jamk

# Kyberturvallisuus liikelentoliikenteessä

Matias Juka, TTV20S1

Opinnäytetyö, AMK
Maaliskuu 2024
Insinööri (AMK), Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

**Kuvailulehti**

**Juka, Matias**

**Kyberturvallisuus liikelentoliikenteessä**

Jyväskylä: Jyväskylän ammattikorkeakoulu. Maaliskuu 2024, 37 sivua.

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

**Tiivistelmä**

Tutkimustyöni tavoitteena oli luoda ajankohtainen tilannekuva siitä, millaisella tasolla liikelentoliikenteen kyberturvallisuus on, ja miten sitä toteutetaan sekä hallitaan. Arvioin työssäni useita eri lentoyhtiöitä ja instrumentteja, ja niiden heikkouksia kyberhyökkäyksiä kohtaan.

Kyberturvallisuuden vaadittava määrä on kasvanut liikelentoliikenteessä huomattavasti viimeisten vuosikymmenien aikana. Lentokoneisiin on teknologian kehittymisen myötä lisätty instrumentteja ja automatiikkaa, joka keskustelee eri tavoin maan, tai muiden instrumenttien tai lentotietokoneen kanssa.

Tässä tutkimustyössä haluan selvittää, millaisella tasolla lentokonevalmistajat, viranomaistahot, sekä lentoyhtiöt ylläpitävät ja hallitsevat kyberturvallisuutta.

Tutkimuksen avulla sain selvitettyä, millaisella tasolla kyberturvallisuutta ylläpidetään nykyajan liikelentoliikenteessä.

**Avainsanat (asiasanat)**

Kyberturvallisuus, lentoliikenne, lentoturvallisuus, ISO/IEC 27001, NIST

**Muut tiedot (salassa pidettävät liitteet)**

-

jamk

**Description**

**Juka, Matias**

**Cyber Security in modern business aviation**

Jyväskylä: JAMK University of Applied Sciences, March 2024, 37 pages

Degree Programme in Information and Communication Technology. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

**Abstract**

In this research work, my aim was to create a topical situational picture of what level cyber security is on in the modern commercial aviation. In my work I evaluated multiple different air carriers and instruments, and what are the main weaknesses towards cyber-attacks.

The necessary amount of cyber security management has increased considerably over the last few decades. As the technology has advanced, airplanes have been fitted with multiple newer-generation instruments and automatism, which is communicating with either the ground, other instruments, or the flight computer.

In this research work I wanted to find out the level of cyber security management upheld by the aircraft manufacturers, authorities, and airlines.

In my research work I was able to find out what the level of cyber security maintenance is in modern commercial aviation.

**Keywords/tags (subjects)**

Cyber security, air traffic, aviation safety, ISO/IEC 27001, NIST

**Miscellaneous (Confidential information)**

-

**Sisältö**

**Kuviot**



**Taulukot**



# 1 Johdanto

Kyberturvallisuus on noussut yhdeksi suurimmista puheen- ja huolenaiheista nykyajan digitalisoituneessa maailmassa. Lentoliikenne on täydellinen kohde hyökkääjille suorittaa hyökkäyksiä, sillä lentokentät, lentoyhtiöt ja muut ilmailualan palveluntarjoajat hallitsevat suuria määriä dataa matkustajista, kuten luottokortti- ja henkilökohtaiset tiedot. Kyberhyökkäykset voivat aiheuttaa yrityksille, ja peräti yksittäisille henkilöillekin suuria taloudellisia kustannuksia, ja esimerkiksi lentoyhtiöille ne aiheuttavat muiden huolien lisäksi myös maineellista haittaa. Jos asiakkaiden turvallisuuden tunne järkkyy yritystä kohtaan, laskee yrityksen kannatus ja suosio turvallisena yrityksenä.

Teknologia ja digitalisaatio tuovat suuria etuja lentoliikenteeseen, mutta myös samalla haasteita kyberturvallisuuden ylläpitämiseen. Teknologian kehittyessä liikelentoliikenteen ja kaiken muunkin lentoliikenteen valvonta ja operointi on digitalisoitunut valtavasti viimeisten vuosikymmenien aikana. Lentokoneista löytyy nykyään matkustajillekin saatavilla olevia IoT (Internet of Things) laitteita, kuten viihdejärjestelmä. Lentokoneiden ja lennonjohdon työvälineiden kyberturvallisuus on joutunut koetukselle, kun muun muassa puolalainen lentoyhtiö LOT joutui perumaan 20 lentoa lentosuunnitelmajärjestelmään kohdistuneen hyökkäyksen takia. (Marsh, 2015)

Työntekijän, tässä tapauksessa lennonjohdon sekä lentoyhtiöiden työntekijöiden rooli vahvan tietoturvallisen ympäristön rakentamisessa on suuri. Nykyään yritykset kouluttavat työntekijöitään mahdollisista kyberturvaan liittyviin asioihin, kuten tietojenkalasteluyrityksen tunnistamiseen. Siitä huolimatta edelleen valtaosa yrityksiin kohdistuvista tietovuodoista aiheutuvat työntekijän virheestä, sillä ihmisen tunteisiin vetoaminen on hyökkääjälle otollista.

Tämän työn tarkoituksena on luoda ajankohtainen ja paikkaansapitävä dokumentti kyberturvallisuuden nykytilasta liikelentoliikenteessä. Kerään verkosta tietoa eri lentoyhtiöistä, ja niiden julkaisemista tiedoista kyberturvallisuuteensa liittyen, ja teen niistä omien arviointien lisäksi taulukon. Käytän työssäni ainoastaan lentoyhtiöitä, joiden EU on sallinut liikennöivän ilmatilassaan.

# 2 Kyberturvallisuuden määrittely

Kyberturvallisuus on yksi turvallisuutta käsittelevä osa-alue, jolla pyritään turvalliseen sähköiseen ja verkotettuun yhteiskuntaan. Kyberturvallisuudessa pyritään tunnistamaan ja ehkäisemään erilaisten järjestelmien häiriöiden vaikutuksia yhteiskunnalle kriittisiin toimintoihin, tässä tapauksessa liikelentoliikenteeseen ja erityisesti lennonjohtoon. (Kyberturvallisuus 2022)

Yleisimpiä uhkia yhteiskunnan kyberturvallisuudelle ovat muun muassa palvelunestohyökkäykset, haittaohjelmat, ja hakkerointi. Kuten aiemmin mainittu, kyberuhat eivät toki koske ainoastaan yhteiskuntaa ja yrityksiä, vaan samat uhat, erityisesti haittaohjelmat voivat vaikuttaa yksittäisen henkilön tietojen turvallisuuteen.

### 2.1 Kyberturvallisuus Suomessa

Suomessa kyberturvallisuuden eteen töitä tekemään on perustettu Traficomin alaisuudessa toimiva Kyberturvallisuuskeskus. Heiltä tulee kansalliset lainsäädännöt ja ohjeet kyberturvallisuuden ylläpitoon ja hallintaan lentoliikenteessä.

## 3 Kyberturvallisuuden hallinta

Kyberturvallisuuden hallinta ilmailualan organisaatiossa kuten lentoyhtiössä on sitä, että organisaatio kykenee tuottamaan keskeisimmät palvelunsa ja toimintonsa turvallisesti. Tämä tarkoittaa sitä, että organisaatiolla tulee olla hallussa ilmailun turvallisuuteen tai turvaamiseen vaikuttavat tietoturvariskit, ja että se on kykeneväinen palautumaan organisaatioon kohdistuneista tietoturvatapahtumista turvallisesti, hallitusti sekä nopeasti. (Traficom 2023)

Organisaatioita auttamaan ja tukemaan on luotu erilaisia standardeja sekä viitekehyksiä, joiden pohjalta organisaation on helpompi hallita omaa tietoturvaansa ja minimoida riskit, mahdolliset vahingot, ja normaaliin liiketoimintaan palautumiseen vaadittava aika.

### 3.1 ISO 27001

ISO 27001 on tietoturvallisuuden hallintaan suunnattu standardi, joka toimii muottina organisaatioille joiden tavoitteena on valvoa, ylläpitää ja parantaa tietoturvallisuuden hallintajärjestelmää ISMS:ää (Information Security Management System). ISMS:n tarkoitus on luoda organisaatiolle riskinhallintaprosessi, joka suojaa organisaation tietojen luottamuksellisuuden ja eheyden. (Jussila N.d)

