistä.

6.2. Tutkimusmenetelmien soveltuvuus

Valittu tutkimusmenetelmä soveltui tutkimukseen, vaikka CEMA vaikuttaa olevan puhtaasti sotilastermi ja siitä suomennettu kyberelektronisen menetelmät esiintyy ensimmäisen kerran tässä tutkielmassa. Nämä menetelmät vaikuttavat sulautuvan kyberin alle eikä elektronisia ja kyber-menetelmiä koeta tarpeelliseksi erotella.

Tutkituista lennokintorjuntajärjestelmistä olisi voinut yrittää saada tietoa suoraan valmistajilta. Esimerkiksi Sensofusion Oy toimii Espoossa, jolloin tiedonvaihto olisi ollut mahdollista. On kuitenkin huomioitava, että tietojen käytettävyyttä olisi saattanut rajoittaa salassapitovelvollisuus, mikä on havaittavissa aiemmin Puolustusvoimille luovutetuissa tiedoissa.

Tutkimuksessa löydettyjen mahdollisten kyberelektronisten menetelmien osalta olisi syytä suorittaa käytännön kokeita. Vaikka menetelmät vaikuttavat kirjallisuuskatsauksen perusteella mahdollisilta, voivat kyber- ja elektroniset menetelmät häiritä toisiaan käytännössä.

Kirjallisuuskatsauksen kokeellinen varmistaminen sekä urheilu ja harraste lennokkien että vaihtoehtoisesti ammattilaiskäyttöön soveltuvien lennokkien osalta osoittautui liian laajaksi ottaen huomioon tutkimukseen varattu aika. Tämän takia vaihtoehtoisesti ammattilaiskäyttöön soveltuvan lennokin ohjauslinkin kokeiden tulokset jäivät alustaviksi. Rajaus olisi ollut realistisempaa tehdä vain yhteen lennokkityyppiin ja perehtyä siihen laajemmin.

6.3. Jatkotutkimustarpeet

Elektroninen vaikuttaminen lennokkia vastaan. Tässä tutkielmassa pääpaino oli kybertoiminnoissa, jolloin lopullinen arvio mahdollisista kyberelektronisista toimintamahdollisuuksista ja niiden eduista vaatii paremman perehtymisen siihen, miten lennokkiin voi vaikuttaa käyttäen tavanomaista elektronista vaikuttamista.

Vastaavasti on tarpeen tutkia tavanomaisen elektronisen tiedustelun kykyä tunnistaa ja kerätä tieto lennokeista.

Multikoptereiden lentoajan mallintaminen tarkemmin voi antaa paremman kuvan lennokin toiminta-ajasta ja sitä voitaisiin hyödyntää osana kalman-suodinta lennokin omissa järjestelmissä.

Inertianavigoinnin käyttämien sensorien häirintä aiheuttamalla resonanssia akustisin keinoin tai virhettä mittauspiiriin sähkömagneettisen induktion avulla voi olla mahdollista. Tämä poistaisi yhden ilmeisen heikkouden, sillä kyberelektronisten keinojen käyttäminen radiohiljaisuudessa lentävään lennokkiin on haastavaa etenkin, jos se ei käytä satelliittinavigointia.

LÄHTEET

[1] 3D Robotics. Solo User Manual V9. Julkaistu 2015. Saatavissa: https://3dr.com/wp-content/uploads/2017/03/v9_02_25_16.pdf

[2] 3D Robotics. 3DR Solo Drone [verkkosivu]. Viitattu 6.4.2019. Saatavissa: https://3dr.com/solo-drone

[3] 3D Robotics. Iris Operation Manual V6. Julkaistu 09.04.2014. Saatavissa: https://3dr.com/wp-content/uploads/2017/03/IRIS-Operation-Manual-v6.pdf

[4] Air Navigation Services Finland Oy. Suomen ilmailukäsikirja WEF 28 FEB 2019. Saatavissa: https://www.ais.fi

[5] Ali-Löytty, Simo. Kalmanin suodatin ja sen laajennukset paikannuksessa. Diplomityö. Tampere, 2004. Tampereen teknillinen yliopisto, Teknis-luonnontieteellinen osasto, Matematiikan laitos. 80 s.

[6] Anu Leena Koskinen. Droneista aiheutuvat ilmatilaloukkaukset ja läheltä piti -tilanteet roimassa nousussa Suomessa: "Aina on niitä, joita ei tunnu kiinnostavan". YLE, 19.7.2018 klo 18:39. Viitattu 3.9.2018. Saatavissa: https://yle.fi/uutiset/3-10312670

[7] Andrei Barysevich. Military Reaper Drone Documents Leaked on the Dark Web. Recorded Future, 10.07.2018. Saatavissa https://www.recordedfuture.com/reaper-drone-documents-leaked

[8] ASSURE. ASSURE UAS Airborne Collision Severity Evaluation Final Report. Saatavissa: http://www.assureuas.org/projects/deliverables/sUASAirborneCollisionReport.php

[9] Autel Robotics. EVO User Manual With XI-5A Gimbal. Saataviss: https://auteldrones.com/pages/downloads

[10] Autel Robotics. https://auteldrones.com/products/evo

[11] Autel Robotics. X-Star (Premium) User Manual. Saatavissa: https://auteldrones.com/pages/downloads

[12] Gatwick ‘no drone’ police comment ‘miscommunicated’. BBC, 24.12.2018. Saatavissa: https://www.bbc.com/news/uk-england-46670714

[13] Bluetooth. Specification Volume 0, Specification of the Bluetooth System, Master Table of Contents & Compliance Requirements, Covered Core Package version: 4.0. Julkaistu 30.06.2010.

[14] Bolanakis, Dimosthenis E. MEMS Barometers Toward Vertical Position Detection: Background Theory, System Prototyping, and Measurement Analysis. Morgan & Claypool publishers. ISBN: 9781627059688

[15] Burtsov, Petri. Drooni pysäytti lennot Frankfurtin lentokentällä. YLE, 22.3.2019 klo 19:23 päivitetty 22.3.2019 klo 19:26. Viitattu 30.3.2019. Saatavissa: https://yle.fi/uutiset/3-10703665

[16] Cherise S. Krochmal M. RFC6761 Special-Use Domain Names. Internet Engineering Task Force (IETF). 2.2013

[17] Cisco. 802.11w Protected Management Frames. Saatavissa: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/11rkw_DeploymentGuide/b_802point11rkw_deployment_guide_cisco_ios_xe_release33/b_802point11rkw_deployment_guide_cisco_ios_xe_release33_chapter_0100.pdf

[18] de Fátima Bento, Maria. Unmanned Aerial Vehicles. InsideGNSS, 2008. p. 54-61. Saatavissa: http://www.insidegnss.com/auto/janfeb08-wp.pdf

[19] Department13. MESMER Counter Drone Solution [esite]. Saatavissa: https://department13.com/dev/wp-content/uploads/2018/03/D13-MESMER-Brochure1.pdf

[20] Digi International. XBee-PRO 900HP DigiMesh Kit Radio Frequency (RF) Module User Guide. Julksaistu 3.2016.

[21] Digi International. XBee SX 868 Radio Frequency (RF) Module User Guide. Julksaistu 5.2018.

[22] Digi International. DIGI XBee-PRO 900HP, Long-range 900 MHz OEM RF module [esite]. Saatavissa: https://www.digi.com/pdf/ds_xbeepro900hp.pdf

[23] Digi International. DIGI XBee SX 868, Low-power RF module for Europe[esite]. Saatavissa: https://www.digi.com/pdf/ds_xbee-sx-868.pdf

[24] Digi International Inc. Digi XBee RF Modules. 2019. Saatavissa: https://www.digi.com/products/embedded-systems/rf-modules

[25] DJI. Mavic Pro User Manual v2.0[käyttöohje]. Julkaistu 12.2017. Saatavissa: https://www.dji.com/mavic/info#downloads

[26] DJI. Phantom 4 User Manual v1.0. Julkaistu 03.2016. Saatavissa: https://dl.djicdn.com/downloads/phantom_4/en/Phantom_4_User_Manual_en_v1.0.pdf

[27] DJI. Phantom 3 standard User Manual v1.4. Julkaistu 10.2015. Saatavissa: https://dl.djicdn.com/downloads/phantom_3_standard/en/Phantom_3_Standard_User_Manual_v1.4_en_0112.pdf

[28] DJI. Inspire 1 User Manual v1.0. Julkaistu 03.2015. Saatavissa: http://download.dji-innovations.com/downloads/inspire_1/en/Inspire_1_User_Manual_v1.0_en.pdf

[29] DJI. Inspire 2 User Manual v1.0. Julkaistu 01.2017. Saatavissa: https://dl.djicdn.com/downloads/inspire_2/20170104/INSPIRE+2+User+Manual+.pdf

[30] DJI. Phantom 2 Manual v1.2. Julkaistu 10.2014. Saatavissa: wnload.dji-innovations.com/downloads/phantom_2/en/PHANTOM2_User_Manual_v1.2_en.pdf

[31] DJI. Matrice 600 User Manual v1.0. Julkaistu 07.2017. Saatavissa: https://dl.djicdn.com/downloads/m600/20170717/Matrice_600_User_Manual_v1.0_EN.pdf

