



LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Viestintäverkkojen ja -palveluiden toimivuuden ja tietoturvallisuuden häiriönhallinta

Paananen, Rauli

2017 Laurea



Laurea-ammattikorkeakoulu

Viestintäverkkojen ja -palveluiden toimivuuden ja tietoturvallisuuden häiriönhallinta

Rauli Paananen
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Toukokuu, 2017

Paananen, Rauli

Viestintäverkkojen ja -palveluiden toimivuuden ja tietoturvallisuuden häiriönhallinta

Vuosi 2017 Sivumäärä 46

Yhteiskunnassa on käynnissä voimakas kaiken mahdollisen digitalisoiminen ja esimerkiksi kaikkia viranomaisia koskee velvollisuus sähköistää keskeiset palvelunsa kuluttajien saataville. Sähköinen asiointi, palveluiden kasvava määrä ja kuluttajien siirtyminen mobiili- ja verkkopalveluihin luo markkinoille uusia innovaatioita ja tuo kansalaisille arjen sujuvuutta hoitaa päivittäisiä asioitaan, ajasta ja paikasta riippumatta. Toisaalta yhteiskunnan toimivuus on entistä haavoittuvampi ja alttiimpi erilaisille tietoturvauhille ja häiriöille. Tietoverkkorikollisuus on voimakkaassa kasvussa, viestintäverkkojen fyysiset komponentit vikaantuvat ja laiterikot ovat aina mahdollisia, joiden lisäksi hätä- ja turvallisuusliikenne voi kärsiä radiohäiriöistä.

Viestintävirasto on keskeisessä roolissa varmentamassa yllä kuvattua digitaalista yhteiskunnan muutosta. Viestintäviraston lakisääteisiin tehtäviin kuuluu muun muassa varmistaa radiotaajuuksien riittävän häiriötön käyttö, turvata viestintäverkkojen ja -palveluiden toimintavarmuutta ja huolehtia siitä, että teleyritykset hoitavat palvelunsa tietoturvallisesti.

Tämän opinnäytetyön kvalitatiivisen ja toiminnallisen tutkimuksen tarkoituksena on lisätä ymmärrystä Viestintäviraston häiriönhallinnasta ja mallintaa viraston kahden eri toimialan, Kyberturvallisuuskeskus ja Taajuushallinto, nykyistä häiriönhallintaprosessia, tulkita valmiina olevia ohjeistuksia ja löytää häiriönhallinnalle yhteismitallinen käsittelytapa ja raportointi. Tutkimuksella on myös eksploratiivinen eli etsinnällinen tavoite jonka yhtenä tarkoituksena on kehittää Viestintäviraston kyberturvallisuuden varmistaminen -prosessia. Prosessin on tarkoitus olla osa viraston kehittyvää toimintaa ja tutkimuksen avulla voidaan löytää jatkotutkimuskysymyksiä häiriönhallinnasta.

Opinnäytetyön tietoperusta pohjautuu pääsääntöisesti julkisiin asiakirjoihin, asiaa koskevaan lainsäädäntöön, kansainvälisen televiestintäliiton Radio-ohjesääntöön sekä Viestintäviraston määräyksiin ja ohjeistuksiin. Tiedonkeruu suoritettiin strukturoidun ja teemahaastattelun yhdistelmänä. Työssä haastateltiin Viestintäviraston Taajuushallinnon asiantuntijoita. Kyberturvallisuuskeskuksen osalta tietopohja perustuu osin opinnäytetyön kirjoittajan kokemukseen.

Opinnäytetyön tutkimuksen perusteella voidaan todeta, että viestintäverkkojen ja -palveluiden toimivuuden ja tietoturvallisuuden häiriönhallintaan liittyvät prosessit eivät ole riittävän yhtenäisiä Viestintävirastossa. Häiriönhallintaan liittyvä ohjeistus on riittävää toimialakohtaisesti, mutta ohjeistusta, häiriönhallintaan liittyvää termistöä ja menettelytapoja tulisi yhtenäistää laadukkaamman lopputuloksen varmentamiseksi. Toimintatapojen osalta erityisesti Taajuushallinnossa menettely oli jossain määrin henkilöriippuvaista, joka saattaa muodostaa pullonkaulan ja riskin häiriöiden ratkaisemisessa.

Tutkimuksen perusteella olisi syytä kyberturvallisuuden varmistaminen -prosessin avulla luoda yhtenäinen ohjeisto Viestintävirastoon. Laadullisesti varmistettu prosessi on erityisen tärkeä niissä tilanteissa, joissa Viestintävirasto raportoi häiriöistä sidosryhmilleen.

Asiasanat: Esineiden internet, Kyber, Radiohäiriö, Tietoturvallisuus

Paananen, Rauli

Incident Management as a Means to Ensure the Functionality and Information Security of Communications Networks and Services

Year 2017 Pages 46

The digitalisation of our society is rapid and, for example, all public authorities must make their key services available to consumers electronically. Electronic access to services, the increasing number of services and consumers switching to mobile and online services create new innovations in the markets and improve the daily lives of citizens as they can access services regardless of time and place. On the other hand, the society's functioning is increasingly vulnerable to various information security threats and incidents. Cybercrime is on the rise, physical components of communications networks fail, equipment breaks down, and distress and safety communication may suffer from radio interference.

The Finnish Communications Regulatory Authority (FICORA) has an important role in securing the evolution of the digital society described above. FICORA's statutory duties include ensuring sufficiently interference-free use of radio spectrum, securing the operational reliability of communications networks and services, as well as monitoring the information security of telecommunications operators' services.

The purpose of the qualitative and functional research carried out is to increase the understanding of FICORA's incident management and to model the current incident management process in two of FICORA's divisions, the National Cyber Security Centre Finland (NCSC-FI) and Spectrum Management, as well as to interpret the existing guidelines and to propose a uniform approach and reporting system for incident management. The research is also partly exploratory: one objective is to improve FICORA's process of ensuring cyber security. The process is intended to be included in the development of FICORA's activities.

The framework of reference covers public documents and legislation on the matter, the Radio Regulations of the International Telecommunication Union (ITU) as well as FICORA's regulations and guidelines. The research data was gathered by combining structured and focused interview techniques. Specialists in Spectrum Management were interviewed.

Based on the research, it can be concluded that FICORA's incident management processes related to the functionality and information security of communications networks and services are not sufficiently uniform. Each division has adequate guidelines on incident management but guidelines, terminology and procedures should be harmonised to ensure a high-quality outcome. In Spectrum Management, in particular, the procedures are somewhat dependent on a person, which may become a bottleneck and a risk in incident management.

The research indicates that there is a need for creating uniform guidelines in FICORA using the process of ensuring cyber security. A process of assured quality is especially critical when FICORA reports incidents to its stakeholders.

Keywords: Cyber, Information security, Internet of Things, Radio interference

Sisälllys

1	Johdanto	7
2	Keskeiset käsitteet ja terminologia	9
2.1	Radiotaajuudet	9
2.2	Häiriötyypit.....	11
2.2.1	Teleyritys	12
2.2.2	Verkkopalvelu ja viestintäverkko.....	12
2.2.3	Radiohäiriöt.....	12
2.2.4	Yleisten viestintäverkkojen ja -palveluiden toimintavarmuuden häiriötilanteet	12
2.2.5	Yleisten viestintäverkkojen ja -palveluiden tietoturvahäiriö.....	13
3	Viestintäviraston toiminta	13
4	Viestintäviraston ydinprosessit.....	14
5	Maailman puhtaimmat verkot	16
5.1	Taajuuksien merkitys digitalisaatiolle.....	17
5.2	Mobiiliverkkojen kattavuus	17
6	Tutkimuksen perusteet	18
6.1	Radiotaajuusmääräys (M4)	18
6.2	Viestintäviraston määräys teletoiminnan häiriötilanteista (M 66).....	19
6.3	Määräys teletoiminnan tietoturvasta (M67)	19
7	Tutkimuskysymykset ja aiheen rajausta	19
7.1	Tutkimusmenetelmät ja tutkimusteoria	20
7.2	Lähdeaineisto	21
8	Häiriönhallinnan nykytila Kyberturvallisuuskeskuksessa ja Taajuushallinnossa	21
8.1	Häiriönhallinnan toimintamalli ja häiriöiden selvittämisen prioriteetit Taajuushallinnossa	21
8.1.1	Tiedonkulku ja laadun varmistaminen Taajuushallinnossa	22
8.1.2	Raportointimallit Taajuushallinnossa	23
8.2	Kyberturvallisuuskeskuksen yhteistyöverkostotoiminta.....	23
8.3	Häiriönhallinnan toimintamalli Kyberturvallisuuskeskuksessa	24
8.3.1	Häiriöiden selvittämisen prioriteetit Kyberturvallisuuskeskuksessa	24
8.3.2	Laadun varmistaminen Kyberturvallisuuskeskuksessa	25
8.3.3	Tiedonkulku Kyberturvallisuuskeskuksessa	27
9	Kyberturvallisuuskeskuksen toiminnan ja prosessien tuntemus	28
10	Asiantuntijahaastattelut	29
10.1	Haastatteluiden tavoiteasetanta	29
10.1.1	Hätä- ja turvallisuusradioliikenteen määrittelmä	30
10.1.2	Hätä- ja turvallisuusradioliikenteen asiakkaiden priorisointi.....	30

10.1.3	Tulossopimustavoitteen toimivuus	31
10.1.4	Radiohäiriöilmoitusten vastaanotto	31
10.1.5	Tiedon jakaminen hätä- ja turvallisuusradioliikenteen häiriöistä	32
10.1.6	Häiriötapauksen vaikutusarvio	32
10.1.7	Häiriötapauksen omistaja.....	32
10.1.8	Sidosryhmäyhteistyö.....	33
10.1.9	Häiriöselvityksen tilannekuvan jakaminen	33
10.1.10	Virka-apupyynnön tekeminen	33
10.1.11	Häiriöistä tiedottaminen Viestintäviraston ulkopuolelle	33
10.2	Haastattelujen yhteenveto	34
11	Johtopäätökset	34
12	Oman työn arviointi	37
12.1	Luotettavuuden arviointi	37
12.2	Jatkotutkimusaiheet	38
	Lähteet.....	40
	Kuviot.. ..	43
	Liitteet	44

1 Johdanto

Viestintäala on ollut lähes jatkuvassa muutoksessa viimeisen yli parinkymmenen vuoden ajan ja muuttuu yhä. Muutos eteni ensin radio- ja televisioverkkojen digitalisointina, matkaviestinverkkojen teknologian nopeana muutoksena, Internetin ja dataliikenteen vahvana käytön sekä sähköisen asiointin ja kaupankäynnin kasvuna. Murrosta jatkavat edelleen globaalit trendit kuten esineiden Internet eli IoT-sovellukset (Internet of Things), keinoäly, automatisaatio, robotisaaatio, 5G-teknologia ja kaikkien mahdollisten laitteiden kytkeytyminen verkkoon. Nämä globaalit ilmiöt ovat tuoneet mukanaan kysymyksiä sähköisten palveluiden käyttöön kohdistuvasta luottamuksesta, yksityisyyden suojasta, omien tietojen hallinnasta sekä laitteiden että palveluiden tietoturvallisuuden huolehtimisesta.

Internetin käyttäjien räjähdysmäinen kasvu, verkkoon liitettävien laitteiden voimakas lisääntyminen ja kaiken mahdollisen digitalisoituminen lisää valtaviin hyötyjen ohella myös riskejä (Valtiovarainministeriö 2016). Tietoturvallisuuteen liittyvät riskit täytyy tunnistaa ja etenkin palveluiden jatkuvuuden turvaaminen tulee varmistaa. Samoin tiedon oikeellisuus ja eheys kaikissa prosesseissa on entistä tärkeämpää. Edellä kuvatut globaalit ilmiöt muuttavat myös tieto- ja kyberturvallisuuden tilannekuvaa. Viestintäviraston raportti Tietoturvan vuosi 2016 kuvaa keskeisempiä tietoturvailmiöitä ja riippuvuuttamme tietoverkoista ja tietojärjestelmistä.

Pysyväksi ilmiöksi tietoturvallisuuden saralla on jäänyt kukoistava nettihuijaus- ja kalastelubisnes. Suomalaisilta kansalaisilta ja yrityksiltä viedään vuosittain erilaisilla huijausmenetelmillä miljoonia euroja rahaa. Haittaohjelmat ovat raportin mukaan muuttuneet yhä enenevässä määrin kiristyshaittaohjelmiksi, joiden tartuntojen määrä Suomessa on kasvussa. Haittaohjelmien tartuttaminen perustuu siihen, että käyttäjä uskoo huijaussähköpostiin ja avaa saastuneen haittaohjelman sisältävän liitetiedoston tai linkin. Käynnistyessään kiristyshaittaohjelma salaa käyttäjän koneen tiedostot ja pyytää käyttäjältä lunnaita tiedostojen vapauttamista varten. Tietoverkkovakoilu ja kohdistetut hyökkäykset koskettavat yhä useampaa organisaatiota. Suomessa verkkovakoilu kohdistuu todennäköisemmin poliittiseen päätöksentekoon, ulkoasiain- ja puolustushallintoon sekä yhteiskunnan kannalta kriittistä tietoa tuottaviin yrityksiin. (Viestintävirasto 2017a.)

Uutena ilmiönä lokakuussa 2016 nähtiin volyyymiennätyksen lyönyt Mirai-bottiverkon palvelunestohyökkäys. Palvelunestohyökkäyksen voima oli ennätyksellinen yli terabitti sekunnissa. Mirai-haittaohjelma murtautui erilaisiin verkkoon kytkeytyneisiin avoimiin laitteisiin (IoT), joiden tunnus ja salasana yhdistelmä oli tehdasasetteinen tai helposti arvattava. Saastuneiden laitteiden avulla muodostettiin niin sanottu bottiverkko, joka valjastettiin samanaikaisesti liikennöimään samaan kohteeseen aiheuttaen valtavan

palvelunestöhyökkäyksen. Edellä kuvattuihin ilmiöihin liittyy kasvava kyberrikollisuus, joka muuttaa ilmiöitä entistä ammattimaisemmiksi ja nopeasti muuttuviksi. (Viestintävirasto 2017a.)