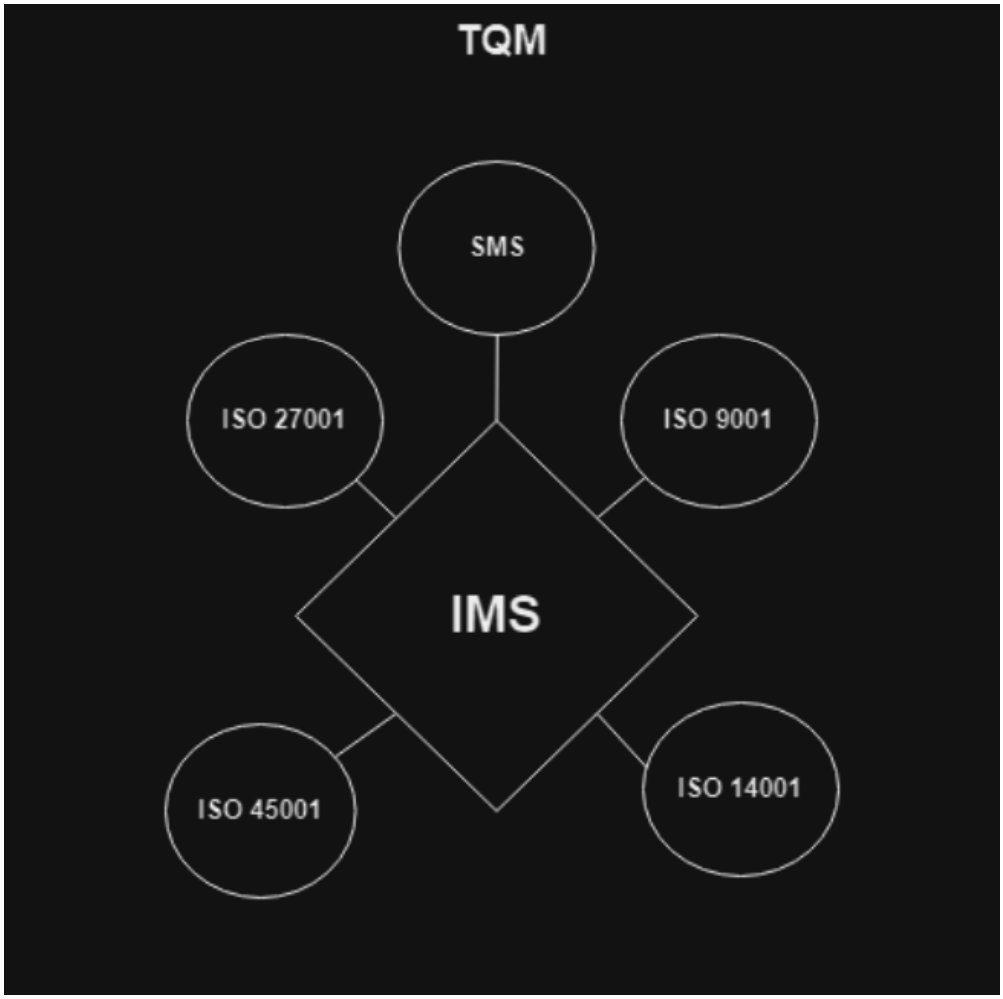
Lentoyhtiöissä ISO 27001 on osa kokonaisvaltaista hallintajärjestelmää. Saksalainen lentoyhtiö Lufthansa on implementoinut standardin käytön kaikkeen liiketoimintaansa, johon kuuluu varsinaisen lentoyhtiön lisäksi Lufthansa Training ja Lufthansa Technik sisaryhtiöt. Lufthansa Cargo, Lufthansan sisaryhtiö on myös implementoinut standardin omaan hallintajärjestelmäänsä. He käsittelevät suurta määrää asiakasdataa omassa päivittäisessä toiminnassaan, ja heidän yrityksensä isoimpiin menestyksen avaimiin kuuluu tietojen vastuullinen käyttäminen ja säilyttäminen. (Security as a corporate culture N.d)

Kuviossa on jäljennetty topologia yrityksen tai organisaation laadunhallintajärjestelmästä, jollaiseen ISO 27001 voidaan implementoida. Integroitu hallintajärjestelmä (IMS) pitää sisällään ISO 9000, ISO 14000, ISO 27000 ja ISO 45000 perheiden standardeja, joiden lisäksi se pitää sisällään turvallisuudenhallintajärjestelmän (SMS). Koko tämä kokonaisuus muodostaa organisaatiossa kokonaisvaltaisen hallintajärjestelmän (TQM).

ISO 27001 ei ole yrityksille pakollinen standardi muutamaa maata lukuunottamatta, mutta kun kyseessä on lentoyhtiö joka käsittelee hyvin salaisia tietoja sekä taloudellista liikennettä, on se

mielestäni erittäin hyvä lisäys hallintajärjestelmään. Tämän lisäksi se herättää asiakkaissa luottamuksen ja turvallisuuden tunnetta, kun he tietävät että heidän tietonsa on hyvin turvattu.

Kuvio 1. ISO 27001 kokonaisvaltaisessa laadunhallintajärjestelmässä




## 3.2 NIST

NIST, eli Yhdysvaltain standardisointi- ja teknologiainstituutti (National Institute of Standards and Technology) on kauppaministeriön alla toimiva virasto Yhdysvalloissa. (Yhdysvaltain standardisointi- ja teknologiainstituutti, 2022.) He ovat luoneet kyberturvallisuuden hallinnan viitekehykset, joka koostuu viidestä eri osasta. Viitekehykset ovat vaihtoehtoisia, eli organisaation ei ole lain mukaan välttämätöntä hyödyntää edellä mainittua materiaalia, mutta se on hyvin

suuresti suositeltua, sillä ne helpottavat kyberturvallisuuden hallintaa ja mahdollisten tapahtumien ennaltaehkäisyä ja niihin reagoimista. (FTC 2018)

### 3.2.1 Tunnista

Ensimmäisenä osana NIST:in laatimaa viitekehystä on tunnistaminen. Organisaation tulee tunnistaa oma topologiansa sekä varansa. Osa tunnistamista on myös kyberturvaan liittyville seikoille yhteisten käytäntöjen luominen. (FTC 2018)

### 3.2.2 Suojaudu

Organisaation tulee suojata oma datansa, ja valvoa aktiivisesti ympäristöön kirjautuvia käyttäjiä, sekä liikennettä. Erilaisten tietoturvasovellusten käyttäminen on erittäin suositeltua, kuten myös salaisten tietojen kryptaaminen. Tämä ei kuitenkaan kertalyönnillä ole valmis, sovelluksia tulee pitää päivitysten osalta ajan tasalla. Suuressa osassa suojautumisprosessia on myös henkilöstön kouluttaminen turvalliseen tietojen käsittelyyn ja jakamiseen. Henkilöstön tulee tietää miten vanhat työkoneet ja tiedostot hävitetään turvallisesti. (FTC 2018)

### 3.2.3 Havainnoi

Tietoja ja tietokoneita tulee valvoa, sekä havainnoida tuntemattomat käyttäjät mahdollisina tietoturvariskeinä. Jokainen normaalista poikkeava kirjautuminen tai muu toiminta tulee tutkia perusteellisesti henkilöstön kanssa. (FTC 2018)

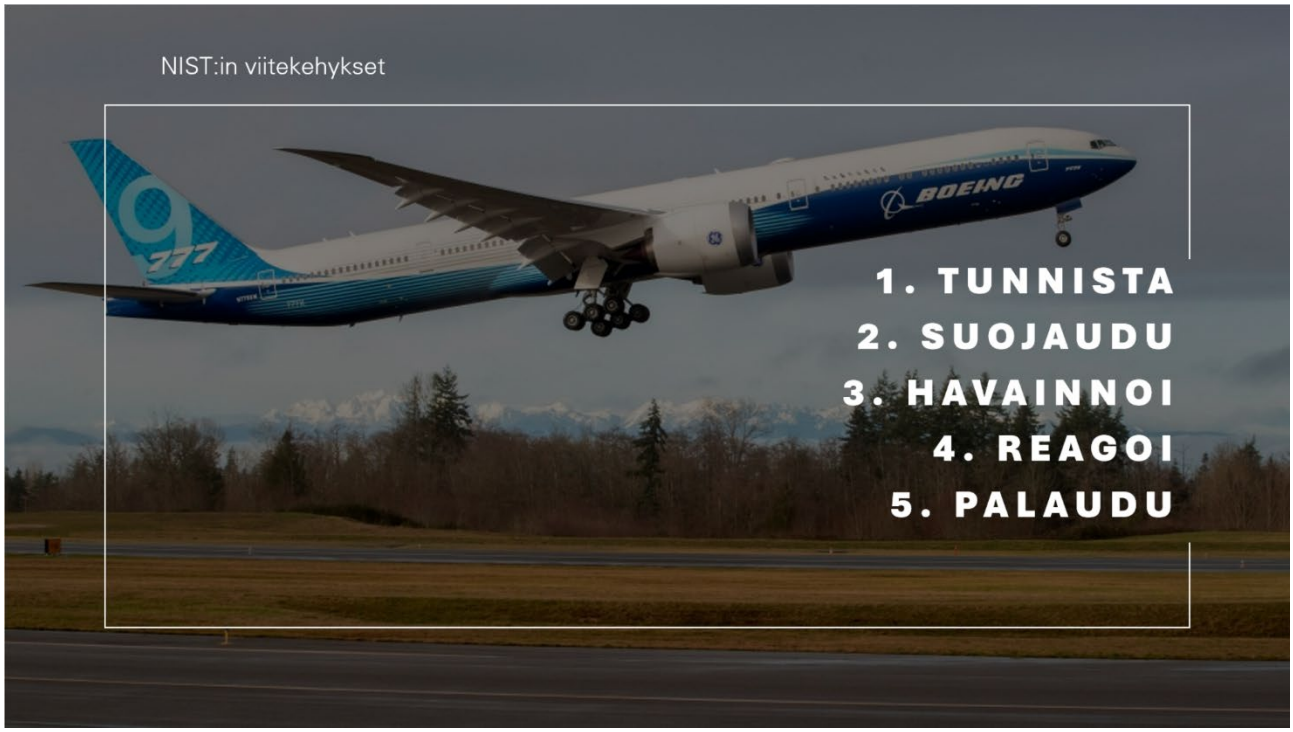
### 3.2.4 Reagoi

Jos ja kun tietoturvavuotoon tai muuhun tapahtumaan törmätään organisaation ympäristössä, tulee organisaatiolla olla valmiiksi laaditut reagointitoimenpiteet, joiden avulla tapahtumaan reagointi on sujuvaa. Asiakkaat ja mahdolliset muut asianomaiset, kenen tiedot tai järjestelmät ovat vaarantuneet tapahtumassa tulee informoida tapahtuneesta. Tapahtumasta tulee myös ilmoittaa viranomaisille, ja tapahtuman tutkinta tulee aloittaa välittömästi. Jokaisessa tietoturvatapahtumassa piilee myös oppi organisaatiolle, joten on myös tärkeää selvittää tapahtunut perinpohjaisesti sekä oppia virheistä, kuten esimerkiksi päivittämällä tietoturvakäytäntöjä. (FTC 2018)