[32] DJI. Matrice 100 User Manual v1.6. Julkaistu 03.2016. Saatavissa: https://dl.djicdn.com/downloads/m100/Matrice_100_User_Manual_V1.6_ES.pdf

[33] DJI. Spark User Manual v1.6[käyttöohje]. Julkaistu 10.2017. Saatavissa: https://www.dji.com/fi/spark/downloads

[34] DJI. Phantom Quick Start Manual v1.7. Julkaistu 25.09.2013. Saatavissa: https://dl.djicdn.com/downloads/phantom/en/PHANTOM_Quick_Start_Manual_v1.7_en.pdf

[35] DJI. Spreading Wings S1000 User Manual v1.00. Julkaistu 24.02.2014. Saatavissa: http://dl.djicdn.com/downloads/s1000/en/S1000_User_Manual_v1.10_en.pdf

[36] DJI. FlameWheel 450 User Manual v2.2. Julkaistu 05.2015. Saatavissa: http://dl.djicdn.com/downloads/flamewheel/en/F450_User_Manual_v2.2_en.pdf

[37] DJI. DJI LightBridge 2 Relese Note. Julkaistu 03.11.2016. Saatavissa: https://dl.djicdn.com/downloads/lightbridge2/20181225/DJI_Lightbridge_2+_Release_Notes_EN.pdf

[38] DJI. DJI Demands Withdrawal Of Misleading Drone Collision Video [Avoin kirje]. Julkaistu 19.10.2018 Saatavissa: https://www.dji.com/fi/newsroom/news/dji-demands-withdrawal-of-misleading-drone-collision-video

[39] DJI. Fly Safe GEO ZONE MAP [verkkosivu]. Viitattu 1.2.2019. Saatavissa: https://www.dji.com/fi/flysafe/geo-map

[40] DJI. DJI Bug Bounty Program Policy[verkkosivu]. Viitattu 30.1.2019. Saatavissa: https://security.dji.com/policy?lang=en_US

[41] DJI. https://www.dji.com/fi/products

[42] Dukowitz, Zacc. What's the Most Popular Drone in the U.S.? New FAA Data Answers This Question and More. UAV Coach, 29.11.2019. Saatavissa: https://uavcoach.com/faa-drone-data/

[43] RPi GPIO Code Sample [wiki]. Saatavissa: https://elinux.org/RPi_GPIO_Code_Samples

[44]Engadget. https://www.engadget.com/2016/09/19/gopro-karma-drone/

[45] Euroopan parlamentin ja neuvoston direktiivi 2004/108/EY, annettu 15 päivänä joulukuuta 2004, sähkömagneettista yhteensopivuutta koskevan jäsenvaltioiden lainsäädännön lähentämisestä ja direktiivin 89/336/ETY kumoamisesta

[46] Euroopan komission täytäntöönpanoasetus N:o 923/2012

[47] Euroopan sähköisen viestinnän komitea. Suositus ECC/REC/(06)04. USE OF THE BAND 5 725-5 875 MHz FOR BROADBAND FIXED WIRELESS ACCESS (BFWA). 2006

[48] Fisher RD Jr. IDEX 2017: Poly reveals Silent Hunter fibre-optic laser system. Jane's Defence Weekly. Julkaistu 20.2.2017. Viitattu 3.9.2018 Saatavissa: https://janes.ihs.com/Janes/Display/1796879

[49] Goodin, Dan. There's a new way to take down drones, and it doesn't involve shotguns. arsTechnica BIZ&IT, 27.10.2016. Saatavissa: https://arstechnica.com/information-technology/2016/10/drone-hijacker-gives-hackers-complete-control-of-aircraft-in-midflight/

[50] GoPro. Karma User Manual. Julkaistu 2016

[51] Half Chrome Drones. Tello Extendted - 2x to 5x Your Range with the Xiaomi Mi WiFi Extender. Saatavissa: https://www.halfchrome.com/mi-wifi

[52] Holm, Sverre. Ultrasound positioning based on time-of-flight and signal strength. 2012 International Conference on Indoor Positioning and Indoor Navigation. 13.-15.11. 2012

[53] Horizon Hobby LLC. Blade Chroma with ST-10+ personal ground station transmitter* Manual. Julkaistu 2015

[54] Horizon Hobby LLC. https://www.horizonhobby.com/media/chroma/BLH8675.html

[55]ICAO. Annex 10 to the Convention on International Civil Aviation Aeronautical Telecommunications Volume V Aeronautical Radio frequency Spectrum Utilization Second Edition. International Civil Aviation Organization. 2001

[56] IEEE. standards-oui.ieee.org/oui/oui.txt

[57] IHS Markit. R&S ARDRONIS radio monitoring and counter-UAV system. Jane's. C4ISR & MISSION SYSTEMS: LAND . Julkaistu 01.11.2017. Saatavissa: https://janes.ihs.com/Janes/Display/jc4il0907-jc4il

[58] Jennings, Gareth. UK signs for Drone Dome C-UAS system. Jane's Defence Weekly. Julkaistu 14.8.2018. Saatavissa: https://janes.ihs.com/Janes/Display/FG_1003944-JDW

[59] JJRC. X3 ENTRY LEVEL AERIAL PHOTOGRAPHY DRONE [verkkosivu]. Viitattu 8.4.2019. Saatavissa: https://www.jjrc.com/goodshow/jjpro-x3-entry-level-aerial-photography-drone.html

[60] Kamkar, Samy. SkyJack [ohjelmistoprojekti]. Saatavissa: https://github.com/samyk/skyjack

[61] Kaplanis Charalampos. Detection and prevention of Man in the Middle attacks in Wi-Fi technology. Aalborg University. Master Thesis. 8.2015.

[62] Karjalainen, Joni. Laajennettujen Kalman-suotimien soveltaminen epäkoherentin sironnan spektritiheysfunktion estimoinnissa. Pro gradu. Oulu, 2016. Oulun yliopisto, Matemattisten tieteiden laitos. 29 s.

[63] Kespry. Saatavissa: https://www.kespry.com/

[64] Knuuttila, Tomi. Kappaleen asennon tunnistus sulautetussa järjestelmässä. Opinnäytetyö. Vaasa, 2013. Vaasan ammattikorkeakoulu, Tietotekniikan koulutusohjelma. 51 s.

[65] Koebler, Jason. DJI Is Locking Down Its Drones Against a Growing Army of DIY Hackers. Motherboard, 7.7.2017. Viitattu 3.9.2018 Saatavissa: https://motherboard.vice.com/en_us/article/3knkgn/dji-is-locking-down-its-drones-against-a-growing-army-of-diy-hackers

[66] Kopp, Carlo. Engagement and Fire Control Radars [tekninen raportti]. Viitattu 26.3.2019 Saatavissa: http://www.ausairpower.net/APA-Engagement-Fire-Control.html

[67] Kortelainen, Antti. Ilma-alukseen kohdistuva kyberuhka. Pro gradu. Helsinki, 2016. Maanpuolustuskorkeakoulu, Sotatekniikan laitos. 60 s.

[68] Kosola, J.& Solanne, T. Digitaalinen taistelukenttä - Informaatioajan sotakoneen tekniikka, ISBN 978-951-25-25034.

[69] Kostas Tigkos. Guardion enters C-UAS fray. Jane's Internationa Defence Review. Julkaistu 25.7.2018. Saatavissa: https://janes.ihs.com/Janes/Display/FG_592279-IDR

[70] Kyasanur, Padeep ja Vaidya H. Nitin. Selfish MAC Layer Misbehaviot in Wireleses Networks. University of Illinois. 4.3.2004

[71] Latonen, Henri. MEMS-magnetometrin kapasitiivisen lukuelektroniikan kehittäminen. Insinöörityö. Metropolia. 26.1.2011.

[72] Liikenne ja viestintäviraston määräys15 AO/2019 M. Määräys luvasta vapaiden radiolähettimien yhteistaajuuksista ja käytöstä. Antopäivä: 9.1.2019

[73] Limer, Eric. It's Dumb Easy to Wreck a $20,000 Camera with Just a Couple Lasers. Gizmodo, 13.7.2013. Viitattu 9.4.2019. Saatavissa: https://gizmodo.com/its-dumb-easy-to-wreck-a-20-000-camera-with-just-a-co-771211069

[74] Loquercio, Antonio.& Maqueda, Ana I.& del-Blanco Carlos R.& Scaramuzza, Davide. DroNet: Learning to Fly by Driving. IEEE ROBOTICS AND AUTOMATION LETTERS, 2018. Vol. 3, no. 2, p. 1088-1095.

[75] Lorenz, Ralph D. Flight Power Scaling of Airplanes, Airships, and Helicopters: Application to Planetary Exploration. Journal of Aircraft, 2001. Vol. 38, No. 2, p. 208-214.