Tietoturvan vuosi 2016-raportti arvioi myös suomalaisia viestintäverkkoja ja sen mukaan matkaviestin- ja joukkoviestintäverkkojen tila on melko hyvä. Vuonna 2016 Viestintävirasto sai teleyrityksiltä yhteensä 151 ilmoitusta merkittävästä toimivuushäiriöstä. Niistä vakavia ja laajoja oli 20 kappaletta. Fyysisille verkoille häiriöitä aiheuttavat eniten vikaantuneet laitteet, myrskyjen aiheuttamat sähkökatkot ja ohjelmistoviat (Viestintävirasto 2017a).

Kyberturvallisuuden ja fyysisten verkkojen häiriöiden lisäksi viestintäalaa muuttaa viestintämarkkinoiden ja verkkojen kehitys. Verkkojen osalta halutuimmat ja kustannustehokkaimmat taajuudet ovat valtaosin jo yhteiskunnan erilaisten langattomien verkkojen käytössä. Taajuuksien riittävän häiriötön suunnittelu ja taajuuksien yhteiskäyttö tulee olemaan tulevaisuudessa yhä monimutkaisempaa ja haastavampaa. Kuluttajien käyttötottumukset muuttuvat digitalisoitumisen myötä ja trendinä on erilaisten hyöty- ja viihdesovelluksien voimakas kasvu.

Myös verkoissa olevien laitteiden määrän on ennakoitu kasvavan rajusti ja siten vaikuttavan merkittävästi verkoissa siirretyn tiedonsiirtomäärän kasvuun. Vuonna 2016 suomalaisissa matkaviestinverkoissa siirrettiin tietoa keskimäärin noin 16 gigatavua kuukaudessa henkilöä kohden, mikä on maailmanlaajuisestikin poikkeuksellisen suurta (Viestintävirasto 2017a).

Osa verkossa olevista laitteista on organisaatioiden suljetuissa verkoissa ja niistä tietää vain yritys itse, tästä syystä tilastoinnin tekeminen on käytännössä hankalaa. Esimerkiksi Gartner Reseach on ennustanut, että vuoteen 2020 mennessä maailmassa olisi 20,8 miljardia Internetiin kytkettyä laitetta ja toisaalta huimimmat ennusteet viittaavat siihen, että vuoteen 2020 mennessä Internetiin kytkettyjä laitteita olisi jopa 75 miljardia kappaletta. (RCRWirelessNews. 2017.) Suomessakin yksistään niin kutsuttuja M2M-liittymiä, Machine-to-Machine eli koneiden välinen viestintä, ja arviolta saman verran niiden kautta verkkoon kytkettyjä muita laitteita, oli vuoden 2015 lopussa reilusti yli 1 miljoonaa kappaletta (Viestintävirasto 2015a). M2M-liittymät ja niiden kautta verkkoon liitetyt laitteet edustavat kuitenkin todennäköisesti vain osaa verkkoon liitettyjen laitteiden määrästä, sillä pohjoismaissa M2M laitteita on arvioitu olevan yli 100 miljoonaa kappaletta (Iltasanomat 2015).

Sähköinen asiointi, sähköisten palveluiden kasvava määrä ja kuluttajien siirtyminen mobiili- ja verkkopalveluihin kasvattaa tulevina vuosina edelleen sekä langattomien että kiinteiden laajakaistaverkkojen kapasiteettitarvetta. Taajuuksien käytön osalta myös globaali ilmiö eli

esineiden internet vaatii ennen kaikkea toimintavarmoja, tietoturvallisia ja häiriöttömiä yhteyksiä.

Pitkäjänteisellä ja suunnitelmallisella kansallisella taajuussuunnitelulla ja kansainvälisellä sopimisella taajuuksien käytöstä, pyritään turvaamaan yhteiskunnan toimintavarmuuden kannalta kriittisten järjestelmien riittävän häiriötön käyttö. Kriittisiksi järjestelmiksi voidaan luonnehtia sellaisia järjestelmiä, joissa on kyse hätä- ja turvallisuusradioliikenteen turvaamisesta.

Tämän opinnäytetyön tarkoituksena on osaltaan kehittää ja yhtenäistää Viestintäviraston häiriönhallintaprosessia siten, että viraston eri tyyppistä häiriönhallintaa tekeville toimialoille, Taajuushallinto ja Kyberturvallisuuskeskus, on yhtenäinen tapa toteuttaa digitalisoituvan yhteiskunnan häiriöttömyyttä laadukkaasti ja dokumentoidusti.

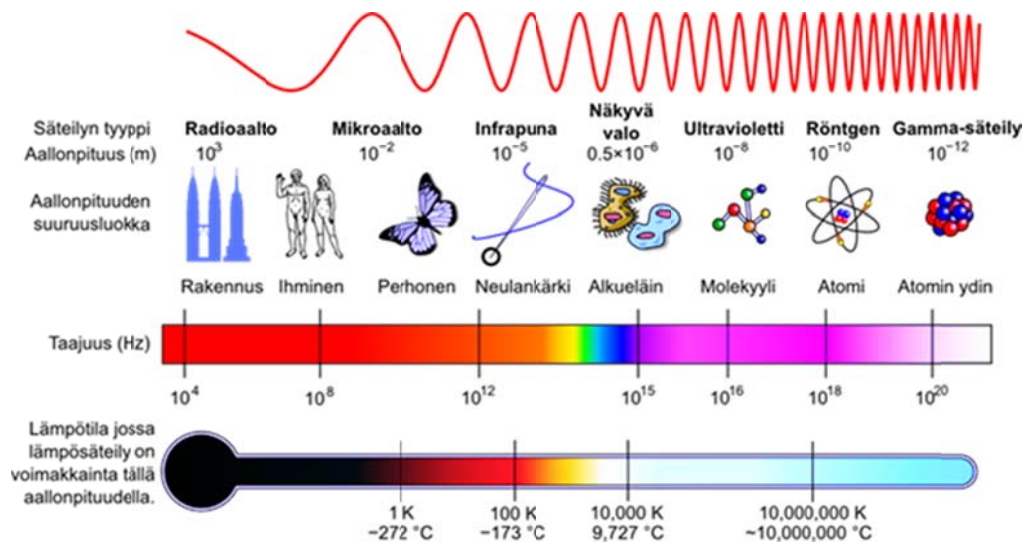
2 Keskeiset käsitteet ja terminologia

Tässä opinnäytetyössä käsitellään terminologiaa, joka ei ole tavanomaisessa arkikielessä tuttua. Viranomaisen yksi tärkeimmistä ja haastavimmista tehtävistä onkin tuottaa sellaista tekstiä, joka olisi ymmärrettävää ja selkeää. Tämän opinnäytetyön termit liittyvät ammatillisesti radiotekniikkaan ja tietoliikennetekniikkaan. Molemmille ammattialoille on tunnusomaista se etteivät keskeiset termit, kuten radiotaajuudet tai tietoturvaloukkaus, niiden kaikkine erilaisine piirteineen ole käsinkosketeltavia, vaan niistä syntyvä ymmärrys on kuvailtava hyötyjen ja haittojen kannalta.

2.1 Radiotaajuudet

Taajuus on fysikaalinen suure, joka kuvaa jonkin toistuvan ilmiön tapahtumien määrää aikayksikköä kohti. Taajuutta merkitään tunnuksella f ja sen yksikkö on $1/s$, tätä kutsutaan nimellä hertsi ja merkitään tunnuksella Hz. Taajuus voidaan ilmoittaa myös aallonpituutena. Aallonpituus on paikan suhteen jaksollisen ilmiön samassa vaiheessa olevan pisteen välinen etäisyys, esimerkiksi siniaallon kahden aallonharjan välinen välimatka. (Äänipää 2005.)

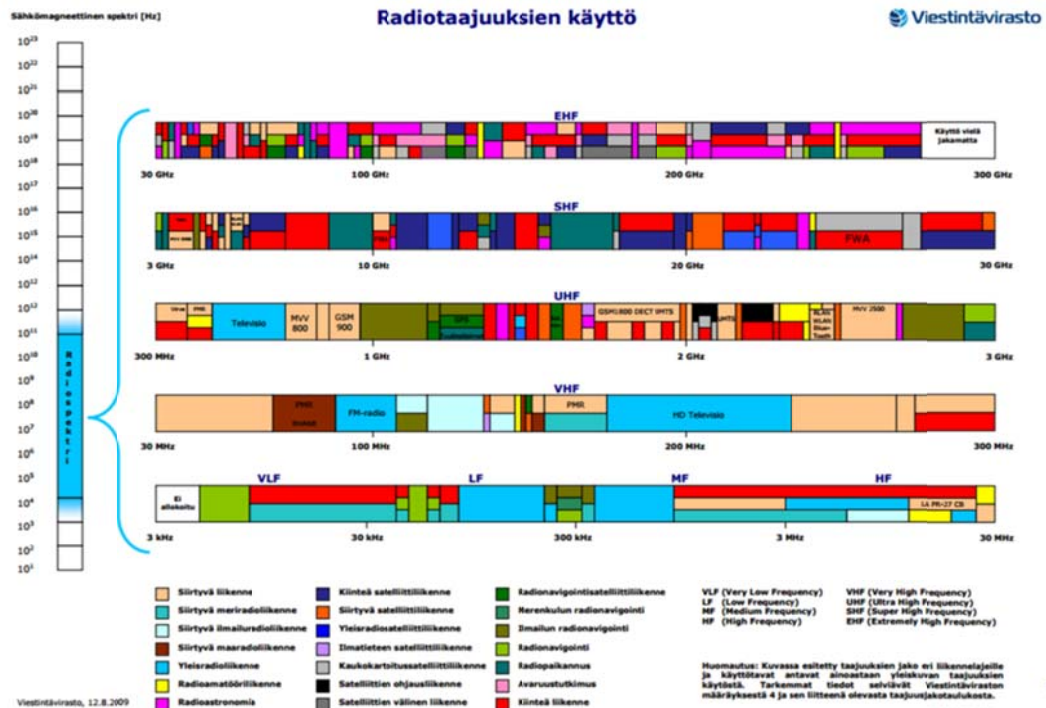
Sähkömagneettisen spektrin osat kuvataan usein niiden säteilyn taajuutena tai aallonpituutena. Näkyvä valo, jonka ihminen pystyy näkemään, löytyy sähkömagneettisen spektrin taajuusalueelta 380-750 THz eli aallonpituutena 400-700 nm (Kuvio 1). Tämä on vain pieni osa kaikesta sähkömagneettisesta säteilystä. Sähkömagneettinen spektri voidaan jaotella osiin alla olevan kuvan mukaisesti. Tässä opinnäytetyössä keskitytään radioaaltoihin eli radiotaajuuksiin, jotka omaavat suurimman aallonpituuden. Muut sähkömagneettisen spektrin osat ovat mikroaallot, infrapunasäteily, näkyvä valo, ultraviolettisäteily, röntgensäteily ja gammasäteily. (Otavan Opisto 2015.)



Kuvio 1: Sähkömagneettinen spektri (Otavan opisto 2015)

Fysikaalisten ominaisuuksiensa mukaisesti radiotaajuudet ovat luonnonvara, jotka eivät kulu eivätkä vähene käytössä, eikä niitä myöskään ilmaannu lisää. Kaikki viestintäverkot hyödyntävät radiotaajuuksia, oli kyse sitten kaupallisista matkaviestinverkoista, viranomaisverkoista tai yksittäisten yritysten omista radioverkoista. Radiotaajuudet siirtävät viestintäverkkojen välityksellä sähköisessä muodossa tekstiä, puhetta, kuvaa ja erilaisia palveluita. Radiotaajuudet ovatkin jatkuva taloudellisen ja poliittisen mielenkiinnon kohde. (HE 80/2001 s.1.)

Suomessa kansallinen radiotaajuuksien käyttö on määritelty Viestintäviraston radiotaajuusmääräyksessä 4. Sen rakenne noudattaa kansainvälisen televiestintäliiton Radio-ohjesäännön mukaista taajuuksien käyttöä, jossa taajuudet on määritelty alueellisesti tai maailmanlaajuisesti tietyille liikennelajeille. Taajuuksien maailmanlaajuisesta käytöstä sovitaan kerran neljässä vuodessa ITU:n maailman radiotaajuuskonferenssissa (World Radio Conference, WRC). Taajuuksien käytöstä saa parhaimman taloudellisen hyödyn, kun niiden häiriöttömästä käytöstä on sovittu maailmanlaajuisesti. Tämä tarkoittaa esimerkiksi päätelaitteiden vapaata kulkua yli maan rajojen. Näin on esimerkiksi pääosa matkaviestinverkkojen taajuuksista suunniteltu ja voimme käyttää älypuhelimia kaikkialla maailmassa. Alla oleva yleiskuva taajuuksien käytöstä Suomessa noudattaa Radio-ohjesäännön liikennelajimäärittelyä (Kuvio 2).



Kuvio 2: Yleiskuva taajuuksien käytöstä Suomessa (Viestintävirasto 2009)

2.2 Häiriöttyypit

Viestintävirasto saa vuosittain satojatuhansia erityyppisiä häiriö- ja poikkeamailmoituksia. Häiriöihin liittyvät yhteydenotot koskevat pääsääntöisesti:

1. Tietoturvahäiriöitä (tietoturvaloukkaukset - ja uhat),
2. matka- ja joukkoviestintäverkkojen komponenttien vikaantumiseen liittyviä häiriöitä tai
3. radiohäiriöitä.

Suomessa toimivilla teleyrityksillä, laatuvarmentajilla ja sähköisen allekirjoituspalvelun tuottajilla sekä erityisluovuttavilla viranomaisen tietoaineistoja käsittelevillä tahoilla ja tietoturvallisuuden arviointilaitoksilla on lakisääteinen velvollisuus ilmoittaa Viestintävirastolle tietoturvaloukkauksista ja -uhista, tietoturvapoikkeamista, sekä vika- ja häiriötilanteista. (917/2014, TYK 275 §; 617/2009 16 §; 588/2004 19 §; 1405/2011 8 §; 1406/2011 9 §; 726/2014 55 §.)