### 3.2.5 Palaudu

NIST:in viitekehyksien viimeinen osio ohjeistaa organisaatiota toipumaan ja palautumaan tapahtumasta tehokkaasti ja turvallisesti. Organisaation täytyy korjata ja palauttaa tapahtuman piiriin jääneet verkon osat ja järjestelmät, ja pitää asiakkaat ja asianomaiset ajan tasalla palautumisprosessista. (FTC 2018)

Kuvio 2. NIST:in viitekehykset




## 3.3 Ihmisen rooli kyberturvallisen ympäristön ylläpitämisessä

Sen lisäksi, että viitekehyksien hyödyntäminen ja verkkolaitteiden turvallisuus on hyvällä tasolla, täytyy myös kyberturvallista ympäristöä hallitessa ottaa huomioon järjestelmiä operoivien käyttäjien, eli ihmisten rooli.

O'Driscollin (2024) mukaan jopa 90% kyberhyökkäyksistä mahdollistui ihmisen tekemän virheen kautta. Tästä syystä lentoyhtiöillä, kuten kaikilla muillakin organisaatioilla on suuri työ ja velvoite kouluttaa työntekijänsä sille tasolle, että mahdollisten esimerkiksi kalastelusähköpostien tunnistaminen olisi helpompaa. Työntekijää tulee myös kouluttaa siitä, miten ja mihin tarkoituksiin

verkkolaitteita käytetään. Täten välttyisimme yksittäisen yrityksen tasolla siltä, että kyberuhan mahdollisuus olisi käyttäjäperäisestä virheestä johtuen korkea.

Proofpointin (2020) julkaisemassa vuosittaisessa raportissa he kertovat, että noin 90% työskentelevistä aikuisista käyttää työnantajan tarjoamia työvälineitä, kuten kannettavia tietokoneita sekä puhelimia henkilökohtaiseen ja perheen sisäiseen käyttöön. Tämä myös on huomattava kyberturvallisuusriski, sillä esimerkiksi kannettavan tietokoneen joka sisältää yrityksen tiedostoja tai työntekijän salasanoja yhdistäminen julkiseen Wi-Fiin altistaa tiedot mahdolliselle kaappaukselle ja väärinkäytölle. Julkisen Wi-Fin kautta tehtäviä hyökkäys- tai kalastelutoimenpiteitä on useita, kuten haittaohjelmien välittäminen laitteelle verkon välityksellä.

ICAO (2022) määrittää raportissaan miten kyberturvallisuus määritetään ja miten sitä tuodaan julki lentoliikenteessä. Raportissa mainitaan avainseikkoja kyberturvallisen ympäristön vahvistamiseen ja ylläpitämiseen, kuten avoin kommunikaatio kyberturvallisuuteen liittyvissä asioissa, kyberturvallisuuden harjoittelu ja opiskelu.

Valitettavasti kuitenkaan en varsinaisesti löytänyt tietoa siitä, miten lentoyhtiöt kouluttavat omaa henkilöstöään kyberturvallisiksi henkilöiksi. Nykyajan työelämässä tieto- ja kyberturvallisuuteen liittyvät koulutukset ovat usein työn perehdytysvaiheen alussa tehtäviä pikakursseja ja tenttejä, joita työuran edetessä ei kuitenkaan tehdä tai lueta uudelleen. Näistä tenteistä perehdytettävän motivaatiosta riippuen jää käteen joko kyberturvallisuuden perusteet, tai ei mitään.

# 4 Liikelentoliikenteen turvaaminen

## 4.1 Riskien tunnistaminen

Muun muassa Finnair on luonut verkkosivuilleen taulukon suurimmista lentoyhtiöön kohdistuvista riskeistä. Taulukon lopusta löytyy osuus, joka käsittelee yhtiön kyberturvallisuutta. Finnair on tunnistanut suurimmiksi kyberturvallisuuteen liittyviksi riskeiksi kyberhyökkäyksen järjestelmiin, joka vaikuttaa negatiivisesti operaatioihin, sopimattomien osapuolien pääsyn salaisiin tietoihin vaarantaen niiden luottamuksellisuuden ja eheyden, ja laajamittaisen hyökkäyksen joka vaikuttaa suoraan Finnairin kykyyn jatkaa liiketoimintaa normaalisti. (Suurimmat riskit 2018) Koen että

Finnair on hoitanut riskientunnistamisen vastuullisesti ja jokainen seikka on käyty huolellisesti läpi ja niistä on luotu asianmukainen dokumentti julkistettavaksi heidän sivuilleen.

Kansainvälinen ilmakuljetusliitto IATA on laatinut kirjastoonsa riskien tunnistamiseen tarvittavan materiaalin CRAGM:in, jossa määritellään operaattorien minimitoimenpiteet riskien tunnistamiseksi. Tämä materiaali on luotu tukemaan lentoyhtiöiden työntekijöiden perusymmärrystä kyberturvallisuudesta ja antaa myös tarvittavat valmiudet tunnistaa riskit.

## 4.2 ENISA

ENISA, eli Euroopan unionin kyberturvallisuusvirasto tekee jatkuvaa työtä eurooppalaisen lentoliikennejärjestelmän kyberturvallisuuden eteen. ENISA:n tehtävänä ja tavoitteena on saavuttaa korkea yhteinen kyberturvallisuuden taso koko Euroopan alueelle edistämällä EU:n kyberpolitiikkaa ja sitä kautta lisäämällä luottamusta digi-, palvelu- ja prosessituotteisiin. (Euroopan unionin kyberturvallisuusvirasto N.d)

## 4.3 CISA

Amerikassa lentoliikenteen ja muun kyberturvallisuuden valvonnan ja koordinoinnin hoitaa CISA (Cybersecurity and Infrastructure Security Agency). CISA on osa Yhdysvaltain kotimaan turvallisuusvirastoa. Heidän verkkosivuillaan on runsaasti artikkeleja sekä blogikirjoituksia kyberturvallisuudesta, haavoittuvuuksista ja niiden mitigoinnista.

## 4.4 Kyberturvallisuus liikelentoliikenteessä

Kyberturvallisuus lentoliikenteessä koostuu useasta eri palasta, jotka muodostavat toimivan muttei kuitenkaan välttämättä pomminvarmaa kokonaisuutta. Lentoliikenteessä on useita eri järjestelmiä ja pisteitä, joita lentoyhtiöiden ja muiden kolmannen osapuolen yritysten tulee pitää suojassa hyökkäyksiltä lentoliikenteen jatkuvuuden kannalta.

## 4.5 Instrumentit ja hallintajärjestelmät

Kuvioon olen mallintanut tärkeimmät kommunikointijärjestelmät, joita lentokone lennon aikana käyttää. Kuten tästä kuvasta jo ilmenee, lentokone kommunikoi todella usean eri maa-aseman

kanssa, mikä myös tarkoittaa että lentokone voi olla haavoittuvainen järjestelmiensä suhteen lennon aikana riippuen myös muiden tekijöiden ja asemien kyberturvallisuudesta.

### 4.5.1 GNSS

Edellisestä kaaviosta ehkä tutuin elementti on GNSS. GNSS (Global Navigation Satellite Systems) on luotettava ja varmatoiminen navigointijärjestelmä, joka kerää tarkkaa tietoa lentokoneen sijainnista ja nopeudesta suhteessa maahan. Satelliitit lähettävät lentokoneelle signaalin, josta lentotietokone kerää tiedot ja näyttää ne piloteille korkeus- ja nopeusindikaatioina instrumenteissa. (ESA 2021)

EUSPA (2023) mukaan GNSS-järjestelmän suorituskyvyn määrittelee neljä eri seikkaa, tarkkuus, yhtenäisyys, jatkuvuus ja saavutettavuus. Tarkkuus määritellään GNSS:n antaman sijainti- ja nopeustiedon vertailusta aktuaaliseen nopeuteen ja sijaintiin. Yhtenäisyys tulkitaan järjestelmän kykeneväisyydestä asettaa kynnys varmuudelle, epänormaalissa sijaintidatan tilanteessa hälytys. Jatkuvuus tarkoittaa järjestelmän kykeneväisyyttä tuottaa sijaintidataa jatkuvasti häiriintymättä. Saavutettavuus tulee järjestelmän prosentuaalisesta määrästä tuotettua dataa, joka täyttää tarkkuuden määritelmät ja vaatimukset.