[76]Lynch M. Fuzzing RTSP to discover an exploitable vulnerability in VLC [blogi]. Julkaistu 30.12.2013. Viitattu 3.9.2018. Saatavissa: https://isecpartners.github.io/fuzzing/vulnerabilities/2013/12/30/vlc-vulnerability.html

[77]MIT. Thermodynamics and Propulsion [oppimisympäristö]. https://web.mit.edu/16.unified/www/FALL/thermodynamics/notes/node97.html

[78] Mogg, Trevor. A consumer drone crashed and burned, and then caused a wildfire. Digital Trends, 03.12.18. Saatavissa: https://www.digitaltrends.com/cool-tech/drone-crash-causes-wildfire/

[79] MultiWii project related stuffs. MultiWii. Saatavissa: http://www.multiwii.com/

[80] Mustonen, Henri. Virtakiskon virran mittaaminen avoimen magneettipiirin Hall-anturilla. Diplomityö. Tampereen Teknillinen Yliopisto. Toukokuu 2015.

[81] Pamela Gregg. Risk in the Sky? University of Dayton. Julkaistu 13.09.2018. Saatavissa: https://udayton.edu/blogs/udri/18-09-13-risk-in-the-sky.php

[82] Panchip. XN297L-ohjekirja [kiinaksi julkaistu] Tutkijan hallussa.

[83] Panchip. XN297LBW-ohjekirja [kiinaksi julkaistu] Tutkijan hallussa.

[84] Parrot SA. Anafi User Guide v2.4. Julkaistu 24.12.2018. Saatavissa: https://www.parrot.com/files/s3fs-public/firmware/anafi_user_guide_v2.4.pdf

[85] PArrot SA. https://www.parrot.com/global/drones/anafi

[86] Parrot SA. Parrot AR Drone2.0 User Guide. Saatavissa: https://www.parrot.com/files/s3fs-public/firmware/ar.drone2_user-guide_uk.pdf

[87] Parrot SA. Parrot Bebop Drone User Guide. Saatavissa: https://www.parrot.com/files/s3fs-public/firmware/bebop-drone_user-guide_uk_v.3.4_0.pdf

[88] Parrot SA. Parrot Bebop 2 Drone User Guide. Saatavissa: https://www.parrot.com/files/s3fs-public/firmware/bebop-2_user-guide_uk_2.pdf

[89] Paukku, Ville. Langattomien verkkojen suojaus maantietukikohtaympäristössä. Pro gradu. Helsinki, 2017. Maanpuolustuskorkeakoulu, Sotatekniikan laitos. 60 s.

[90] Pietiläinen, Samuli. Tutkimustulosten vaihto. Lync-keskustelu. 06.04.2019.

[91] Robinson, Rick. No Pictures Please: Researchers Develop System to Thwart Unwanted Video and Still Photography. Georgia Tech Research News. 17.6.2006. Viitattu 9.4.2019 Saatavissa: http://gtresearchnews.gatech.edu/newsrelease/anti-camera.htm

[92] roboremo. ChiNRF - Arduino library for NRF24L01+ clones: RFM73, RFM75, LCX24G, XN297 [ohjelmistoprojekti]. Saatavissa: https://github.com/roboremo/ChiNRF

[93] Rodday N. Exploring security vulnerabilities of unmanned aerial vehicles. Master Thesis. University of Twente. 7.2015. Amsterdam

[94] Salminen, Ari. Mikä kirjallisuuskatsaus? - Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasa, 2011. ISBN: 978-952-476-349-3

[95] Schulzrinne H, Rao A, Lanphier R, Westerlund M, Stiemerling M. RFC7826 Real-Time Streaming Protocol Version 2.0. Internet Engineering Task Force (IETF). 21.2016

[96] Shen, Shaojie.& Mulgaonkar,Yash.& Michael, Nathan.& Kumar, Vijay. Multi-Sensor Fusion for Robust Autonomous Flight in Indoor and Outdoor Environments with a Rotorcraft MAV. 2014 IEEE International Conference on Robotics & Automation (ICRA). Hong Kong Convention and Exhibition Center. 31.5. - 7.6.2014. Hong Kong, Kiina.

[97] Sensofusion. Airfence Technical Specifications. Julkaistu 2017. Tutkijan hallussa.

[98] Sensofusion. Sensofusion. 2019. Saatavissa: https://www.sensofusion.com/

[99] Silvennoinen, A. IEEE 802.11b and IEEE 802.11g WLAN sytem performance in hidden node situation. Jormakka, J. Candolin, C. Military Ad Hoc Networks. Helsinki. Edita Prima Oy. 2004. 137 s. ISBN 951-25-1544-X

[100] Stiennon Richard. There Will Be Cyberwar - How The Move To Network-Centric Warfighting Set The Stage For Cyberwar. IT-Harvest Press, Birmingham, MI, 2015. ISBN-13: 078-0-9854607-8-5

[101] Suomen kyberturvallisuusstrategia. Valtioneuvoston periaatepäätös 24.1.2013. Helsnki: Forssa print, 2013. ISBN: 978-951-25-2434-1

[102] MoD removes anti-drone military hardware from Gatwick. The Guardian, 2.1.2019. Saatavissa: https://www.theguardian.com/uk-news/2019/jan/02/mod-removes-anti-drone-military-hardware-from-gatwick

[103] Torniainen, Aki. DRONE-UHKA! - Miehittämättömien lennokkien valvonta ja torjunta. Poliisiammattikorkeakoulun opinnäytetyö/AMK. Tampere, 2018. Poliisiammattikorkeakoulu. 34 s.

[104] Trafin määräys OPS M1-32. KAUKO-OHJATUN ILMA-ALUKSEN JA LENNOKIN LENNÄTTÄMINEN. Antopäivä 23.12.2016. Voimaantulopäivä 1.1.2017. Voimassa toistaiseksi

[105] US reconnaissance plane operated drones that attacked Hmeymim — defense official. TASS, 25.10.2018.Saatavissa: http://tass.com/defense/1027736

[106] Ulvestad, A. A Brief Review of Current Lithium Ion Battery Technology and Potential Solid State Battery Technologies. 2018. Viitattu: 20.02.2019. Saatavissa: https://arxiv.org/pdf/1803.04317.

[107] Head of the Russian General Staff's Office for UAV Development Major General Alexander Novikov holds briefing for domestic and foreign reporters. Venäjän Puolustusministeriö, 11.01.2018. Saatavissa: http://eng.mil.ru/en/news_page/country/more.htm?id=12157872@egNews

[108]van Blyenburgh P. UNMANNED AIRCRAFT SYSTEMS - The Current Situation. EASA UAS Workshop Pariisi 01.02.2018

[109] Vanhoe, Mathy ja Pienssens Frank. Advanced Wi-Fi Attacks Using Commodity Hardware. 08.12.2014

[110] Vanhoe, Mathy ja Pienssens Frank.Predicting, Decrypting, and Abusing WPA2/802.11 Group Keys. Katholieke Universitet Leuven. 20.08.2016. Seminaarijulkaisu 25th USENIX Security Synopsium. Austin Texas

[111] Valouch, Jan & Urbancokova, Hana. (2016). Electromagnetic Weapons as Means of Stopping Vehicles A Proposal of a Stationary Electromagnetic Device for Stopping Vehicles. University in Zlin. Zlin, Czech Republic

[112] Visuo. VISUO_XS809HW USER MANUAL. Tutkijan hallussa.

[113] Wang, Le. Detection of Man-in-the-middle Attacks Using Physical Layer Wireless Security Techniques. Masters Theses. 27.08.2013. Worcester Polytechnic Institute

[114] Wi-Fi Alliance. Wi-Fi Certified WPA3. Viitattu 27.01.2019. Saatavissa: https://www.wi-fi.org/discover-wi-fi/security

[115]Yhdysvaltain puolustusministeriö. Kenttäohjesääntö(FM) 3-38 Cyber Electromagnetic Activities. 12.022014. Washington DC

[116] Air Force Doctrine, ANNEX 3-13 INFORMATION OPERATIONS. Yhdysvaltain Ilmavoimat, Curtis E. Lemay Center, 28.04.2016.

[117] Yuneec. Mantis Q User Manual V1.0. Julkaistu 21.09.2018

[118]Yuneec. https://us.yuneec.com/shop-mantis-q

[119] Yuneec. Typhoon H User Manual V1.1

[120] Yuneec. Typhoon Q500 4K Instruction Manual V12302015

[121] L 18.8. 2000/755. Aluevalvontalaki.

[122] L 11.5. 2007/551. Laki puolustusvoimista.

[123] L 7.11. 2014/864. Ilmailulaki.

[124] HE 223/2018. Hallituksen esitys eduskunnalle laiksi poliisilain 2 luvun muuttamisesta. Helsinki. 8.11.2018.

[125] L 19.12. 1889/39. Rikoslaki.

[126] DroneDeploy. DroneDeploy [verkkosivu]. Saatavissa: https://www.dronedeploy.com/

[127] Pix4D SA. Pix4D [verkkosivu]. Saatavissa: https://www.pix4d.com/

[128] Duque de Quevedo, Álvaro.& Ibañez Urzaiz, Fernand.& Gismero Menoyo, Javier.& Asensio López, Alberto. Drone Detection and RCS Measurements with Ubiquitous Radar. Tutkimusraportti. Madrid. Universidad Politécnica de Madrid, Information Processing and Telecommunications Center.

