Saija Myrsky

KYBERTURVALLISUUS LENTOLIIKENTEESSÄ:

NÄKÖKULMIA HAASTEISIIN JA TOIMINTAYMPÄ-RISTÖÖN

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Myrsky, Saija
Kyberturvallisuus lentoliikenteessä: näkökulmia haasteisiin ja toimintaympäristöön
Jyväskylä: Jyväskylän yliopisto, 2024, 43 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Vuorinen, Jukka

Maailmanlaajuisen lentoliikenteen ennustetaan kaksinkertaistuvan vuoteen 2037 mennessä, minkä takia kyberturvallisuusriskien ymmärtäminen ja niiden vähentäminen on tullut olennaiseksi. Ilmailualan kyberturvallisuus on ensisijaisen tärkeää ja samalla erittäin monimutkaista. Sen ylläpito edellyttää jatkuvaa arviointia ja kehitystä, taatakseen matkustajien ja alan toimijoiden turvallisuuden ja luottamuksen. Tämä kandidaatintutkielma keskittyi tarkastelemaan kyberturvallisuuden roolia ja merkitystä kaupallisen lentoliikenteen alalla. Siinä korostettiin lentoliikenteelle erityisiä piirteitä sekä lentoyhtiöiden operatiivisia menettelytapoja ja viestintästrategioita kyberturvallisuuden näkökulmasta. Tutkimusmenetelmänä toimi systemaattinen kirjallisuuskatsaus sekä empiirinen analyysi. Näiden avulla selvitettiin, miten lentoyhtiöt käsittelevät ja viestivät kyberturvallisuudesta markkinoinnissaan, kun lentoliikenne muuttuu yhä digitaalisemmaksi ja kyberuhkat lisääntyvät. Tutkimuskysymyksen avulla syvennyttiin lentoliikenteen ainulaatuisiin haavoittuvuuksiin sekä kyseisten kyberuhkien seurauksiin. Tavoitteena oli arvioida nykyisten kyberturvallisuustoimenpiteiden tehokkuutta ja tunnistaa mahdollisia kehityskohteita. Tutkielmassa korostuivat kyberhyökkäysten aiheuttamat riskit ja niiden vaikutukset sekä liiketoimintaan että asiakasluottamukseen. Näitä tarkasteltiin erityisesti lentoliikenteen kyberturvallisuuden erityispiirteiden, hallinnan ja kansainvälisen sääntelyn kautta. Tarjoamalla näkemyksiä siihen, kuinka kyberturvallisuus integroidaan lentoyhtiöiden toimintoihin ja markkinointistrategioihin, tutkimus pyrkii parantamaan luottamuksen ja turvallisuuden käsityksiä matkustajien keskuudessa, muuttuvassa digitaalisessa ympäristössä.

Asiasanat: kyberturvallisuus, kyberuhka, kaupallinen lentoliikenne, turvallisuus, kyberturvallisuuden hallinta, viestintä

ABSTRACT

Myrsky, Saija
Cybersecurity in Aviation: Perspectives on Challenges and the Operating Environment
Jyväskylä: University of Jyväskylä, 2024, 43 pp.
Information Systems, Bachelor's Thesis
Supervisor(s): Vuorinen, Jukka

With global air traffic projected to double by 2037, understanding and reducing cybersecurity risks has become essential. This thesis explored the importance of cybersecurity in the commercial aviation industry, highlighting its relevance in air travel operations, airline procedures, and communication strategies. Through a systematic literature review and empirical analysis, it examined how airlines address and convey their cybersecurity practices in their marketing materials. This exploration took place amidst the increasing digitalization of the aviation sector and the corresponding rise in cyber threats. The study analysed the unique vulnerabilities and consequences associated with cyber threats in aviation, aiming to assess the effectiveness of current cybersecurity measures and identify areas for improvement. These were examined particularly through the lens of aviation cybersecurity's unique characteristics, governance, and international regulations. By providing insights into the integration of cybersecurity into airline operations and marketing strategies, the study contributes to enhancing trust and safety perceptions among passengers in an evolving digital landscape.

Keywords: cybersecurity, cyber threat, commercial air travel, safety, cybersecurity management, communication

TAULUKOT

SISÄLLYS

1 JOHDANTO

Kun lähdetään tarkastelemaan kyberturvallisuutta ja sen vaikutuksia lentoliikenteeseen, huomataan aiheen olevan laaja. Kyberturvallisuuden vaikutuksia lentoliikenteeseen voidaan tarkastella useasta näkökulmasta, joita ovat esimerkiksi turvallisuus, operatiivisuus, liiketoiminta, infrastruktuuri sekä sääntely. Näihin kaikkiin näkökulmiin liittyy omanlaisensa uhat ja niiden ehkäisykeinot.

Lentoliikenteen määrä on lisääntynyt huomattavasti 2000-luvulla ja ilmailuala on yksi maailman nopeimmin kasvavista aloista. Maailmanlaajuisen ilmaliikenteen arvioidaankin kaksinkertaistuvan vuoteen 2037 mennessä, ja Euroopan suurimmat lentokentät käsittelevät päivittäin jopa 3000 lähtöä sekä laskeutumista (Lehto, Sestorp, Khan & Gurtov, 2021, s.1). Näin ollen maailmanlaajuisen ilmatilan käyttäjien nopean kasvun seurauksena ilmaliikenteen hallinnasta on tullut entistä tärkeämpää (Elmarady & Rahouma, 2021, s.1). Tämän myötä myös lentoliikenteeseen kohdistuvat uhat ovat kasvaneet merkittävästi viime vuosina. Etenkin lentoteollisuuden siirtyminen yhä enemmän digitaaliseen ympäristöön on luonut aivan uudenlaisia kyberuhkia. Lentoliikenteen kyberuhkien torjuntaan on syntynyt uusia haasteita teknologisten ratkaisujen ja verkostoitumisen lisääntyessä. Kyberhyökkäykset eivät enää rajoitu perinteisiin muotoihin, vaan ne voivat käsittää monimutkaisempia uhkia, kuten tietomurtoja, lentokoneiden järjestelmien manipulointia ja muita edistyneempiä hyökkäystapoja.

Monet toimialat kohtaavat samanlaisia uhkia, mutta ilmailualalla erityisenä piirteenä on näiden hyökkäysten vakavat seuraukset. Infrastruktuurin kestävyys on ratkaisevan tärkeää lentoliikenteen toiminnallisen luotettavuuden turvaamiseksi, sillä jopa pienet virheet tai laiminlyönnit voivat aiheuttaa laajoja vahinkoja ja menetyksiä. Näihin kuuluvat muun muassa kuolemantapaukset; sidosryhmien, henkilöstön ja asiakkaiden henkilökohtaisten tietojen menetys tai paljastuminen; tunnistetietojen varastaminen; sekä immateriaalioikeuksien ja tiedustelutiedon menetys (Ukwandu ym., 2022, s. 2). Tämä korostaa tarvetta kehittää jatkuvasti päivittyviä kyberturvallisuusstrategioita lentoturvallisuuden ja sujuvan toiminnan varmistamiseksi.

Tämän tutkimuksen tarkoituksena on tarkastella kyberturvallisuutta systemaattisen kirjallisuuskatsauksen sekä empiirisen analyysin avulla. Tutkimus on rajattu käsittelemään kaupallista lentoliikennettä ja tutkimuskysymys on:

- Millaisia ovat lentoliikenteen erityispiirteet kyberturvallisuuden näkökulmasta ja miten ne vaikuttavat alan toimintaan?

Tutkimuskysymystä pyritään selvittämään ensimmäiseksi systemaattisen kirjallisuuskatsauksen avulla, jossa aiheeseen relevanttia lähdekirjallisuutta haettiin Google Sholarista sekä eri tietokannoista, kuten Scopuksesta ja IEEE:stä. Pääsääntöisinä hakutermeinä käytettiin sanoja: lentoliikenne, kyberturvallisuus, cybersecurity, aviation, cyber safety, cybersecurity management. Hakutuloksia täsmennettiin vielä ”AND”, ”OR” ja ”IN” termien avulla sekä muodostamalla pidempiä tarkkoja lauseita. Tutkielmaan on pyritty valitsemaan lähteitä, jotka ovat vertaisarvioituja ja vähintään Jufo 1-tasoa. Kirjallisuuskatsauksessa keskitytään pohtimaan aihetta seuraavien kysymysten kautta:

- Millaisia erityispiirteitä lentoliikenteen kyberturvallisuudella on?
- Kuinka kyberturvallisuus on huomioitu organisaatioiden eli lentoyhtiöiden toiminnassa, ja mitkä säädökset sitä ohjaavat?

Kirjallisuuskatsauksessa käsitellään ensimmäiseksi aikaisempiin tutkimuksiin perustuvia mahdollisia kyberturvallisuuden erityispiirteitä, jotka ovat lentoliikenteelle tyypillisiä. Seuraavaksi perehdytään lentoyhtiöiden operatiiviseen toimintaan ja kansainvälisiin säännöksiin, joilla pyritään varmistamaan kyberturvallisuuden tehokas toiminta.

Tutkimuksen empiirisen osan tarkoituksena on syventyä lentoyhtiöiden omiin verkkosivuihin ja selvittää, miten niissä kerrotaan kyberturvallisuudesta. Aihetta tarkastellaan seuraavan kysymyksen kautta:

- Kuinka lentoyhtiöt tuovat omassa markkinointimateriaalissaan kyberturvallisuuden esille?

Tämä toteutetaan tutkimalla useaa lentoyhtiötä ympäri maailmaa, jotta voidaan luoda mahdollisimman kattava käsitys aiheesta. Empiirinen tutkimus muodostui kolmesta päävaiheesta, joita olivat tiedon kerääminen, analyysin tekeminen ja johtopäätöksien vetäminen. Lentoyhtiöiden nettisivuilta kerättiin relevanttia dataa, jonka pohjalta tehtiin kokoavaa ja vertailevaa analyysia. Lopulta vedettiin johtopäätöksiä ja yhdistettiin löydökset kirjallisuuskatsauksessa ilmi tulleisiin havaintoihin.

Näitä kahta näkökulmaa on tärkeää tutkia ja yhdistää, sillä niiden avulla on mahdollista muodostaa kokonaisvaltainen ymmärrys lentoliikenteen kyberturvallisuuden tilanteesta sekä siitä, kuinka se heijastuu lentoyhtiöiden toimintaan ja asiakassuhteisiin.

Toisessa luvussa käsitellään tutkimuksen kannalta oleellisia käsitteitä, joiden avulla aiheeseen on helpompi syventyä. Kolmannessa luvussa puolestaan tarkastellaan lentoliikenteen kyberturvallisuuteen liittyviä erityispiirteitä, kuten erilaisia järjestelmiä ja niiden kohtaamia uhkia. Neljäs luku keskittyy

kyberturvallisuuden hallintaan ja siihen, kuinka se näkyy lentoyhtiöiden toiminnassa. Kyseisessä luvussa esitellään myös kansainvälisiä säädöksiä, jotka määrittävät lentoyhtiöiden toimintaa tiettyyn suuntaan. Viidennessä luvussa tarkastellaan empiirisen analyysin kautta lentoyhtiöiden verkkosivujen asiakasviestintää kyberturvallisuuteen liittyen ja lopussa on vielä yhteenveto.

2 RELEVANTIT KÄSITTEET

Tutkimuksen kannalta on hyvä perehtyä muutamiin oleellisiin käsitteisiin, jotta aihetta voidaan ymmärtää paremmin. Tässä luvussa pyritään määrittelemään ensimäiseksi kyberturvallisuus, jonka jälkeen selitetään lyhyesti myös digitalisaatio sekä markkinointimateriaalit.

2.1 Kyberturvallisuus

Tarkasteltaessa kyberturvallisuuden määritelmää, voidaan huomata sen sisältävän useita eri näkemyksiä. Tätä havaintoa tukee Craigen, Diakun-Thibault ja Purse (2014), sillä heidän mukaansa kyberturvallisuudelta puuttuu tiivis ja laajasti hyväksytty määritelmä, koska aiheena se on erittäin moniulotteinen. He lisäävät vielä, että kyberturvallisuuden käsite on yleisesti käytetty termi, jonka määrittelyssä on havaittu merkittävää vaihtelua, kontekstiriippuvuutta sekä subjektiivisuutta (Craigen ym., 2014, s. 13).

Määriteltäessä kyberturvallisuutta pyritään saavuttamaan laaja ja kattava kuva. Craigen ym. (2014, s.13) kuvaavat artikkelissaan kyberturvallisuutta monitieteelliseksi käsitteeksi sisältäen useita eri menetelmiä ja teknologioita, joiden avulla suojataan tietoverkkoja sekä niihin liittyviä tietoja kyberhyökkäyksiltä ja muilta haitallisilta häiriöiltä. Hieman erilaisen näkemyksen puolestaan antavat Seemma, Nandhini ja Sowmiya (2018, s. 125). Heidän mukaansa kyberturvallisuuden voidaan ajatella myös olevan internettiin kytkettyjen järjestelmien, kuten laitteiden, ohjelmistojen ja tietojen suojaamista hyökkäyksiltä. Suppean Cambridgen sanakirja kuvauksen nostavat esille Kagalwalla ja Churi (2019, s.1), jonka mukaan kyberturvallisuus tarkoittaa ”tapoja suojata tietokonejärjestelmiä uhilta, kuten viruksilta”. Vielä neljännen kattavamman kyberturvallisuusongelman määrittämiseen keskittyvän näkemyksen tarjoavat Singer ja Friedman (2014). Ensinnäkin he tuovat esille, kuinka kyberturvallisuuden ala kattaa laajan kirjon aiheita, jotka ulottuvat pankkitiliesi ja verkkoidentiteettisi turvallisuudesta laajempiin kysymyksiin siitä, kuinka mikä tahansa hallitus voi päästä käsiksi

henkilökohtaisiin arkaluonteisiin tietoihisi ja jopa siihen, milloin ja missä maasi aloittaa sodan (Singer ja Friedman, 2014, s.8). He kertovat myös kyberturvallisuusongelman syntyvän silloin, kun vastapuoli pyrkii hyötymään jostakin toiminnasta, kuten esimerkiksi yksityistietojen hankkimisesta, järjestelmän alentamisesta tai sen laillisen käytön estämisestä. Tämä on heidän mukaansa erottava tekijä tavallisten kyberongelmien ja kyberturvallisuusongelmien välillä (Singer ja Friedman, 2014, s.34). Eli vastapuolen tavoite hyödyntää toimintaa omaksi edukseen syntyy ongelmaksi kyberturvallisuuden kontekstissa. Myös tämä määritelmä auttaa muodostamaan kattavan käsityksen kyberturvallisuuden laajuudesta ja sen sisällöistä käsitteenä. Näistä toisistaan hieman poikkeavista määritelmistä huomataan kaikkien pyrkivän kuvaamaan samaa asiaa painottaen kuitenkin eri näkökulmia.