Kuviossa näkyy myös, kuinka lentokone kommunikoi radioaaltojen avulla ILS:n (Instrument Landing System) kanssa. ILS luo radiosignaalin saatuaan pilotille keinotekoisen horisontin navigointinäytölle, ja X ja Y akseleille merkit, joiden avulla pilotti pystyy ohjaamaan lentokonetta oikeaan suuntaan vertikaalisesti ja horisontaalisesti laskeutuessa kohti kiitorataa vaikka näkyvyys olisikin heikko tai olematon. (Instrument landing system 2024)

GNSS:n suurin heikkous kyberturvallisuuden kannalta on radioaaltoihin kohdistuva häirintä. Muun muassa Laukkanen (2023) kertoo Finnairin kärsineen GPS-häirintää Lähi-Idän alueella, jossa lentokoneen navigointijärjestelmiä häirittiin johtaen GPS:ää hyödyntävien järjestelmien automaattiseen sammumiseen lennon aikana.

### 4.5.2 Lennonjohdon valvonta

Lennonjohdolla on päivittäisessä työssään käytössä tutkia, joilla lennonjohdon työntekijät valvovat lentokoneiden sijaintia ja tilaa. PSR (Primary Surveillance Radar) lähettää maasta kaikuja, jotka kimpoavat lentokoneen pinnoista takaisin maahan luoden arvion siitä, missä lentokone sijaitsee. SSR (Secondary Surveillance Radar) tekee samaa, vahvistaen PSR:n tietoa lentokoneen aktuaalisesta sijainnista. (Durgut 2020)

ADS-B (Automatic Dependent Surveillance – Broadcast) on järjestelmä, joka vastaanottaa lentokoneen yhteydenottoja instrumenteista, jotka sisältävät lentokoneen järjestelmien ilmoittamat tiedot lentokoneen sijainnista broadcastilla. Broadcast-viestintä tarkoittaa sitä, että tiedon lähettävällä taholla (tässä tapauksessa lentokone) ei ole tietoa siitä kuka vastaanottaa lähetetyn datan. (Automatic Dependent Surveillance – Broadcast 2024)

ADS-B:n avulla pilottien turvallisuuden taso nousee. Järjestelmä antaa piloteille pääsyn TIS-B:iin (Traffic Information Service – Broadcast), joka antaa piloteille tiedon muiden lennonjohdon tutkakontrollissa olevien lentokoneiden sijainnista, korkeudesta ja nopeudesta 15 merimailin ja 3500 jalan etäisyydellä pilotin ohjaamasta lentokoneesta. (FAA, 2022) Tämä teknologia mahdollistaa myös TCAS:in (Traffic Collision Avoidance System). Järjestelmä tunnistaa ADS-B:n avulla lähellä lentävät lentokoneet ja antaa tarvittaessa pilotille kovaäänisen varoituksen, jos lentokone on vaarassa törmätä toiseen lentokoneeseen. (Traffic collision avoidance system 2024)

### 4.5.3 VHF & HF

VHF (Very High Frequency) ja HF (High Frequency), ovat radiotaajuusalueita joiden avulla lentokoneen pilotit voivat muun muassa keskustella lennonjohdon kanssa. Radioaaltoja voidaan myös käyttää navigointiin. (HF, VHF and UHF: What does it all mean? N.d.)

Radioaaltojen huono puoli kyberturvallisuuden kannalta on niiden helppo ja vaivaton salakuuntelu. Lennonjohdon ja lentokoneiden välistä kommunikaatiota on laillista kuunnella taajuuksilla, mutta taajuuden häiritseminen ja taajuudelle kommunikointi ilman lisenssiä on laitonta, mutta melko helppoa.

### 4.5.4 ACARS

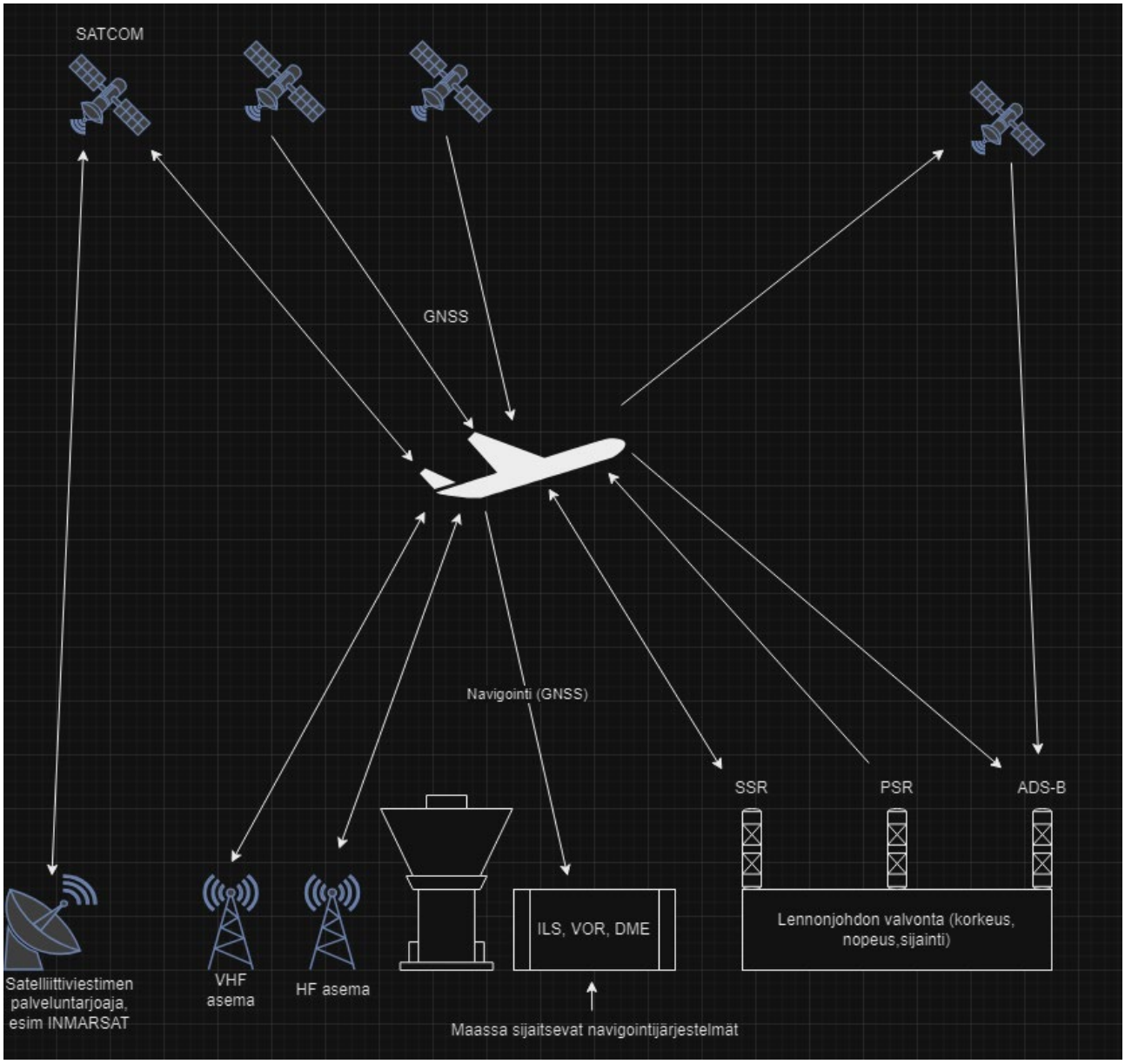
ACARS (Aircraft Communication Addressing and Reporting System) on radio- tai satelliittiyhteyksiä hyödyntävä tiedonsiirtojärjestelmä, jonka kautta lentokone ja maa voivat keskustella lyhyillä tekstiviesteillä. ACARS-järjestelmää voidaan muun muassa käyttää ATIS (Automatic Terminal Information Service) viestien ja useiden muiden hieman tavallisempien viestien lähettämiseen, kuten painolaskelmat. (ACARS 2023)

### 4.5.5 Satcom

SATCOM on satelliitti, joka vastaanottaa radiosignaaleja maasta tai tässä tapauksessa lentokoneesta ja heijastaa ne takaisin maahan vastaanottimiin.

Eurocontrolin (N.d.) mukaan SATCOM-järjestelmä voidaan kategorisoida kolmeen eri ICAO:n (Kansainvälinen siviili-ilmailujärjestö) luokkaan suorituskyvyn mukaan. C-luokkaan kuuluu SATCOM-järjestelmät, jotka toimivat nykyisten SATCOM standardien mukaisesti, B-luokkaan kuuluu järjestelmät, joilla on tuki Baseline 2 ATS vaatimuksiin, eli lyhyesti tiivistettynä valmiudet uudempiin SATCOM:in versioihin. A-luokan SATCOM-järjestelmän tulee pitää sisällään valmiudet Baseline 3 ATS vaatimuksiin, eli tulevaisuudessa käytettäviin SATCOM-järjestelmän eri versioihin.