[129] Li, Chenchen J. An Investigation on the Radar Signatures of Small Consumer Drones. IEEE ANTENNAS AND WIRELESS PROPAGATION LETTERS, 2017. Vol. 16, p. 649-652.

[130] Summers, J.E.& Clarke, J. Radar receiver burnout by other radars. IEEPROC, 1981. Vol. 128, Pt. A, No. 9, p. 615-620.

[131] Nordic Semiconductor. nRF24L01 Single Chip 2.4GHz Tranceiver Product Specification. 2007. Tutkijan hallussa.

[132] Be-Nazir Ibn Minar, Nateq.& Tarique, Mohammed . BLUETOOTH SECURITY THREATS AND SOLUTIONS: A SURVEY. International Journal of Distributed and Parallel Systems (IJDPS), 2012. Vol.3, No.1, p. 127-128.

[133] Waddell, Kaveh. What If Cameras Stopped Telling the Truth? New technology to block photography at concerts hints at an alarming future for smartphones. The Atlantic, 13.07.2016. Saatavissa: https://www.theatlantic.com/technology/archive/2016/07/what-if-cameras-stopped-telling-the-truth/491150/

[134] Zerodium. Our Exploit Acquisition Program [verkkosivu]. https://zerodium.com/program.html

LITTEET

LIITE1 kaupallisten lennokkien esittely

Tässä liitteessä listaan kaupallisista lennokeista löytyviä toiminnallisuuksia, joita voi käyttää hyväksi osana kybervaikuttamista tai jotka vaikeuttava sitä. Lisäksi olen nostanut esiin mahdollisia poikkeavia verkkoratkaisuja, jotka ovat mahdollinen haavoittuvuus. Hinnat on haettu valmistajien sivuilta tammikuussa 2019. Ne sisältävät vähintään lennokin ja siihen liittyvän ohjaimen, muut lisävarusteet vain pakettihinnoissa. Korkeampi hinta antaa viitettä siitä, että lennokki ei ole harrastekäytössä, vaan sen operaattori on tietoinen mahdollisista ilmatilarajoituksista.

Top 30 Non-Hobbyist Drones

Manufacturer	Model	Quantity
DJI	Phantom 4	26189
DJI	Phantom 3	16944
DJI	Mavic	13902
DJI	Inspire 1	7787
Intel	Shooting Star 2	4800
3DR	Solo	3269
DJI	Inspire 2	2669
DJI	Phantom 2	2272
Intel	Shooting Star	1838
Yuneec	Typhoon H	1609
Yuneec	Typhoon Q500	1505
Autel Robotics	X-Star Premium	1234
Kespry	Kespry Drone 2.0	1042
GoPro	Karma	938
DJI	Matrice 600	883

Manufacturer	Model	Quantity
DJI	Matrice 100	801
DJI	Spark	747
senseFly	eBee	686
DJI	Phantom 1	676
Parrot	AR Drone 2.0	540
Parrot	Bebop 2	450
3DR	Iris	439
Unknown	Hamilton2	426
Parrot	Bebop	401
DJI	S1000	380
Unknown	R1	329
Blade	Chroma	300
Hitec	Q-Box 450	272
Flyzone	FLZA-3000	215
DJI	F450	208

Kuva 1 30 eniten rekisteröityä lennokkia, Ilmoitettu valmistaja, malli ja lukumäärä.[42]

Kuvassa 1 on listattu FAA (Federal Aviation Authority) julkaisema 30 yleisimmän rekisteröidyn lennokin lista vuodelta 2017. Tarkastelun ulkopuolelle jätetään seuraavat lennokit:

- Intel lennokit ovat parveilevia valoshow-laitteita, eikä niitä myydä kuluttajille.
- R1 ja Hamilton2 ovat tuntemattomilta valmistajilta ja kaikki niiden yksilöt on rekisteröity erissä. Jokainen R1 Redwood Cityyn ja jokainen Hamilton2 Menlo Parkiin.
- eBee ja FLZA-3000 ovat kiinteäsiipisiä.
- Hitec Q-Box 450 lennokista ei löydy tietoja

Autel Robotics, DJI, Parrot ja Yuneec ovat julkaisseet uusia lennokkeja, joista tähän liitteeseen on poimittu lippulaivamalleja.

1. DJI

DJI on selkeästi isoin vaihtoehtoisesti ammattilaiskäyttöön soveltuvien lennokkien valmistaja. Phantom sarja vaikuttaa olevan ensisijaisesti harrastelijavalokuvaajia varten. Mavic ja Spark ovat urheilullisempi lennokkeja, joilla voi lentää virkistysmielessä, mutta niiden kamera on myös korkealaatuinen. Inspire lennonkit soveltuvat korkealaatuiseen ilmakuvaukseen ja ne ovat merkittävästi aiempia kalliimpia. Matrice, S1000 ja F450 ovat ominaisuuksiensa puolesta muunneltavissa. Valitsemalla vain tarpeelliset sensorit, niiden hyötykuorma on parempi, kuin kuvauskoptereilla. DJI ei juuri julkaise uusia lennokkeja, vaan se päivittää olemassa olevia.

Phantom 4

Kuva 17 Phantom 4 [41]

Gimbaaliin asennettavalla kameralla varustettu nelikopteri. Kolme lentomoodia, P-moodisa (Positioning) vakauttaa itsensä käyttäen GNSS (GPS ja GLONASS)ja estesensoreita, S-moodissa (Sport)estesensorit pois käytöstä, nopeusraja 20 m/s, A-moodissa (Attitude) ei GNSS tai estenseroita, säilyttää korkeuden barometrin perusteella. RTH palaa tallennetulle kotipisteelle, kun ohjaussignaali katoaa 3 sekunniksi (fail-safe), akun lataus on tarpeeksi alhainen tai käyttäjä aktivoi tilan. RTH vaatii GNSS-signaalin, sen voi keskeyttää ja lennokki on ohjattavissa. [26] Ilman GNSS-signaalia todennäköisesti nousee painesensorin perusteella 20 metriin ja odottaa kunnes akun lataus vaatii laskeutumaan.[lähde] Lennokissa on runkoon asenettu stereonäkö eteen- ja alaspäin, jonka avulla se kykenee väistämään esteitä. Lisäksi lennokissa on ultraäänisensori alaspäin käytettäväksi matalilla korkeuksilla. Lennokki ei väistä esteitä Fail-Safe tilassa. Lennokki laskeutuu automaattisesti, kun akun lataus on niin matala, että se riittää vain laskeutumiseen nykyiseltä korkeudelta. Moottoreissa on hätäseis ominaisuus, jolla moottorit sammuvat välittömästi ja lennokki putoaa. Mahdollisesta autorotaatiosta ei ole mainintaa, mutta putoamisen aiheuttamasta lennokin vaurioitumisesta varoitetaan.[26] Verollinen hinta 1 399-1 699€.

Phantom 3

Kuva 18 Phantom 3 [41]

Gimbaaliin asennettavalla kameralla varustettu nelikopteri. P, A ja F (Function) moodit. F-moodissa lennokki noudattaa tiettyjä ohjelmoituja lentotiloja, kuten reitin seuraaminen ja lentosuunnan lukitseminen. Muutoin kuten Phantom 4, mutta ei estesensoreita.[27] Valmistaja ei enää myy näitä.

Mavic 2.0 Pro

Kuva 19 Mavic 2 [41]

Gimbaaliin asennettavalla kameralla varustettu nelikopteri. P ja S moodit. P on jaettu GPS ja ATTI alamoodeihin. ATTI on käytännössä Phantomin A. GPS alamoodi käyttää sekä GPS-navigointia, että optisia sensoreita lennokin vakauttamiseen. Matalilla korkeuksilla käytössä on myös ultraäänisensori. Sama RTH kuin Phantom 4, mutta laskeutumisen yhteydessä käyttää optisia sensoreita ja yrittää laskeutua tarkasti tai ainakin turvallisesti. Lennokissa on runkoon asenettu stereonäkö eteenpäin, jonka avulla se kykenee väistämään esteitä. Moottorin hätäseis pitää erikseen mahdollistaa sovelluksesta, ennen kuin sitä voi käyttää. Moottorit pysähtyvät automaattisesti myös, jos lennokin lentotietokone havaitsee kriittisen virheen. Lennokissa on "musta laatikko". Lennokki on kokoontaitettava, mikä helpottaa kuljettamista.[25] Verollinen hinta 1499€.

Kuva 20 Mavic 2 Enterprice eri kameroilla [41]

Mavic 2 Enterprice on uusin mavicin versio. Siinä gimbaaliin on mahdollista saada joko optisella zoomilla varustettu kamera tai kaksoiskamera, jossa on sekä infrapuna, että näkyvän valon kamera.

Inspire

Kuva 21 Inspire laskeutuneena ja ilmassa [41]

Nelikopteri. P, A ja F moodit. P on jaettu GPS, OPTI ja ATTI alamoodeihin. OPTI käyttää optisia sensoreita vakauttamiseen. Lennokissa on ultraäänisensori ja kamera alaspäin OPTI-järjestelmän käyttöön, mutta ei muita estesensoreita. RTH mahdollista myös ohjaimen koordinaatteihin, ohjaimessa GPS. Muutoin kuten Phantom 4.[28] Verollinen hinta 2088-4987€, riippuen kameramoduulista, halvin ilman pääkameraa.