Tietoyhteiskuntakaaren mukaan (917/2014, TYK 348 §), jos radiolähetin aiheuttaa häiriöitä radioviestinnälle tai muille radiolaitteille, radiolähettimen haltijan ja omistajan on poistettava häiriö tai rajoitettava sitä. Niiden häiriöiden osalta, joita haltijat tai omistajat eivät saa

itsenäisesti poistetuksi tai huolehdituksi, ottavat organisaatiot yhteyttä viraston Taajuusvalvontaan häiriöiden selvittämiseksi.

2.2.1 Teleyritys

Lain määritelmän mukaan teleyrityksellä tarkoitetaan sitä, joka tarjoaa verkkopalvelua tai viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille eli harjoittaa yleistä teletoimintaa. (917/2014, TYK 3 §.)

2.2.2 Verkkopalvelu ja viestintäverkko

Lain määritelmän mukaan verkkopalvelulla tarkoitetaan palvelua, jossa teleyritys (verkkoyritys) tarjoaa omistamaansa tai muulla perusteella hallussaan olevaa viestintäverkkoa käytettäväksi viestien siirtoon tai jakeluun. Viestintäverkolla tarkoitetaan lain määritelmän mukaan toisiinsa liitetyistä johtimista sekä laitteista muodostuvaa järjestelmää, joka on tarkoitettu viestien siirtoon tai jakeluun johtimella, radioaalloilla, optisesti tai muulla sähkömagneettisella tavalla. Yleisellä viestintäverkolla tarkoitetaan viestintäverkkoa, jota käytetään viestintäpalvelujen tarjontaan ennalta rajaamattomalle käyttäjäpiirille. (2014/917, TYK 3 §.)

2.2.3 Radiohäiriöt

Radiolähetin käyttää tyypillisesti tiettyä taajuutta ja sillä on tietty maksimiteho. Radiolähtimen muodostaa ympärilleen tietyn peittoalueen, jossa esimerkiksi matkapuhelimen kuuluvuus on hyvä. Kaikki radiolähettimet vaikuttavat sähkömagneettisten ominaisuuksiensa vuoksi muihin sen läheisyydessä oleviin radiolaitteisiin. Vaikutus on sitä suurempi mitä lähempänä laitteet ovat toisiaan. Riippuen radiolaitteiden tehosta tai antennien suuntauksesta vuorovaikutus voi olla liian suuri, jolloin vuorovaikutus ilmenee haitallisena häiriönä tai laitteen toimimattomuutena. Häiriö voi tarkoittaa siirtokapasiteetin pienenemistä tai siirron laadun heikkenemistä tai laite ei kykene toimimaan lainkaan. (Viestintävirasto 2017d.)

Radiohäiriö voi syntyä myös radiolaitteen vikaantumisen tai sen käytöstä väärään tarkoitukseen, kuten käyttämällä luvaton lähetintä liian suurella teholla. Ulkomailta ja nettikaupasta ostetun laitteen osalta tulee myös varmistaa, että sitä saa käyttää laitteen taajuusalueella Suomessa ja sen käyttötarkoitus on oikea.

2.2.4 Yleisten viestintäverkkojen ja -palveluiden toimintavarmuuden häiriötilanteet

Tapahtumat, jotka estävät viestintäpalvelun toimivuuden tai häiritsevät niitä olennaisesti tai häiriö joka näkyy loppukäyttäjälle palvelun käytettävyydessä. Tällaisia tilanteita voivat olla esimerkiksi:

- pitkittynyt sähkökatko joka pudottaa mobiiliverkon tukiasemia verkosta

- palvelunestohyökkäys joka tukkii verkon dataliikenteen
- kaapelikatkos sekä ensisijaisella että varmentavalla reitillä tai
- tietoliikennelaitetilan tuhoutuminen (Viestintävirasto 2015b).

2.2.5 Yleisten viestintäverkkojen ja -palveluiden tietoturvahäiriö

Tietoturvahäiriöitä ovat tilanteet, joissa teleyrityksen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus. Tällaisia tilanteita voivat olla esimerkiksi verkon konfiguraatiotietojen joutuminen väärin käsiin, verkon reititykseen vaikuttavat hyökkäykset, äkillinen dataliikenteen kasvu harvinaisiin ulkomaan suuntiin ja tietoturva-aukko, jonka kautta pääsee teleyrityksen asiakastietoihin (Viestintävirasto 2015b).

3 Viestintäviraston toiminta

Viestintävirasto on liikenne- ja viestintäministeriön hallinnonalalla toimiva asiantuntijavirasto, jonka toiminnan pääpaino on viestintämarkkinoiden toimivuuden ja tehokkuuden turvaamisessa sekä viestintäverkkojen teknisen toimivuuden ja turvallisuuden edistämässä. Tavoitteena on varmistaa kilpailun toteutuminen viestintämarkkinoilla sekä taata kaikille käyttäjille häiriöttömät ja turvalliset viestintäyhteydet. Toiminnallaan virasto rakentaa ja ylläpitää suomalaista digiyhteiskuntaa. Helsingissä sijaitsevassa virastossa työskentelee noin 240 henkilöä kuudella eri toimialalla (Kuvio 3). Ulkoiset toimialat Kyberturvallisuuskeskus, Taajuushallinto ja Markkinat toimivat viraston asiakasrajapinnassa ja huolehtivat muun muassa alla kuvatuista tehtävistä. (Viestintävirasto 2017b.)

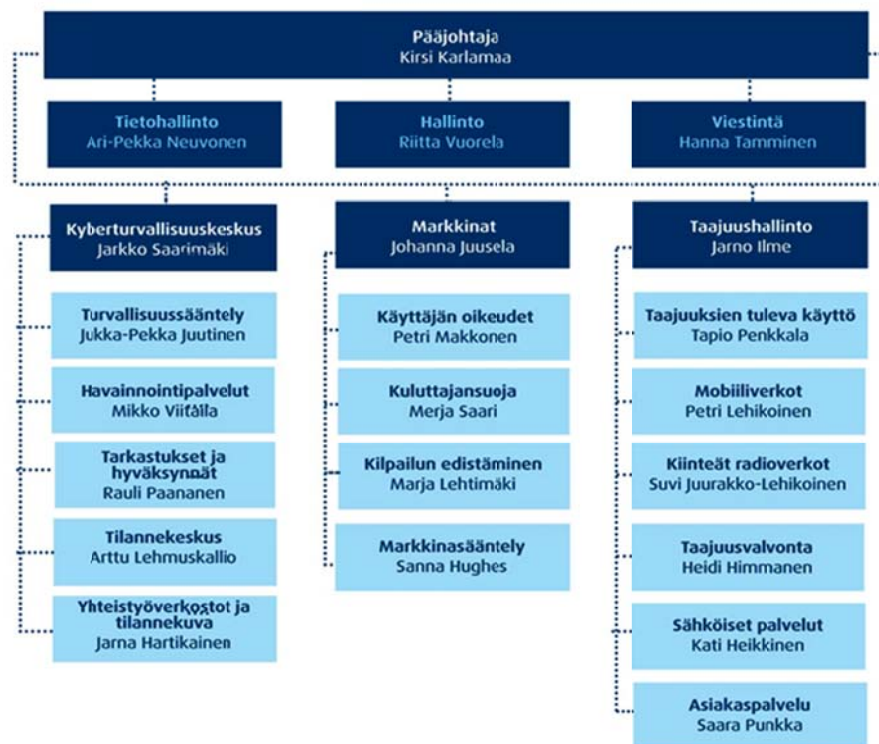
Viestintäviraston Kyberturvallisuuskeskus hoitaa sähköisen viestinnän yksityisyyden suojaan ja tietoturvaan liittyviä tehtäviä. Tietoliikenneturvallisuuteen liittyvien tehtävien tavoitteena on edistää sähköisen viestinnän turvallisuutta ja luotettavuutta. Viraston tehtävänä on myös hoitaa tietoturvaloukkausten tiedonkeruuta ja selvittämistä sekä tiedottaa tietoturva-asioista sekä vastata salassa pidettävää tietoa sisältävien tietojärjestelmien ja verkkojen vaatimuksemukaisuudesta. (Viestintävirasto 2017c.)

Viestintävirasto ohjaa radiotaajuuksien käyttöä Suomessa ja huolehtii siitä, että Suomen kansallinen etu otetaan huomioon taajuuksien käyttöä koskevassa kansainvälisessä päätöksenteossa. Tavoitteena on varmistaa, että radiotaajuuksia on käytettävissä riittävästi ja tasapuolisesti ja että asiakkaat saavat käyttöönsä riittävän häiriöttömät taajuudet. (Viestintävirasto 2017c.)

Viestintämarkkinoiden taloudellisella valvonnalla taataan, että kilpailu markkinoilla toimii ja että yritykset noudattavat säädettyjä hinnoittelu- ja toimintavelvoitteita. Toimiva ja tehokas kilpailu on kuluttajien ja asiakkaiden etu. (Viestintävirasto 2017c.)

Virasto vastaa myös verkkotunnusten teknisestä rekisterinpidosta sekä ylläpitää ja hallinnoi fi-juuren nimipalvelimia. Tietoyhteiskuntakaaren (917/2014, TYK 164 §) mukaisesti kesästä 2016 fi-verkkotunnuksen ja kaikki siihen liittyvät palvelut voi hankkia ainoastaan omalta verkkotunnusvälittäjältään. Viestintävirasto takaa edelleen fi-verkkotunnuksen laadun ja luotettavuuden. Viestintävirasto valvoo, että televisio- ja radio-ohjelmat täyttävät ohjelmiston eurooppalaisuutta, mainontaa ja sponsorointia koskevat vaatimukset. Lisäksi virasto valvoo postitoimintaa ja koordinoi postialan standardointia Suomessa. (Viestintävirasto 2017c.)

Sisäiset toimialat Hallinto, Tietohallinto ja Viestintä huolehtivat nimiensä mukaisista tehtävistä viraston sisäisen toiminnan takaamiseksi sillä lisäyksellä, että Viestintä-toimialalla on merkittävä rooli myös viraston ulkoisessa viestinnässä.

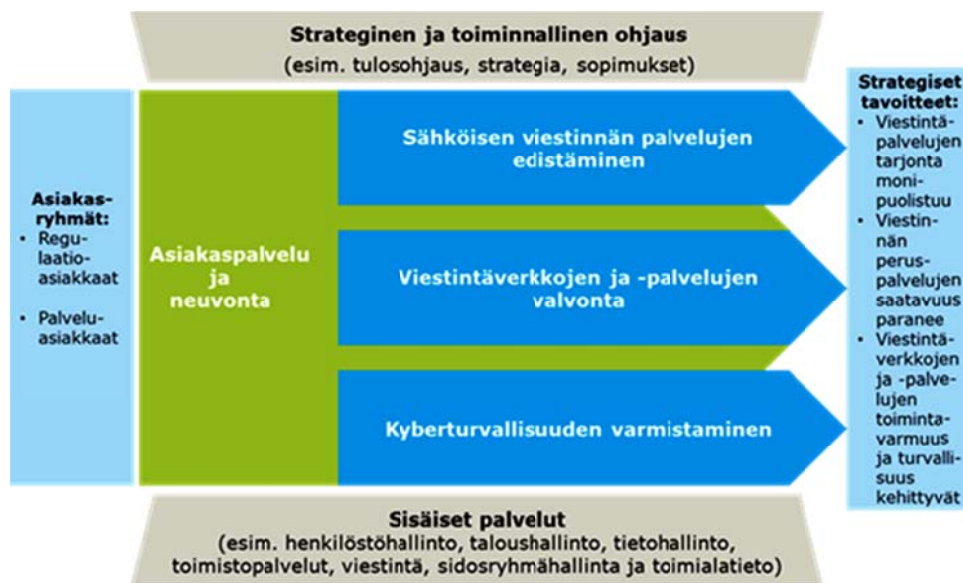


Kuvio 3: Viestintäviraston organisaatio (Viestintävirasto 2017)

4 Viestintäviraston ydinprosessit

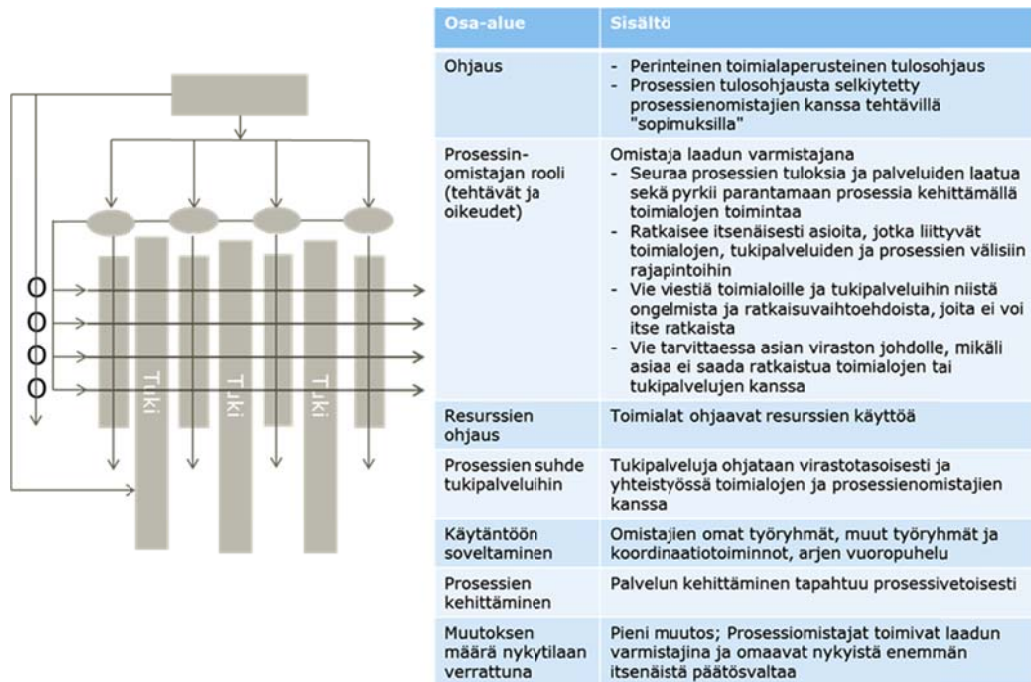
Tutkimuksen kohteena oleva häiriönhallintaprosessi on osa Viestintäviraston kyberturvallisuuden varmistamisen -ydinprosessia. Työn tarkoituksena on kehittää viraston ydinprosessia ja tuottaa prosessimalli virastolle, johon sekä Taajuushallinnon että Kyberturvallisuuskeskuksen henkilöstö sitoutuu sujuvoittamaan ja tehostamaan työtapoja sekä varmentamaan työn laatua.