Kuvio 3. lentoliikenteen kommunikointi- ja paikannusjärjestelmät




## 4.6 Boeing 777

Boeing 777 on amerikkalaisen lentokonevalmistaja Boeing Commercial Airplanesin laajarunkoinen kaksimoottorinen pitkän matkan lentokone. Kyseinen lentokone pitää tällä hetkellä hallussa titteliä maailman suurimpana kaksimoottorisena lentokoneena. 777 on maailman ensimmäinen pelkästään tietokoneen avulla suunniteltu matkustajalentokone. (Boeing 777 2023)

Lentokoneen ohjaus on toteutettu fly-by-wire tekniikalla kuten myös A350 ja useat muut 90-luvun loppupuolella suunnitellut lentokoneet. Fly-by-wire tarkoittaa sitä, että pilotin ohjaussauvan

liikkeet tunnistetaan sensorien avulla, ja lentotietokone siirtää lentokoneen ohjauspintoja sensoreista saadun signaalin mukaisesti. Fly-by-wire teknologia poistaa myös suurimmaksi osaksi pilotin tekemien virheiden riskin ja parantaa täten lentoturvallisuutta. Lentotietokone tunnistaa pilotin asettamat ohjaussauvan liikkeet, eikä anna pilotin tehdä liikkeitä jotka vaarantaisi lentokoneen rakenteellisen kestävyyden tai lennon jatkuvuuden. (Fly-by-wire 2024)

### 4.6.1 Tietoliikennekaavio & lentotietokone

Yllä näkyvässä topologiassa näkyy, miten pilottien instrumentit ovat yhteydessä toisiinsa. Pilottien näytöt, lentokannen kommunikaatio, lennonhallinta, ilmastointi ja keskushuoltojärjestelmä ovat kytkettynä kommunikaatio-ohjelman rajapintaan ja reitittimeen. Rajapinnassa on myös kiinni aikaisemmin mainittu ACARS-järjestelmä, joka on yhteydessä lentokoneen palvelimeen. Rajapinnasta löytyy myös tulostin, jota lentäjät käyttävät vastaanottaakseen ja lähettääkseen lentosuunnitelmia ja viestejä.

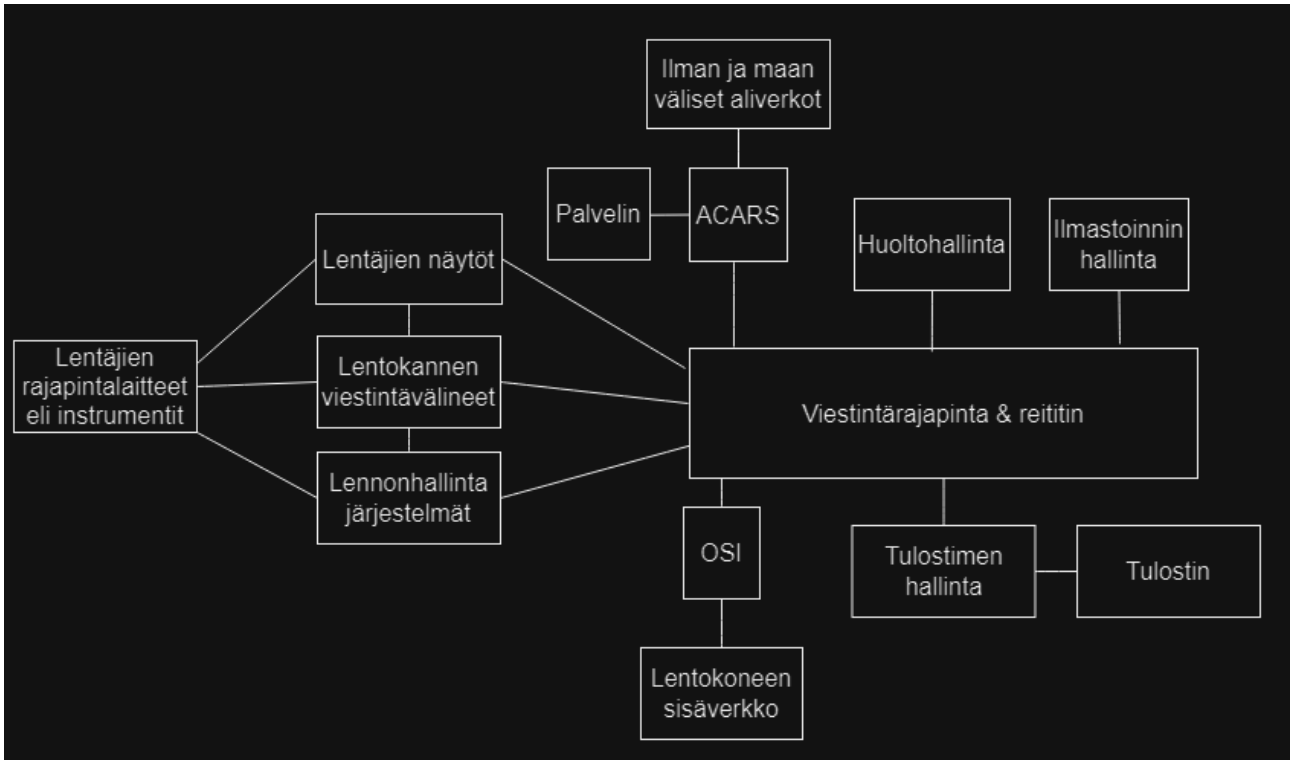
OSI (Other Service Information) on yhteydessä lentokoneen LAN-verkkoon, jossa on muunmuassa matkustamossa sijaitseva matkustajien käytettävissä oleva langaton verkko.

Lentokoneissa oleva langaton verkko on käyttäjien kesken suojaamaton. On mahdollista, että matkustajan laitteet altistuu kyberhyökkäyksille, jos matkustamossa on henkilö jonka aikeena on tutkia suojaamattoman verkon laitteita ja mahdollisesti hyökätä niihin.

### 4.6.2 Kommunikaatio maahan

Kaaviossa näkyy ACARS:in olevan yhteydessä maan ja lentokoneen välisiin verkkoihin. Lentäjät voivat perinteisen VHF ja HF radioliikenteen lisäksi kommunikoida ATIS viesteillä. Lentokone kommunikoi myös automaattisesti maan asemien kanssa, kertoen sen sijainnista ja nopeudesta.

Kuvio 4. Boeing 777 -tietoliikennekaavio




## 4.7 Airbus A350 XWB

Airbus A350 XWB on eurooppalaisen lentokonevalmistaja Airbusin valmistama kaksimoottorinen, laajarunkoinen pitkän matkan lentokone. (Wikipedia, 2024) Kone on erittäin suosittu lentoyhtiöiden keskuudessa, sillä sen kahdella moottorilla saavutettu lentoaika ja matka ovat erityisen pitkät. Kuten Boeing 777:aa käsittelevässä kappaleessa jo mainitsin, A350 käyttää myös ohjaukseensa fly-by-wire teknologiaa.

### 4.7.1 Tietoliikennekaavio

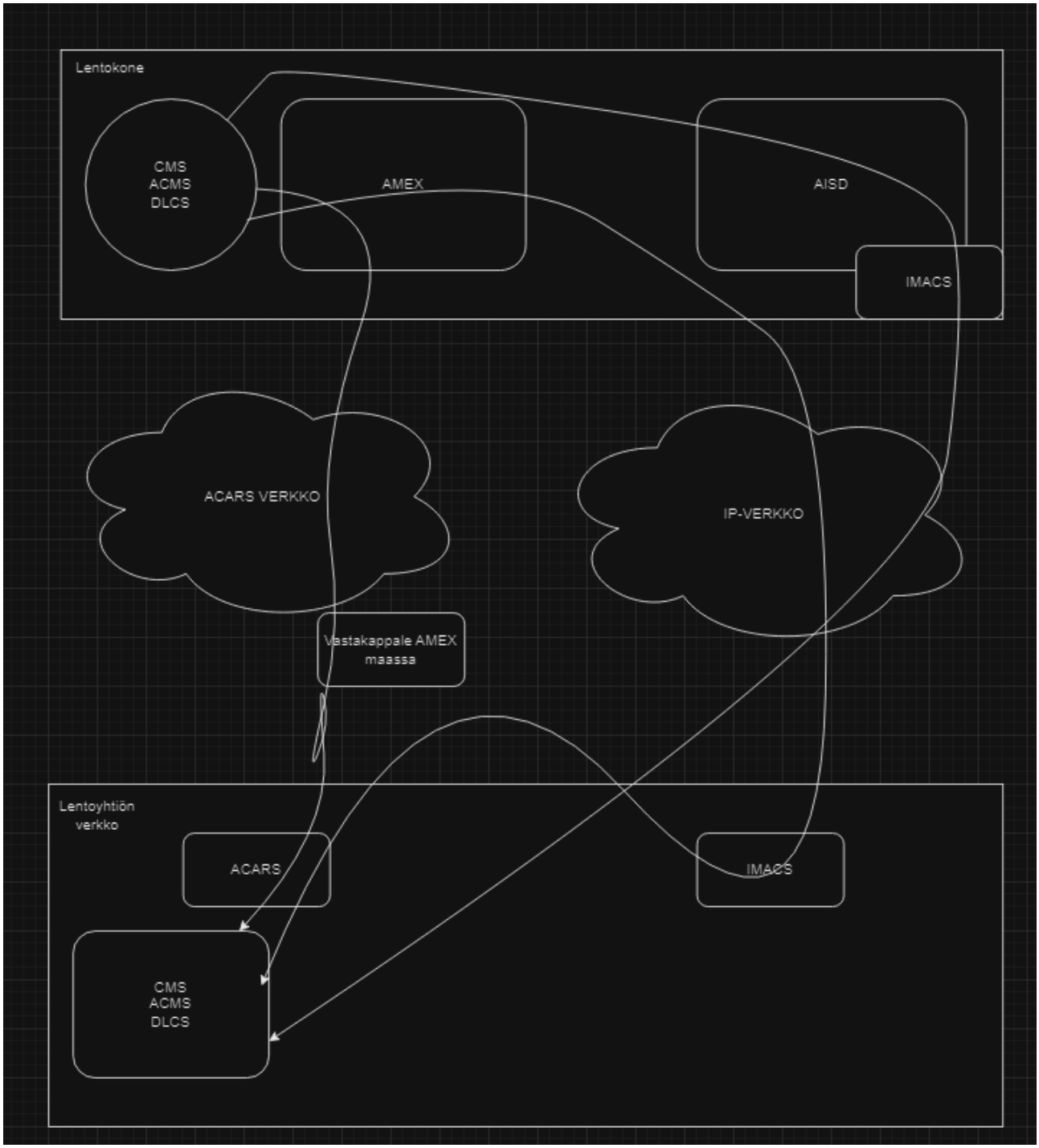
Topologiassa esitettynä A350 lentokoneen kommunikaatiojärjestelmät ja niiden yhteys maahan. Vasemmassa yläkulmassa on koneen ACD (Aircraft Control Domain). ACD on yhteydessä