Inspire 2

Kuva 22 Inpire 2 laskeutuneena ja ilmassa [41]

Nelikopteri. P, S ja A moodit. P alamoodit ja käytettävät sensorit kuten Mavicissa. RTH lennetään käyttäen optisten sensorien nauhoittamaa maastokarttaa. Maastokartan käyttö edellyttää, että sen nauhoittaminen on onnistunut ja kompassi toimii normaalisti. Optinen sensori kykenee varautumaan jopa 300 metrin päässä oleviin esteisiin, jos valoisuus on 300(tai 10 tai 100) - 10 000 luxia, mutta V1.0 ohjelmisto ei vielä tue tätä. RTH aktivoituu samoilla periaatteilla kuin Phantom 4ssä. Lennokissa on streonäkö eteenpäin ja infrapunasensori ylöspäin. Lennokin hätäseis on erikseen aktivoitava sovelluksesta.[29] Verollinen hinta 3 399-14 250€, riippuen kameramoduulista ja muista lisävarusteista, halvin ilman pääkameraa.

Phantom 2

Kuva 23 Phantom 2 [41]

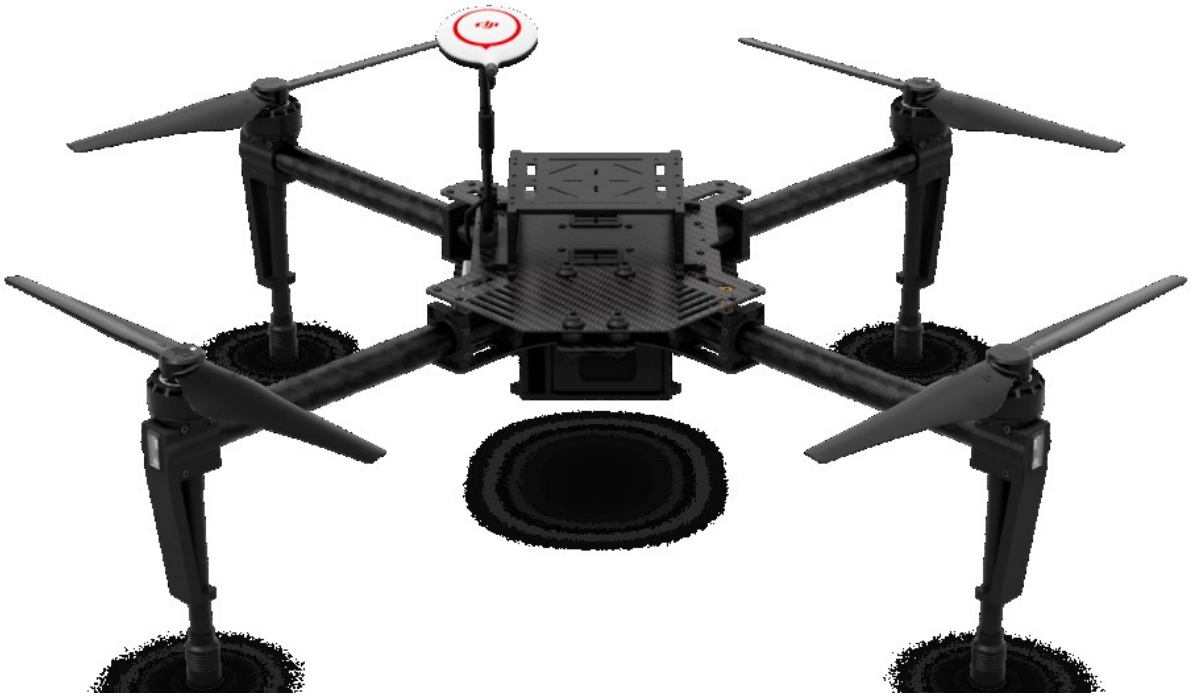
Nelikopteri. ATTI ja GPS moodit, sekä IOC. Failsafe jos ohjaimen signaali menetetään tai siinä on häiritötä. Manuaalinen aktivointi voidaan mahdollistaa sovelluksesta. Jos gps on käytössä lentää lähtöpisteelle, jos ei laskeutuu. Laskeutuu automaatisesti myös akun varauksen tai jänniteen pudotessa. Moottoreissa hätäseis. Vain barometri, kiihtyvyyssensori, GPS ja elektroninen kompassi, ei estesensoreita. Bluetooth datalinkki, 2,4GHz ohjain ja erillinen 2,4GHz datalinkkiyksikkö.[30] Valmistaja ei enää myy näitä.

Matrice 600

Kuva 24 Matrice 600 laskeutuneena [41]

Heksakopteri 5,5 kilon kuormille. Lentomoodit kuten Phantom 3. RTH kuten Phantom 4, mutta ei estesensoreita. Moottoreissa hätäseis, samalla näppäinyhdistelmällä kuin Inpire 2, mutta ei vaadi erillistä aktivointia.[31] Verollinen hinta 5 699€.

Matrice 100



Kuva 25 Matrice 100 runko [41]

Nelikopteri noin kilon kuormille. Toiminnallisuudet riippuvat kokoonpanosta, kaikki DJI lentomoodit mahdollisia. RTH kuten Phantom 4, mutta estesensorit asennettava erikseen.[32] Verollinen hinta 3 599 €

Spark

Kuva 26 Spark [41]

Nelikopteri. P ja S lentomoodit, P jaettu ATTI ja GPS moodeihin. 3D infapunasensori eteen- ja alaspäin. Eteen- ja alaspäin käännettävä kamera, sekä erillinen kamera alaspäin. RTH kuten Phantom 4, mutta odottaa WiFi ohjauksessa 10 sekunttia ennen failsafe aktivointia. Lisäksi lennokin ollessa alle 100m lähtöpaikalta väistää esteitä. Tarkuuslaskeutuminen Mavicin tavoin. Lennokissa on "musta laatikko". Moottorien hätäseis vaatii 1,5 sekunnin CSC:n (combined stick command).[33] Verollinen hinta 499€. Ohjaimen kantama vain kaksi kilometriä (linkkinä WiFi). Markkinoinnissa korostetaan eleohjausta.Tehty lennätettäväksi näköyhteyden päässä.

Phantom 1

Kuva 27 Phantom 1 [41]

Nelikopteri. GPS ja ATTI lentomoodit. GPS ja elektroninen kompassi (asennettava erikseen). RTH kuten Phantom2. [34] Valmistaja ei enää myy näitä.

S1000

Kuva 28 S1000 runko [41]

Oktokopteri noin 7 kilon kuormille. Ei ilmeisesti mitään älyä valmiina. [35] Valmistaja ei enää myy näitä - ilmeisesti korvattu Matrice 600 sarjalla.

F450 ”FlameWheel”

Kuva 29 F450 runko ja tarvikkeita [41]

Nelikopterin runko, johon voi liittää haluamiaan ominaisuuksia.[36] Valmistaja ei enää myy näitä - ilmeisesti korvattu Matrice -100 sarjalla.

2. 3DR

3DR on ensisijaisesti ohjelmistoyritys, joka on erikoistunut lennokeilla suoritettavaan datan keräämiseen rakennustyömaan työnohjausta varten. Ohjelmisto on käytettävissä useissa tässä liitteessä esitellyistä lennokeista. 3DR lennokit olivat kehitysalustoja SiteSurvey ohjelmistolle ja niiden myynti on lopetettu. Lennokeissa ei ole mitään muita sensoreita kuin elektroninen kompassi ja niiden lentäminen perustuu GPS-paikkatietoon.

Solo

Kuva 30 3DR Solo varustettuna Sonyn kameralla [2]

GoPro HERO3, 3+ ja 4 kanssa yhteensopiva nelikopteri. Käyttää Pixelhawk2 autopilottia, joka pohjautuu ArduPilot Copter ohjelmistoon. Hätäpysäytys, joka saa lennokin pysähtymään nykyiseen sijaintiin käyttäen GPS:ää. Ohjelman pysäytys, jolla esiohjelmoitu reitti tai lentoohjelma pysäytetään ja lennokki siirtyy ohjaimen hallintaan. Return Home ohjaimesta aktivoitava toiminto, jolla lennokki palaa suorinta reittiä lähtöpisteelle. Lennokki ei väistä esteitä tässä tilassa. Hätälaskeutuminen, jossa lennokki laskeutuu välittömästi yrittäen säilyttää sijaintinsa GPS:n avulla. Hätäseis, jolla kopterin moottorit saa pysäytettyä. GPS-yhteyden kadotessa lennokki laskeutuu välittömästi. Jos lennokki menettää yhteyden ohjaimeen, Return Home aktivoituu. Akun varauksen ollessa 10% Return Home aktivoituu. Lennokki putoaa, jos akku tyhjenee paluulennon aikana. [1]

IRIS

Kuva 31 IRIS [3]

Ainakin GoPro HERO 3 kanssa yhteensopiva nelikopteri. Pixlhawk autopilotti autopilottia, joka pohjautuu ArduPilot Copter ohjelmistoon. Return Home ohjaimesta aktivoitava toiminto, jolla lennokki palaa suorinta reittiä lähtöpisteelle. GPS:n tai ohjaussignaalin menetys sekä vähäinen akun varaus saa lennokin laskeutumaan. Jos lennokilla on GPS, se yrittää palata lähtöpisteelle ennen laskeutumista. Ohjaimen lisäksi, lennokki voi ohjata erillisellä maa-asemaradiolla, joka on liitettävissä älylaitteeseen tai tietokoneeseen. [3]

3. Yuneec

Alunperin sähkölentokoneita ja lennokin osia valmistanut yritys, joka julkaisi ensimmäisen nelikopterin vuonna 2014. Yrityksen lennokit ovat ensisijaisesti tarkoitettu ilmakuvaukseen. Lennokkeihin on saatavilla pienoisohjain, joka mahdollistaa huomaamattoman ohjaamisen.