Kehityksen kannalta olisi merkittävää saada muodostettua näitä eri näkökulmia kokoava yhtenäinen käsite kyberturvallisuudesta. Tämä on tärkeää, sillä Craigen ym. (2014) mukaan selkeän, tiiviin ja yhtenäisen määritelmän puuttuminen hidastaa teknologista ja tieteellistä kehitystä. Se vahvistaa pääasiassa teknistä näkökulmaa kyberturvallisuuteen ja erottaa tieteenalat toisistaan, vaikka niiden tulisi työskennellä yhdessä monimutkaisten kyberturvallisuushaasteiden ratkaisemiseksi. He esittävät uuden määritelmän, joka ottaa huomioon nämä seikat. Sen mukaan kyberturvallisuus tarkoittaa resurssien, prosessien ja rakenteiden järjestämistä ja kokoamista. Tämä on suunniteltu suojaamaan kyberavaruutta ja siihen perustuvia järjestelmiä tapahtumilta, jotka ovat oikeudellisesti ristiriidassa todellisten omistusoikeuksien kanssa (Craigen ym., 2014, s. 17–18).

On tärkeää ymmärtää, että juuri lentoliikenteen näkökulmasta kyberturvallisuuden merkitystä ei voida sivuuttaa. Viime aikoina kyberturvallisuus on saanut huomattavaa lisävauhtia, kun lentoliikenteen ohjausjärjestelmät ovat siirtyneet perinteisistä analogisista maanpäällisistä järjestelmistä digitaalisiin avaruusperustaisiin järjestelmiin vastauksena lentoliikenteen valtavaan kasvuun (Elmarady & Rahouma, 2021, s.).

2.2 Digitalisaatio

Digitalisaatio on uusien digitaalisten elementtien käyttöönottoa organisaatioissa sekä digitaalisten teknologioiden hyödyntämistä liiketoimintaprosessien tehostamiseksi ja resurssien käytön optimoimiseksi (Antikainen, Uusitalo, & Kivikytö-Reponen, 2018, s. 45). Se tehostaa kiertotalouden järjestelmiä, mahdollistaen läpinäkyvän tiedonkulun tuotteiden resurssien kulutuksesta. Sen avulla lisätään myös tuotteiden elinkaaren tehokkuutta, mikä puolestaan edistää kiertotalouden kehitystä (Antikainen ym., s. 46). Digitalisaatio on mullistanut maailman niin yksittäisen ihmisen, kuin liike-elämän ja yhteiskunnan toiminnankin näkökulmasta. Lindgren, Mokka, Neuvonen & Toponen (2019, s. 8) kertovat, että se on muuttanut maailmanlaajuista talousjärjestelmää, joka oli aiemmin pääosin kansallisvaltojen rajoittama. Heidän mukaansa tämä muutos on tehnyt markkinoille pääsystä helpompaa ja poistanut perinteiset liiketoiminnan fyysiset esteet. Näin

ollen se on avannut tien todelliselle kansainväliselle kaupalle, joka houkuttelee valtavan määrän uusia kuluttajia ja innovatiivisia toimijoita markkinoille (Lindgren ym., 2019, s. 8).

Sama muutos vaikuttaa myös ilmailualalla, jossa lentoyhtiöt ovat ottaneet käyttöön digitaalisia ratkaisuja ja teknologioita liiketoimintaprosessiensa tehostamiseksi. Tämä voidaan havaita esimerkiksi online-varausjärjestelminä, itsepalvelupisteinä lentokentillä tai sähköisenä asiakaspalveluna. Digitalisaatiolla on merkittävä rooli lentoliikenteen kyberturvallisuuden näkökulmasta. Lentoyhtiöiden, lentokenttien ja lennonvalvonnan erilaiset järjestelmät ovat yhä enemmän riippuvaisia digitaalisista ratkaisuista, jotka voivat olla alttiita kyberuhille.

2.3 Markkinointimateriaalit

Markkinoinnilla tarkoitetaan liiketoiminnan strategista toimintaa, jonka avulla pyritään luomaan ja ylläpitämään asiakassuhteita sekä vaikuttamaan kuluttajien ostopäätöksiin (Kannan, 2017). Markkinointi on muuttuva ja dynaaminen liiketoiminnan toiminto, jonka rooli on muuttunut merkittävästi erilaisten kriisien vaikutuksesta (Bala & Verma, 2018, s.323) Lentoyhtiöiden tapauksessa markkinointi ilmennetään digitaalisen markkinoinnin prosessina, jonka tarkoituksena on keskittyä yrityksen asettamiin tavoitteisiin tehokkuuden ja kestävyyden rajoissa (Basal & Suzen, 2023, s.3) Markkinointimateriaalit puolestaan ovat erilaisia digitaalisia välineitä ja sisältöjä, joita käytetään viestimään sekä edistämään tuotteita tai palveluja verkossa. Materiaaleihin voivat kuulua esimerkiksi verkkosivut, sosiaalisen median kampanjat, sähköpostimarkkinointi ja muut digitaaliset markkinointikanavat (Kannan, 2017).

Tämän tutkimuksen kontekstissa on hyvä huomioida, että lentoyhtiöiden sivustoilla kyberturvallisuutta koskevat tiedot ovat nimenomaan markkinointimateriaalia ja siten tuovat esille vain lentoyhtiön itse haluamat asiat.

3 LENTOLIIKENTEEN KYBERTURVALLISUUDEN ERITYISPIIRTEET

Kyberturvallisuus on huomattava tekijä lentoturvallisuudessa, eikä sen merkitystä lentoliikenteelle voida sivuuttaa, sillä se kohtaa useita haasteita ja riskejä. Vaikka lentoyhtiöt kohtaavat samanlaisia kyberturvallisuusuhkia, kuin muutkin organisaatiot, voidaan kuitenkin tunnistaa alalle erittyisiä piirteitä. Näitä ovat lentoliikenteen hyödyntämät prosessit ja järjestelmät sekä mahdolliset seuraamukset uhkiin. Tässä luvussa tarkastellaan, kuinka kyberturvallisuutta on tutkittu lentoliikenteen näkökulmasta. Tämä pitää sisällään syventymisen GPS-häirintään, langattomiin verkkopalveluihin, verkkoturvallisuusinfrastruktuuriin sekä erilaisiin kommunikaatioprotokolliin.

3.1 GPS-häirintä

Global Positioning System (GPS) -häirinnällä tarkoitetaan satelliittinavigointijärjestelmän, kuten Global Navigation Satellite Systemin (GNSS), toiminnan häirintää tai häiriöitä (Enge, Enge, Walter & Eldredge, 2015, s. 19). Tämä voi ilmetä esimerkiksi signaalien tarkoituksellisena häiritsemisenä tai manipulointina, jonka seurauksena pystytään vaikuttamaan negatiivisesti satelliittinavigointijärjestelmän toimintaan ja siten myös lentokoneiden navigointiin (Enge ym., 2015, s. 27; Gebre-Egziabher, Hayward, & Powell, 1996, s. 3234). GPS-järjestelmät parantavat satelliittipaikannuksen tarkkuutta ja luotettavuutta. Ne mahdollistavat vaikuttamisen GPS-signaaleihin, mikä puolestaan näkyy lennonohjausjärjestelmissä.

Tämä on merkittävää lentoliikenteen kannalta, sillä GPS-häirinnän avulla voidaan aiheuttaa vakavia riskejä. Viime aikoina ilmiö on noussut esille sosiaalisessa mediassa ja ollut myös merkittävänä aiheena uutisissa. Esimerkiksi Ylen 27.4.2024 julkaisemassa artikkelissa kerrotaan kahden Finnairin lentokoneen joutuneen palaamaan Viron Tartosta takaisin Suomeen juuri GPS-häirinnän takia. Artikkelissa todetaan myös Suomeen kohdistuvan GPS-häirinnän lisääntyneen.

Tämän häirinnän aiheuttajaksi on epäilty Venäjää (Kangas, 2024). Voidaan huomata, että tällaisiin hyökkäyksiin saattaa liittyä useita motiiveja, kuten taloudellisia, poliittisia tai terrorismiin liittyviä tarkoituksia. Vaikka GPS-häirintä tuntuu yleistyneen, sen laajuus ja tarkat motiivit ovat kuitenkin edelleen osittain epäselviä.

GPS-järjestelmät kohtaavat useita kyberturvallisuuden heikentämiseen pyrkiviä uhkia. Järjestelmissä yhtenä riskinä ovat toimintahäiriöt, jotka voivat vaikuttaa niiden suorituskykyyn. Enge ym., (2025, s.32) toteavat, etteivät perinteiset ilmailujärjestelmät enää ole riittäviä suorituskyvyn varmistamiseen, jos GPS-järjestelmät häiriintyvät. Tämä herättää kysymyksen siitä, kuinka merkittävä rooli GPS:llä onkaan nykyaikaisessa ilmailussa ja mitä seurauksia sen toimintahäiriöillä voi olla turvallisuuteen. Näin ollen on erityisen tärkeää kehittää vaihtoehtoisia järjestelmiä ja uutta tekniikkaa häiriöiden torjumiseksi.

Toimintahäiriöiden lisäksi GPS-järjestelmissä voi ilmaantua laitteistojen vakautta ja luotettavuutta vaarantavia tekijöitä. Gebre-Egziabher ym., (1996) kertovat, että erityisesti halvemman tason ajoneuvokohtaiset inertiasensorit eivät ole välttämättä tarpeeksi vakaita pitkäaikaisiin katkoksiin GPS-signaalissa. Inertiasensorilla tarkoitetaan laitteita, jotka mittaavat ja tarjoavat tietoa esineen tai järjestelmän liikkeen ja asennon muutoksista suhteessa ympäristöön (El-Sheimy & Youssef, 2020, s. 1). Niistä muodostuu asento- ja suuntaviitejärjestelmä eli Attitude and Heading Reference System (AHRS), jota käytetään ohjaamaan lentokoneen asentoa reaaliajassa, ja GPS:ää puolestaan kalibroimaan antureiden havaitsemia virheitä lennon aikana (Gebre-Egziabher ym., 1996, s. 519). Merkittävänä uhkana lentoliikenteelle on häirinnän vaikutus signaalin luotettavuuteen, minkä seurauksena lentokoneen asennon määrittämisessä voi tapahtua virheitä. Lisäksi, jos GPS-signaali katkeaa tai on epävakaa, AHRS:n on kyettävä jatkamaan toimintaansa luotettavasti pelkän inertiaalianturitiedon varassa, mikä voi olla haasteellista erityisesti lyhytaikaisissa GPS-ulosajoissa (Gebre-Egziabher ym., 1996, s. 520). GPS-järjestelmien kyberuhat liittyvät siten GPS-asennon määrittämisen virheisiin ja siihen, kuinka näitä virheitä käsitellään ja pystytään suodattamaan pois mahdollisimman hyvin.

3.2 Langattomat verkkopalvelut

Kyberturvallisuuden rooli lentoliikenteessä on keskeinen, erityisesti jatkuvien kyberhyökkäysten vuoksi, joiden seurauksena syntyy vahinkoa ja poliittisia sekä taloudellisia konflikteja (Elmarady & Rahouma, 2021, s.1). Lentoliikenne käyttää monimutkaisia järjestelmiä ja verkostoitunutta teknologiaa, mikä altistaa sen monille kyberuhkille. Tämä herättää kysymyksen siitä, kuinka voidaan varmistaa lentomatkustuksen turvallisuus samalla kun hyödynnetään uusinta teknologiaa ja langattomia verkkopalveluita entistä enemmän.

Kagalwallan ja Churin (2019) mukaan langattomilla verkkopalveluilla on merkittävä vaikutus lentoyhtiöiden kehitykseen. Yhdistetty lentokone -termi viittaa Pollardin ja Clarkin (2019) havaitsemaan kehitykseen, jossa langattomien,

Internet-protokollapohjaisten yhteyksien käyttö on kasvanut merkittävästi, yhdistäen lentokoneet, satelliitit ja maanpäälliset tietojärjestelmät. Tämä kehitys on merkittävä lentoliikenteen kannalta, koska se integroi erilaisia järjestelmiä, mutta samalla lisää myös kyberturvallisuusriskejä, erityisesti langattomien verkkopalvelujen käytön lisääntyessä. Pollardin ja Clarkin (2019) mukaan tämä edistysaskel on johtanut tuhansien upotettujen automaattisten antureiden integroimiseen lentokoneiden turvallisuuskriittisiin järjestelmiin, kuten moottoreihin ja ohjausjärjestelmiin. Näiden antureiden lähettämä jatkuva data lisää lentokoneiden elintärkeiden järjestelmien valvontaa, parantaen siten turvallisuutta. Kuitenkin yhdistämällä lentokoneet Internetiin, ilmassa toimivat järjestelmät altistuvat vakaville kyberturvallisuusuhille, joista monet matkustajat eivät ole tietoisia. Tämä tietämättömyys voi jatkua, kunnes kyberhyökkäyksen seurauksena ilmenee onnettomuus tai vastaava tilanne (Pollard & Clark, 2019, s.1).

Myös teknologian kehityksessä näkyy kaupallisen lentoliikenteen asiakaspalvelun painopiste. Kagalwallan ja Churin (2019) mukaan lentokoneiden järjestelmiin on sisällytetty enemmän tekniikkaa, joka tarjoaa matkustajille parempaa palvelua. Langattomat liitännät, kuten Wi-fi ja Bluetooth, mahdollistavat matkustajille monia käyttömahdollisuuksia lennon aikana, kuten suoratoistetun viihteen katselun ja internetyhteyden käytön. Lentoyhtiöt voivat parantaa toimintaansa ja tarjota matkustajilleen parempaa palvelua erityisesti hyödyntämällä asioiden internet eli Internet of Things -teknologiaa (IoT) ja pilvilaskentaa. IoT tarjoaa lentoliikenteen toimijoille kustannustehokkuutta ja tärkeää tietoa, kun taas pilvilaskenta mahdollistaa joustavan ja skaalautuvan IT-infrastruktuurin ilman ylimääräisiä resursseja (Kagalwalla & Churi, 2019). Kuitenkin tämän kehityksen myötä lentokoneet eivät enää toimi suljettuina järjestelminä, mikä lisää kyberuhkien ja -riskien todennäköisyyttä (Kagalwalla & Churi, 2019). Elmarady ja Rahouma (2021, s.1) huomauttavat myös, että monet ilmailun ohjauslaitteet ovat suunniteltu avoimiksi, mikä saattaa johtaa turvallisuuskysymysten laiminlyöntiin. Tämä korostaa tarvetta kehittää ja soveltaa tehokkaita turvallisuustoimenpiteitä lentoyhtiöiden IT-infrastruktuurissa ja lentokoneiden järjestelmissä.