lennonjohtoon. ACD pitää sisällään mm. CMS:n (Cabin Management System) sekä ACMS:n (Aircraft Condition Monitoring System). ACD lähettää kyseisistä järjestelmistä tietoa maahan ACARS:in kautta maassa sijaitsevaan ACARS palvelimeen ja myös instrumentin vastakappaleisiin.

ACD:n käyttää MIAM (Media Independent Aircraft Messaging) protokollaa, joka sekin muiden instrumenttien tavoin hyödyntää ACARS-verkkoa.

Lentokoneesta löytyy ACD:stä erillään AISD (Airline Information Services Domain), joka tarjoaa reititystä ja kommunikaatiopalvelua lentokoneesta löytyville myös avioniikkaan että matkustajiin liittyville järjestelmille, kuten esimerkiksi matkustamon viihdejärjestelmä ja langaton verkko. Kaikki sen data kulkee IP- ja ACARS- verkkoa pitkin maahan palvelimille. (ICAO 2014)

Kuvio 5. Airbus A350 -tietoliikennekaavio




# 5 Tutkimuksen toteutus

Selvittääkseni lentoliikenteen kyberturvallisuuden tason, aion selvittää millaisia viitekehyksiä lentoyhtiöt käyttävät ylläpitääkseen turvallista tietoliikenneympäristöä.

## 5.1 Tutkimusmenetelmä

Toteutan tutkimukseni luomalla taulukon, joka sisältää suurimmat lentoyhtiöt joiden tukikohta on Euroopassa, Aasiassa tai Pohjois- ja Etelä-Amerikassa tai Oseaniassa. Vertailen lentoyhtiöitä, ja sitä millaisien viitekehysten ympärille yhtiöt ovat oman kyberturvallisuuden hallintaympäristön rakentaneet. Tästä saamme tutkimukselle hyvän pohjan, ja yleiskuvan siitä miten kyberturvallisuutta ylläpidetään ja hallitaan liikelentoliikenteessä.

## 5.2 Viitekehyksien vertailu

Taulukko 2: Eurooppalaiset lentoyhtiöt (Ryanair 2022, 38-39; CAPA 2020; AirFranceKLM Group 2022, 193-194; Turkish Airlines N.d; EasyJet 2023, 2-3; Wizz Air Holdings PLC 2023, 68; TAP Group 2015; Aegean 2017; ITA Airways N.d; Finnair 2018; Pegasus N.d, 2.10.2; Icelandair 2022; AirBaltic 2022; Swiss 2021)

| **Otsikko, vuosi** | **Tekijä, julkaisija** | **Lentoyhtiö** | **ISO 27001** | **NIST - viitekehykset** |
|---|---|---|---|---|
| Aviation on purpose. 2022, 38-39. | Ryanair | Ryanair | **x** | **x** |
| Lufthansa Group receives ISO 27001 information security management system certification. 2020. | CAPA | Lufthansa Group | **x** | |
| Universal Registration Document 2022. 2022. | AirFranceKLM | Air France-KLM | **x** | |
| Information Security Policy. N.d. | Turkish Airlines | Turkish Airlines | **x** | |

| | | | | |
|---|---|---|---|---|
| Digital Safety. 2023. | EasyJet | EasyJet | **x** | **x** |
| Wizz Air at a glance. 2023 | Wizz Air Holdings PLC | Wizz Air | **x** | **x** |
| Sustainability report. 2015. | TAP Group | TAP Air Portugal | **x** | |
| Sustainable Development Report. 2017. | Aegean | Aegean Airlines | | |
| The ITA Airways sustainability manifesto. N.d | ITA Airways | ITA Airways | | |
| Vastuullisuusraportti. 2018 | Finnair | Finnair | | |
| General Terms & Conditions. N.d | Pegasus | Pegasus Airlines | **x** | |
| Annual and Sustainability Report. 2022 | Icelandair | Icelandair | **x** | |
| Sustainability and annual report. 2022 | airBaltic | airBaltic | **x** | |
| Swiss-AS now certified according to ISO/IEC 27001. 2020 | Swiss-AS | Swiss | **x** | |

Taulukko 2: Aasialaiset lentoyhtiöt (The Emirates Group N.d; Japan Airlines N.d; Singapore Airlines 2022; ANA Group N.d; Qatar Airways 2023; Vietnam Airlines 2017; CAPA 2013; Cathay Pacific 2019; Royal Jordanian 2020)

| **Otsikko** | **Tekijä** | **Lentoyhtiö** | **ISO 27001** | **NIST viitekehykset** |
|---|---|---|---|---|
| Cyber Security Policy. N.d. | The Emirates Group | Emirates | | |
| Information Security. N.d. | Japan Airlines | Japan Airlines | **x** | |
| Sustainability report. 2022 | Singapore Airlines | Singapore Airlines | | |
| Information Security. N.d | ANA Group | All Nippon Airways | **x** | |
| Qatar Airways Achieves IT Service Management System Excellence | Qatar Airways | Qatar Airways | **x** | |

| | | | | |
|---|---|---|---|---|
| Certification. 2023 | | | | |
| Annual report. 2017 | Vietnam Airlines | Vietnam Airlines | **x** | |
| Malaysia Airlines receives ISO 27001 certification for information security management system. 2013 | CAPA | Malaysia Airlines | **x** | |
| Sustainable Development Report. 2019 | Cathay Pacific | Cathay Pacific | | |
| Annual report. 2020 | Royal Jordanian | Royal Jordanian | **x** | |

Taulukko 3: Pohjois- ja Etelä-Amerikkalaiset lentoyhtiöt (Air Canada 2021; Air Transat N.d; Avianca N.d; NIST N.d; United N.d)

| **Otsikko** | **Tekijä** | **Lentoyhtiö** | **ISO 27001** | **NIST viitekehykset** |
|---|---|---|---|---|
| Citizens of the World. 2021 | Air Canada | Air Canada | | |
| Our Privacy Policy. N.d | Air Transat | Air Transat | | |
| Information Security Pol-icy. N.d | Avianca | Avianca | | |
| Current Risk Management Practices | NIST | American Airlines | **x** | |
| Corporate Responsibility Report. N.d | United | United Airlines | | |

Taulukko 4: Oseanialaiset lentoyhtiöt (Qantas 2023; Air New Zealand N.d)

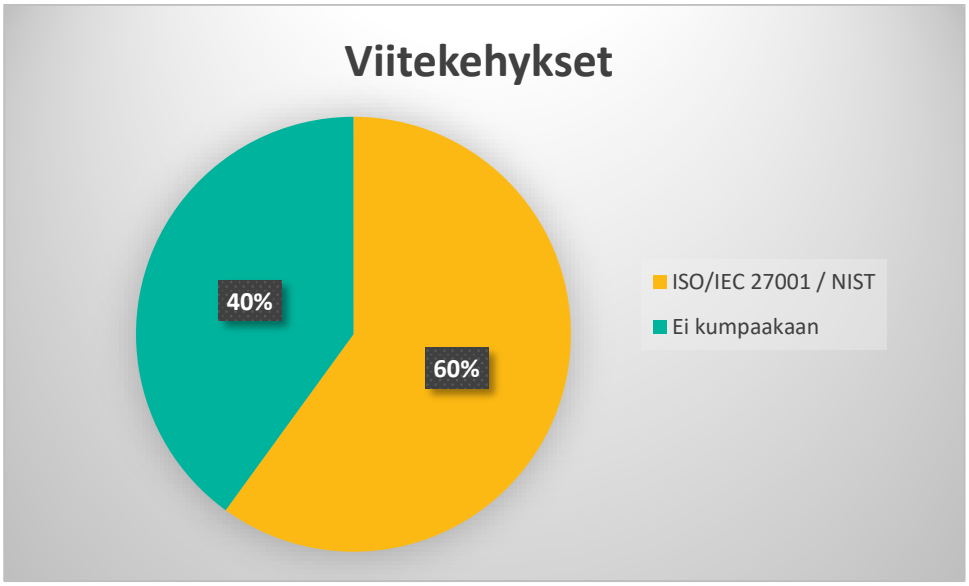
| **Otsikko** | **Tekijä** | **Lentoyhtiö** | **ISO 27001** | **NIST viitekehykset** |
|---|---|---|---|---|
| Privacy and security. 2023 | Qantas | Qantas | | |
| Cyber Security at Air New Zealand. N.d | | Air New Zealand | | |

# 6 Yhteenveto lentoyhtiöistä

Suurimmalta osin lentoyhtiöissä hyödynnetään NIST:in ja ISO:n standardeja sekä viitekehyksiä kyberturvallisuuden hallinnan parantamiseen ja kehittämiseen. 60% otannasta hyödynsi joko ISO/IEC 27001 sertifikaattia, tai NIST:in viitekehyksiä.