Typhoon Q500

Kuva 32 Typhoon Q500 [120]

Gimbaaliin asennettavalla kameralla varustettu nelikopteri. Lennokkissa on GPS ja elektroninen kompassi, ohjaimessa GPS. Ohjaimesta aktivoitava Home Mode, jossa lennokki nousee 10m korkeuteen ja palaa lähtöpaikalleen. Lennokki on rajallisesti ohjattavissa Home Modessa. Home Mode aktivoituu, jos yhteys ohjaimeen menetetään. GPS-yhteyten menetyksen jälkeen lennokki on ohjattavissa ohjaimellla, mutta se ei tee automaattisesti mitään toimentpiteitä. Vähäinen akun varaus ei aiheuta automaattista laskeutumista, vaan lennokki putoaa varauksen loputtua. Jos lennokilla on GPS-yhteys, sitä ei voi lennättää 6,4 kilometrin päässä isoilta lentokentiltä (No-Fly Zone).[120] Verollinen hinta 599,99€.

Typhoon H

Kuva 33 Typhoon H [119]

Gimbaaliin asennettavalla kameralla varustettu heksakopteri. Ohjaimessa on Android käyttöjärjestelmä. Toiminnallisuuksiltaan kuten Q500, mutta Home Modessa ei ole korkeusrajaa. Lennokissa on pelkästään WiFi videolinkki.[119] Verollinen hinta 899,99-1 499,99€. Jälkimmäinen estesensoreilla.

Mantis Q

Kuva 34 Mantis Q [118]

Mavic-klooni. Lennokki on liian uusi ollakseen liitteen aiheena olevalla top 30 listalla, mutta siinä olevat ominaisuudet poikkeavat aiemmin esitellyistä Yuneecin lennokeista. Se on kokoontaitettava, mikä helpottaa kuljettamista. RTH korkeus on 8 metriä, mutta muutoin identtinen DJI:n lennokkien kanssa. Mavicin ja Sparkin tavoin ohjaimessa ei ole näyttöä vaan siihen on liitettävä älylaite.[117] Lennokin eleohjaus ja ohjaimen rajallinen kantama viittaavat siihen, että lennokki on tarkoitettu näköyhteydellä lennettäväksi.

4. Autel Robotics

Markkinoi itseään korkean teknologian kuvauskoptereita valmistavana yrityksenä. Autel Robotics valmistaa kahta lennokkia- X-Star ja EVO. Molemmissa lennokeissa on Smart Flight System, jonka kokoonpano on pääosin sama.

- IMU (inertial measurement system) kolmiakselinen gyroskooppi, sekä kolmiakselinen kiihtyvyysanturi, joka mahdollistaa inertiapaikantamisen ja lennon vakauttamisen
- Elektroninen kompassi
- GNSS vastaanotin, jossa on sekä GPS, että GLONASS tuki
- Barometri
- Ultraäänisensori korkeuden tarkkaan mittaamiseen
- Stereonäkö eteen ja alaspäin (vain EVO)
- Infrapunasensori taaksepäin (vain EVO)
- Yksivärikamera alaspäin paikan vakauttamiseen (vain X-Star)

X-star

Kuva 35 X-star [11]

Gimbaaliin asennettavalla kameralla varustettu nelikopteri. Kaksi lentomoodia, GPS ja ATTI. GPS pyrkii säilyttämään lennokin sijainnin ja ATTI pelkästään korkeuden. Ohjaimesta käynnistettävä Go Home toiminnallisuus, jossa lennokki nousee 30 metrin korkeuteen ja palaa kotipisteelleen, joka on lennokin lähtöpaikka, jos sitä ei ole muutettu. Jos ohjaimen signaali menetetään, GNSS-yhteydellä paluu kotipisteelle, ilman yrittää muodostaa yhteyden 10 sekunnin ajan ja jos ei onnistu, laskeutuu välittömästi. Lennokki laskee jatkuvasti kotipisteelle paluuseen tarvittavaa akun varausta. Jos tämä raja tulee vastaan, lennokki aloittaa Go Home toimenpiteet. Akun varauksen ollessa 15% lennokki laskeutuu välittömästi, jos sitä ei aktiivisesti pidetä ilmassa ohjaimella. Moottoreissa on hätäseis. Lennokissa on hätäpysäytys. Lennokissa on No-Fly Zone ominaisuus, joka estää sitä nousemasta ilmaan 2,4 kilometrin päässä lentokentistä kilometrin päässä rajoitusalueista, kuten valtion rajat. Lentokenttien läheisyydessä korkeus on rajoitettu kartiomaisesti siten että 2,4 kilometrissä 10,5 metriin ja 8 kilometrissä 120 metriin. Jos lennokki lentää tällaiselle alueelle, se laskeutuu välittömästi. No-Fly Zone ominaisuus on mahdollista kiertää lentämällä lennokkia ilmana GNSS-yhteyttä. 5,8GHz ohjaussignaali ja 2,4GHz WiFi videolinkki. Ohjaimen kantaman on alle kilometri.[11] Verollinen hinta $749 (~650€).

EVO

Kuva 36 Autel Robotics EVO [10]

Yuneec MantisQ:n tavoin uusi Mavic klooni. Käyttää alaspäin suunnattuja sensoreita turvalliseen laskeutumiseen. Ohjaimen taajuudet 2,4 sekä 902MHZ WiFi kaistat. Ohjaimen kantama jopa 7 kilometriä. Muut ominaisuudet kuten X-Star.[9] Verollinen hinta $999 (~875€)

5. Kespry

Kesbry ei myy lennokkeja, vaan maanmittaus- ja rakennustyömaan datankeräyspalvelua käyttäen hyväksi pilveen liitettyjä lennokkeja. Lennokeissa on lidar ja korkearesoluutioinen kamera. Jatkuva yhteys pilveen turvataan WiFi ja LTE yhteyksillä. Palvleun hinta on välillä 2 500-3 958$ kuukaudessa ja minimitilaus on 12 kuukautta.[63]

6. GoPro

Go Pro on ensisijaisesti urheilukameravalmistaja sen kameroita on käytetty useammassa aiemmin tässä liitteessä esitellyssä lennokissa.

Karma

Kuva 37 Karma lennokki HERO4 kameralla ja ohjain [44]

Kokoontaitettava nelikopteri, jossa on vakautettu asennus GoPro-kameroille. Ohjaimesta aktivoitava laskeutuminen, jolla lennokki laskeutuu joko lähtöpaikalleen, ohjaimen luokse tai nykyiselle paikalleen. Vähäisellä akun varauksella lennokki palaa lähtöpaikalleen. Ohjaussignaalin menetettyään lennokki palaa viimeiselle tunnetulle ohjaimen sijainnille. Kriitisen virheen sattuessa lennokki laskeutuu nykyiselle sijainnilleen. Lennokki on ohjattavissa näissä tiloissa. Moottoreissa hätäseis, mikä vaatii 5 sekunnin syötteen ohjaimeen. Käyttöohje ei ota kantaa GPS-yhteyden menettämiseen.[50] Verollinen hinta ei saatavilla, mutta ohjain 469,99€ ja kamera (HERO7 White) 219,99€

7. Parrot

Parrot SA on langattomaan teknologiaan erikoistunut elektroniikkavalmistaja, jonka tuotteisiin kuuluu myös lennokkeja.