Viestintäviraston asiakaspalvelun tehtävänä on toimia asiakasyhteydenottojen ensivasteena (Kuvio 4) ja tarvittaessa ohjata yhteydenotot viraston eri toimialoille kuten Kyberturvallisuuskeskus ja Taajuushallinto. Oleellista prosessissa on niin sanottu yhden luukun periaate eli asiakas ottaa yhteyttä yhteen paikkaan ja saa myös vastuksen yhdestä paikasta ilman, että hän tietää onko vastauksen laatimiseen käytetty viraston muita asiantuntijatasoja. Luonnollisesti tämä asettaa ammattitaidollisia vaatimuksia kaikille viraston asiantuntijatasoille sekä asiakaspalvelussa käytetyille Tapahtumienhallintatietojärjestelmälle (TAHA), jonka kautta asiakasyhteydenotot siirretään tarvittaessa Viestintäviraston muiden toimialojen ja prosessien käsiteltäväksi.



Kuvio 4: Viestintäviraston ydinprosessit (Viestintävirasto 2015)

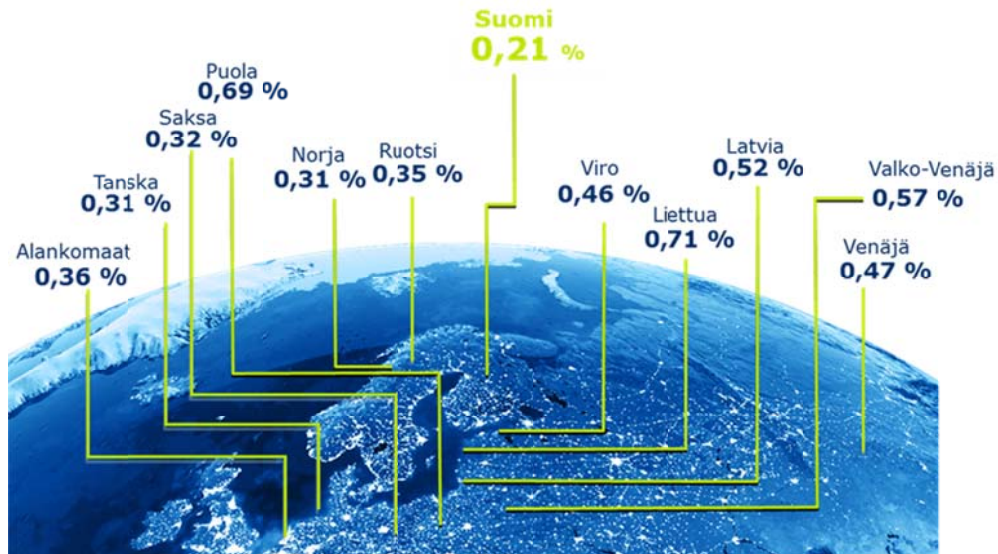
Osana viraston ydinprosessien laadun varmistamista ja viraston sisäisen yhteistyön rajapintojen kehittämistä, on virastossa vastuutettu ydinprosessien laadun varmistaminen toimialojen johtajille. Johtajien tehtävänä on, osana ydinprosessien kehittämistä, tunnistaa yhtäläisyyksiä ja rajapintoja viraston eri toimialojen prosessien osalta (Kuvio 5). Tämän opinnäytetyön yhtenä tarkoituksena on tunnistaa rajapinnat Kyberturvallisuuskeskuksen ja Taajuushallinnon häiriöiden hallinnassa sekä kehittää mahdollisimman yhtenäinen prosessi molemmille toimialoille kyseiseen tehtävään liittyen.



Kuvio 5: Laadun varmistaminen (Viestintävirasto 2015)

5 Maailman puhtaimmat verkot

Kansainvälisessä vertailussa Microsoftin 21:n Security Intelligence Report (SIR)-raportin mukaan Suomessa on maailman puhtaimmat tietoverkot (Kuvio 6). Verkkojen puhtautta mitataan arvioimalla kuinka usein verkkoon liitetyt järjestelmät joutuvat poistamaan haittaohjelman. Luvut perustuvat Microsoft Malicious Software Removal Tool (MSRT):n raportointiin. Raportin tietojen mukaan Suomessa havaittujen haittaohjelmataruntojen määrä oli vuoden 2016 toisella neljänneksellä maailman alhaisin: 2,1 haittaohjelmasta puhdistettua tietokonetta tuhatta tietokonetta kohti. Tilaston laskennassa on huomioitu vain tietokoneet, jotka raportoivat tietoturvatiedot suoraan Microsoftille eli Internetiin kytketyt ja lisensoidut Microsoftin käyttöjärjestelmää käyttävät tietokoneet. Näitä tietokoneita on maailman laajuisesti noin 600 miljoonaa kappaletta. Seuraavilla sijoilla olivat Japani (0,22 %), Norja (0,31 %) ja Tanska (0,31 %). Maailmanlaajuinen keskiarvo oli 0,88 %. Huonoin tilanne oli Libyassa, jossa 7,83 % tietokoneista on saanut tartunnan ja puhdistettu. (Microsoft 2016.)



Kuvio 6: Microsoftin 21:n Security Intelligence Report tilastoja (Viestintävirasto 2016)

5.1 Taajuuksien merkitys digitalisaatiolle

Kansainvälinen televiestintäliitto (engl. International Telecommunication Union, ITU) on selvittänyt tietoliikennetarpeen kasvua, sen eri muodoissaan, vuoteen 2030 saakka (ITU 2015). ITU:n raportin perusteella voidaan arvioida, että taajuustarpeet 2017-2030 keskittyvät digitalisoinnin edistämiseen matkaviestinverkoissa. Taajuuksien taloudellinen merkitys tulee edelleen kasvamaan tulevaisuuden 5G-tekniikan tarjoamien erilaisten palveluiden ja verkkoon pääsyn kautta. Euroopan komissiolla on tavoitteena, että jokaisessa jäsenmaassa voisi jo vuonna 2018 toimia esikaupallinen 5G-verkko (Euroopan komissio 2015). 5G-verkot tulevat mahdollistamaan digitaalisen yhteiskunnan tarvitsemat pienet viiveet tiedonsiirrossa, suuren tiedonsiirtokapasiteetin ja pienen energiakulutuksen. Verkkoon pääsy tulee helpottumaan monilla eri yhteiskunnan sektorilla ja se puolestaan kasvattaa esineiden internetin mahdollisuuksia ja suosiota.

5.2 Mobiiliverkkojen kattavuus

Suomessa on väestöpeitoltaan ja maantieteelliseltä peitoltaan varsin kattavat matkaviestinverkot. Palveluiden saatavuutta on lisätty Pohjois- ja Itä-Suomessa kahden operaattorin, Telia Finland Oyj ja DNA Oyj, yhteisvoimin Suomen Yhteisverkko Oy nimisenä yhtiönä (Yhteisverkko 2017). Parantunut verkon kuuluvuus ja siirtokapasiteetti tarkoittaa tulevaisuudessa entistä häiriöttömämpää toimintaa erilaisille digitaalisille palveluille ja sovelluksille.

Suomessa on käytössä kaupallisten viestintäverkkojen lisäksi maanlaajuinen viranomaisverkko VIRVE. Verkon operoinnista vastaa 100 % valtio-omisteinen Suomen Erillisverkot konserniin kuuluva Suomen Virveverkko Oy (Erillisverkot 2017). Viranomaisverkoilla ei ole häiriötilanteiden ilmoitusvelvollisuutta Viestintävirastolle, kuten kaupallisilla matkaviestinverkoilla. Ilmoit-

taminen erilaisista häiriötilanteista VIRVE-verkosta Viestintävirastolle toimii yhteistyön varassa, vaikkakin lakisääteisen teknisen turvallisuus- ja toimivuustarkastuksen kohteena voi olla myös viranomaisverkko. (2014/917, TYK 250 § & 316 §.)

6 Tutkimuksen perusteet

Viestintävirasto on keskeisessä roolissa varmentamassa aiemmin kuvattua yhteiskunnan digitaalista muutosta. Viestintäviraston lakisääteisiin tehtäviin kuuluu muun muassa varmistaa radiotaajuuksien riittävän häiriötön käyttö, turvata viestintäverkkojen- ja palveluiden toimintavarmuutta ja huolehtia siitä, että teleyritykset hoitavat palvelunsa tietoturvaselvästi.

Viestintähallinnosta annetussa laissa (625/2001, 2 §) on säädetty Viestintäviraston tehtävät ja erikseen se lainsäädäntö, joissa säädetään niistä Viestintäviraston tehtävistä jotka liittyvät tietoturvaselvyyteen ja häiriönhallintaan:

- Tietoyhteiskuntakaari (917/2014)
- Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009)
- Laki kansainvälisistä tietoturvaselvyysvelvoitteista (588/2004)
- Turvaselvyyslaki (726/2014)
- Laki tietoturvaselvyyden arviointilaitoksista (1405/2011)
- Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvaselvyyden arvioinnista (1406/2011)

Tämän opinnäytetyön aiheen kannalta oleellisin on tietoyhteiskuntakaari (917/2014, TYK 96 §, 97 §, 244 §, 247 §, 272 §, 274 § & 275 §), jossa on säädetty Viestintävirastolle määräksenantovaltuus muun muassa teletoimintaan liittyvistä häiriötilanteista ja teletoiminnan tietoturvaselvästä sekä radiotaajuuksien häiriöttömästä käytöstä.

6.1 Radiotaajuusmääräys (M4)

Viestintävirasto hallinnoi radiotaajuuksien käyttöä Suomessa ja radiotaajuuksien käyttö on määritelty viraston radiotaajuusmääräyksessä 4. Määräyksellä turvataan radiotaajuuksien saatavuus sekä tarkoituksenmukainen ja riittävän häiriötön käyttö. Määräys osoittaa eri käyttö-tarkoitukset radiotaajuusspektrin välille 9kHz - 400 GHz. Määräys sisältää oleelliset tiedot radiohäiriöiden hallintaa varten, kuten vaatimukset lähetys- ja vastaanottotaajuuksista, kanavaväleista, lähetystehoista ja muista teknisistä ominaisuuksista. Määräyksessä on huomioitu kansainvälisen televiestintäliiton Radio-ohjesääntö, joka on saatettu Suomessa voimaan liikenne- ja viestintäministeriön asetuksella vuonna 2000. (Viestintävirasto 2017d.)

6.2 Viestintäviraston määräys teletoiminnan häiriötilanteista (M 66)

Määräyksessä 66 (Viestintävirasto 2014a) yleisten viestintäverkkojen ja -palveluiden toimivuuden häiriötilanteet on luokiteltu neljään erilaiseen vakavuusluokkaan A, B, C ja D niiden viestintäpalveluille aiheuttamien vaikutusten perusteella. Luokassa A häiriö koskee satoja tuhansia käyttäjiä, luokassa B kymmeniä tuhansia käyttäjiä, luokassa C tuhansia käyttäjiä ja luokassa D alle tuhansia käyttäjiä.

Määräyksen tarkoituksena on varmistaa yleisten viestintäverkkojen ja -palvelujen häiriötilanteiden ja uhkien havaitseminen, edistää häiriötilanteiden nopeaa korjaamista, turvata käyttäjien tiedonsaanti häiriötilanteista ja varmistaa Viestintäviraston tiedonsaanti häiriötilanteista (Viestintävirasto 2014a).

6.3 Määräys teletoiminnan tietoturvasta (M67)

Määräyksessä 67 (Viestintävirasto 2014b) on määritelty tietoturvan toteuttamista koskevat vähimmäisvaatimukset joilla pyritään siihen, että tietoturvallisuus huomioidaan teleyrityksessä osana jokapäiväistä toimintaa rutiininomaisesti tehokkailla prosesseilla osana viestintäverkkojen ja viestintäpalveluiden toteuttamista.

Määräyksen noudattamisella turvataan sähköisen viestinnän luottamuksellisuus, yksityisyyden suojan toteutuminen, tietoturvallisuuden toteutuminen teleyrityksessä ja yleisten viestintäverkkojen ja -palvelujen tietoturvallisuuden edistyminen (Viestintävirasto 2014b).

7 Tutkimuskysymykset ja aiheen rajaus

Viestintävirastolla on yhteiskunnallisesti vaikuttava tehtävänä erilaisten häiriöiden hallinnassa ja toimintavarmuuden varmistajana. Tästä johtuen on mielekästä valita opinnäytetyön tutkimuskohteeksi radiohäiriöt hätä- ja turvallisuusradioliikenteessä, viestintäverkkojen- ja palveluiden toimivuuden ja tietoturvallisuuden häiriönhallinta.

Tutkimuksen kannalta keskeisiä kysymyksiä ovat:

- 1) miten yhtenäisiä Taajuushallinnon ja Kyberturvallisuuskeskuksen häiriönhallintaprosessit ovat,
- 2) miten varmistetaan häiriöhallinnan laatu ja raportoinnin yhdenmukaisuus

Lisäksi selvitetään Viestintäviraston Kyberturvallisuuskeskuksen ja Taajuushallinnon tapoja ja menettelyjä toimia häiriötilanteissa ja määritellä viraston häiriöhallinnan prosessien nykytila. Työssä huomioidaan lainsäädännön antamat velvoitteet, viraston antamat taajuuksien hallintaa ja tietoturvallisuutta ohjaavat määräykset, yhteistyöverkostojen toimintatavat ja mallit sekä toimialoilla tehdyt ohjeistukset.

Lakisääteisen ilmoitusvelvollisuuden nojalla virastoon tulee vuosittain viestintäverkkoihin liittyviä ilmoituksia noin 35–45 kpl, radiohäiriöihin liittyviä ilmoituksia noin satakunta, teleyritysten vikailmoituksia noin 300 000 kpl ja vapaaehtoisia tietoturvaloukkemaimoituksia noin 200 000 kpl.