Osassa tapauksista kyberturvallisuuden hallintaan oli kehitetty sisäisiä vastaavia viitekehyksiä, niitä en kuitenkaan sisällyttänyt tähän kuvioon selkeyden vuoksi.

Kuvio 6: Viitekehykset




## 6.1 Hyökkäykset lentoyhtiöihin

Hyökkäyksiä lentoliikenteen infraa ja palveluita kohtaan tulee usein, ja ne on yleensä melko laajavaikutteisia, sillä hyökkäykset kohdistuvat asiakasdatapalvelimiin ja tietokantoihin.

Esimerkiksi espanjalainen lentoyhtiö Air Europa joutui tietomurron kohteeksi, ja matkustajien luottokorttitiedot vaarantuivat. Air Europalla on aiempaa historiaa myös tietomurroista, vuonna 2021 yhtiötä rankaistiin 600 000€ sakolla tietomurron takia. (Air Europa suffers credit card data breach 2023)

## 6.2 Kehityskohteet

Mielestäni lentoyhtiöt ovat tehneet erittäin hyvää työtä käsitellessään kyberturvallisuuteen liittyviä asioita instrumenteilla ja lentokoneilla joita heille on saatavilla. Enemmän fokukseni tässä tutkimuksen kehittämiskohteiden osiossa kohdistuu lentokoneiden valmistajiin, ja viranomaisiin jotka määrittävät standardit ja vaatimukset sille, milloin lentokone saavuttaa lentokelpoisuuden ja sen sertifikaatin.

Suurimpana kehityksen kohteena näen itse kyberturvallisuutta koskevat asetettavat vaatimukset lentokoneen valmistajille. FAA:n (2023) mukaan lentokelpoisuustesteihin ei sisälly erillinen tietoliikennejärjestelmien penetraatiotestaus, eli hetkellä mikään viranomaistaho ei ole vielä asettanut lentokelpoisuusehtoihin kyberuhkia koskevia säädöksiä. Kyberhyökkäyksiin liittyvät penetraatiotestaukset eivät ole lentokelpoisuuden vaatimuksissa esillä.

Kokisin, että ICAO:n, Euroopassa EASA:n, ja Pohjois-Amerikassa CISA:n täytyisi tuoda esille sekä asettaa pikimmiten lentokelpoisuustesteihin lentojärjestelmien penetraatiotestaus ja arviointi hyökkäysten todennäköisyydestä.

Teknologian kehittyessä ennenkuulumatonta vauhtia on ensisijaisen tärkeää luoda viitearvot ja rajat sille, kuinka resilienttejä lentokoneiden ja järjestelmien tulee olla hyökkäyksille. Lentoyhtiöt ovat tehneet hyvää työtä, sillä he ovat suorittaneet omatoimisesti lentojärjestelmille penetraatiotestausta, mutta mielestäni sen tulisi olla osa lentokelpoisuustestiä.

Lentokonevalmistajien tulisi myös mielestäni katsoa suurennuslasin kera lentokoneisiin varustettua matkustajille tarkoitettua langatonta verkkoa. Voi olla, että kaikkia verkossa olevia järjestelmiä ei välttämättä ole eritelty toisistaan tarvittavilla toimenpiteillä, joka vaarantaa sekä matkustajien laitteiden tietoturvan mutta myös pahimmassa tapauksessa koko lentokoneen verkon.

Loppukäyttäjien, eli työntekijöiden kouluttaminen kyberturvallisuuden perusteisiin on nostettava korkeammalle tasolle. Nykyhetkellä liian moni vuosittain tapahtuvista tietomurroista on saanut alkunsa inhimillisestä virheestä tai huolimattomuudesta.

## 6.3 Yhteenveto

Lentoyhtiöt ovat pääsääntöisesti hyvin ajan tasalla kyberturvallisuuden hallinnasta ja siihen liittyvistä standardeista ja viitekehyksistä. Euroopan alueella vaalitaan korkeaa kyberturvallisuuden tasoa, joka on mielestäni erittäin hyvä ja kunnioitettava asia.

Datamurtoja tapahtuu hälyttävän useasti etenkin muutaman viime vuoden aikana. Murroissa on kuitenkin hopeareunukset, sillä jokaisesta tietomurrosta voidaan oppia uutta ja kehittää ympäristöä entistä varmemmaksi.

Oma huoleni lentoliikenteen turvallisuudesta pohjautuu lentokonevalmistajien lentokelpoisuustesteistä puuttuvaan säädökseen siitä, ettei penetraatiotestausta vaadita kelpoisuuden saavuttamiseksi.

Kyberturvallisuuden opiskelu ja kouluttautuminen on myös vajaavaisella tasolla. Koen, että lentoyhtiöillä olisi suuri velvoite kouluttaa omat työntekijänsä asianmukaisella ja riittävän kattavalla materiaalilla paremmiksi kyberturvallisuuden perusteiden osaajiksi.

# Lähteet

ACARS. 2023. Wikipedia. Viitattu 03.02.2024. https://fi.wikipedia.org/wiki/ACARS

Airbus A350 XWB. 2024. Wikipedia. Viitattu 24.01.2024. https://fi.wikipedia.org/wiki/Airbus_A350_XWB

Air Europa suffers credit card data breach. 2023. Airport Technology. Julkaistu 10.10.2023. Viitattu 05.02.2024. https://www.airport-technology.com/news/air-europa-credit-card-data-breach/

Annual report. 2020. Royal Jordanian, 40. Viitattu 05.02.2024. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiOrq6Pqp-EAxWfExAIHfwtBugQFnoECA8QAQ&url=https%3A%2F%2Fwww.rj.com%2F-%2Fmedia%2FFinance%2FAnnual-Report%2FAnnual-Report-2020-English.pdf%3Frev%3D-1%26hash%3D79511888C543E01B6F027A8CBC016D23&usg=AOvVaw3BOhdgE69OUHdA2y6NYCak&opi=89978449

Annual report. 2017. Vietnam Airlines, 125. Viitattu 05.02.2024. https://www.vietnamairlines.com/~/media/FilesDownload/AboutUs/Investor-Relations/Bao-Cao-Thuong-Nien/bao-cao-thuong-nien-2017-english.pdf

Annual and Sustainability Report. 2022. Icelandair. Viitattu 04.02.2024. https://annualreport2022.icelandairgroup.is/sustainability/corporate-governance/

Automatic Dependent Surveillance – Broadcast. 2024. Wikipedia. Viitattu 02.02.2024. https://en.wikipedia.org/wiki/Automatic_Dependent_Surveillance–Broadcast

Aviation with purpose. 2022. Ryanair, 38-39. Viitattu 03.02.2024. https://corporate.ryanair.com/wp-content/uploads/2022/07/Ryanair-2022-Sustainability-Report-Interactive.pdf#page=40&zoom=100,0,0

Boeing 777. 2023. Wikipedia. Viitattu 25.01.2024. https://fi.wikipedia.org/wiki/Boeing_777

Citizens of the World. 2021. Air Canada. Viitattu 05.02.2024. https://www.aircanada.com/content/dam/aircanada/portal/documents/PDF/en/corporate-sustainability/2021-cs-report.pdf

Corporate Responsibility Report. N.d. United. Viitattu 05.02.2024. https://crreport.united.com/governance/cybersecurity

Current Risk Management Practices. N.d. NIST. Viitattu 05.02.2024. https://www.nist.gov/system/files/documents/2017/06/01/041213_american_airlines.pdf

Cyber Security at Air New Zealand. N.d. Air New Zealand. Viitattu 05.02.2024. https://www.airnewzealand.com.au/cyber-security

Cyber Security Policy. N.d. The Emirates Group. Viitattu 05.02.2024. https://www.theemiratesgroup.com/assets/pdf/Cyber_Security_Ambition_Policy.pdf

Digital Safety. 2023. EasyJet, 2-3. Viitattu 04.02.2024. https://corporate.easyjet.com/files/esg/Digital-Safety-ESG-Factsheets_230421.pdf

Durgut, M. 2020. PSR – SSR principles, advantages, limitations. Aviationfile 27.05.2020. Viitattu 02.02.2024. https://www.aviationfile.com/psr-ssr-principles-advantages-limitations/