Tarkasteltaessa lentoliikenteen teknologista kehitystä, Kagalwalla ja Churi (2019) korostavat nopeiden yhteyksien merkitystä verkottuneissa lentokonejärjestelmissä. He kertovat, että tämän avulla lentoyhtiöiden on mahdollista laajentaa toimintaansa ja saada lentokoneet toimimaan saumattomasti muiden lentoyhtiön yritysverkon lentokoneiden kanssa. Kehityksen myötä lentoyhtiöt pystyvät myös automatisoida entistä enemmän manuaalisia prosesseja hyödyntämällä Internet of Things (IoT) -laitteita, pilvipalveluita, pilvitallennusta ja koneoppimista (Kagalwalla & Churi, 2019, s.1). Tämä herättää kysymyksen siitä, kuinka voidaan varmistaa lentoliikenteen turvallisuus ja luotettavuus samalla kun otetaan käyttöön näitä edistyneitä teknologioita. On tärkeää löytää tasapaino innovaatioiden ja riskienhallinnan välillä, jotta pystytään hyödyntää teknologian tarjoamat mahdollisuudet täysimääräisesti.

3.3 Verkkoturvallisuusinfrastruktuuri

Verkkoturvallisuusinfrastruktuurilla tarkoitetaan järjestelmiä, verkkoja ja prosesseja, jotka ovat suunniteltu suojaamaan tietojärjestelmiä sekä verkkoympäristöjä erilaisilta uhilta ja hyökkäyksiltä (Ali, Ayyasamy, Akbar, Ponnusamy & Heng, 2022, s.1). Kuten aikaisemmassa kappaleessa mainittiin, lentoyhtiöiden erilaiset verkkoinfrastruktuuriin liittyvät järjestelmät sisältävät heikkouksia, jotka vaikuttavat lentoyhtiöiden kyberturvallisuuteen. Tällaisia käytössä olevia järjestelmiä ovat yksittäinen kirjautuminen, verkkopääsyn hallinta sekä hajautettu palvelunesto.

3.3.1 Yksittäinen kirjautuminen

Kagalwallan ja Churin (2019) kertovat, että yksittäisellä kirjautumisella eli Single Sign-on-todennuksella (SSO) tarkoitetaan keskitettyä istunto- ja käyttäjätodennuspalvelua, jonka avulla yhdellä kirjautumistunnistesarjalla voidaan käyttää useita sovelluksia. Se on heidän mukaansa yksi lentoyhtiöiden suurimmista haavoittuvuuksista verkkopääsyn valvonnan ja hajautetun palveluneston lisäksi. Näiden takia lentoyhtiöiden ydinverkon suojaaminen on erityisen tärkeää (Kagalwalla & Churi, 2019, s.2). Tästä eteenpäin yksittäisestä kirjautumisesta käytetään lyhennettä SSO. Myös Pandey ja Nisha (2021) antavat SSO-todennuksella vastaavanlaisen, mutta hieman tarkemman määritelmän. Heidän mukaansa SSO-todennus käyttää keskitettyä istuntokonseptia toimien palveluna, joka vahvistaa yksittäisen tietyn alustan. Sen jälkeen, kun käyttäjä on tunnistettu yhdellä määritetyllä alustalla, voidaan käyttää erilaisia palveluita kirjautumatta joka kerta uudelleen (Kagalwalla & Churi, 2019, s.2; Pandey & Nisha, 2021, s.2).

SSO-todennukseen liittyy kuitenkin omat haasteensa. Tähän kuuluvana turvallisuusriskinä toimii Kagalwallan ja Churin (2019) mukaan se, että SSO:n avulla voidaan saada yhden käyttäjätunnuksen kautta pääsy kaikkiin käyttäjän oikeuksiin, jolloin portit tai säätimet eivät estä täydellistä hallintaa tai kompromisseja. Pandeyn ja Nishan (2021) kertovat puolestaan, että kyberturvallisuusriskejä aiheuttavat myös yhden pisteen epäonnistuminen eli Single Point of Failure (SPOF), palvelimen murtuminen ja tietojen jakaminen kolmannen osapuolen kanssa. Yhden pisteen epäonnistumisella tarkoitetaan heidän mukaansa tilannetta, jossa SSO-toimittajan ongelmien seurauksena toiminta keskeytyy ja asiakkaat eivät välttämättä pääse varmistamaan identiteettiään, mikä johtaa koko järjestelmän toiminnan pysähtymiseen. Pandey ja Nisha (2021) pitävät yhden palvelimen murtumista tai hakkerointia varsin todennäköisenä, mikä voi aiheuttaa tietojen menetystä sekä altistaa asiakkaiden luottamukselliset tiedot uhkaajalle, koska kaikki vahvistusvaltuudet ovat samassa paikassa. Riski tämän tapahtumiseen korostuu, jos SSO:n ja monivaiheisen todennuksen yhdistelmää ei käytetä.

Riskiä lisää yhden kirjautumisen käyttöönotossa myös asiakastietojen jakaminen kolmannelle osapuolelle (Pandey & Nisha, 2021, s.8). Tietojen jakaminen kolmannen osapuolen kanssa voi altistaa tietojen vuotamiselle tai niiden väärinkäytölle, mikä puolestaan korostaa tarvetta tehokkaalle tietoturvakäytännölle

sekä mahdollisille varotoimenpiteille. Näiden kaikkien seikkojen takia SSO:n voidaan ajatella olevan ilmailussa suuri haavoittuvuus ja siihen liittyvän merkittävä kyberturvallisuusriski, joka lentoyhtiöiden tulisi ottaa huomioon toiminnassaan.

3.3.2 Verkkopääsyn valvonta

Toisena merkittävänä haavoittuvaisuutena lentoyhtiöissä on Kagalwallan ja Churin (2019) mukaan verkkopääsyn valvonta eli Network Access Control (NAC). Tästä eteenpäin tutkielmassa tullaan käyttämään lyhennettä NAC. Sillä tarkoitetaan käytäntöjen käyttöönottoa, jotka säätelevät laitteiden ja käyttäjien pääsyä verkkoihin (Kagalwallan & Churin, 2019, s.2). Myös Qiu, Jianwei, Zhihong ja Shuofei (2011) antavat samankaltaisen määritelmän. Heidän mukaansa NAC on tehokas ja joustava järjestelmä, jonka tarkoitus on estää haitallisten tietojen leviäminen verkossa ja erityisesti suurissa verkkoympäristöissä (Qiu ym., 2011, s.1). Yuxian, Lianhuan ja Xinfeng (2011, s.2) puolestaan määrittelevät NAC:n järjestelmäksi, jonka avulla voidaan varmistaa kaikkien verkon resursseihin pyrkivien laitteiden noudattavan tiettyä turvallisuuspolitiikkaa ennen niiden pääsyä kyseiseen verkkoon. He korostavat, että tämän saavuttamiseksi järjestelmä käyttää erilaisia välineitä, kuten päätesovelluksia, reitittimiä, kytkimiä ja palomuureja, jotta vain oikeutetut laitteet voivat käyttää verkon resursseja. Lisäksi NAC sisältää automatisoidun käsittelyprosessin, jonka avulla verkkolaitteet, kuten reitittimet ja kytkimet, voivat tiiviisti yhteistyössä palvelimen ja käyttäjän tietokoneen kanssa varmistaa tietojärjestelmän turvallisen toiminnan ennen käyttäjän interaktiota (Yuxian ym., 2011, s.2). Se auttaa siis parantamaan verkon turvallisuutta ja tehokkuutta torjumalla haitallisia kyberturvallisuusuhkia.

NAC ei ole kuitenkaan aukoton, sillä useat kyberturvallisuusriskit ovat sille ominaisia. Toimivalle verkkopääsyn hallinnalle haasteen luo muun muassa se, että työntekijöillä sekä asiakkailla on mahdollisuus päästä lentokentän verkkoon (Kagalwallan & Churin, 2019, s.2). Merkittävänä kyberturvallisuusuhkana tähän liittyy IoT-laitteiden kasvu, jonka seurauksena kaikki laitteet tulee suojata asianmukaisesti. Kagalwallan ja Churin (2019) mukaan erityistä ongelmaa aiheuttaa lentokentän verkkoon yhdistetyt työntekijöiden henkilökohtaiset laitteet kuten puhelimet ja tabletit, sillä niistä puuttuu valmiiksi asennetut virustorjuntaohjelmat sekä ne voivat sisältää koko verkkoa uhkaavia sovelluksia. He kertovat vielä, että näiden tekijöiden takia verkkopääsyn valvonnan integroiminen palomuureihin ja kyberuhkien havaitsemiseen on välttämätöntä (Kagalwallan & Churin, 2019, s.2).

Tämän lisäksi Yuxian ym., (2011, s.2) esittävät NAC:n kohtaavan nollapäiväiskujen uhkaa, jolloin hyökkääjät voivat hyödyntää tunnettuja haavoittuvuuksia ennen kuin niihin on saatu korjaustiedostoja. Tältä on kuitenkin mahdollista välttyä, jos verkon kulunvalvontajärjestelmä on tarpeeksi päivittynyt (Yuxian ym., 2011, s.2). Myös suuret verkottavat aiheuttavat ongelmia. Sekä Qui ym., (2011) että Yuxian ym., (2011) korostavat NAC-järjestelmien tehokkuutta ja optimointia suurille verkoille. Qui ym., (2011, s.1) kertovat, että NAC-järjestelmän tehottomuus tai soveltumattomuus suurille verkoille voi johtaa liikenteen

hidastumiseen ja järjestelmän ylikuormittumiseen, mikä heikentää verkon suorituskykyä ja vakautta. Heidän mukaansa NAC-järjestelmien laajentaminen suuriin verkkoihin vaikeuttaa niiden hallintaa ja näin ollen voivat lisätä virheitä sekä vaikeuttaa ylläpitoa. Yuxian ym., (2011, s.2) puolestaan tuovat esille, että erityisesti suurien verkkojen kohdalla perinteinen skannaaminen voi olla resursseja kuluttavaa, mikä johtaa järjestelmän suorituskyvyn heikkenemiseen. Tämän lisäksi heidän mukaansa paljon resursseja voivat vaatia joillakin NAC-teknologioilla olevat monimutkaiset vaatimukset.

Myös mahdollisista määrittelyvirheistä aiheutuu haitallisia seurauksia. Jos NAC-järjestelmät on määritelty virheellisesti, ne voivat aiheuttaa vaurioita verkossa tai tahattomasti evätä laillisen liikenteen pääsyn sallittuihin resursseihin (Qui ym., 2011, s.1). Tämän lisäksi uhan aiheuttaa myös verkonkulunvalvontajärjestelmän epäonnistuminen päälaitteiden havaitsemisessa, minkä seurauksena haitalliset laitteet voivat pysyä verkossa pidempään esimerkiksi varastaen tietoja tai suorittaen verkkojen vakoilua (Yuxian ym., 2011, s.2). Merkittävän haasteen voivat luoda myös yhteensovittamisongelmat. Tällöin NAC-järjestelmän integroimisessa olemassa olevaan verkkoinfrastruktuuriin ja sen laitteisiin syntyy ongelmia, jotka vaikuttavat järjestelmän tehokkuuteen ja toimintaan (Qui ym., 2011, s.1).

Voidaan todeta, että verkkopääsyn valvonnalla on keskeinen rooli laitteiden turvallisuuden hallinnassa verkossa. Lentoyhtiöiden näkökulmasta tästä on hyötyä, sillä ne käsittelevät paljon arkaluontoisia tietoja, kuten matkustajien henkilötietoja. On siis kriittisen tärkeää, että lentoyhtiöiden verkkoon pääsevät vain tietoturvakriteerit täyttävät turvalliset laitteet, jotta lentoyhtiöt voivat säilyttää asiakasluottamuksensa sekä edistää omaa liiketoimintaansa.

3.3.3 Hajautettu palvelunesto

Kagalwallan ja Churin (2019) esittävät, että kolmas merkittävin heikkous lentoliikenteen kannalta on hajautettu palvelunesto eli Distributed Denial of Service (DDoS). Heidän mukaansa tällä tarkoitetaan verkkosivustoihin ja -palveluihin kohdistuvia hyökkäyksiä, joiden tarkoituksena on ylikuormittaa ne suuremmalla liikenteellä kuin palvelin tai verkko voi käsitellä. Tämän avulla hyökkääjä pyrkii tekemään hyökkäyksen kohteesta käyttökelvottoman (Kagalwallan & Churin, 2019, s.2). Vaikka nämä hyökkäykset eivät ole uusi uhka, ne ovat edelleen merkittävä turvallisuushaaste (Osanaiye, Choo & Dlodlo, 2016, s.1).

Ilmailualan näkökulmasta hajautetulla palvelunestolla voidaan aiheuttaa suuria vaaratilanteita. Hajautettu palvelunesto mahdollistaa esimerkiksi lentokoneen pysäyttämisen, sen toiminnan estämisen ilmassa sekä virheellisten lentosuunnitelmia lataamisen (Kagalwallan & Churin, 2019, s.2). Tällainen toiminta voi aiheuttaa katastrofaalisia seurauksia etenkin, jos hyökkäys toteutetaan pilvipalvelimissa. Pilvipalvelimissa toteutetut hajautetun palveluneston hyökkäykset voivat nimittäin ruuhkauttaa infrastruktuurin ja jopa lamauttaa lentoyhtiön (Kagalwallan & Churin, 2019, s.2). Tällainen pilvipohjaisen hajautetun paleluneston hyökkäyksen torjuminen tarjoaa uudenlaisia ratkaisuja perinteiseen

tietojenkäsittelyyn nähden, hyödyntäen pilviteknologian arkkitehtuuria ja sen tarjoamia ominaisuuksia (Osanaiye, Choo & Dlodlo, 2016, s.1).

Vuonna 2015 puolalainen lentoyhtiö LOT Airlines joutui palvelunestohyökkäyksen kohteeksi, minkä seurauksena vähintään 22 lentoa viivästyi tai peruuntui, koska lentokoneissa odottavat lentäjät eivät saaneet lähtöohjeita (Kagalwallan & Churin, 2019, s.2). Tällaiset hyökkäykset vaikuttavat lentoyhtiöiden liiketoimintaan, sillä lentokoneiden lähtöjä joudutaan viivästyttämään tai perumaan. Näiden seurauksena puolestaan lentoyhtiön maine ja asiakastyytyväisyys voivat vahingoittua sekä lentoyhtiölle ja matkustajille aiheutua merkittäviä taloudellisia menetyksiä.