Häiriöilmoitusten suuren määrän vuoksi opinnäytetyössä rajoitetaan käsittelemään häiriötilanteita, jotka ovat yhteiskunnan kannalta kaikkein kriittisimpiä tai vaikutukseltaan laajoja ja vakavia. Työ keskittyy radiohäiriöiden osalta hätä- ja turvallisuusradioliikenteeseen ja tietoturvallisuuden osalta tietoturvaloukkauksiin sekä matka- ja joukkoviestintäverkkojen fyysisen verkkorakenteen häiriöihin ja vikoihin. Opinnäytetyöstä rajataan häiriöiden osalta pois tietoturvauhat ja ilmiöt sekä TV- vastaanoton häiriötilanteet.

7.1 Tutkimusmenetelmät ja tutkimusteoria

Tämän kvalitatiivisen ja toiminnallisen opinnäytetyön tarkoituksena on lisätä ymmärrystä Viestintäviraston häiriönhallinnasta ja mallintaa viraston kahden eri toimialan nykyistä häiriönhallintaprosessia, tulkita valmiina olevia ohjeistuksia ja löytää häiriönhallinnalle yhteismitallinen käsittelytapa ja raportointi. Tutkimuksessa perehdytään sisällönanalyysin avulla jo toteutuneisiin tietoturvaloukkauksien ja häiriöiden dokumentaatioihin. Tavoitteena on analysoida dokumenttiaineistoa järjestelmällisesti ja yleispätevästi (Tuomi & Sarajärvi 2002, 105).

Tuomen ja Sarajärven (2002, 98-99) mukaan sisällönanalyysiin kuuluu aineiston pelkistäminen ja ryhmittely. Tässä työssä aineisto ryhmitellään rajauksen mukaisesti fyysisten verkkojen vikoihin ja häiriöihin, tietoturvaloukkauksiin sekä hätä- ja turvallisuusradioliikenteeseen.

Laadullisessa tutkimuksessa, joksi tämänkin toiminnallisen opinnäytetyön voi luokitella tiedonkeruumenetelmien perusteella, itse analysointitavalla ei ole yhtä ja ainoaa tapaa, joka määräytyisi jonkinlaisen säännön mukaan. Laadullisessa tutkimuksessa on tavanomaista, että aineistoa on kerätty vaihteittain eri menetelmien avulla. Tästä syystä analysointia ja tiedonkeruuta voidaan tehdä koko tutkimuksen ajan samanaikaisesti. Tähän työhön valikoitui analysointimenetelmäksi teemoittelu. Muita laadulliseen aineistoon käytettyjä menetelmiä ovat tyypittely, sisällönerittely sekä diskurssi- ja keskustelunanalyysi. (Hirsjärvi, Remes & Sajavaara 2007, 218-219.)

Teemoittelun peruserä on, että aineisto on pilkottu pienempiin osiin eri teemojen alle jotka rakentuvat tiedonkeruumenetelmien sekä teorian avulla. Teemoittelu voidaan suorittaa esimerkiksi poimimalla haastatteluista kyseiseen teemaan liittyvät asiakohdat ja kuten tässäkin työssä haastatteluissa esiintyvät eri teemat voivat toimia myös itse analyysin teemoina. Kokemuseräisen aineiston tiedonkeruussa käytetään teemahaastattelun ja strukturoidun

haastattelun yhdistelmää, joka antaa asiantuntijoille vapautta vastauksiin, vaikka tietoa opinnäytetyötä varten haetaankin valmiin kysymyslomakkeen pohjalta (Aaltola & Valli 2001, 24-25, 100-101). Teemoittelun yhteydessä materiaali lajitellaan teemojen alle uudelleenlaisiksi kokonaisuuksiksi, joilla pyritään ratkaisemaan myös tutkimuskysymysten vastauksia. (Tuomi & Sarajärvi 2009, 93-95.)

Tutkimuksella on myös eksploratiivinen eli etsinnällinen tavoite, jonka yhtenä tarkoituksena on kehittää Viestintäviraston kyberturvallisuuden varmistaminen-prosessia. Prosessin on tarkoitus olla osa viraston kehittyvää toimintaa ja tutkimuksen avulla voidaan löytää myös jatkotutkimuskysymyksiä häiriönhallinnasta.

7.2 Lähdeaineisto

Tutkimus pohjautuu pääsääntöisesti julkisiin asiakirjoihin ja lainsäädännön osalta tietoyhteiskuntakaareen (917/2014, TYK), lakiin viestintähallinnosta (625/2001), kansainvälisen televiestintäliiton Radio-ohjesääntöön sekä Viestintäviraston määräyksiin ja ohjeistuksiin. Osa taustamateriaalista, esimerkiksi häiriöiden selvitykseen liittyvät dokumentit, saattavat olla salassa pidettäviä. Tämä huomioidaan opinnäytetyön sisällön tuottamisessa.

8 Häiriönhallinnan nykytila Kyberturvallisuuskeskuksessa ja Taajuushallinnossa

Häiriönhallinta on yksi Viestintäviraston keskeisimmistä tehtävistä. Virasto tuottaa vuodessa noin 500 kappaletta erilaisia häiriöihin liittyvää raporttia tai uutista, jotka julkaistaan viraston verkkosivuilla (Viestintävirasto 2016a.) Tämän lisäksi virasto tuottaa sektorikohtaista raportointia elinkeinoelämälle sekä valtiohallinnolle kokonaistilannekuvaa tai erityistarpeisiin liittyvää raportointia. Raportointi koostuu pääosin tietoturvahäiriöistä, mutta viime aikoina myös enenevässä määrin radiohäiriöiden raportoinnista.

Tuottaakseen tasalaatuista, ymmärrettävää ja selkeää tilannekuvaa, on viraston selvitettävä sekä Kyberturvallisuuskeskuksen ja Taajuushallinnon häiriönhallinnan nykytila ja tunnistettava siihen liittyvät kehitystoimet.

8.1 Häiriönhallinnan toimintamalli ja häiriöiden selvittämisen prioriteetit Taajuushallinnossa

Viestintäviraston Taajuusvalvonta-ryhmä selvittää radioliikenteelle aiheutuneita häiriöitä ja suuritehoisten radioasemien ympäristössään aiheuttamia häiriöitä sähkölaitteille. Radiohäiriöiden selvittämisen vastuu on jaettu Taajuusvalvonnassa kolmelle henkilölle siten, että myös vastuujärjestys on tiedossa. Kriittisten häiriöiden koordinoinnista vastaa ensisijaisesti Taajuusvalvonnan päällikkö (Sisäinen ohje A 2017).

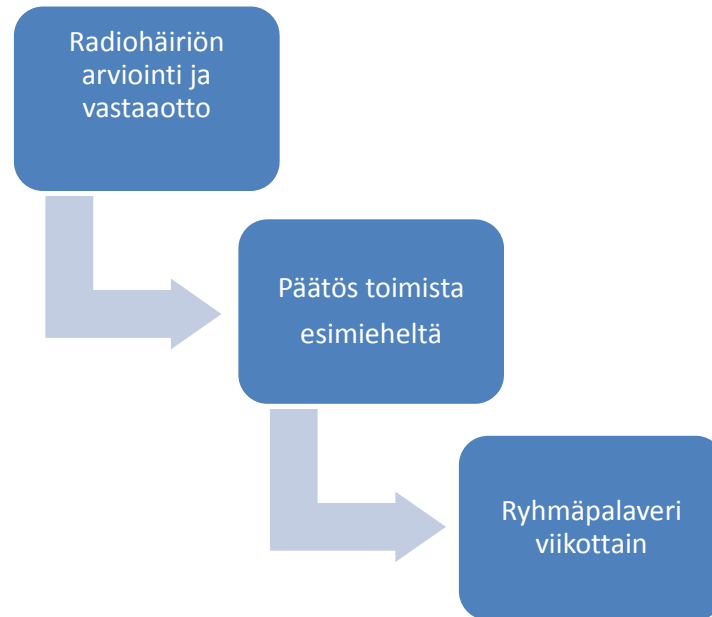
Kiireellisyysjärjestyksessä etusijalla ovat hätä- ja turvallisuusradioliikenteelle, viranomaisverkoille, tele- ja matkaviestinverkon runkoyhteyksille, joukkoviestinnän ohjelmasiirtoyhteyksille sekä energiahuollon ja kunnallistekniikan radioverkoille aiheutuneiden häiriöiden selvittäminen ja toiminnan palauttaminen normaaliksi. Hätä- ja turvallisuusradioliikenteeseen kuuluvat muun muassa tyypillisesti tietyt ilmailun, merenkulun, viranomaisverkkojen, satelliittiliikenteen ja radionavigointiliikenteen taajuudet. Arvio häiriön ja sen vaikutusten vakavuudesta tehdään aina tapauskohtaisesti. Hätä- ja turvallisuusradioliikenteen sekä viranomaisverkon radiohäiriöiden selvittämisen aikatavoite, 16 tuntia virka-aikana, on määritelty liikenne- ja viestintäministeriön ja Viestintäviraston tulossopimuksessa osana viraston ulkoista toiminnanohjausta (Viestintävirasto 2017e). Viestintävirastolla on mahdollisuus saada virka-apua radiohäiriöiden selvittämiseksi Rajavartiolaitokselta ja Puolustusvoimilta. (2014/917, TYK 309 §.)

8.1.1 Tiedonkulku ja laadun varmistaminen Taajuushallinnossa

Radiohäiriöilmoitus Viestintävirastolle tehdään ensisijaisesti sähköisellä ilmoituslomakkeella, jotta ilmoitus saadaan suoraan sähköiseen käsittelyyn viraston TAHA-järjestelmään (Viestintävirasto 2016b). Radiohäiriöilmoituksen voi jättää myös puhelimitse tiettyyn Viestintäviraston soittosarjaan tai suoraan Taajuusvalvonnan henkilöstölle. Tällöin neuvotaan täyttämään myös sähköinen ilmoituslomake.

Kiireellisiksi ilmoitetut kriittisten hätä- ja turvallisuusradioliikenteen radiohäiriöt käsitellään korkealla prioriteetilla. Mikäli yhteydenottovaiheessa käy ilmi, että kyse on priorisoiduista liikenteestä, reagoidaan yhteydenottoon mahdollisimman nopeasti. Tieto uudesta radiohäiriöstä toimitetaan välittömästi Taajuusvalvonnan päällikölle ja virka-aikana myös tietyille viraston sisäiselle sähköpostijakelulle (Kuvio 7). Päällikkö tai koordinaattori tiedottaa myös Taajuushallinnon johtajaa ja apulaisjohtajaa. (Sisäinen ohje A 2017.)

Tämän jälkeen otetaan yhteyttä radiohäiriön ilmoittajaan, kysytään lisätietoja ja arvioidaan tilanne. Erityisen tärkeää on kartoittaa radiohäiriön laajuus, tunnistaa häiriintyvä taajuus, selvittää häiriön luonne eli onko se satunnaista vai jatkuvaa ja arvioida johtuuko häiriö mahdollisesti omasta verkosta tai laiteviasta. Ilmoittajan on tehtävä radiohäiriöilmoitus aina myös kirjallisena, jotta häiriön selvittämiseen saadaan oleelliset ja oikeat tekniset tiedot. Suullisen ja kirjallisen ilmoituksen välillä voi olla ristiriitoja ja tällöin noudatetaan kirjallista ilmoitusta ja pyydetään tarvittaessa selvennystä tilanteeseen (Sisäinen ohje A 2017). Tietoa hätä- ja turvallisuusradioliikenteen häiriöselvityksistä jaetaan tarpeen mukaan Taajuushallinnon toimialapalavereissa ja viikoittain tapaukset käsitellään tarkemmin, oppimismielessä, Taajuusvalvonta-ryhmässä (Kuvio 7).



Kuvio 7: Kiireellisten hätä- ja turvallisuusradioliikenteen käsittely

8.1.2 Raportointimallit Taajuushallinnossa

TAHA:an dokumentoidaan kaikki Taajuusvalvonnan asiakasyhteydenotot, jotka voivat olla radiohäiriöitä, neuvontaa, markkinavalvontaa tai muita valvonta-asioita. Dokumentoinnin tulee olla mahdollisimman tarkkaa, jotta TAHA-tiketti voidaan tarvittaessa helposti siirtää toiselle henkilölle käsiteltäväksi. Tällöin vältetään myös päällekkäisiltä toimenpiteiltä samaan asiakasyhteydenottoon liittyen. Lisäksi tarkasti dokumentoiduista tiketeistä voidaan muodostaa automaattisesti vuosittaiset radiohäiriötilastot ja tarpeen mukaan muitakin tilastoja. TAHA-tikettiä päätettäessä lisätään Yhteenvedo-kenttään tiivis kuvaus häiriön selviämisestä. Selvittämiseen liittyvät suuremmat dokumentit tallennetaan viraston asianhallintajärjestelmään, jotta ne ovat myöhemmin helpommin käsiteltävissä. (Sisäinen ohje A 2017.)

8.2 Kyberturvallisuuskeskuksen yhteistyöverkostotoiminta

Viestintäviraston Kyberturvallisuuskeskuksen yhteistyöverkostojen tarkoitus on mahdollistaa tietoturva-asioiden luottamuksellinen käsittely osallistujien kesken sekä tähän perustuva organisaatioiden tietoturvaosaamisen lisääminen ja Kyberturvallisuuskeskuksen kokonaistilannekuvan kehittäminen. Yhteistyöverkostojen toiminta perustuu säännöllisiin tapaamisiin sekä määritettyihin toimintamalleihin ja osallistujiin. (Viestintävirasto 2014c.)

Yhteistyöverkostoihin kuuluvat ensisijaisesti yhteiskunnallisen merkityksensä tai vaikuttavuutensa vuoksi tärkeät organisaatiot. Yhteistyöverkostojen toimintaan osallistumisen tärkein kriteeri on kuitenkin toimijan aktiivisuus ja ryhmälle antama lisäarvo, jolloin verkostoihin voidaan tarvittaessa ottaa mukaan myös muita kuin pääasiakasryhmiin kuuluvia toimijoita. Yh-

teistyöverkostojen lisäksi Kyberturvallisuuskeskuksella on useita muita koti- ja ulkomaisia verkostoja ja kumppaneita, joiden kautta se saa ja jakaa tietoa. (Viestintävirasto 2014c.)