AR Drone 2.0

Kuva 38 AR Drone 2.0 [86]

Eteenpäin katsovalla kameralla varustettu nelikopteri. Ohjataan älylaitteella ohjaus- ja videolinkkinä WiFi. Moottoreissa hätäseis. Pelkästään alaspäin suunnattu ultraäänisensori.[86] SkyJack lennokinkaappausohjelmiston käyttämä lavetti.[60]

Bebop

Kuva 39 Bebop [87]

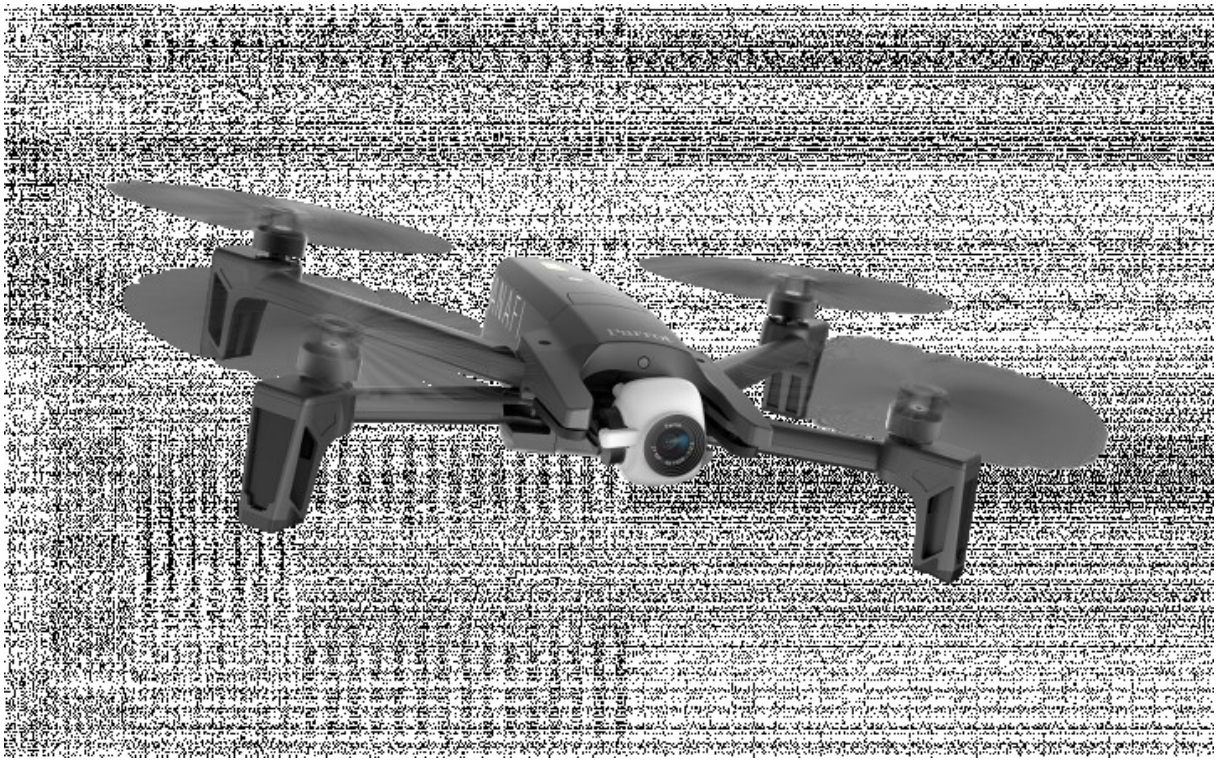
Eteenpäin katsovalla kameralla varustettu nelikopteri. Ohjataan älylaitteella tai ohjaimella ohjaus- ja videolinkki 2,4 tai 5GHz WiFi. Linkki on vaihdettavissa sovelluksesta. Return to starting point, lennokki nousee 10 metrin korkeuteen ja palaa lähtöpisteelleen. Aktivoitavissa älylaitteesta ja aktivoituu automaattisesti WiFi yhteyden katketessa 2 minuutiksi. Jää leijumaan 2 metrin korkeudelle lähtöpisteellä. Lennokissa on vain GPS ja kamera ei muita sensoreita.[87]

Bebop 2

Kuva 40 Bebop 2 [88]

Kuten Bebop, mutta paluu 20 metrin korkeudessa ja voi palata myös ohjaavan älylaitteen koordinaatteihin.[88] Verollinen hinta sisältäen ohjaimen, lisäakut ja FPV virtuaalilasit 699€.

ANAFI



Kuva 41 Anafi [85]

Aiempien vastaavien tavoin uusi Mavic-klooni. Ohjaus joko älylaitteella tai ohjaimella. Ohjaus- ja videolinkki 2,4 tai 5GHz WiFi. Ohjaimen kantama jopa 4 kilometriä. Ohjaimessa ei näyttöä vaan siihen liitetään muiden Mavic-kloonien tavoin älypuhelin usb-kaapelilla.RTH joko ohjaimesta, ohjaussignaalin katketessa tai akun varauksen ollessa liian alhainen. Paluuseen tarvittava varaus lasketaan jatkuvasti. GNSS-yhteyden menetys ei aiheuta failsafe toimenpiteitä. Kriittinen akun varaus saa lennokin laskeutumaan hallitusti. Tarkkuuslaskeutuminen perustuu ohjaimeen lähetettyyn alaspäin suunnatun kameran kuvaan, ei automaatioon. Lennokissa ei ole estesensoreita.[84] Verollinen hinta 699€.

8. Blade

Yuneecin ST10+ ohjainta ja Wizard-pienoisohjainta käyttävien Chroma lennokkien ympärille rakennettu brändi. Osassa lennokeista käytössä myös Yuneecin käyttämä CGO-kamera. Brändillä ei ole verkkosivuja, vaan käyttöohjeen linkit johtavat horizonhobby.comin alasivulle.

Chroma

Kuva 42 Chroma CGO3-kameralla, kaksi laentoakkua ja ST10+ -ohjain [54]

Gimbaaliin asennettavalla kameralla varustettu nelikopteri. Ohjaimesta aktivoitava return home. GPS-signaalin menetettyään lennokki on edelleen ohjattavissa. Ohjeessa ei mainintaa failsafe tiloista. Moottoreissa hätäseis. WiFi videolinkki.[53] Verollinen hinta kamerasta riippuen 699,99-1 099,99€. Yhteensopiva myös GoPro kameroiden kanssa.

LIITE 2 Kaupallisten lennokkien käyttämät taajuudet ja ohjaimen kantamat

Taulukko 4 Liiteessä 1 käsiteltyjen lennokkien taajuudet ja ohjauslinkin kantamat koostettuna lennokkien käyttöohjeista

	Ohjauslinnki ala	Ohjauslinnki ylä	Videolinkki ala	Videolinkki ylä	Kantama USA	Kantama EU	HUOM
Phantom 4	2400	2483	2400	2483	5	3,5	
Phantom 3	5725	5825	2400	2483	1	1	
Phantom 3 (JAP)	922,7	927,7	2400	2483			
Mavic 2 Pro	2400	2485	5725	5850	7	5	Yhdistetty
Mavic 2 Pro (USA)	2400	2485	5150	5250	7	5	
Inspire 1	2400	2483	5725	5825	2	2	Yhdistetty
Inspire 1 (JAP)	2400	2483	922,7	927,7			
Solo	2412	2462	2412	2462	0,8	0,8	
Inspire 2	2400	2483	5725	5825	7	3,5	Yhdistetty
Phantom 2	2400	2500	2400	2500	1	1	
Typhoon H	5200	5800	5200	5800	0,5	0,5	
Typhoon Q500	2400	2500	5200	5800			
X-Star	5745	5799	2412	2462	1	0,5	
X-Star Premium	5745	5799	902	928	2		
Matrice 600	2400	2483	5725	5825	5	3,5	Yhdistetty
Matrice 600 (JAP)	2400	2483	920,6	928			
Matrice 100	2400	2483	5725	5825	5	3,5	Yhdistetty
Matrice 100(JAP)	2400	2483	922,7	927,7			
Spark	2412	2462	5745	5825	2	0,5	WiFi / Yhdistetty
Parrot	2412	2462	5180	5825			WiFi / Yhdistetty
Iris	433	915			1	1	3DR maa-asema

Taulukkoon on merkitty maakohtaisia rajoituksia taajuusalueiden ja lähetystehojen osalta. Huom kentässä oleva ”Yhdistetty” tarkoittaa, että lennokissa ei ole erillistä video- ja ohjauslinkkiä, vaan niissä käytetään samaa linkkiä molemmille. Tällöin molemmat taajuusalueet ovat kuitenkin käytettävissä, mutta niitä ei käytetä yhtä aikaa.

LIITE 3 DoS-hyökkäys TELLO nelikopteriin

Tässä liitteessä esitellään kahden eri DoS-hyökkäyksen (Denial of Service, palvelunesto) toteutus TELLO nelikopteriin ja arvioidaan niiden vaikutavuutta. Hyökkäykset toteutetiinn Rasbperry Pi 2B pienoistietokoneeseen asennetulla Kali Linuxilla. Wlan sovitin oli Zyxel NWD2205, johon Kalissa on valmiiksi ajuri, jolloin paketti-injektio on mahdollista.

TELLO käyttää ohjaus- ja videolinkkinä 2,4GHz wlania. Se toimii tukiasemana, johon liitytään puhelimella. Ohjaaminen tapahtuu käyttämällä puhelimeen asennettavaa sovellusta. Ohjaamisen helpottamiseksi puhelimeen oli liitetty Xbox-ohjain ja sen komennot siirettiin TELLO-sovellukseen käyttäen Octopus-sovellusta. TELLO:n firmwaren versio oli 01.04.78.01 ja ohjaussovelluksen versio 1.3.0.0. Lisäksi sovellus ilmoitti ”Loader Version” tiedon arvolla 00.00.01.05.