3.4 Kommunikaatioprotokollat

Ilma-maaviestintä on yksi tärkeimmistä ilmailunavigointipalveluista, jota on ylläpidettävä lentoturvallisuuden varmistamiseksi. Radiokommunikaatiojärjestelmät ovat merkittävässä roolissa lennonjohtajan ja lentäjän välisessä viestinnässä, varmistaen lentokoneen turvallisen reitin lentämisen. Ne siirtävät myös olennaista tietoa esimerkiksi selvityksiä, lentokoneiden erottelua ja säätiedotteita, sekä muita tarpeellisia tietoja, kuten lentojen suunnittelua ja huoltoa (Elmarady & Rahouma, 2021, s.5–6). Tätä kommunikaatiota varten käytössä on yleisiä kommunikaatioprotokollia, joihin liittyvät omat kyberturvallisuusriskinsä. Yleisiä protokollia Elmaradyn ja Rahouman (2021) mukaan ovat:

- erittäin korkeataajuinen äänikommunikaatio eli Very-High Frequency Voice Communication (VHF),
- ohjaaja – lentäjä tietoliikenneyhteys eli Controller-Pilot Data Link Communication (CPDLC) sekä
- ilma-aluksen viestintäosoitus- ja raportointijärjestelmä eli Aircraft Communication Addressing and Reporting System (ACARS).

Näitä viestintäjärjestelmiä kohtaa useat kyberturvallisuusuhat, koska niiden suunnittelussa ei ole historiallisesti otettu huomioon turvallisuutta (Lehto, Sestorp, Khan & Gurtov, 2021, s.1). Sen sijaan turvallisuus on perustunut toimintamenetelmiin sekä lennonjohtojärjestelmien ja lentäjän väliseen luottamukseen, minkä seurauksena järjestelmissä on epävarmuuksia (Lehto ym., 2021, s.1). Tämän takia on erityisen tärkeää jatkuvasti kehittää uusia turvamekanismeja, jotka kykenevät vastaamaan kasvaviin kyberuhkiin ja täten varmistamaan lentoliikenteen viestinnän toimivuuden sekä lisäämään turvallisuutta. Seuraavaksi tarkastellaan yleisimpiä viestinnässä käytettyjä kommunikaatioprotokollia ja niiden heikkouksia kyberturvallisuuden näkökulmasta.

3.4.1 Erittäin korkeataajuinen äänikommunikaatio

Erittäin korkeataajuinen äänikommunikaatio eli Very-High Frequency Voice Communication (VHF) tarkoittaa Elmaradyn ja Rahouman (2021) mukaan ilma-

maaviestintäjärjestelmiä, jotka ovat perinteisiä radiokanavia, mutta niitä käytetään lentokoneiden ja lennonjohtotornien väliseen kommunikaatioon. He tuovat esille, että nämä järjestelmät hyödyntävät amplitudimoduloituja kantoaaltoja ja toimivat tietyn taajuusalueen sisällä. Koska VHF-järjestelmät eivät tarjoa sisäänrakennettuja turvaprotokollia, niiden kommunikaatio on altis kyberuhille (Elmarady & Rahouma, 2021, s.6). Kamali (2010) puolestaan kertoo VHF:n olevan ilmailun viestintään varattu lyhytaaltoinen radiotaajuusalue, jonka kapasiteetti lähestyy kuitenkin nopeasti täyttymispistettään sekä Yhdysvalloissa että Euroopassa. Oleellisena osana kapasiteettiä voidaan pitää VHF:n spektriä eli radiotaajuuskaistaa. Tämä on 19 MHz leveä ja sijoittuu 118–127 MHz:n taajuuskaistalle, mahdollistaen 760 AM-radiokanavaa, joiden spektriväli on 25 kHz (Kamali, 2010, s.1).

Kun VHF toimii lentoliikenteen kommunikaation välineenä ja otetaan huomioon sen alttius kyberuhille, on olennaista ymmärtää, miten nämä haavoittuvuudet voivat vaarantaa turvallisuuden. VHF kohtaa monipuolisia uhkia ominaisuuksiensa takia. Elmaradyn ja Rahouman (2021) kertovat ettei sen viestintäliikennettä ole salattu, mikä avaa mahdollisuuden salakuuntelulle ja ulkoisille häiriöille. Nämä häiriöt voivat olla heidän mukaansa tahattomia tai tahallisia lähetyksiä. Lisäksi he korostavat mahdollisuutta väärentämishyökkäyksiin, joiden tarkoituksena on välittää lentokoneisiin luvattomia ohjeita ja näin ollen aiheuttaa haitallisia tai jopa tuhoisia seuraamuksia (Elmarady & Rahouma, 2021, s.6). Kamalin (2010) mukaan VHF:n turvallisuusuhat johtuvat pääasiassa ilmailuliikenteen odotetusta noin kahden prosentin vuosittaisesta kasvusta, samalla kun sille varattu radiotaajuusalue pysyy lähes ennallaan. Tämä vaikuttaa erityisesti ilmatilan hallintajärjestelmiin, jotka ovat keskeisiä sekä kansallisille että maailmanlaajuisille ilmailujärjestelmille niiden turvallisuuden, tehokkuuden ja kasvun näkökulmasta (Kamalin, 2010). Jotta viestinnän turvallisuus ja tehokkuus voidaan taata, tarvitaan siis uusia viestintäjärjestelmiä vastaamaan ilmailuliikenteen kasvaviin tarpeisiin.

3.4.2 Ohjaaja – lentäjä tietoliikenneyhteys

Lehto ym., (2021) mukaan Ohjaaja – lentäjä tietoliikenneyhteys eli Controller-Pilot Data Link Communication (CPDLC) on otettu käyttöön juuri helpottamaan tätä VHF:n liiallista kuormittumista. He kertovat, että CPDLC täydentää VHF-radioääniyhteyttä käsittelemällä vähemmän kriittistä viestintää, minkä seurauksena sen käyttöönoton jälkeen väärinymmärrykset ovat vähentyneet ja viestinnän tehokkuus parantunut (Lehto ym., 2021). Elmarady ja Rahouma (2021) tarkentavat, että CPDLC:llä tarkoitetaan digitaalista tietolinkkikommunikaatioprotokollaa lennonjohtajien ja lentäjien välillä. Heidän mukaansa sen avulla voidaan kommunikoida tekstimuotoisesti, mikä vähentää ruuhkautumista perinteisillä VHF-äänikanavilla ja mahdollistaa automatisoidun tiedonvälityksen. He kertovat myös CPDLC:n parantavan lentoturvallisuutta tarjoamalla selkeitä ja tarkkoja viestejä, mikä puolestaan alentaa väärinkäsitysten riskiä lisäten kommunikaation tehokkuutta. Tämä taas pienentää inhimillisten virheiden riskiä ja tehostaa lennonhallintaa (Elmarady & Rahouma, 2021, s.7–8).

CPDLC:n ei kuitenkaan ole kyberturvallisuuden näkökulmasta täysin aukoton etenkin kommunikaatiojärjestelmien kuormituksen kasvaessa. Historiallinen tilanne, jossa viestintäjärjestelmät ovat perustuneet luottamukseen lennonjohtojärjestelmän ja lentäjän välillä, luo epävarmuutta järjestelmille, kuten CPDLC:lle. (Lehto ym., 2021, s.1). Muiden avoimien ja salattomien kommunikaatiojärjestelmien tavoin, myös CPDLC on luonteeltaan turvaton puuttuvien sisäänrakennettujen turvaprotokollien takia (Elmarady & Rahouma, 2021, s.7–8). Tämä puolestaan asettaa ne alttiiksi monenlaisille kyberuhille.

Kyberturvallisuutta uhkaavat helposti saatavilla olevat ja kevyet laitteet, kuten ohjelmistomääritellyt radiot, jotka mahdollistavat pääsyn kehittyneisiin radio-ohjauksen manipulointityökaluihin (Lehto ym., 2021, s.1). Lehto ym., (2021, s.1) kertovat tämän poistavan aikaisemmin ilmailun kommunikaatiota suojanneen teknisen edun. Elmarady ja Rahouma (2021, s.7–8) puolestaan listaavat useita CPDLC:n kohtaamia uhkia. Näitä ovat heidän mukaansa välimieshyökkäykset, joihin kuuluvat esimerkiksi salakuuntelu sekä aktiiviset hyökkäykset. Muita heidän mainitsemiaan uhkia ovat häirintä eli kanavien tukkiminen; tulvaaminen eli useiden CPDLC-tietopakettien lähettäminen samalle vastaanottavalle taholle; injektiot eli mahdollisesti virheellisten ja luvattomien viestien lähettäminen; muuntaminen eli viestin sisällön muuttaminen sekä teeskentely, jossa hyökkääjä tekeytyy valtuutetuksi käyttäjäksi (Elmarady & Rahouma, 2021, s.7–8). Näitä monipuolisia kyberturvallisuusuhkia tarkastelemalla voidaan arvioida CPDLC:n riittävyyttä kommunikaatiossa, varsinkin otettaessa huomioon sen turvallisuuden puutteellisuus. Vaikka se tarjoaa lukuisia etuja perinteisempään VHF:ään verrattuna, ovat kyberturvallisuushaasteet huomattavia. Tämä korostaa tarvetta jatkuvasti kehittyville järjestelmille, turvamekanismeille sekä turvallisuusjohtamiselle, jotta järjestelmien käyttö ja näin ollen myös lentoliikenteen viestintä olisi mahdollisimman turvallista ja luotettavaan.

3.4.3 Ilma-aluksen viestintäosoitus- ja raportointijärjestelmä

Ilma-aluksen viestintäosoitus- ja raportointijärjestelmä eli Aircraft Communications Addressing and Reporting System (ACARS) tarkoittaa lentokoneiden ja lentokoneoperaattoreiden välistä datalinkkikommunikaatioprotokollaa (Elmarady & Rahouma, 2021, s.8). Toisin sanottuna se on laajasti käytetty viestintä-, osoite- ja raportointijärjestelmä, joka mahdollistaa tiedonsiirron lentokoneiden ja maanpäällisten toimijoiden välillä (Smith, Moser, Strohmeier, Lenders & Martinovic, 2018, s.105). Sitä käytetään myös monipuolisesti lentokaluston hallinnasta aina ilmaliikenteen ohjaukseen (Smith ym., 2018, s.105). ACARS tarjoaa erilaisia tietopalveluita, kuten esimerkiksi säätietoja ja lentosuunnitelmia, sekä se hyödyntää erilaisia datalinkkejä, kuten VHF:ää, SATCOM:ia ja HF:ää (Elmarady & Rahouma, 2021, s.8).

Emalradyn ja Rahouman (2021) mukaan myös ACARS, kuten edellä mainitutkin kommunikaatioprotokollat, on altis kyberhyökkäyksille, koska se ei sisällä oletusarvoisesti turvaprotokollia. Smith ym., (2018) kertovat, kuinka useimmat järjestelmän nykyään tarjoamista palveluista eivät kuuluneet sen alkuperäiseen tarkoitukseen, joka oli miehistön työtuntien kirjaaminen. Heidän mukaansa

ACARS:ia käytetään nykyään muun muassa ATC-lupien pyytämisessä, tiedotuspalveluissa, lentosuunnitelmissa, sijaintiraporteissa, diagnostiikkatiedoissa ja vapaatekstiviesteissä (Smith ym., 2018, s.107). Emalradyn ja Rahouman (2021) esittävät ACARS-järjestelmän kohtaamat kyberuhat. Heidän mukaansa se on altis muiden kommunikaatioprotokollien tavoin salakuuntelulle ja monenlaisille aktiivisille hyökkäyksille, kuten injektioille, muuntamiselle ja valehtelulle. He mainitsevat myös, että ACARS-viestiliikenne voi helposti joutua kaapatuksi edullisilla laitteilla, mikä mahdollistaa sen käytön etäisissä hyökkäyksissä lentäjien hallintajärjestelmiä vastaan (Elmarady & Rahouma, 2021, s.8–9). Nämä uhat voivat aiheuttaa vakavia turvallisuusriskejä lennon aikana.

4 KYBERTURVALLISUUDEN HUOMIOIMINEN LENTOYHTIÖIDEN TOIMINNASSA

Tässä luvussa käsitellään, kuinka kyberturvallisuus huomioidaan lentoyhtiöiden operatiivisessa toiminnassa. Lentoyhtiöt ovat nykyään yhä enemmän riippuvaista tietoteknisistä järjestelmistä, jotka vastaavat lennonvalvonnasta, matkustajatiedoista ja lentokoneiden suojauksesta. Tämä korostaa kyberturvallisuuden valvonnan käytäntöjen ja prosessien merkitystä, pyrittäessä varmistaa toiminnan jatkuvuus ja matkustajien turvallisuus. Kattava valvonta, kuten järjestelmien jatkuva seuranta sekä turvallisuusprotokollat, ovat elintärkeitä lentoliikenteessä, jossa pienikin häiriö voi saada aikaan laajoja seurauksia. Lisäksi kansainväliset säädökset ja standardit ovat lentoyhtiöille korvaamattomia kyberturvallisuuden näkökulmasta, sillä ne määrittelevät vaatimukset ja puitteet, joiden mukaan toimia on suoritettava. Siksi lentoyhtiöiden on tarkasti noudatettava eri maiden lainsäädäntöä ja kansainvälisiä sopimuksia, jotka koskevat tietoturvaa ja kyberuhkien torjuntaa alalla.

4.1 Lentoyhtiöiden kyberturvallisuuden hallinta

Digitaalisen maailman ja uusien teknologioiden jatkuva kehittyminen on synnyttänyt kasvavan trendin kyberrikollisuudessa. Tämä tarkoittaa sitä, että organisaatiot joutuvat yhä useammin kohtaamaan vakavia kyberturvallisuushyökkäyksiä. Näiden päivittäisten hyökkäysten kustannukset nousevat vuosittain jopa 375–575 miljardiin dollariin (Carcary, Doherty & Conway, 2019, s.78). Lentoyhtiöt eivät ole välttyneet tämän kehityksen vaikutuksilta. Digitaalisen muutoksen myötä uudet teknologiat ovat muuttaneet lentoliikenteen toimintaa, mikä on samalla avannut uusia mahdollisuuksia, mutta myös lisännyt niiden alttiutta kyberuhkille. Lentoyhtiöt kohtaavat nykyään entistä monimutkaisempia kyberturvallisuushaasteita, sillä hyökkäykset niiden järjestelmiä vastaan voivat vaikuttaa suoraan tietojen lisäksi myös lennonvalvontaan ja matkustajien turvallisuuteen. Kun laitteiden, järjestelmien ja infrastruktuurin välinen vuorovaikutus

lisääntyy asiakkaiden, toimittajien ja kumppaneiden keskinäisen vuorovaikutuksen myötä, myös IT-infrastruktuurin haavoittuvuus kasvaa (Carcary ym., 2019, s.78). Tämä vahvistaa entisestään tarvetta lentoyhtiöiden kyberturvallisuuden hallinnalle.