8.3 Häiriönhallinnan toimintamalli Kyberturvallisuuskeskuksessa

Pääsääntöisesti tietoturvaloukkauksiin ja -uhkiin liittyvät yhteydenotot otetaan vastaan sähköisellä ilmoituslomakkeella, kuten viraston Taajuushallinnossakin. Ilmoitus saadaan tätä kautta suoraan sähköiseen käsittelyyn viraston TAHA-järjestelmään. Kyberturvallisuuskeskuksessa toimii varallaoloon perustuva 24/7- päivystystoiminta. Huoltovarmuuskriittiset toimijat voivat ottaa suoraan yhteyttä Kyberturvallisuuskeskuksen päivystäjään puhelimitse, sähköpostilla tai muulla erikseen sovitulla viestivälillä. Päivittäisestä toiminnasta vastaa viikon kerrallaan vuorossa oleva 1-päivystäjä, joka tekee yhteydenoton vakavuusarvion ja käsittelee niistä saapumisen jälkeen rutiinomaisesti hoidettavat tapaukset. Tämän lisäksi 1-päivystäjä tekee päivittäistä uutisseurantaa. Jos tilanne ruuhkautuu tai kriisiytyy, vakavuusarvioinneissa ja tilanteiden hallinnassa avustaa niin sanottu 2-päivystäjä. Tietoturvaloukkausten- ja uhista tiedottaminen on 2-päivystäjän vastuulla. (Sisäinen ohje B.)

Päivystäjien lisäksi Kyberturvallisuuskeskuksessa toimii kolmen viikon vuoroissa oleva tilannekuvakoordinaattori. Tilannekuvakoordinaattori seuraa tapahtumien kokonaisuutta ja ottaa ohjaukseensa merkittävät tapaukset kuten A- ja B-luokan häiriötilanteet tai tapaukset, joiden seuranta ja selvittäminen kestävät pitkään tai tarvitsee toimialan useimpien ryhmien yhteistyötä. Tilannekuvakoordinaattorin tehtävänä on seurata tehtyjä toimenpiteitä, tiedottaa ja suunnitella mitä seuraavaksi on tehtävä häiriön poistamiseksi, estämiseksi tai tilanteesta toimimiseksi. Päivystäjien ja tilannekuvakoordinaattoreiden apuna on lisäksi muuta henkilöstöä, jotka osallistuvat tapausten analysointiin ja raportointiin. (Sisäinen ohje B.)

Kyberturvallisuuskeskuksen johto pidetään tietoisena kriittisistä ja merkittävistä tapahtumista, sekä viikoittaisesta kokonaistilanteesta. Tilannekuvakoordinaattori raportoi päivittäin toimialan johdolle kyberturvallisuuden tilanteen ja tämän lisäksi kerran viikossa päivystäjän vuoron vaihdossa päivystäjä käy läpi koko viikon tapahtumat, tehdyt toimenpiteet ja seurattavat kohteet.

8.3.1 Häiriöiden selvittämisen prioriteetit Kyberturvallisuuskeskuksessa

Tietoturvaloukkauksen eli häiriön tyyppi, vakavuus ja käsittelytapa arvioidaan yhteydenoton saapuessa oikeiden toimenpiteiden määrittelemiseksi ja suorittamiseksi. Tyypillisimmille häiriöille on laadittu omat menettelyohjeet. Jos tapaus täyttää useamman tyyppin piirteitä tai on monimutkainen, valitaan tapausta parhaiten vastaava ohje. Vakavuusarvio perustuu häiriön tiedettyyn tai oletettuun laajuuteen, käyttäjämäärään, organisaation, ohjelmiston yleisy-

teen tai tiedon tasoon, esimerkiksi henkilötiedot tai turvallisuusluokitellut tiedot. (Sisäinen ohje B.)

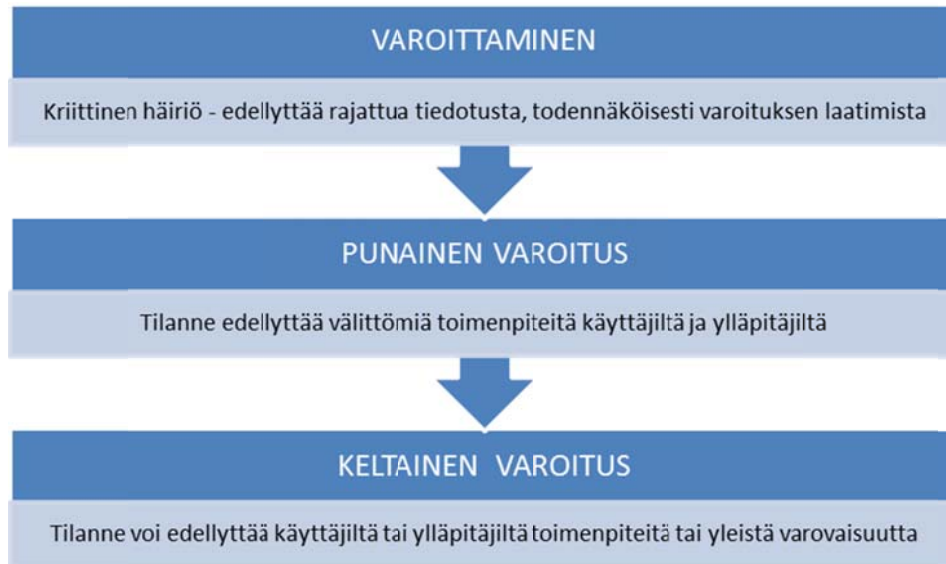
Vakavuusarviota hyödynnetään toimenpiteiden suorittamisen kiireellisyyden ja tehtävien priorisoinnin arvioinnissa. Vakavuusarviota voi muuttaa tietojen tarkentuessa tai muuttuessa. Alkuarvioinnin jälkeen käynnistetään häiriöstä toipumiseen tähtäävät toimenpiteet. Tilannekartoituksella arvioidaan kokonaislaajuus ja avustavat toimenpiteet, jotka tähtäävät tilanteesta palautumiseen. Tiedotuksessa on arvioitava, auttaako tiedottaminen häiriöstä toipumista vai lisääkö se uhkaa häiriön laajenemiselle. Selvitysten perusteella käynnistetään tiedonsaanti-tarpeen mukainen tiedotus joka voi olla julkinen tai rajattu ja tarvittaessa tilanteesta varoit-taminen. (Sisäinen ohje B.)

8.3.2 Laadun varmistaminen Kyberturvallisuuskeskuksessa

Laadunvarmistusta tukee vakavuusluokittelu joka tehdään tilanteen vakavimman arvion mu-kaisesti. Yhdenkin kriteerin täytyminen riittää luokitteluun. Vakavuusarviota hyödynnetään tiedotustarpeessa ja tehtävien priorisoinnissa, kun käsittelyssä on useita tapauksia yhtä aikaa. Vakavuusarviota voidaan tilanteen edistyessä muuttaa, mikäli tiedot muuttuvat ensiarviosta.

Kriittinen häiriö tai sen uhka voi kriittisen laajasti vaikuttaa käyttäjien turvallisuuteen, esi-merkiksi suureen käyttäjämäärään, maantieteelliseen alueeseen tai tietojen suojaustarpee-seen perustuen. Häiriön laajuuden vuoksi tiedotus ja sen nopeus on tärkeää vahinkojen mini-moimiseksi ennakoimalla tulevaa, kertomalla nykytilanteesta sekä kertomalla käyttäjille ja ylläpitäjille palauttavista toimenpiteistä. Tämä edellyttää usein punaisen varoituksen anta-mista. (Sisäinen ohje B.)

Vakava häiriö tai sen uhka vaikuttaa laajasti käyttäjien turvallisuuteen. Tiedotuksella on mer-kittävä rooli tilanteen palauttamisessa tai uhan ennaltaehkäisyssä, minkä avulla voidaan myös kiinnittää huomiota yleiseen varovaisuuteen tai korjaaviin toimenpiteisiin. Tämä voi edellyt-tää keltaisen varoituksen antamista (Kuvio 8).

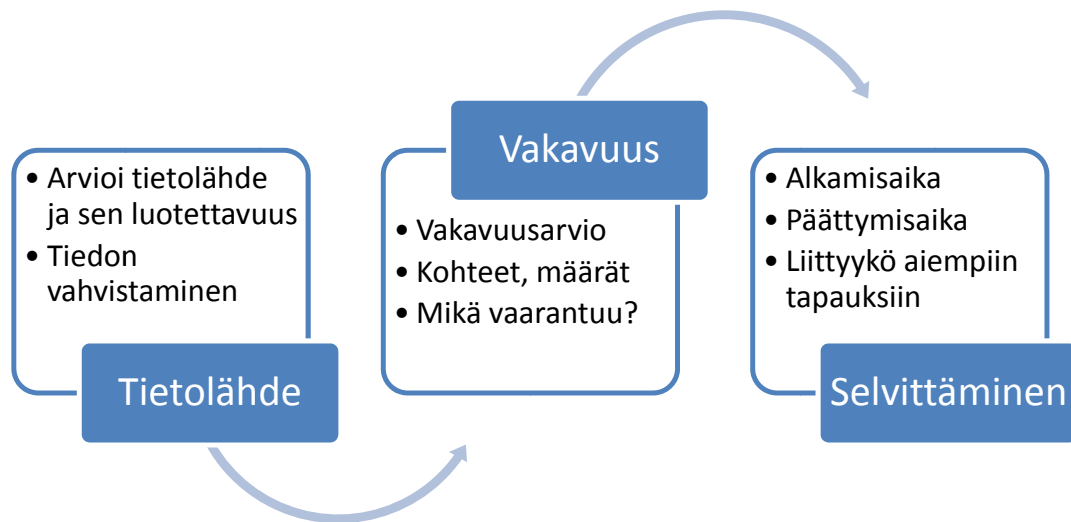


Kuvio 8: Varoituksen tasot

Häiriön luonteesta riippuu, kuinka nopeasti se on tarve käsitellä vahinkojen minimoimiseksi ja laadukkaan tilannetiedon jakamiseksi. Arvioinnin alkuvaiheessa on tärkeää varmistaa, että tieto on luotettavaa ja tiedon alkuperä on vahvistettu. Tapaukset, joissa häiriö vaikutuksineen on meneillään vaativat nopeaa reagoitua varsinkin, jos häiriö koskettaa laajasti kansalaisia tai elinkeinoelämää. Uhkaavat tapaukset, joista ei ole selkeää varmuutta edellyttävät usein selvityksiä toimenpiteiden suorittamiseksi ja asiasta riittävän täsmälliseksi tiedottamiseksi. Tämän lisäksi hoidetuista tapauksista on pohdittava, onko tapauksen opeista hyödynnettävää tiedonjaossa ja onko tieto tapahtumasta oleellinen yleistietoisuuden kannalta (Kuvio 9).

Häiriöt, jotka ovat juuri meneillään vaativat nopeaa reagoitua vahinkojen minimoimiseksi ja ongelmasta tiedottamiseksi. Tyypillisiä esimerkkejä ovat:

- Viestintäverkkojen ja -palvelujen häiriöt: Palvelun käyttäminen on häiriintynyt tai estynyt ja käyttäjät havaitsevat ongelman
- Palvelunestohyökkäys: Palvelu ei ole käytettävissä tai on erittäin hidas käyttäjille
- Tietovuoto: Tietomurron kautta saadut tiedot on vuodettu julkisuuteen ja välittömästi hyödynnettävissä
- Haittaohjelma: Haittaohjelma leviää verkkosivuston tai sähköpostin kautta.
- Huijaukset: Phishing- tai muu esim. sähköpostitse tai tekstiviestein leviävä huijauksetkampanja.



Kuvio 9: Tapauksen arviointi ja käsittely

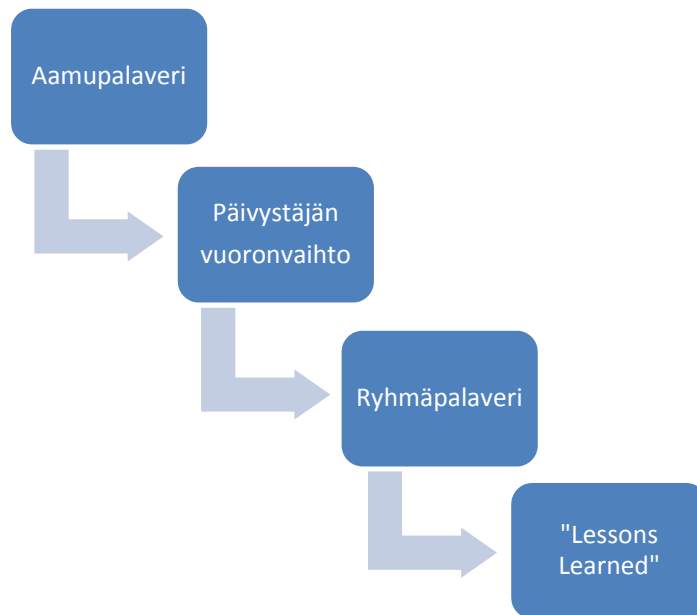
8.3.3 Tiedonkulku Kyberturvallisuuskeskuksessa

Kyberturvallisuuskeskuksessa tiedonkulku jakaantuu kahteen eri osaan: viraston sisäiseen tiedonkulkuun ja ulkoiseen tiedottamiseen tietoturvahäiriöiden poistamiseksi ja estämiseksi. Tietoturvahäiriön poistamiseksi voidaan tiedottaa kohdennetusti jotakin tiettyä sektoria kuten esimerkiksi energia- tai rahoitussektoria tai virasto voi julkaista yleisen Tietoturva Nyt-uutisen, joka voidaan kohdentaa kansalaisille tai yrityksille. Vakavissa häiriötilanteissa virasto antaa asian kriittisyyteen liittyvän varoituksen. Tietoturvahäiriöistä tiedotettaessa ei koskaan paljasteta tietoturvaloukkauksen kohteeksi joutunutta asianomaista, vaan tapauksesta välitetään muiden organisaatioiden suojaksi anonymisoidut tekniset tunnisteen. Kaikissa vakavissa tietoturvahäiriöissä riittävän ajoissa tehty tiedottaminen on ensiarvoisen tärkeää. (Sisäinen ohje B.)