1. Authentication flood

Authentication flood hyökkäys toteutettiin komennolla:

```
mdk3 wlan0mon a -a 60:60:F1:D0:34:A9
```

Ensimmäinen parametri on alustettu sovitin wlan0mon. Sovitin alustetaan käyttäen iwconfig ja airmon-ng -työkaluja.

```
#pysäytetään verkkoa käyttävät prosessit, jotka voivat haitata toimintaa
airmon-ng check kill
#selvitetään saatavilla olevat sovittimet
iwconfig
#alustetaan löydetty wlan0 sovitin
airmon-ng start wlan0
```

Toinen parametri a tarkoittaa, että kyseessä on Auhentication flood hyökkäys

Kolmas parametri on kohteen MAC-osoite, joka ilmoitetaan käyttäen tunnistetta -a. Osoitteen kolme ensimmäistä osaa (60, 60 ja F1) ovat pääteltävissä, koska kyseessä on DJI-lennokki. Loput kolme ovat laitekohtaisia. Ne voi kuunnella airodump-ng -työkalulla.

```
#listataan kaikki kantamassa olevat laitteet
airodump-ng wlan0mon
```

Tämä komento listaa tukiasemat ja niissä kiinni olevat asiakkaat. Komennon ajo on jatkuva, eli se on keskeytettävä näppäinyhdistelmällä ctrl+c, ennen kuin voidaan siirtyä seuraavaan vaiheeseen. Oleellisia tietoja tässä ovat BSSID ja kanava. Oikea BSSID voidaan päätellä joko siitä, että ESSID saattaa alkaa TELLO tai että se on alkuosan perusteella DJI-laite*[56]*. Seuraavaksi sovitin lukitaan löydetylle kanavalle.

```
#lukitaan sovitin kanavalle 8
airodump-ng -c 8 wlan0mon
```

Nyt on vihdoin mahdollista toteuttaa komento:

```
mdk3 wlan0mon a -a 60:60:F1:D0:34:A9
```

Jolloin TELLO:n authentikointi-taulu alkaa täyttyä. Raspberry Pi ei ole kovin nopea, sillä injektionopeus on parhaimmillaan 370-pakettia sekunnissa. TELLO ei vaikuta reagoivan hyökkäykseen millään tavalla mdk3 tuloste antaa ymmärtää, että kohde ei ole haavoittuvainen hyökkäykselle.

Tämä ilmenee vasta, kun TELLO on ilmassa, sillä maassa ollessaan se ylikuumenee herkästi. Hyökkäys vaikuttaa nopeuttavan ylikuumenemista, mutta käytännössä tämä ei ole järkevä hyökkäys, sillä ilmassa ollessa ylikuumeneminen ei ole enää ongelma roottorien ilmavirran takia. Ylikuumentuessaan kesken hyökkäyksen TELLO sammui, eikä siihen enää voinut yhdistää puhelinta ilman resetointia.

2. Deauhentication hyökkäys

Deauthentication hyökkäys toteutettiin käyttämällä aireplay-ng -työkalua. Pohjatyö on jo tehty edellisessä hyökkäyksessä, jolloin komento voidaan suorittaa heti.

```
#lähetetään deauth sanoma kaikkiin TELLO:ssa kiinni oleviin asiakkaisiin 5000 kertaa
aireplay-ng --deauth 5000 -a 60:60:F1:D0:34:A9 wlan0mon
```

Hyökkäyksen voi tarvittaessa kohdentaa vain yhteen asiakkaaseen käyttämällä -c <asiakkaan MAC-osoite> parametria. Tämä ei kuitenkaan ollut tarpeen, sillä yhteys saatiin katkeamaan muutamassa sekunnissa käyttämällä broadcast-sanomia. TELLO indikoi välkkyvällä keltaisella valolla, että se on menettänyt yhteyden puhelimeen. Mikään ohjauskomento ei toiminut enää tässä kohtaa, eli yhteyden katkeaminen ei ollut asteittainen, vaan välitön. TELLO leijui paikallaan noin minuutin, jonka jälkeen se laskeutui lähelle maata jääden leijuman noin 15 senttimetrin korkeudelle.

Tässä kohtaa keskeytin aireplayn-ng:n ajon näppäinyhdistelmällä ctrl+c , mutta puhelin oli jo siirtynyt pois kanavalta ja yhdistänyt kotiwlaniin, jolloin se piti manuaalisesti yhdistää takaisin TELLO:on. Uusin kokeen niin, että kotiwlan oli pois päältä. Puhelin ei tässäkään tapauksessa yhdistänyt TELLO:on hyökkäyksen päätyttyä. Manuaalisen yhdistämisen jälkeen TELLO ilmoitti olevansa laskeutumassa, mutta se jatkoi leijuntaa kunnes ohjasin sen erikseen laskuun.

Automaattinen yhdistäminen toimi, kun deauth lähetettiin vain viisi kertaa ja sen jälkeen hyökkäys lopetettiin. Tällöin TELLO ei ehtinyt aloittaa laskeutumista koska yhteys palautui tarpeeksi nopeasti.

LIITE 4 Lentämiseen vaadittavan tehon kaavat

MIT opetuspaketissa [77] on seuraava kaava lentämisen vaatimalle teholle

$$P_{\text{req}} = \frac{1}{2}\rho V^3 S C_{D_0} + \frac{W^2}{\frac{1}{2}\rho V S}\left(\frac{1}{\pi e AR}\right).$$

rho on ilman tiheys kg/m^3

V on ilma-aluksen nopeus m/s

S on siipien pinta-ala

C on ilmanvastusvakio oletetaan tässä tapauksessa 0.02

W on ilma-aluksen paino Newtoneina

e on siipien hyötysuhde oletetaan tässä tapauksessa 1

AR on siipien suhde mikä saadaan jakamalla siipien kärkivälin neliö siipien pintalalla

Avataan yhtälö paremmin tätä tutkimusta palvelevaksi

$$P = \frac{1}{2}\rho_{ilma} * {v_{lento}}^3 * A_{siivet} * C_{D_0} + \frac{2 * {m_{ilma-alus}}^2 * g^2}{\rho_{ilma} * v_{lento} * \pi * {L_{siivet}}^2}$$

Vastaavasti roottorin vaatima teho suhteessa sen pinta-alaan on laskettavissa Journal of Aircraft artikkelista [75] löytyvästä kaavasta

$$P = T^{1.5} / \sqrt{2\rho \cdot A}$$

Kun huomataan, että helikopterin leijuessa T = W, voidaan kaava muuttaa muotoon

$$P = \frac{{m_{ilma-alus}}^{1,5} * g^{1,5}}{\sqrt{2\rho * A_{roottori}}}$$

LIITE 5 Tutkayhtälö

Tutkimuksessa käytettään tutkayhtälöä muodossa:

$$P_{rx} = \frac{P_{tx} G^2 \lambda^2 \sigma_m}{(4\pi)^3 R^4}$$

Missä:

- P_{rx} on tutkan vastaanottama teho
- P_{tx} on tutkan lähettämä teho
- G on tutkan antennivahvistus
- λ on tutkan aallonpituus
- σ_m on maalin tutkapoikkipinta-ala neliömetreinä
- R on maalin etäisyys tutkasta

LIITE 6 Käsitteet ja määritelmät

CTR, Control Zone Lähialue	Lentopaikkaa ympäröivä ilmatila, jossa on ylläpidettävä jatkuvaa kaksisuuntaista radioyhteyttä lennonjohtoelimen kanssa. Lennonjohtaja vastaa turvallisesta toiminnasta ilmatilassa. [4]
FIZ Flight Information Zone Lentotiedotusvyöhyke	Lentopaikkaa ympäröivä ilmatila, jossa annetaan lentotiedotuspalvelua. Ilma-aluksen päällikkö vastaa turvallisesta toiminnasta ilmatilassa. [4]
RMZ Radio Mandatory Zone Radiovyöhyke	Lentopaikkaa ympäröivä ilmatila, jossa on kuunneltava jatkuvasti asianmukaista yhteydenpitokanavaa. Ennen saapumista radiovyöhykkeelle ilma-aluksen ohjaajan on lähettävä asianmukainen avauskutsu. [46]
IoT Internet of Thing Esineiden internet	Kodinkoneiden muodostama verkko jonka avulla käyttäjä ja valmistaja saavat tietoa koneen toiminnasta ja kone päivityksiä. Mahdollistaa joissain tapauksissa kodinkoneen ohjaamisen, esimerkiksi älyvalaistuksen tapauksessa.
Spoofing	Tässä tutkimuksessa sanomien väärentäminen esimerkiksi toistamalla paketti, jonka otsikkokehys on kopioitu, mutta datakehys muokattu hyökkääjälle edullisella tavalla
Lennokin paikkatieto	Tässä tutkimuksessa tietoja jotka liittyvät lennokin sijaintiin esimerkiksi korkeus, etäisyys ohjaimesta ja absoluuttinen sijainti suhteessa geoidiin
Lennokin tilatieto	Tässä tutkimuksessa tietoja jotka liittyvät lennokin lentotilaan, kuten lentosuunta ja nopeus
Security through obscurity	Tietojärjestelmän toiminnan suojaaminen peittelemällä sen käyttämää logiikkaa ja rajapintoja mahdollisimman paljon