Khatun, Wagner, Jung ja Glaß (2023) mukaan kyberturvallisuuden hallinta organisaatiossa perustuu riskien tunnistamiseen ja niihin reagoimiseen. Tämä lähestymistapa määrittelee selkeät prosessit, vastuut ja hallinnan kyberuhkien torjumiseksi, mikä varmistaa tehokkaan suojauksen (Khatun ym., 2023, s.3). Koska hyökkäykset lentoyhtiöitä vastaan voivat vaikuttaa suoraan niin tietoihin, lennonvalvontaan kuin matkustajien turvallisuuteenkin, on kriittisen tärkeää, että lentoyhtiöt kehittävät ja panostavat laajoihin kyberturvallisuusstrategioihin. Carcary ym., (2019) mukaan organisaatiot pyrkivät estämään kyberturvallisuusloukkauksia erilaisilla lähestymistavoilla, jotka voivat vaihdella suuresti. He kertovat joidenkin organisaatioiden olevan erittäin tiukkoja toimintatavoissaan, mikä saattaa vaikeuttaa normaalia liiketoimintaa. Sen sijaan toiset ovat liian huolimattomia, mikä altistaa ne tarpeettomille riskeille. Organisaation on löydettävä oikea tasapaino varmistaakseen IT-resurssiensa turvallisuus estämättä tehokasta liiketoimintaa (Carcary ym., 2019, s.78). Khatun ym., (2023, s.3) puolestaan kertovat, että kyberturvallisuuden hallinnassa pyritään varmistamaan riskien tehokas hallinta ja valvonta hyödyntäen organisaation sisäisiä sääntöjä, politiikkoja, vastuita, hallintoa ja käytäntöjä järjestelmällisellä lähestymistavalla. Seuraavassa taulukossa kuvataan Carcaryn ym., (2019) näkemystä, jossa kyberturvallisuuden hallinnan teemat ovat jaettu kahdeksaan osa-alueeseen ja niiden tarkoituksiin.

TAULUKKO 1 Kyberturvallisuuden hallinnan osa-alueet (Carcary ym., 2019, s.80)

Osa-alue	**Tarkoitus**
Verkkoturvallisuusstrategia ja hallinto	Tarjoavat johdonmukaista strategista suuntaa ja valvontakriteerejä, joilla mahdollistetaan tehokas verkkoturvallisuuden hallinta.
Kyberturvallisuustietoisuuden hallinta	Helpottaa vastaamista uusiin riskeihin, tilanteisiin ja haavoittuvuuksiin liittyvään tiedustelutietoon sekä edistää kyberturvallisuusteknologioiden ja hallintamenetelmien kehitystä.
Tekniset turvatoimet	Asettavat tietoturvatoimenpiteet varmistaakseen kaikkien IT-ratkaisujen suojauksen ja määrittelevät turvallisuuskriteerit niiden suunnittelulle, kehitykselle ja toteutukselle.
Tietoturvahallinto	Luokittelee dataa ja informaatiota turvallisuusryhmiin ja tarjoaa ohjeita niiden elinkaaren turvallisuuden hallintaan.
Identiteetin ja pääsynhallinta	Tarjoavat tarvittavat turvatasot ja pääsynhallintalaitteet suojatakseen kyberturvallisuushäiriöiltä.
Kyberturvallisuusriskien hallinta	Arvioi, priorisoi, käsittelee ja valvoo erilaisia kyberturvallisuuteen liittyviä riskejä, joita organisaatio kohtaa.

Kyberturvallisuushäiriöiden hallinta	Tunnistaa ja käsittelee kyberturvallisuusvälikohtauksia, ymmärtäen niiden juurisyyn ja vaikutukset liiketoimintaan.
Liiketoiminnan jatkuvuuden hallinta	Takaa organisaation jatkuvuuden kyberhäiriön tapahtuessa.

Dou (2020) tuo myös esille keskeisiä tapoja kyberturvallisuuden hallintaan ilmailualla. Hänen mukaansa organisaatiot keräävät valtavia määriä tietoa eri lähteistä, kuten lentokoneiden suorituskyvystä, toimintaympäristöstä ja lentotoiminnan hallinnasta. Tämä tieto analysoidaan käyttämällä suurten tietomäärien analyysimenetelmiä, jotka voivat tunnistaa poikkeavuuksia ja ennakoida mahdollisia riskejä (Dou, 2020, s.7).

Tietojärjestelmien suunnittelu ja toteutus ilmailualalla edustavat myös olennaista osaa kyberturvallisuuden hallinnassa. Hallintajärjestelmien tavoitteena on tiedon ja osaamisen jakaminen, riskien vähentämiseen tähtäävien hallintarakenteiden suunnittelu sekä turvallisuutta edistävien prosessien toteuttaminen (Khatun ym., 2023, s.2). Dou (2020) kertoo ilmailualan hyödyntävän monimutkaisia tietojärjestelmiä, jotka kattavat kaiken lentokoneiden suunnittelusta ja suorituskyvyn parantamisesta aina lennonhallintaan ja matkustajapalveluihin. Näiden järjestelmien suunnittelussa ja toteutuksessa on ensisijaisen tärkeää huomioida kyberturvallisuus, mikä tarkoittaa tietoturva- ja tietosuojaominaisuuksien asianmukaista integrointia (Dou, 2020, s.5). Dou (2020) lisää, että suuret tietomäärät mahdollistavat tehokkaan digitaalisen suunnittelun ja valmistuksen, joilla optimoidaan lentokoneiden suorituskykyä ja vähennetään kustannuksia. Älykkäät kyberturvallisuusjärjestelmät, jotka hyödyntävät suuria tietomääriä, parantavat merkittävästi ilmailuteollisuuden turvallisuutta ja tehokkuutta (Dou, 2020, s.11).

Ilmailualan monimutkaisuus ja sen kriittinen merkitys yleiselle turvallisuudelle korostavat kyberturvallisuuden jatkuvan kehittämisen tarvetta. Isot datamäärät ovat uusi ilmiö, eikä niihin liittyvät lait ja säännökset ole vielä täysin vakiintuneet, erityisesti ilmailualalla (Dou, 2020, s.2). Pelkkä lainsäädäntö ja kansainväliset standardit eivät enää riitä, vaan lisäksi tarvitaan aktiivista seurantaa ja jatkuvaa päivittämistä, jotta pystytään vastaamaan muuttuviin uhkiin ja ongelmiin.

Kansainvälisyys asettaa omat haasteensa ilmailualan turvallisuudelle. Doun (2020, s.10) mukaan turvallisuuden parantamiseksi tarvitaan globaali ilmailun suurten tietomäärien alusta ja tietojärjestelmä, joka auttaa valvomaan kaikkia lentoja. Tehokas yhteistyö ja tiedonvaihto eri maiden ja organisaatioiden välillä ovat välttämättömiä lentoturvallisuuden takaamiseksi. Tämä saattaa edellyttää globaalien tietojärjestelmien ja tiedonvaihtomekanismien kehittämistä sekä yhteisten standardien ja protokollien noudattamista kaikkien osapuolten kesken. Toimijoiden sitoutuminen kyberturvallisuuteen toiminnassaan voi sisältää esimerkiksi koulutusta, tietoisuuden lisäämistä ja resurssien kohdentamista tietoturvatoimiin.

Hallintajärjestelmien avulla pyritään luomaan turvallisuuskulttuuri organisaatioon ja varmistamaan turvallisuuden tehokkuus sen toiminnassa (Khatun

ym., 2023, s.3). Carcary ym., (2019) kertovat, että organisaatioiden on päivitettävä kyberturvallisuuden hallintalähestymistapojaan vanhojen menetelmien riittämättömyyden vuoksi. Heidän mukaansa tarvitaan kokonaisvaltaisempia ja ennakoivampia lähestymistapoja, jotka joustavasti torjuvat uusia uhkia ja minimoivat haitalliset vaikutukset. Samalla on tärkeää arvioida, kuinka tehokkaasti nykyiset kyberturvallisuustoimenpiteet vastaavat muuttuviin olosuhteisiin (Carcary ym., 2019, s.78). Näin ollen voidaan päätellä, että lentoyhtiöiden on investoitava kyberturvallisuuteen strategisena prioriteettina. Tämä vaatii paitsi teknologisten järjestelmien päivittämistä myös henkilöstön koulutusta ja organisaation kyberturvallisuuskulttuurin vahvistamista.

4.2 Valvonnan käytännöt ja prosessit lentoliikenteen alalla

Lentoliikenteen kyberturvallisuuden kontekstissa on oleellista ymmärtää kansainvälisten säädösten ja prosessien merkitys. Nämä standardit luovat puitteet lentoyhtiöiden kyberturvallisuuden hallinnalle, varmistaen yhtenäiset käytännöt ja turvallisuuden toteutumisen.

4.2.1 Kansainväliset säädökset

Euroopan parlamentti on sitoutunut edistämään lentoliikenteen turvallisuutta kyberturvallisuuden näkökulmasta tukemalla eurooppalaisen ilmatilan yhtenäistämistä ja vahvan eurooppalaisen turvajärjestelmän kehittämistä (Euroopan parlamentti, 2022a). Lisäksi parlamentti korostaa tarvetta sopeutua alan kehityssuuntauksiin, kuten ilmailun kasvuun ja teknologian monimutkaistumiseen. Tämä kannustaa komissiota ja neuvostoa varmistamaan riittävät resurssit ja henkilöstön Euroopan lentoturvallisuusviraston (EASA) turvallisuusnormien täyttämiseksi (Euroopan parlamentti, 2022a).

EASA:n eli Euroopan turvallisuusviraston tehtävänä on edistää lentoliikenteen turvallisuutta. Tähän sisältyy sääntelyä, sertifioinnin yhdenmukaistamista, EU:n ilmailualan sisämarkkinoiden kehittämistä ja ilmailutoiminnan teknisten sääntöjen laatimista (Euroopan unioni, 2024). Virasto vastaa myös ilmaalusten ja niiden komponenttien tyyppihyväksynnästä; ilmailutuotteita suunnittelevien, valmistavien ja huoltavien yritysten hyväksynnästä; sekä ilmailun turvallisuusvalvonnasta ja turvallisuuteen liittyvän tuen tarjoamisesta EU-maille. Näiden lisäksi EASA edistää turvallisuusstandardeja ja tekee yhteistyötä kansainvälisten sidosryhmien kanssa turvallisuuden parantamiseksi Euroopassa. Myös EU:ssa kiellettyjen lentoyhtiöiden sisältävän mustan listan ylläpitäminen kuuluu EASA:n tehtäviin yhdessä sidosryhmien kanssa.

Euroopan parlamentti säätää lentoliikennettä kyberturvallisuuden näkökulmasta myös huolehtimalla ilmailun turvaamisesta, pyrkien estämään lentokoneisiin kohdistuvat vahingonteot ja laittomat teot (Euroopan parlamentti, 2022b). Se ottaa aktiivisesti huomioon terrori-iskujen jälkeiset turvallisuushaasteet ja päivittää säännöksiä vastaamaan uusia riskejä. EU:n säädöskehys kattaa

koko lentoliikenneketjun ja soveltuu kaikkiin unionin siviili-ilmailukäytössä oleviin lentoasemiin ja niiden palveluntarjoajiin sekä lentoliikenteen harjoittajiin. Jäsenvaltiot laativat lisäksi kansalliset siviili-ilmailun turvaohjelmat, jotka täydentävät EU:n toimenpiteitä (Euroopan parlamentti, 2022b). Euroopan parlamentti (2022b) korostaa tarvetta tehokkaaseen turvajärjestelmään samalla varmistaen kansalaisten perusoikeuksien, kuten yksityisyyden ja ihmisarvon, suojan.

Euroopan yleinen tietosuoja-asetus (GDPR) puolestaan asettaa yrityksille ja organisaatioille tarkkoja vaatimuksia, jotka liittyvät henkilötietojen keräämiseen, säilytykseen ja hallintaan (Euroopan unioni, 2024). Lisäksi Euroopan unionin NIS2-lainsäädäntö täydentää GDPR:ää korostaen erityisesti kyberturvallisuuden merkitystä lentoliikenteen alalla. NIS2-lainsäädäntö edistää lentoliikenteen turvallisuutta tukemalla myös eurooppalaisen ilmatilan yhtenäistämistä ja kehittämällä vahvaa eurooppalaista turvajärjestelmää (Euroopan unioni, 2022). NIS2:n keskeinen tavoite on varmistaa lentoliikenteen verkko- ja tietojärjestelmien turvallisuus, mikä on olennaista lentoturvallisuuden vahvistamiseksi nykyaikaisessa digitaalisessa ympäristössä (Euroopan unioni, 2022). Nämä säännökset koskevat sekä eurooppalaisia organisaatioita, jotka käsittelevät EU:ssa henkilötietoja että EU:n ulkopuolisia organisaatioita, joiden henkilötietojen käsittely kohdistuu EU:ssa asuviin henkilöihin (Euroopan unioni, 2022, 2024).

Merkittävänä tekijänä toimii myös Kansainvälinen ilmakuljetusliitto eli International Air Transport Association (IATA), joka on lentoyhtiöitä edustava maailmanlaajuinen lentoliikenteen alan ammattijärjestö. Sen tehtävänä on edistää lentoliikenteen turvallisuutta, luotettavuutta ja tehokkuutta sekä helpottaa kansainvälistä ilmakuljetusalan yhteistyötä. Tämä tapahtuu muun muassa standardien ja käytäntöjen kehittämisen, koulutuksen ja asiantuntijapalveluiden tarjoamisen kautta (IATA, 2024). IATA toimii myös lentoyhtiöiden edunvalvojana alan kansainvälisissä foorumeissa ja vastaa lentoliikenteen lippuvarausjärjestelmästä sekä antaa suosituksia lentolippujen hinnoittelusta ja muista toimialaan liittyvistä asioista (IATA, 2024). Tämä korostaa IATA:n merkitystä ilmailualalla, sillä sen tarjoamat standardit ja suositukset ovat keskeisessä asemassa lentoliikenteen toiminnan tehokkuuden ja turvallisuuden varmistamisessa.

4.2.2 Kansainväliset standardit

Kansainväliset standardit ovat toinen olennainen osa nykyaikaista tietoturvaa ja tietojärjestelmien hallintaa. Näiden avulla organisaatiot voivat luoda ja ylläpitää tehokkaita tietoturvakäytäntöjä, joiden avulla suojataan niiden tietoja ja tietojärjestelmiä. Kaksi merkittävää kansainvälistä standardia ovat National Institute of Standards and Technology (NIST) -tietoturvastandardi ja ISO27001-standardi. Ne tarjoavat kattavia kehyksiä ja suosituksia tietoturvan hallintaan sekä parhaiden käytäntöjen toteuttamiseen organisaatioissa.

National Institute of Standards and Technology -standardi (NIST) on vakiinnuttanut asemansa keskeisenä tietoturvan ja tietotekniikan hallinnan välineenä sekä Yhdysvalloissa että maailmalla. Stastnyn ja Stoican (2022) mukaan siinä esitetään nykyiset teollisuuden parhaat käytännöt kyberturvallisuuden alalla. Tämä auttaa heidän mukaansa organisaatioita täyttämään Kansainvälisen

siviili-ilmailujärjestön (ICAO) asettamat tietoturvavaatimukset, kuten Annex 17:sta määritellyt korkean tason turvallisuusstandardit lentoliikenteelle (Stastny & Stoica, 2022, s.3).