ESA. 2021. Aviation Applications. Viitattu 06.02.2024. https://gssc.esa.int/navipedia/index.php/Aviation_Applications

Eurocontrol. Satellite communications datalink. Viitattu 25.01.2024 https://www.eurocontrol.int/system/satellite-communications-datalink

Euroopan unionin kyberturvallisuusvirasto (ENISA). N.d. Euroopan Unioni. Viitattu 05.01.2023. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_fi

EUSPA. 2023. ”What is GNSS”. Viitattu 20.01.2024. https://www.euspa.europa.eu/european-space/eu-space-programme/what-gnss

FAA. 2023. Airworthiness certification. Viitattu 06.02.2024. https://www.faa.gov/aircraft/air_cert/airworthiness_certification

FAA. 2022. Benefits. Viitattu 21.01.2024. https://www.faa.gov/air_traffic/technology/equipadsb/capabilities/benefits

Fly-by-wire. 2024. Wikipedia. Viitattu 02.02.2024. https://en.wikipedia.org/wiki/Fly-by-wire

FTC, 2018. The NIST cybersecurity framework. Viitattu 04.01.2024. https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework

General Terms & Conditions. N.d. Pegasus, 2.10.2. Viitattu 05.02.2024.
https://www.flypgs.com/en/useful-info/info-about-flights/general-rules

“HF, VHF and UHF: What does it all mean?”. N.d. Barrett. Viitattu 02.02.2024.
https://www.barrettcommunications.com.au/news/hf-vhf-and-uhf-what-does-it-all-mean/

IATA. N.d. Current Airline Members. Viitattu 02.02.2024.
https://www.iata.org/en/about/members/airline-list/

ICAO. 2022. Cybersecurity Culture in Civil Aviation. Viitattu 27.02.2024.
https://www.icao.int/aviationcybersecurity/Documents/Cybersecurity%20Culture%20in%20Civil%20Aviation.EN.pdf

ICAO. 2014. Definition of Aircraft Domains. Viitattu 26.01.2024.
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwijnLL-5oSEAxXlDRAIHeHWDOkQFnoECA8QAw&url=https%3A%2F%2Fwww.icao.int%2Fsafety%2Facp%2Facpwgf%2Facp-wg-s-web%2520meeting%25205%2Facp-wg-s_wp02%2520definitions%2520of%2520various%2520aircraft%2520domains.docx&usg=AOvVaw0ZWgZ1gWnX6qdk3fkBbRTI&opi=89978449

Information Security. N.d. ANA Group. Viitattu 05.02.2024.
https://www.ana.co.jp/group/en/csr/risk_management/security/

Information Security. N.d. Japan Airlines. Viitattu 05.02.2024.
https://www.jal.com/en/sustainability/governance/riskmanagement/information-security/

Information Security Policy. N.d. Avianca. Viitattu 05.02.2024.
https://www.avianca.com/en/legal-information/information-security-and-cybersecurity-policy/

Information Security Policy. N.d. Turkish Airlines. Viitattu 04.02.2024.
https://www.turkishairlinesholidays.com/en-tr/information-security-policy

Instrument landing system. 2024. Wikipedia. Viitattu 02.02.2024.
https://en.wikipedia.org/wiki/Instrument_landing_system

Jussila, A. N.d. ISO/IEC27001. Viitattu 14.12.2023.
https://www.mv.helsinki.fi/home/jussantt/arkkitehtuuri/iso27001.html

Kyberturvallisuus. 2022. Wikipedia. Viitattu 21.11.2023.
https://fi.wikipedia.org/wiki/Kyberturvallisuus

Laukkanen, J. 2023. ”Finnairin lennot joutuneet häirinnän kohteeksi nyt Lähi-Idässäkin”. Iltalehti 26.10.2023. Viitattu 20.01.2024. https://www.is.fi/kotimaa/art-2000009948827.html

Lufthansa Group receives ISO 27001 information security management system certification. 2020. CAPA. Julkaistu 17.01.2020. Viitattu 03.02.2024. https://centreforaviation.com/news/lufthansa-group-receives-iso-27001-information-security-management-system-certification-969213

Malaysia Airlines receives ISO 27001 certification for information security management system. 2013. CAPA. Julkaistu 22.07.2013. Viitattu 05.02.2024. https://centreforaviation.com/news/malaysia-airlines-receives-iso-27001-certification-for-information-security-management-system-248084

Marsh, R. 2015. Hackers successfully ground 1,400 passengers. CNN 22.6.2015. Viitattu 20.11.2023. https://edition.cnn.com/2015/06/22/politics/lot-polish-airlines-hackers-ground-planes/index.html

O’Driscoll, A. The role of human error in cybersecurity: what the stats tell us. 2024. Viitattu 22.02.2024. https://www.comparitech.com/blog/information-security/human-error-cybersecurity-stats/

Our Privacy Policy. N.d. Air Transat. Viitattu 05.02.2024. https://www.airtransat.com/en-CA/legal-notice/privacy-policy

Privacy and security. 2023. Qantas. Viitattu 05.02.2024. https://www.qantas.com/au/en/support/privacy-and-security.html

Proofpoint. 2020. User risk report. Viitattu 22.02.2024. https://www.proofpoint.com/sites/default/files/2020-05/gtd-pfpt-us-tr-user-risk-report-2020_0.pdf

Qatar Airways Achieves IT Service Management System Excellence Certification. 2023. Qatar Airways. Julkaistu 17.09.2023. Viitattu 05.02.2024. https://www.qatarairways.com/press-releases/en-WW/229993-qatar-airways-achieves-it-service-management-system-excellence-certification

Security as a corporate culture. N.d. Artikkeli Lufthansan sivuilla. Viitattu 20.12.2023. https://www.lufthansa-cargo.com/ci/security

Sustainability report. 2022. Singapore Airlines. Viitattu 05.02.2024. https://www.singaporeair.com/saar5/pdf/Investor-Relations/Annual-Report/sustainabilityreport2122.pdf

Sustainable Development Report. 2019. Cathay Pacific. Viitattu 05.02.2024. https://sustainability.cathaypacific.com/wp-content/uploads/2020/06/Cathay-Pacific-SD-Report-2019_EN.pdf

Sustainable Development Report. 2017. Aegean. Viitattu 04.02.2024. https://en.about.aegeanair.com/Magazine-issue/CSR-Report-2017-en/offline/download.pdf

Sustainability and annual report. 2022. AirBaltic. Viitattu 04.02.2024. https://www.airbaltic.com/sustainability/report/2022/airBaltic_Sustainability_Annual_Report.pdf

Sustainability report. 2015. TAP Group, 21. Viitattu 05.02.2024. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi334jjl5-EAxW9HRAIHe0-AHoQFnoECA8QAQ&url=https%3A%2F%2Fwww.tapairportugal.com%2Fen%2F-%2Fmedia%2FInstitucional%2FPDFs%2FAnual-reports%2F2015%2FRS_2015_EN.pdf%3Fla%3Den%26hash%3D8B419BAE4760FCE78085A761018A53095EC1544E&usg=AOvVaw0N0eUbZhFoNooChDeRNbSh&opi=89978449

Suurimmat riskit. 2018. Artikkeli Finnairin sivuilla. Viitattu 07.12.2023. https://investors.finnair.com/fi/governance/risk-management/major-risks

Swiss-AS now certified according ISO/IEC 27001. 2020. Swiss. Julkaistu 26.04.2021. Viitattu 05.02.2024. https://www.swiss-as.com/news-events/news/swiss-as-now-certified-according-isoiec-27001

The ITA Airways sustainability manifesto. N.d. Artikkeli ITA Airwaysin sivuilla. Viitattu 04.02.2024. https://www.ita-airways.com/en_gb/fly-ita/ita-world/sustainability.html

Traffic collision avoidance system. 2024. Wikipedia. Viitattu 02.02.2024. https://en.wikipedia.org/wiki/Traffic_collision_avoidance_system

Traficom. 2023. Ilmailun kyberturvallisuutta koskeva lainsäädäntö. Viitattu 06.02.2024. https://www.traficom.fi/fi/liikenne/ilmailu/ilmailun-kyberturvallisuutta-koskeva-lainsaadanto?toggle=Mitä%20tarkoitetaan%20tietojärjestelmien%20turvallisuudella

Universal Registration Document 2022. 2022. AirFranceKLM Group, 193-194. Viitattu 04.02.2024. https://www.airfranceklm.com/sites/default/files/2023-04/AFK_URD_2022_VA_24-04-23.pdf

Vastuullisuusraportti. 2018. Finnair. Viitattu 04.02.2024. https://investors.finnair.com/~/media/Files/F/Finnair-IR/documents/fi/reports-and-presentation/2019/finnair-vastuullisuusraportti-2018.pdf

Yhdysvaltain standardisointi- ja teknologiainstituutti. 2022. Wikipedia. Viitattu 04.01.2023. https://fi.wikipedia.org/wiki/Yhdysvaltain_standardisointi-_ja_teknologiainstituutti

Wizz Air at a glance. 2023. Wizz Air Holdings PLC, 68. Viitattu 04.02.2024. https://wizzair.com/static/docs/default-source/downloadable-documents/corporate-website-transfer-documents/annual-reports/wizz_air-annual-report-and-accounts-f23-final_e93a9644.pdf