Sisäisen tiedonkulun osalta ensiarvion ja vakavuusluokittelun tietoturvahäiriöstä tekee vuorossa oleva päivystäjä. Päivystäjä tai tilannekuvakoordinaattori voi tehdä päätöksen keltaisen varoituksen julkaisemisesta Viestintäviraston verkkosivustolla. Keltainen varoitus tarkoittaa tilannetta, jossa käyttäjiltä ja ylläpitäjiltä edellytetään toimenpiteitä tai yleistä varovaisuutta. Punaisen varoituksen antamisesta päättää esimies. Punainen varoitus tarkoittaa tilannetta, jossa käyttäjiltä ja ylläpitäjiltä vaaditaan välittömiä toimenpiteitä (Sisäinen ohje B). Varoituksista sisäinen tiedottaminen ei ole tällä hetkellä johdonmukaista. Niistä tiedotetaan vaihtelevasti Kyberturvallisuuskeskuksen johtoryhmää, henkilöstöä, viestintätiimiä tai pääjohtajaa. Myöskään varoituksen peruuttamisesta tiedottaminen ei ole johdonmukaista.

Päivystäjä ja tilannekuvakoordinaattori tekevät tiivistä yhteistyötä. Tilannekuvakoordinaattori raportoi joka aamu Kyberturvallisuuskeskuksen johdolle ja kaikille muillekin keskuksen henkilöille, kuluneen vuorokauden tapahtumat ja tietoturvahäiriöt. Aamupalaverissa koordinoidaan tapauksien selvittämiseen tarvittavat resurssit sekä tehdään mahdollisia arviointeja töiden prioriteettijärjestyksestä. Päivystäjän viikko loppuu niin sanottuun päivystäjän vuoronvaihtopalaveriin, jossa käydään läpi viikon tapahtumat ja niihin liittyvät seurannat. Aamupalavereista ja vuoronvaihtopalavereista nousseet keskeisimmät tapaukset käsitellään Tilannekeskus- ja Tilannekuva ja yhteistyöverkostot-ryhmien viikkopalavereissa. (Sisäinen ohje B.)

Toimintatapojen yhdenmukaistamiseksi ja toiminnan kehittämiseksi käydään kerran kuukaudessa niin sanottu "lessons learned"-palaveri. Palaverin tarkoituksena on käydä kaikki kuukauden aikana tapahtuneet merkittävimmät tapaukset läpi ja arvioida keskustellen miten tapaus käsiteltiin ja mitä parannettavaa toiminnassa on. Tarkoituksena olisi se, että parannusehdotukset päivitettäisiin sisäisiin ohjeistuksiin ja ne koulutettaisiin koko keskuksen henkilöstölle (Kuvio 10).



Kuvio 10: Tiedonkulku Kyberturvallisuuskeskuksessa

9 Kyberturvallisuuskeskuksen toiminnan ja prosessien tuntemus

Tutkimuksessa haastatellaan Taajuushallinnon henkilöstöä häiriöhallintaan liittyvien kysymysten pohjalta. Kyberturvallisuuskeskuksen toiminnan ja prosessien osalta vertailu Taajuushallinnon toimintaan tehdään perustuen kirjoittajan omaan osaamiseen, näkemykseen ja kokemukseen.

Olen työskennellyt salassa pidettävän tiedon ja tietoturvallisuuden parissa jo yli 20 vuotta. Opinnäytetyön kannalta oleellimmat ovat kolme viimeisintä työtehtävääni, jotka kattavat ajallisesti vuodet 2004-2017. Näihin kuuluvat toimiminen Maanpuolustuskorkeakoulun ja sisäministeriön ensimmäisenä tietoturvapäällikkönä, jolloin tehtäviini kuului muun muassa molempien organisaatioiden tietoturvaohjeistuksen, -prosessien kehittäminen ja toiminta erilaisissa tietoturvahäiriöissä.

Viestintävirastossa tehtäviini on kuulunut muun muassa uuden lakisäätöisen, kansainvälisistä tietoturvavelvoitteista vastaavan, määrätyn turvallisuusviranomaisen perustaminen Suomeen sekä sen toiminnan kehittäminen. Turvallisuusviranomaisen perustamisen oleellisena osana on ollut EU:lta tulevien turvallisuusvaatimusten ja ohjeiden täytäntöönpano osaksi operatiivista toimintaa. Vastuullani on ollut myös Kyberturvallisuuskeskuksen perustamiseen liittyviä tehtäviä. Kyberturvallisuuskeskuksen perustamisen yhteydessä perehdyin CERT-toimintaan sekä teleyritysten varautumisen ja tietoturvallisuuden sääntelyyn. Ennen kuin viraston ydinprosessit siirrettiin Viestintävirastossa toimialojen johtajien vastuulle, olin tässä opinnäytetyössä kuvatun kyberturvallisuuden varmistaminen-prosessin omistaja.

10 Asiantuntijahaastattelut

Yksi tärkeimmistä haastattelun tavoitteista on saada käsitys siitä, mitä haastateltava henkilö ajattelee ja saada esille hänen näkemyksiään tutkimuskysymysten ratkaisemiseksi. Haastattelun vahvuutena voidaan pitää sitä, että pelkistetyn kysymyssarjan sijaan tutkija voi kysymyksiä tarkentamalla tai lisäkysymyksillä saada varmuuden siitä, että haastateltava on ymmärtänyt kysymysten tarkoitusperän. (Hirsjärvi & Hurme 2009, 34.)

Hirsjärven ja Hurmeen mukaan (2009, 35 & 126) haastattelun vahvuutena voidaan pitää myös sitä, että haastatteluiden kautta saatu tieto on yhdistettävissä suurempiin asiayhteyksiin. On kuitenkin huomioitava, että haastattelun onnistumiseen vaikuttaa haastateltavien henkilöiden motivaatio ja ajankäyttö joka saattaa johtaa siihen, ettei haastateltava keskity haastattelutilanteeseen. Haastattelujen avulla saatujen tietojen analysoinnille ei sinänsä ole olemassa oikeita tai vääriä tapoja, joten tulokinnan suhteen tulee noudattaa erityistä huolellisuutta.

10.1 Haastatteluiden tavoiteasetanta

Haastatteluiden tarkoituksena oli selvittää haastateltavien näkemys Taajuushallinnon häiriönhallinnan nykytilanteesta ja millaisia uudistustarpeita toimintaan on vai tulisiko toiminta säilyttää nykyisellään. Haastateltaviksi valikoitui Taajuushallinnon henkilöitä jotka työskentelevät organisaation eri tasoilla, työuran eri vaiheissa ja joiden työtehtäviin kytkeytyy hätä- ja turvallisuusradioliikenteen häiriöselvitykset. Haastattelut suoritettiin haastateltavien

anonymiteettiä kunnioittaen. Kaikki haastattelukysymykset eivät olennaisesti liittyneet opin-
näytetyön aihepiiriin ja vähemmän olennaisten kysymysten tarkoituksena olikin perehdyttää
opinnäytetyön kirjoittaja laajemmin Taajuushallinnon häiriönhallintaan.

10.1.1 Hätä- ja turvallisuusradioliikenteen määritelmä

Kahdelle haastateltavista hätä- ja turvallisuusradioliikenteen perusmääritelmä oli tuttu maa-
ilman Radio-ohjesäännöstä ja ITU konvention liitteestä. Radio-ohjesääntö on valtiosopimus-
tasoinen sopimus, josta tulevat häiriönselvitystyön arkeen myös toimintatavat ja periaatteet.
He jakoivat käsityksen, että määritelmää on tulkittu kansallisesti viraston toimesta. Yhden
haastateltavan mukaan kansallisia supistuksia on tehty, koska ei ole kalustoa valvoa kaikkia
taajuuksia ja on katsottu, että hyöty valvonnasta on pieni tietyillä taajuuksilla. Lisäksi todet-
tiin, että VIRVE on kansallinen lisäys hätä- ja turvallisuusradioliikenteen osalta.

Peruslinjan mukaisesti hätä- ja turvallisuusradioliikenteen määrittely on tehty taajuusalueit-
tain ja maantieteellisten alueiden mukaan. Kaksi haastateltavaa piti edellä mainitun ryhmit-
telyn mukaista asiakaskuntaa selkeänä. Hätä- ja turvallisuusradioliikennettä on tämän lisäksi
tarkennettu nykyisen Taajuusvalvonnan päällikön toimesta. Ensimmäisenä prioriteettina ovat
aina olleet ihmisen terveyteen tai turvallisuuteen liittyvät tapaukset. Toisaalta kyseessä saat-
taa olla yksittäinen pieni häiriö, mutta jolla on laaja yhteiskunnallinen tai jopa globaali vaiku-
tus. Yhteiskunnallinen vaikutus voi olla esimerkiksi, jos kyse on lento- tai meriliikenteen häi-
riötilanteista. Yhden haastateltavan mukaan pääasialliset asiakasryhmät ovat myös tiedossa,
sillä ne koostuvat hätä- ja turvallisuusradioliikenteen taajuusalueen käyttäjistä. Kaksi haasta-
teltavista piti puolestaan ongelmallisena sitä, että huoltovarmuuden turvaamisen kannalta
keskeisten radiotaajuuksien käyttäjiä ja käyttäjäryhmiä ei ole määritelty. Kaksi haastatelta-
vaa ei tuntenut Radio-ohjesääntöä tai sen määritelmiä.

10.1.2 Hätä- ja turvallisuusradioliikenteen asiakkaiden priorisointi

Kaikki haastateltavat pitivät hätä- ja turvallisuusradioliikenteen asiakkaiden priorisointia sel-
keänä. Tiedossa ei kuitenkaan ollut, onko asiakkaat priorisoitu vielä kyseisen kategorian sisäl-
lä siltä varalta, että useammalle asiakkaalle sattuisi häiriö samanaikaisesti. Yksi haastatelta-
vista koki, että priorisointiin ei ole ollut tarvetta, koska kahdelle kategorian asiakkaalle ei ole
pitänyt lähteä yhtäaikaisesti selvittämään häiriötä. Kahden haastateltavan mukaan häiriöti-
lanteissa olisi todennäköistä, että prioriteeteissa korkealla olisivat lento- ja meriliikenteen
taajuuksien turvaaminen. Yhden haastateltavan mukaan olisi todennäköistä, että Radio-
ohjesäännön mukaiset hätätaajuudet ajaisivat ohi priorisointitilanteessa. Ainostaan yksi
haastateltavista koki, että viraston resurssien olevan rajalliset ja kaikkea häiriöiden selvittä-
mistä ei voida rakentaa Viestintäviraston varaan, vaan myös asiakkailta tulisi olla omaa kykyä
häiriöiden selvittämiseen.

10.1.3 Tulossopimustavoitteen toimivuus

Yksi neljästä haastateltavasta piti liikenne- ja viestintäministeriön ja Viestintäviraston välisen tulossopimuksen tavoitetta, hätä- ja turvallisuusradioliikenteen häiriön selvittämiseen enintään kuluva aika (16 h) tuntia virka-aikana, vähintäänkin epäselvänä. Hänen mukaansa tulkinta on tarkentunut vuosien varrella ja toisaalta vastaavasti selvitysaika on lyhentynyt samanaikaisesti. Selvitykseen kuluva aika on monitulkintainen, koska välillä on häiriöitä, jotka saattavat poistua jopa vuorokausiksi ja palata sen jälkeen uudestaan. Samoin on ollut häiriöitä, jotka ovat tosiasiallisesti olleet pitkäkestoisia ja jatkuneet kuukausia ja yhtäkkiä virastoa on vaadittu selvittämään häiriö 16 tunnin aikarajan sisällä. Käytännössä se, milloin häiriön katsotaan olevan kyseisen aikarajan piirissä, on hyvin pitkälle viraston omaa tulkintaa ja tapauskohtaista arviointia. Aikarajan sisällä oleviin häiriöselvityksiin on kuitenkin pystytty ja samalla asiakkaille on pyritty levittämään tietoa häiriöiden selvittämisiin liittyvistä realiteeteista.

Yksi haastateltavista puolestaan piti hätä- ja turvallisuusradioliikenteen häiriön selvittämiseen kuluva aikarajaa, jonkinlaisena kompromissina. Hänen mukaan 16 tunnissa pystytään juuri ja juuri palvelemaan koko Suomen maantieteellistä aluetta. Nykyinen tulkinta voi olla sellainen, että kiireellisissäkin hätätilanteissa selvitys voisi käytännössä kestää kaksi päivää (8+8h). Toisaalta on ollut tilanteita, joissa häiriö on alkanut lauantaiamuna ja tapaus on selvitetty, ennen kuin varsinainen virka-aika alkaa maanantaina. Lisäksi hän arvioi, että virkajan ulkopuolella tapahtuvan häiriöselvityksen on mahdollistanut henkilöstön kiinnostus ja sitoutuminen toimintaan sekä se, että häiriöselvityksestä päättävä esimies on ollut aina tavoitettavissa.

Yhden haastateltavan mukaan tavoite voisi yhtä hyvin olla 48 tuntia ilman sitomista virka-aikaan. Nykyinen tulossopimuksen tavoitteen muotoilu tarkoittaa käytännössä sitä, että joulunpyhien alussa alkanut häiriö selvitettäisiin vasta viikon kuluessa. Lisäksi yksi haastateltavista toi esille, että 16 tunnin aikaraja virka-aikana, on haasteellinen Suomen suuren koon takia, vaikka selvitystyöhön käytettävä kalustoa onkin nykyään pienempää ja helpommin lentoteitse kuljetettavaa.

10.1.4 Radiöhäiriöilmoitusten vastaanotto

Kaikki neljä haastateltavaa oli yhtä mieltä siitä, että yhteydenotot radiöhäiriöistä saapuvat virastoon joko sähköisen yhteydenottolomakkeen kautta tai puhelimitse. Sähköisen yhteydenottolomakkeen kautta ilmoitukset siirtyvät suoraan TAHA-järjestelmään ja puhelimitse tapahtuvan yhteydenoton asiantuntija kirjaa itse TAHA-järjestelmään. Häiriöselvitys otetaan käsittelyyn TAHA-järjestelmän kautta. Lisäksi viraston asiakaspalvelussa on soittosarja, joka toimii samalla tietynlaisena suodattimena, ennen tapauksen siirtymistä Taajuusvalvonnan asiantun-

tijalle. Lisäksi yksi haastateltavista piti erityisen hyvänä sitä, että suorista yhteydenotoista asiantuntijoille ollaan pääsemässä eroon ja siirrytään kohti keskitettyjä järjestelyitä.