Toinen merkittävä kansainvälinen standardi, ISO27001, puolestaan asettaa vaatimukset ja antaa ohjeet organisaatioiden tietoturvajärjestelmille. Parra, Crespo, Alvarez, Huerta ja Paton (2016, s.2898) kertovat, että sen avulla organisaatiot voivat kehittää, toteuttaa, ylläpitää ja jatkuvasti parantaa tietoturvaansa. Standardi käsittelee myös erilaisia osa-alueita, kuten tietojen suojausta, riskien hallintaa, tietoturvan valvontaa ja jatkuvuuden hallintaa (Parra ym., 2016, s.2898). Sen tarkoituksena on varmistaa tietojen luottamuksellisuus, eheys ja saatavuus kaikissa organisaatioissa, koosta riippumatta.

5 TIETOTURVAVIESTINTÄ LENTOYHTIÖIDEN VERKKOSIVUILLA

Tässä luvussa syvennytään tarkastelemaan ulkopuolisille tekijöille näkyvillä olevaa lentoyhtiöiden kyberturvallisuusviestintää empiirisen tutkimuksen kautta. Merkittävänä tietona tämä osio tarjoaa kuvan siitä, kuinka nämä organisaatiot suhtautuvat tietoturvaan ja millaisia painotuseroja materiaalien välillä on. Lisäksi keskitytään siihen, kuinka lentoyhtiöt viestivät asiakkailleen ja sidosryhmilleen tietoturvaan liittyvistä riskeistä ja toimenpiteistä.

5.1 Empiirisen tutkimuksen toteuttaminen

Tutkimuksessa analysoitiin lentoyhtiöiden verkkosivujen markkinointisisältöjä. Tavoitteena oli syventää käsitystä siitä, miten ne kommunikoivat turvallisuudesta asiakkailleen, ja mitä näkökulmia lentoyhtiöt haluavat tuoda erityisesti esille. Aiheen tutkiminen on olennaista, sillä lentoyhtiöt ovat yhä riippuvaisempia digitaalisista kanavista asiakaskommunikaatiossaan, ja tietoturva on keskeinen huolenaihe kyseisellä alalla.

Tätä tutkimusta varten vertailtiin kuutta eri kaupallista lentoyhtiötä ympäri maailmaa, jotta saatiin mahdollisimman kattava käsitys kyberturvallisuuden merkityksestä ja asiakasviestinnän painopisteistä. Syvälliseen tarkasteluun valitut lentoyhtiöt olivat suomalainen Finnair, irlantilainen Ryanair, saksalainen Lufthansa, yhdysvaltalainen American Airlines, Singaporen kansallisen lentoyhtiö Singapore Airlinesin sekä Yhdistyneiden arabiemiirikuntien The Emirates Group. Kuten aikaisemmin mainittiin, juuri nämä kyseiset lentoyhtiöt valittiin, jotta tutkimuksesta ja sen tuloksista saatiin mahdollisimman kattavat. Kyseiset lentoyhtiöt edustavat eri tasoluokkia, mikä näkyy muun muassa palvelun tasossa, hintaluokassa, kohdemarkkinassa ja brändi-imagossa. Kaikki lentoyhtiöt ovat kuitenkin maailmalaajuisesti tunnettuja ja edustavat myös eri kulttuureja sekä maanosia. Vertailu näiden erilaisten lentoyhtiöiden välillä auttaa

hahmottamaan, miten kyberturvallisuuden näkökulma vaihtelee, ja miten se voi olla sidoksissa lentoyhtiön asemaan ja strategiaan.

Empiiristä tutkimusta lähdettiin suorittamaan keräämällä lentoyhtiöiden verkkosivuilta kyberturvallisuutta koskevia tietoja, kuten erilaisia käytäntöjä, toimenpiteitä, sertifikaatteja ja muita turvallisuuteen liittyviä asioita. Tämän jälkeen hyödynnettiin sisällönanalyysia kerätyn materiaalin tarkasteluun ja vertailemiseen. Kyseistä dataa kerättiin pääsääntöisesti verkkosivujen osioista ja artikkeleista, joissa käsiteltiin turvallisuutta. Lopulta näiden pohjalta muodostettiin painopisteiden eroavaisuuksia ja toimenpiteiden samankaltaisuuksia kokoavat näkemykset.

On oleellista muistaa, että tutkimuksessa käsitellään vain verkkosivuilla mainittuja asioita, sillä monet kyberturvallisuuteen vaikuttavat toimenpiteet ovat salattuja. Tämä toimii siten tutkimusta rajoittavana tekijänä. Tarkastelun kohteena oli siis eri lentoyhtiöiden julkisen materiaalin kyberturvallisuuden painotukset ja näkökulmat. Toisena rajoittavana tekijänä oli se, että käytetyt lähteet ja aineistot painottavat enimmäkseen suurten kansainvälisten lentoyhtiöiden näkökulmaa, jolloin pienempien ja alueellisten toimijoiden haasteet sekä erityispiirteet jäävät vähemmälle huomiolle. Lisäksi tutkimus keskittyy pääasiassa länsimaisiin standardeihin ja säädöksiin, kuten ISO27001:een ja GDPR:ään, jolloin muiden alueiden, kuten esimerkiksi Aasian ja Afrikan, sääntelykehyksiä ja käytäntöjä ei suoranaisesti käsitellä.

5.2 Verkkosivujen analyysi

Lentoyhtiöiden verkkosivut toimivat keskeisenä kanavana tiedonvälityksessä asiakkaille, palveluiden markkinoinnissa sekä käytännön ohjeiden tarjoamisessa. Eri lentoyhtiöiden verkkosivuja tarkastelemalla huomattiin nopeasti, että kyberturvallisuusviestinnän painotuksissa ja lähestymistavoissa on vaihtelevuutta. Analyysi suoritettiin syventymällä kerättyyn materiaaliin ja muodostamalla siitä vertailukelpoista. Tämän avulla tutkittiin lentoyhtiöiden eroavaisuuksia ja samankaltaisuuksia.

Muista lentoyhtiöistä poiketen Lufthansan kyberturvallisuusmateriaalia etsiessä huomattiin, että tietoa löytyy Lufthansa Cargon ja Lufthansa Industry Solutionsin puolelta. Verkkosivujen vertailua varten näitä molempia tarkasteltiin erikseen. Vaikka molemmat ovat osa Lufthansa-konsernia, saattaa niillä olla omia kyberturvallisuuteen liittyviä käytäntöjä ja prosesseja. Kun konsernia tarkastellaan kokonaisuutena, voidaan olettaa, että sen kaikilla liiketoimintayksiköillä on runsaasti yhteisiä piirteitä kyberturvallisuuden näkökulmasta. Tämä pitää sisällään myös kaupallisen lentoliikenteen. Ilman kaikkien liiketoimintayksiköiden tarkkaa tarkastelua ei voida varmasti sanoa, kuinka paljon tiettyjä käytäntöjä sovelletaan juuri kaupalliseen lentoyhtiöön. Lufthansa Crago kuitenkin ilmaisee kokonaisvaltaisen politiikkajärjestelmän, joka noudattaa Lufthansa-konsernin tietoturvapolitiikkaa, ja se korostaa olevansa olennainen osa Lufthansan tietoturvaorganisaatiota.

Seuraavaan taulukkoon on koottu havaintoja lentoyhtiöiden painotusten ja lähestymistapojen välisistä eroista, joiden avulla on mahdollista hahmottaa, mitä aihealueita ne korostavat materiaalissaan.

Taulukko 2 Eroavaisuudet

Lentoyhtiö	**Eroavaisuudet kyberturvallisuuden lähestymistavassa**
Finnair	- Keskeiset riskit on kategorisoitu ja niille on määritelty toimenpiteitä - Pääpaino maineen ja liiketoiminnan vaikutuksissa
Ryanair	- Viittaa NIST-kehykseen ja suorittaa säännöllisiä ulkoisia tarkastuksia - Painottaa vuosittaista kyberturvallisuuskoulutusta ja penetraatiotestejä
Lufthansa (Cargo)	- Noudattaa ISO27001-standardia ja käyttää ulkoisia tarkastuksia - Painottaa ilman tietotekniikkaa asiakaslupauksen täyttämistä - Toimii osana Lufthansa-konsernia - Mainitsee BitSight-luokituksen: Bitsight Security Rating on tehokas työkalu, jota tietoturva- ja riskijohtajat käyttävät arvioidakseen, seuratakseen, priorisoidakseen ja viestiäkseen kyberriskit. Se tarjoaa objektiivisen, dataan perustuvan näkökulman organisaation tietoturvaohjelman tilaan (Bitsight (2024).
Lufthansa Industry Solutions	- Korostaa työntekijöiden huolimattomuuden ja tiedonpuutteen roolia kyberrikollisuuden torjunnassa - Keskittyy NIS2-lainsäädännön toteuttamiseen - Mainitsee kyberuhkien lisääntyvän uhan ja varautumisen tarpeen - Tarjoaa räätälöityjä tietoturvapalveluita ja järjestää hätätilanneharjoituksia
American Airline	- NIST-kehyksen käyttö ja ulkoisten tietoturva-asiantuntijoiden arvioinnit - Omistautunut tietoturva-tiimi ja tietoturvaohjelma - Painottaa tietoturvakoulutusta ja sisäisiä auditointeja
Singapore Airlines	- Painotuksena asiakkaiden varoittaminen huijausyrityksistä ja henkilötietojen suojaaminen - Tarjoaa ohjeita kalasteluviestejä ja -tekstiviestejä vastaan - Rekisteröity lähettäjätunnus ja yhteistyö Kyberturvallisuusviraston kanssa
The Emirates Group	- Asiakkaiden tietojen turvallisuus ensisijaisena - Ympäristön turvallisuus varmistaa tietojen turvallisuuden - Korostaa turvallista pääsyä tietoihin ja riskienarviointia - Kansainvälisten standardien noudattaminen

Lentoyhtiöiden markkinointimateriaalien panopisteiden välillä oli huomattavia eroavaisuuksia. Etenkin Singapore Airlinesin materiaalin painopiste eroaa merkittävästi muista. Se keskittyi asiakkaiden varoittamiseen ja opastamiseen kyberuhkien suhteen, kun taas esimerkiksi Finnair keskittyi lisäämään tietoisuutta yksittäisistä kohtaamistaan uhista ja tarvittavista toimenpiteistä. American Airlines puolestaan korosti riskienhallintaa ja reagointikykyään, ja Ryanair taas mainitsi kolmansien osapuolien suorittamat tarkastukset ja arvioinnit. The Emirates Group keskittyi sisäiseen riskinarviointiin, Lufthansa työntekijöiden rooliin kyberrikollisuuden torjunnassa ja Lufthansa Cargo asiakkaidensa tietojen suojaamiseen.

Myös kyberturvallisuustoimenpiteiden kuvailun tarkkuudessa ja yksityiskohtaisuudessa oli merkittäviä eroja. Esimerkiksi Ryanair ja American Airlines kertoivat noudattavansa NIST-kehystä, Lufthansa Cargo puolestaan ISO27001-standardia sekä Lufthansa Industry Solutions NIS2-lainsäädäntöä. Muut lentoyhtiöt eivät tuoneet yhtä tarkasti esille, millaisia säädöksiä ne noudattavat, vaikka oletettavasti kaikki ovat myös samojen vaatimusten alaisia. Myös henkilöstön koulutusta ja tietoisuutta painotettiin eri tavoin. Esimerkiksi Ryanair mainitsi vuosittaisen kyberturvallisuuskoulutuksen kaikille työntekijöilleen, kun taas American Airlines mainitsi neljännesvuosittaiset tiedotteet ja tiimikohtaiset koulutusohjelmat.

Lentoyhtiöiden välillä oli havaittavissa myös paljon yhteistä. Tässä taulukossa tarkastellaan puolestaan lentoyhtiöiden samankaltaisuuksia tietoturvatoimenpiteiden kautta. Siihen on merkattu toimenpiteitä ja lentoyhtiöt, jotka ovat maininneet ne omilla sivuillaan.

Taulukko 3 Samankaltaisuudet

Toimenpiteet	**Lentoyhtiöt**
Säännölliset riskiarvioinnit	Finnair, Ryanair
Tietoturvavalvonta	Finnair, Ryanair, American Airlines, Lufthansa Cargo
Omistavat tai ylläpitävät omistautuneita tietoturvatyöryhmiä	Ryanair, American Airlines
Henkilöstön jatkuva kouluttaminen tietoturvaan liittyen	Finnair, Ryanair, American Airlines, Singapore Airlines
Tietosuojaan liittyvät ohjeet ja suositukset	Finnair, Ryanair, Singapore Airlines, Lufthansa Cargo
Kyberturvallisuuskoulutus ja -tietoisuus	Finnair, Ryanair, American Airlines, Singapore Airlines
Tietosuojan ja tietoturvan valvonta ja seuranta	Finnair, Ryanair, American Airlines, Singapore Airlines, The Emirates Group
Henkilötietojen suojaamiseen liittyvät toimenpiteet	Finnair, Ryanair, American Airlines, Singapore Airlines, The Emirates Group, Lufthansa Cargo
Ulkoiset tietoturvaa koskevat tarkastukset	Finnair, Ryanair, American Airlines, Singapore Airlines, The Emirates Group, Lufthansa Cargo
Kyberturvallisuusstrategian säännöllinen arviointi	Ryanair, American Airlines
Sopimusvelvoitteet tietoturvan suhteen	Finnair, Ryanair, American Airlines, The Emirates Group
Tietosuojalainsäädännön noudattaminen	Finnair, Ryanair, American Airlines, The Emirates Group
Tietojärjestelmien säännölliset päivitykset ja testaukset	Finnair, Ryanair, American Airlines, Singapore Airlines, The Emirates Group
Jatkuva riskienhallinta ja valmiussuunnittelu	Finnair, Ryanair, American Airlines, The Emirates Group, Lufthansa Industry Solutions

Kaikkien tarkasteltujen lentoyhtiöiden sivuilla nousi yhteisiä teemoja sekä toimenpiteitä, joiden avulla ne pyrkivät varmistamaan kybertuvallisuuttaan. On siis selvää, että kaikki lentoyhtiöt pitävät kyberturvallisuutta tärkeänä. Tämä korostaa lentoyhtiöiden yhteistä pyrkimystä turvata matkustajien ja henkilöstön tietoturvallisuus sekä liiketoiminnan jatkuvuus kyberuhkien kasvaessa. Monet lentoyhtiöt kuten Finnair, Ryanair, American Airlines ja Lufthansa Cargo harjoittivat aktiivista tietoturvavalvontaa, mikä näkyi esimerkiksi Finnairilla riskienhallintatoimissa ja valmiussuunnittelussa sekä American Airlinesillä muun muassa tietoturva-aukioiden hallintotason valvonnassa.

Samankaltaisuuksia tarkasteltaessa nousi esiin myös säännöllisten tarkastuksien ja testauksien merkitys, jotka ovat olennainen osa tietoturvatoimenpiteitä. Kuten Samankaltaisuudet -taulukosta (taulukko 2) huomataan, lentoyhtiöt korostavat erityisesti myös henkilöstönsä kouluttamista ja haluansa lisätä tietoisuutta kyberuhista ja -käytännöistä. Nämä näkyvät kohdista Henkilöstön jatkuva kouluttaminen tietoturvaan liittyen sekä Tietosuojaan liittyvät ohjeet ja suositukset. Molemmissa kohdissa huomataan Finnair, Ryanair, Singapore Airlines.

Tietoisuuden lisäämisestä huomataan, että useat lentoyhtiöt ovat huolissaan etenkin matkustajiensa henkilötiedoista. Esimerkiksi Singapore Airlinesin verkkosivujen materiaali keskittyi pääsääntöisesti verkkosivujensa kyberturvallisuusosiossa tiedottamaan matkustajia mahdollisista kyberturvallisuusuhista, joita he voivat kohdata. Tällaisia olivat esimerkiksi kalasteluviestit, väärennetyt puhelinnumerot sekä esiintyminen lentoyhtiön työntekijöinä. Näillä huijarit tavoittelevat yleensä asiakkaiden henkilökohtaisia tietoja. Etenkin varoitetaan Singapore Airlinesin työntekijöinä esiintyvistä sähköposti- ja tekstiviesteistä sekä sosiaalisen median tileistä ja puheluista. Heidän sivuillaan korostui vahvasti matkustajien ohjeistaminen erilaisissa tilanteissa, joissa kyberturvallisuuden riski on olemassa. Myös Finnair käy tarkasti sivuillaan läpi, kuinka se käsittelee henkilötietoja sekä mihin tarkoituksiin ja mille tahoille niitä mahdollisesti jaetaan.

5.3 Tulosten tarkastelu

Analyysissä lentoyhtiöiden verkkosivujen kyberturvallisuusmateriaalia tutkittiin havaittujen eroavaisuuksien ja samankaltaisuuksien näkökulmasta. Tutkimuksessa keskityttiin erityisesti lentoyhtiöiden painotuksiin ja lähestymistapoihin kyberturvallisuuden viestinnässä. Lufthansan tapauksessa huomattiin, että kyberturvallisuusmateriaalia löytyi sekä Lufthansa Cargon että Lufthansa Industry Solutionsin osalta, mikä viittaa osittain erillisiin käytäntöihin ja prosesseihin.

Lentoyhtiöiden välillä havaittiin merkittäviä eroja painotuksissa. Esimerkiksi Singapore Airlines painotti asiakkaiden varoittamista ja neuvomista kyberuhkien osalta, kun taas Finnair keskittyi lisäämään tietoisuutta yksittäisistä uhkista ja tarvittavista toimenpiteistä. American Airlines puolestaan korosti riskienhallintaa ja reagointikykyään. Merkittävänä eroavaisuutena lentoyhtiöiden

välillä oli myös informaation yksityiskohtaisuus, mikä näkyi lentoyhtiöiden noudattamissa erilaisissa standardeissa ja säädöksissä, kuten NIST-kehys tai ISO27001-standardi. Yhteisiä teemoja lentoyhtiöiden kyberturvallisuustoimenpiteissä ovat muun muassa säännölliset tarkastukset ja testaukset sekä henkilöstön kouluttaminen ja tietoisuuden lisääminen kyberuhkista. Tietoisuuden lisäämisessä lentoyhtiöt ovat erityisen huolissaan matkustajiensa henkilötiedoista ja pyrkivät ohjeistamaan asiakkaitaan erilaisissa tilanteissa, joissa kyberturvallisuuden riski on olemassa.

Eroavaisuuksien ja samankaltaisuuksien pohjalta huomataan, että lentoyhtiöt sovittavat viestintäänsä omiin tarpeisiinsa. Samankaltaisuuksista voidaan päätellä, että lentoyhtiöt ymmärtävät kyberturvallisuuden tärkeyden ja ovat omaksuneet monipuolisia toimenpiteitä tietoturvan varmistamiseksi sekä sisäisessä että ulkoisessa toiminnassaan. Nämä toimenpiteet ulottuvat sisäisistä riskiarvioinneista ja valvonnasta aina henkilöstön koulutukseen ja ulkoisiin tarkastuksiin asti. Tällainen kokonaisvaltainen lähestymistapa kyberturvallisuuteen on välttämätöntä nykypäivän digitalisoituneessa liiketoimintaympäristössä, erityisesti sellaisella alalla kuin lentoliikenne, jossa tietoturvan merkitys on korostunut entisestään.

5.4 Johtopäätökset

Kyberturvallisuuden erityispiirteiden ja hallinnan sekä lentoyhtiöiden markkinointimateriaalien välillä on syvällinen ja monipuolinen vuorovaikutus lentoliikenteen kontekstissa. Lentoyhtiöiden markkinointimateriaalit eivät ainoastaan pyri houkuttelemaan asiakkaita, vaan ne tarjoavat myös väylän viestiä yrityksen arvoista, käytännöistä ja sitoutumisesta kyberturvallisuuteen.

Lentoyhtiöiden markkinointimateriaaleissa heijastuu kyberturvallisuuden erityispiirteiden ja hallinnan merkitys. Lentoyhtiöt voivat käyttää markkinointiviestintäänsä välineenä viestiä sitoutumisestaan kyberturvallisuuteen ja asiakkaiden tietoturvaan. Tämä puolestaan sisältää tietoa käytetyistä teknologioista, turvallisuusstandardeista ja -protokollista sekä yrityksen kyberuhkien torjuntatoimenpiteistä. Markkinointimateriaalit luovat luottamusta lentoyhtiöön ja vahvistavat sen mainetta turvallisena ja luotettavana toimijana. Niiden avulla myös jaetaan tietoa lentoyhtiöiden sitoutumisesta kyberturvallisuuteen ja tarjotaan yleistä informaatiota käytetyistä teknologioista ja menetelmistä. Kyseinen materiaali ei kuitenkaan välttämättä tarjoa yksityiskohtaista tietoa kaikista kyberturvallisuuden erityispiirteistä ja hallintatoimenpiteistä.

Lentoyhtiöt eivät maininneet markkinointimateriaaleissaan kyberturvallisuuden erityispiirteitä, kuten GPS-häirintää, langattomia verkkopalveluita, verkkoturvallisuusinfrastruktuuria tai kommunikaatioprotokollia. Ne ovat olennainen osa lentoliikenteen digitaalista kokonaisuutta, minkä takia niiden tuominen esille markkinoinnissa saattaa olla kannattavaa. Lentoyhtiöt käyttävät näitä teknologioita monissa prosesseissaan, kuten lentoliikenteen hallinnassa, asiakaspalvelussa ja liiketoiminnan tukitoiminnoissa. Kyseisten teknologioiden

käyttöönotto luo myös uusia haavoittuvuuskohtia ja riskejä, jotka vaativat asianmukaista hallintaa ja suojatoimenpiteitä. Lisäksi markkinointimateriaaleissa voitaisiin kertoa, kuinka lentoyhtiöt käyttävät kyseisiä teknologioita monissa prosesseissaan, kuten esimerkiksi asiakaspalvelussa ja liiketoiminnan tukitoiminnoissa, mikä entisestään vakuuttaa asiakkaat yhtiön sitoutumisesta turvallisuuteen.

Kyberturvallisuuden hallinta on keskeisessä roolissa lentoyhtiöiden liiketoiminnan jatkuvuuden ja turvallisuuden varmistamisessa. Lentoyhtiöt kohtaavat jatkuvasti monimutkaisia kyberuhkia, jotka voivat vaikuttaa suoraan niiden toimintaan, tietojärjestelmiin ja asiakkaiden turvallisuuteen. Tämän vuoksi on kehitettävä laajoja kyberturvallisuusstrategioita ja investoitava huomattavasti kyberuhkien torjuntaan. Näihin strategioihin sisältyy riskien tunnistaminen, reagointi, valvonta ja ennaltaehkäisy, jotka ovat olennaisia liiketoiminnan suojaamiseksi. Sitoutunut kyberturvallisuuden toiminta organisaatiossa pitää sisällään muun muassa koulutusta ja tietoisuuden lisäämistä, mikä havaittiin myös lentoyhtiöiden markkinointimateriaaleja tarkasteltaessa.

Kyberturvallisuuden hallinnassa markkinointiviestinnän avulla lentoyhtiöt voivat korostaa strategioidensa kattavuutta ja investointejaan turvallisuusteknologioihin. Tämä vahvistaa asiakkaiden luottamusta yhtiön toimintakykyyn ja turvallisuuteen, luoden samalla lisää arvoa. Lisäksi markkinointimateriaalit voivat havainnollistaa, kuinka yhtiö tunnistaa, reagoi ja ennaltaehkäisee riskejä, ja siten ylläpitää liiketoiminnan jatkuvuutta.

Kyberturvallisuuden hallintaan liittyy myös kansainvälisten standardien ja sääntelykehyksien noudattaminen. Lentoyhtiöt joutuvat noudattamaan tiukkoja standardeja ja määräyksiä, kuten NIST-kehystä, ISO27001-standardia ja GDPR:ää. Kyseisten standardien noudattaminen on keskeisessä asemassa lentoyhtiöiden kyberturvallisuusstrategiaa ja viestii samalla sitoutumisesta parhaisiin käytäntöihin ja luotettavaan liiketoimintaan. Markkinointiviestinnän avulla on mahdollista tuoda esille kansainvälisiin standardeihin ja sääntelykehyksiin sitoutuminen, mikä näkyi myös empiirisessä tutkimuksessa. Lisäksi markkinointiviestinnällä voidaan selittää, miten näiden standardien mukaiset käytännöt integroituvat yhtiön päivittäisiin operaatioihin ja kyberturvallisuusstrategiaan. Tämä kuitenkin jäi tutkimuksen lentoyhtiöiltä puuttumaan.

Kokonaisuutena kyberturvallisuuden erityispiirteet ja hallinta vaikuttavat merkittävällä tavalla lentoyhtiöiden toimintaan ja markkinointiviestintään. Lentoyhtiöiden kyberturvallisuuspyrkimykset ovat osa laajempaa sitoutumista matkustajien ja henkilöstön turvallisuuteen sekä liiketoiminnan jatkuvuuteen, mikä korostaa kyberuhkien torjunnan merkitystä lentoliikenteessä. Samalla ne voivat hyödyntää markkinointiviestintäänsä luottamuksen rakentamiseen asiakkaidensa keskuudessa.

6 YHTEENVETO

Lentoliikenteen kyberturvallisuuden merkitys on kasvanut entistä keskeisemmäksi lentoyhtiöiden ja kaikkien lentoliikenteen toimijoiden kannalta. Kyberturvallisuuteen panostaminen on tärkeää, koska ala toimii monimutkaisessa ja vaativassa ympäristössä, joka vaikuttaa suoraan miljoonien matkustajien turvallisuuteen sekä liiketoiminnan jatkuvuuteen. Kyberhyökkäysten aiheuttamat uhat, kuten tietojen vuotaminen, salakuuntelu, GPS-häirintä ja hajautettu palvelunesto, voivat aiheuttaa todellisia haittoja ja vaaratilanteita.

Kyberhyökkäyksistä aiheutuvat mahdolliset taloudelliset vahingot vaikuttavat merkittävästi lentoyhtiöiden ja koko lentoliikenteen alaan. Lentotoiminnan häiriöiden, kuten lentokoneiden myöhästymisen ja lentojen peruuntumisen, seurauksena liiketoiminnan tulokset voivat heikentyä. Näiden lisäksi lentoyhtiöiden on huomioitava myös asiakkaidensa luottamus, sillä kyberhyökkäykset saattavat vaikuttaa negatiivisesti niiden maineeseen ja luottamukseen. Tämä puolestaan johtaa asiakkaiden menetykseen ja liiketoiminnan vähenemiseen.

Tässä tutkielmassa käsiteltiin kyberturvallisuuden merkitystä lentoliikenteeseen erityisesti alan erityispiirteiden, lentoyhtiöiden toiminnan sekä asiakasviestinnän kautta. Tutkielma koostui systemaattisesta kirjallisuuskatsauksesta ja empiirisestä tutkimuksesta, jotka tarjosivat laajan ja monipuolisen katsauksen lentoliikenteen kyberturvallisuuden nykytilanteeseen ja haasteisiin.

Tutkielmassa todettiin, että merkittäviä lentoliikenteen erityispiirteitä olivat muun muassa GPS-häirintä, langattomien verkkopalveluiden vaikutus, verkkoturvallisuusinfrastruktuuri ja kommunikaatioprotokollat, sillä niillä on olennainen rooli alan turvallisuuden kannalta. Näissä erityispiirteissä korostuivat mahdolliset riskit sekä ongelmakohdat, joihin kuului esimerkiksi langattomien verkkopalveluiden kehitys. Tämän kehityksen myötä lentokoneet eivät enää toimi suljettuina järjestelminä, mikä lisää kyberuhkien ja -riskien todennäköisyyttä. Näin ollen voitiin todeta, että tehokkaiden turvallisuustoimenpiteiden kehittäminen IT-infrastruktuurissa sekä lentokoneiden järjestelmissä on erityisen tärkeää.

Merkittävässä roolissa olivat myös lentoyhtiöiden kyberturvallisuuden hallinta sekä noudatettavat kansainväliset säädökset, sillä ne vaikuttavat suoraan

lentoyhtiöiden kykyyn suojata tietojaan ja palveluitaan kyberuhilta. Näitä tarkastelemalla havaittiin, että organisaatioiden kyberturvallisuuden hallintatavat vaihtelevat. Tämä puolestaan korostaa oikean tasapainon löytämisen tärkeyttä, mikä mahdollistaa IT-resurssien suojaamisen ja samalla liiketoiminnan tehokkaan toiminnan.

Kyberturvallisuuden hallinnan ongelmakohtia, kuten kansainvälisyyttä ja suurta datamäärää, tulisi ratkaista aktiivisella uhkien ja haasteiden seurannalla sekä jatkuvalla kyberturvallisuuden hallinnan päivittämisellä. Pelkkä lainsäädäntö ja kansainväliset standardit eivät enää yksin riitä näiden haasteiden ratkaisemiseen. Myös tehokas yhteistyö ja tiedonvaihto eri maiden sekä organisaatioiden välillä todettiin välttämättömäksi lentoturvallisuuden takaamisen kannalta. Merkittäviä esiteltyjä kansainvälisiä tekijöitä olivat esimerkiksi Euroopan unioni ja parlamentti sekä Kansainvälinen ilmakuljetusliitto, koska ne asettavat koko ilmailualaa koskettavia säädöksiä. Näiden säädösten tavoitteena on parantaa turvallisuutta maailmanlaajuisesti.

Tutkimuksessa analysoitiin lentoyhtiöiden verkkosivujen kyberturvallisuusmateriaaleja, jotka tarjoavat arvokasta tietoa alan toimijoille ja matkustajille ajankohtaisista kysymyksistä ja käytännöistä. Vaikka tutkimus kattoi lentoliikenteen kyberturvallisuuden tärkeät näkökulmat, se keskittyi pääasiassa suuriin kansainvälisiin lentoyhtiöihin ja länsimaisiin sääntelykehyksiin. Pienempien toimijoiden ja muiden alueiden erityispiirteet jäivät siten vähemmälle huomiolle.

Analysoimalla lentoyhtiöiden verkkosivujen kyberturvallisuusmateriaalia, havaittiin niiden välillä merkittäviä eroja ja samankaltaisuuksia. Lentoyhtiöt korostivat erilaisia näkökulmia, kuten asiakkaiden varoittamista, uhkien tiedottamista ja riskienhallintaa. Vaikka viestintä sovitettiin kunkin lentoyhtiön tarpeisiin, yhteisinä teemoina nousivat säännölliset tarkastukset, henkilöstön koulutus ja matkustajien ohjeistaminen kyberuhkatilanteissa. Lentoyhtiöt olivat ymmärtäneet kyberturvallisuuden merkityksen ja ottaneet käyttöön monipuolisia toimenpiteitä tietoturvan varmistamiseksi. Tutkimuksen perusteella kaikki valitut lentoyhtiöt osoittivat vahvaa sitoutumista kyberturvallisuuteen ja käyttivät erilaisia strategioita sekä toimenpiteitä varmistaakseen tietojensa turvaamisen ja liiketoiminnan jatkuvuuden. Näihin monipuolisiin strategioihin kuuluivat ensinnäkin riskienhallinta sekä reagointikyvyn parantaminen, jotka sisälsivät säännölliset tarkastukset, testaukset ja henkilöstön koulutuksen. Lisäksi osa lentoyhtiöistä kertoivat noudattavansa tiukkoja kansainvälisiä standardeja sekä sääntelykehyksiä, kuten NIST-kehystä ja ISO27001-standardia. Eroavaisuuksia havaittiin kuitenkin erityisesti kyberturvallisuusviestinnän lähestymistavoissa ja painopisteissä. Tämä näkyi esimerkiksi siinä, että eräs lentoyhtiö keskittyi asiakkaiden varoittamiseen ja neuvomiseen kyberuhkien osalta, kun taas toinen lentoyhtiö painotti yksittäisten uhkien tiedostamista ja tarvittavien toimenpiteiden esille tuomista.

Jatkotutkimuksen kannalta keskeisiä aiheita voivat olla esimerkiksi lentoliikenteen kyberturvallisuuden teknologisten innovaatioiden vaikutukset, kansainvälisen yhteistyön merkitys sekä kyberhyökkäysten torjuntakeinojen kehittäminen. Vaikka tässä tutkielmassa käsiteltiin näitä näkökulmia pintapuolisesti,

niitä olisi syytä edelleen tutkia syvemmän tarkastelun ja kehityksen kautta. Esimerkiksi teknologisten innovaatioiden, kuten tekoälyn ja IoT:n roolit lentoliikenteen kyberturvallisuudessa tarjoavat runsaasti tutkimusmahdollisuuksia. Samoin kansainvälisen yhteistyön kehittäminen ja uusien kyberhyökkäysten torjuntakeinojen arviointi ovat tärkeitä jatkotutkimusalueita, jotka voivat edistää lentoliikenteen turvallisuutta entisestään.

Jatkossa myös tässä tutkielmassa suoritettua tutkimusta voitaisiin laajentaa kattamaan suurempi maantieteellinen alue sekä useammat erilaiset ilmailualan toimijat. Tämän lisäksi olisi hyödyllistä syventyä tarkemmin lentoyhtiöiden sisäisiin käytäntöihin ja prosesseihin, kuten koulutusohjelmiin ja henkilöstön tietoisuuteen kyberturvallisuusasioista. Erityisesti empiirisetä tutkimusta hyödyttäisi mahdollisesti myös laajempi otanta sekä monipuolisemmat tutkimusmenetelmät. Esimerkiksi haastattelut ja tapaustutkimukset auttaisivat syventämään ymmärrystä käytännön toimenpiteistä ja haasteista entisestään.

Kyberturvallisuus lentoliikenteessä on tärkeä ja monimutkainen aihealue, joka vaatii jatkuvaa tarkastelua ja kehitystä matkustajien sekä alan toimijoiden turvallisuuden varmistamiseksi. On oleellista, että tulevaisuudessa tutkitaan, kuinka lentoyhtiöt voivat entistä paremmin integroida kyberturvallisuusstrategiansa päivittäiseen toimintaansa ja viestiä tästä tehokkaasti myös asiakkailleen. Kyberturvallisuuden merkitys on elintärkeä lentoyhtiöille, lentokentille ja koko lentoliikenteen järjestelmälle, jotta matkustajien turvallisuus voidaan taata, liiketoiminta pysyy sujuvana ja asiakkaiden luottamus säilyy.

LÄHTEET

Ali, A. B. A., Ayyasamy, R. K., Akbar, R., Ap Ponnusamy, V., & Heng, L. E. (2022, August). Cybersecurity infrastructure adoption model for malware mitigation in small medium enterprises (SME). *2022 5th International Symposium in Robotics and Manufacturing Automation (ROMA)* (pp. 1-6). IEEE.

American Airlines. (20.2.2023). *Cybersecurity Policy Statement*. https://www.aa.com/pubcontent/en_US/customer-service/about-us/cybersecurity-policy-statement.jsp

Antikainen, M., Uusitalo, T., & Kivikytö-Reponen, P. (2018). Digitalisation as an enabler of circular economy. Procedia Cirp, 73, 45–49.

Basal, M., & Suzen, E. (2023). The importance of digital marketing in the strategic management of aviation. *E3S Web of Conferences* (Vol. 402, p. 02010). EDP Sciences.

Bala, M., & Verma, D. (2018). A critical review of digital marketing. *International Journal of Management, IT & Engineering*, 8(10), 321–339. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3545505

Bitsight. What is Bitsight security rating. Viitattu 26.5.2024. https://www.bitsight.com/security-ratings

Carcary, M., Doherty, E., & Conway, G. (2019, July). A framework for managing cybersecurity effectiveness in the digital context. European Conference on Cyber Warfare and Security (pp. 78-86). Academic Conferences International Limited.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology innovation management review*, 4(10). https://www.timreview.ca/article/835

Dou, X. (2020). Big data and smart aviation information management system. *Cogent Business & Management*, 7(1), 1766736. https://www.tandfonline.com/doi/full/10.1080/23311975.2020.1766736

Elmarady, A. A., & Rahouma, K. (2021). Studying cybersecurity in civil aviation,

including developing and applying aviation cybersecurity risk assessment. *IEEE access*, 9, 143997–144016. https://ieeexplore.ieee.org/abstract/document/9579414

El-Sheimy, N., & Youssef, A. (2020). Inertial sensors technologies for navigation applications: State of the art and future trends. Satellite Navigation, 1(1), 2.

Enge, P., Enge, N., Walter, T., & Eldredge, L. (2015). Aviation benefits from satellite navigation. New Space, 3(1), 19–35. https://www.liebertpub.com/doi/full/10.1089/space.2014.0011

Euroopan parlamentti. (2022a). Lentoturvallisuus. Viitattu 5.2.2024. https://www.europarl.europa.eu/factsheets/fi/sheet/134/lentoturvallisuus

Euroopan parlamentti. (2022b). Lentoliikenne: siviili-ilmailun turvaaminen. Viitattu 5.2.2024. Viitattu 5.2.2024. https://www.europarl.europa.eu/factsheets/fi/sheet/132/lentoliikennesiviili-ilmailun-turvaaminen

Euroopan unioni. (27.12.2022). Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555. *Euroopan unionin virallinen lehti*. Viitattu 25.5.2024. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0080.01.FIN&toc=OJ%3AL%3A2022%3A333%3AFULL

Euroopan unioni. *Euroopan unionin lentoturvallisuusvirasto (EASA)*. Viitattu 25.5.2024. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-aviation-safety-agency-easa_fi

Euroopan unioni. *Yleinen tietosuoja-asetus*. Viitattu 25.5.2024. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm

Finnair. *Suurimmat riskit*. Viitattu 20.2.2023. https://investors.finnair.com/fi/governance/risk-management/major-risks

Finnair. *Finnairin tietosuojaseloste*. Viitattu 20.2.2023. https://www.finnair.com/fi-fi/info/finnairin-tietosuojaseloste

Gebre-Egziabher, D., Hayward, R. C., & Powell, J. D. (1996, April). A low-cost GPS/inertial attitude heading reference system (AHRS) for general aviation applications. *1998 Position Location and Navigation Symposium (Cat. No. 98CH36153)* (pp. 518-525). IEEE.

IATA. About us. Viitattu 26.5.2024. https://www.iata.org/en/about/

IATA. Aviation cyber security. Viitattu 26.5.2024. https://www.iata.org/en/programs/security/cyber-security/#tab-4

Kagalwalla, N., & Churi, P. P. (2019, September). Cybersecurity in aviation: An intrinsic review. 2019 5th international conference on computing, communication, control, and automation (ICCUBEA) (pp. 1-6). IEEE.

Kangas, L. (27.4.2024). *Kaksi Finnairin konetta joutui palaamaan Virosta takaisin Suomeen GPS-häirinnän takia*. Yle.fi. Viitattu 28.4.2024. https://yle.fi/a/74-20086036

Kannan, P. K. (2017). Digital marketing: A framework, review and research agenda. *International journal of research in marketing*, 34(1), 22–45. https://www.sciencedirect.com/science/article/abs/pii/S0167811616301550

Kamali, B. (2010, May). An overview of VHF civil radio network and the resolution of spectrum depletion. 2010 Integrated Communications, Navigation, and Surveillance Conference Proceedings (pp. F4-1). IEEE. https://ieeexplore-ieee-org.ezproxy.jyu.fi/document/5503256

Khatun, M., Wagner, F., Jung, R., & Glaß, M. (2023). An application of DE MATEL and fuzzy DEMATEL to evaluate the interaction of safety management system and cybersecurity management system in automated vehicles. *Engineering Applications of Artificial Intelligence*, 124, 106566. https://www.sciencedirect.com/science/article/pii/S0952197623007509

Lehto, A., Sestorp, I., Khan, S., & Gurtov, A. (2021, April). Controller pilot data link communication security: A practical study. 2021 Integrated Communications Navigation and Surveillance Conference (ICNS) (pp. 1-11). IEEE.

Lindgren, J., Mokka, R., Neuvonen, A., & Toponen, A. (2019). *Digitalisaatio: Murroksen koko kuva*. Tammi.

Lufthansa Crago. *Security as corporate culture*. Viitattu 20.2.2023. https://www.lufthansa-cargo.com/ci/security

Lufthansa Industry Solutions. *Cyber Security Survey*. Viitattu 20.2.2023. https://www.lufthansa-industry-solutions.com/de-en/newsroom-downloads/news/new-white-paper-and-survey-on-cyber-security

Lufthansa Industry Solutions. *IT Security consulting: cutting edge IT security services for business*. Viitattu 20.2.2023. https://www.lufthansa-industry-solutions.com/de-en/solutions-products/it-security

Osanaiye, O., Choo, K. K. R., & Dlodlo, M. (2016). Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. *Journal of Network and Computer Applications*, 67, 147–165. https://www.sciencedirect.com/science/article/abs/pii/S1084804516000023

Pandey, P., & Nisha, T. N. (2021, July). Challenges in single sign-on. *Journal of Physics: Conference Series* (Vol. 1964, No. 4, p. 042016). IOP Publishing. https://iopscience.iop.org/article/10.1088/1742-6596/1964/4/042016/meta

Parra, A. S. O., Crespo, L. E. S., Alvarez, E., Huerta, M., & Paton, E. F. M. (2016). Methodology for dynamic analysis and risk management on ISO27001. *IEEE Latin America Transactions*, *14*(6), 2897-2911. https://ieeexplore-ieee-org.ezproxy.jyu.fi/document/7555273

Pollard, T., & Clark, J. (2019). Connected aircraft: Cyber-safety risks, insider threat, and management approaches.

Qiu, J., Jianwei, Y., Zhihong, T., & Shuofei, T. (2011, August). Design, implementation and optimization of network access control system based on routing diffusion. 2011 6th IEEE Joint International Information Technology and Artificial Intelligence Conference (Vol. 2, pp. 121-125). IEEE.

Ryanair. (20.2.2023). *Cyber Security*. https://corporate.ryanair.com/about-us/cyber-security/

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. *International Journal of Advanced Research in Computer and Communication Engineering*, 7(11), 125-128. https://www.researchgate.net/profile/Nandhini-Sundaresan/publication/329678338_Overview_of_Cyber_Security/links/5c1640b3299bf139c75c29e7/Overview-of-Cyber-Security.pdf

Singer, P. W., & Friedman, A. (2014). Cybersecurity: What everyone needs to know. Oup USA.

Singapore Airlines. *Keeping your data safe*. Viitattu 22.2.2023. https://www.singaporeair.com/en_UK/security/

Singapore Airlines. *Advisory on phishing scams and good cybersecurity practices*. Viitattu 22.2.2023. https://www.singaporeair.com/en_UK/au/media-centre/news-alert/?id=jjofpgqj

Smith, M., Moser, D., Strohmeier, M., Lenders, V., & Martinovic, I. (2018). Undermining privacy in the aircraft communications addressing and reporting system (ACARS). *Proceedings on Privacy Enhancing Technologies*, 2018(3), 105–122. https://www.research-collection.ethz.ch/handle/20.500.11850/294042

Stastny, P., & Stoica, A. M. (2022, February). Protecting aviation safety against cybersecurity threats. *IOP Conference Series: Materials Science and Engineering* (Vol. 1226, No. 1, p. 012025). IOP Publishing.

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., ... & Bellekens, X. (2022). Cyber-security challenges in aviation industry: A review of current and future trends. Information, 13(3), 146. https://www.mdpi.com/2078-2489/13/3/146

The Emirates Group. *Cyber Security Policy*. Viitattu 22.2.2023. https://www.theemiratesgroup.com/assets/pdf/Cyber_Security_Ambition_Policy.pdf

Yuxian, Y., Lianhuan, L., & Xinfeng, Y. (2011, December). Analysis and

comparison on new network security access technology-NAC and NAP. Proceedings of 2011 International Conference on Computer Science and Network Technology (Vol. 3, pp. 1877-1880). IEEE.