10.1.5 Tiedon jakaminen hätä- ja turvallisuusradioliikenteen häiriöistä

Kaikkien haastateltavien mukaan tietoa häiriöselvityksistä jaetaan ajankohtaispalaverissa ja viikoittain menneen viikon tapaukset sekä mahdollisesti tiedossa olevat tulevat tapaukset käsitellään Taajuusvalvonta-ryhmässä (lessons learned). Yksi haastateltavista piti kirjallista raportointia puutteellisena, vaikka tilanne onkin parantunut TAHA:n käyttöönoton myötä. Toinenkin haastateltava piti TAHA:n käyttöönottoa hyvänä raportoinnin ja muun dokumentoinnin välineenä. Kolme haastateltavista tunnisti tarpeen jakaa häiriöselvitystietoa myös ylöspäin organisaatiosta ja he totesivat, että tämä on Taajuusvalvonnan päällikön vastuulla.

10.1.6 Häiriötapausten vaikutusarvio

Häiriöiden arvioinnin osalta yhdellä haastateltavista ei ollut tietoa miten radiohäiriön tapausarviointi tehdään tai onko käyttötarkoitukseen perustuvaa kriteeristöä valmiina. Hänen mukaansa Euroopan laajuista haittavaikutustaulukkoa on yritetty laatia vuosia, ja että Alankomailla olisi jonkinlainen sovellettava malli. Haastateltavan näkemyksen mukaan matemaattista mallia on mahdoton laatia. Eräs tapa, jolla tapausarviointia voisi alkaa tekemään, olisi säännönmukainen dokumentointi eri häiriöselvityksistä. Tämä loisi perusteet sille, miksi päädyttiin johonkin ratkaisuun selvittämisen kiireellisyyden osalta tai miksi ei tehty mitään. Yhden haastateltavan mukaan tapausarvioinnissa tulisi hyödyntää taajuustietokantaa ja tarkastaa sieltä perusteet, missä häiriön alla olevat taajuudet ovat maantieteellisesti käytössä. Samalla tulisi tarkastaa myös millaisia antennia alueella on käytössä, jotta saataisiin suoraan selvyttä mihin maantieteelliseen suuntaan kannattaa panostaa häiriöselvityksessä. Haastateltavan mukaan hätä- ja turvallisuusradioliikenteen häiriöt ovat varsin paikallisia, joka helpottaa häiriön selvittämistä.

10.1.7 Häiriötapausten omistaja

Kaksi neljästä arvioi, että häiriötapausten vastaanottaja omistaa tapauksen siihen saakka, kunnes päällikkö päättää ketkä lähtevät häiriöselvitykseen, jolloin jompikumpi ottaa vastuun ja TAHA-tiketin omistukseen. Molemmat pitivät riskinä sitä, että päätös hätä- ja turvallisuusradioliikenteen häiriöselvitykseen lähdöstä on pelkästään päällikkötasolla. Lisäksi yhden haastateltavan mukaan kaikki Taajuusvalvonnan päällikön sijaiset eivät välttämättä ole taajuusvalvonnan ammattilaisia ja eivät voikaan täysin ymmärtää häiriöiden merkitystä. Kahden haastateltavan mukaan asiantuntijat pystyisivät itsekin arvioimaan tarpeen häiriöselvitykseen lähdöstä, toki ymmärtäen, että esimiehiäkin tarvitaan päätöksentekoon, sillä häiriöselvitykseen liittyy lähes aina lisäkustannuksia. Kaikki haastateltavat olivat yhtä mieltä siitä, että päätöksen häiriöselvitykseen lähdöstä tekee Taajuusvalvonnan päällikkö tai hänen sijaisensa.

10.1.8 Sidosryhmäyhteistyö

Sidosryhmäyhteistyön osalta yksi haastateltava olisi sitä mieltä, että sidosryhmiä ei tiedoteta säännöllisesti muuta kuin vuosiraportoinnin, toimialakatsauksen yms. yhteydessä. Hän myös arvioi, että joitain yhteistyöpalavereita saattaa olla joidenkin keskeisten tahojen kanssa ja niissä keskitytään vain joihinkin tiettyihin ongelmakohtiin. Yhden haastateltavan mukaan te-leoperaattoreiden kanssa tapauksia on käyty läpi ja tuotu esille, että myös heidän itsensä pitäisi toimia häiriön selvittämiseksi oman kyvykkyytensä puitteissa. Lisäksi hän totesi, ettei säännöllistä ja kohdennettua asiakaspalautetta kerätä kyselyiden muodossa. Yksi haastateltavista puolestaan totesi, ettei ole täysin selvillä siitä, keitä sidosryhmiä tulisi informoida eikä säännöllistä sidosryhmätyötä ole olemassa. Kolme haastateltavaa neljästä toi esille sen että, Taajuushallinnon ja erityisesti Taajuusvalvonnan tulisi ottaa oppia Kyberturvallisuuskeskuksen sidosryhmätyöstä. Lisäksi yksi heistä totesi, että varsinkin siihen tulisi kiinnittää huomiota miten Kyberturvallisuuskeskus viestii kansantajuisesti ja selkokielellä.

10.1.9 Häiriöselvityksen tilannekuvan jakaminen

Kaksi haastateltavaa arvioi, että paras tilannekuva on Taajuusvalvonnan päälliköllä, jolle kerrotaan tapauksesta heti kun on syntynyt riittävästi jaettavaa tietoa. Taajuusvalvonnan päällikkö puolestaan vastaa tiedon jakamisesta muille esimiehille ja Taajuushallinnon johdolle. Yhden haastateltavan mukaan kulloinkin vastuussa oleva koordinaattori jakaa häiriöselvityksiin liittyvät työtehtävät päällikön valtuutuksella, joten kokonaistilannekuva on koordinaattoreilla ja päälliköllä. Hän arvioi, että selkeiden toimintamallien luomisen jälkeen voivat koordinaattorit ja asiantuntijat ottaa enemmän vastuuta. Kaikkien lankojen ei tulisi olla päällikön käsissä kuten nyt, jolloin päällikkö päättää häiriöselvitykseen lähtemisestä. Hän toteaa myös, että vuositasolla Taajuushallinnon johdolle syntyy tilannekuva eri häiriöselvityksistä tehtävän raportin pohjalta. Tällä on suora vaikutus taajuussuunnitteluun ja sitä kautta myös koko toimialan toiminnan vuosisuunnitteluun.

10.1.10 Virka-apupyynnön tekeminen

Kolmen haastateltavan mukaan päätöksen virka-avun pyytämisestä tekee Taajuusvalvontaryhmän asiantuntija tai päällikkö. Yksi haastateltavistaan puolestaan arvioi, että pyynnön virka-avusta tekee Viestintäviraston pääjohtaja ainakin periaatteellisella tasolla. Hänen mukaan osa virka-aputoiminnasta on myös liiaksi henkilösuhteisiin perustuvaa.

10.1.11 Häiriöistä tiedottaminen Viestintäviraston ulkopuolelle

Kaksi haastateltavaa arvioi, että hätä- ja turvallisuusradioliikenteen häiriöistä tiedottaminen tehdään Viestintäviraston ulkopuolelle pääsääntöisesti vain liikenne- ja viestintäministeriön varalla olevalle päivystäjälle (VOP) ja mahdollisesti valtioneuvoston tilannekeskukselle (VNTI-

KE). Kaksi haastateltavista totesi myös, että hätä- ja turvallisuusradioliikenteen häiriöistä tiedottaminen valtioneuvoston tilannekeskukselle (VNTIKE) voitaisiin hyvin tehdä Kyberturvallisuuskeskuksen toimesta, koska keskuksella on rutinoituneet toimintatavat VNTIKE:n suuntaan asiointissa. Yhden haastateltavan mukaan olisi kuitenkin huomioitava Taajuusvalvonnan tietopohja tiedotteiden laatimisessa, jotta asiat tulevat huomioituksi oikein substanssin näkökulmasta. Kaksi haastateltavista ei tuntenut valtioneuvoston tilannekeskuksen eikä liikenne- ja viestintäministeriön varallaoloon perustuvaa päivystystoimintaa lainkaan.

10.2 Haastattelujen yhteenveto

Haastatteluista voidaan todeta, että häiriöilmoitukset tallennetaan viraston TAHA-järjestelmään yhdenmukaisella tavalla. TAHA-järjestelmää käytetään myös työtehtävien ja kamamiseen yhdenmukaisella tavalla. Hätä- ja turvallisuusradioliikenteen määritelmän tuntemisesta, hätä- ja turvallisuusradioliikenteen taajuuksien käyttäjäryhmien häiriötapauksien priorisoinnista ja häiriötapauksen vaikutusarvioinnin tekemisestä ei löydy täysin yhdenmukaista käsitystä. Häiriötapauksien arvioinnin onnistuminen ja priorisointi on pitkälti perustunut siihen, ettei yhtäaikaista vakavia häiriötapauksia ole ollut. Yhtä mieltä oltiin siitä, että häiriötapaukset käsitellään viikoittain Taajuusvalvonnan ryhmäpalaverissa. Haastateltavat kokivat, että asiantuntijat voisivat ottaa enemmän vastuuta häiriöselvitykseen lähtemisestä, jos toimintamallit olisivat selkeämmät ja samalla helpotettaisiin henkilöriippuvuutta. Virka-avusta päättäminen oli osin epäselvää ja tiedottaminen virastosta sidosryhmille kaipaa myös kehittämistä.

11 Johtopäätökset

Viestintävirastossa on pyritty ydinprosessien avulla yhtenäistämään häiriöhallintaprosessia siten, että päätöksentekoprosessi olisi sujuvaa, vastuut selkeitä, tuotettava tieto olisi tasa-laatuista ja sidosryhmätiedotus olisi vaikuttavaa. Opinnäytetyön haastattelut tukevat muuta tutkimusaineistoa sekä havaintoja siitä, että Viestintäviraston toimialakohtaisten prosessien yhtenäistämässä ja yhteensovittamisessa tulee vastaan vielä useita kysymyksiä liittyen tiedon luotettavuuteen, tiedon analysointiin, päätöksentekoprosessiin, tilannekuvan tuottamiseen sekä sisäiseen että ulkoiseen tiedottamiseen.

Tämä opinnäytetyö on ensimmäinen virastossa tehty tutkimus, jossa arvioidaan kyberturvallisuuden varmistaminen ydinprosessin nykykäytäntö sekä siihen liittyvää ohjeistusta ja operatiivista toimintaa. Opinnäytetyö osoitti, että on olemassa tiettyjä ristiriitoja prosessien yhtenäistämisen tahtotilan ja käytännön tekemisen välillä. Tämä osaltaan lisää myös tutkimuksen luotettavuutta ja uskottavuutta sekä korostaa tarvetta häiriöhallinnan yhtenäistämiseen virastossa. Opinnäytetyö tehtiin relevanttia lähdeaineistoa hyödyntäen ja objektiivisesta lähtö-

kohdasta. Asiantuntijahaastattelussa nousi toistuvasti esiin samoja keskeisiä teemoja ja kysymyksiä, joita oli jo opinnäytetyön suunnitteluvaiheessa otettu esille.

Opinnäytetyö keskittyi vakaviin häiriöpoikkeamiin eli radiohäiriöiden osalta hätä- ja turvallisuusradioliikenteeseen, tietoturvallisuuden osalta tietoturvaloukkauksiin ja yleisten viestintäverkkojen osalta verkkorakenteen häiriöihin ja vikoihin. Kyberturvallisuuskeskuksessa on sisäisessä ohjeistuksessa tarkoin määritelty viestintäverkkojen- ja palveluiden toimivuuden häiriötilanteet ja vakavuudet kuten myös luokittelut ja vakavuusarviot tietoturvahäiriöistä. Nämä edellä mainitut luokittelut perustuvat aihealueista annettuihin Viestintäviraston määräyksiin. Radiohäiriöiden osalta on ollut jossain määrin haastavaa luokitella taajuuksien käyttäjäryhmiä hätä- ja turvallisuusradioliikenteeseen, koska huoltovarmuus kriittisiä käyttäjäryhmiä ei olla määritelty tarkkaan viranomaisten toimesta. Nykykäytäntö perustuu omaan kansalliseen arvioon, muiden maiden parhaisiin käytänteisiin ja Radio-ohjesäännön yleiseen määrittelyyn hätä- ja turvallisuusradioliikenteen liikennelajista.

Häiriöhallintaan liittyvässä tiedonkulussa on kehitettävää sekä Kyberturvallisuuskeskuksessa että Taajuushallinnossa. Sisäisessä tiedonjaossa tulisi käyttää jo olemassa olevia tai tarpeen mukaan uusia jakelulistoja yksittäisten henkilöiden tiedottamisen sijaan. Samoin vakavan häiriön ilmoittamisen jälkeen tulisi muistaa tiedottaa myös häiriön poistamisesta tai varoituksen tarpeettomuudesta. Sisäistä tiedottamista tulisi arvioida viraston yhteisen kyberturvallisuuden varmistaminen -prosessin näkökulmasta, ei yksittäisen toimialan näkökulmasta. Kyberturvallisuuskeskuksen ulkoinen sidosryhmätiedottaminen on erittäin hyvällä tasolla, tärkeät yhteiskunnan sektorit on tunnistettu ja tiedottamista voidaan kohdistaa oikeille tahoille. Yleinen varoittaminen toimii myös prosessinomaisesti. Taajuushallinnon osalta yleistä tiedottamista radiohäiriöistä tapahtuu varsin vähän ja tiedottaminen koostuu lähinnä kahdenvälisistä keskusteluista häiriön selvittämisen ja siitä toipumisen yhteydessä. Yleisesti ottaen häiriöhallintaan liittyvää palautekyselyä järjestetään virastossa vähän ja sitä tulisikin lisätä hyvän ja laadukkaan asiakasnäkökulman kehittämiseksi.

Häiriöhallinnassa ilmoituksen vastaanottajalla ja häiriön vakavuuden arvioitsijalla on vastuu siitä miten häiriötapaus lähtee prosessissa etenemään ja miten asiasta tiedotetaan. Kyberturvallisuuskeskuksessa on sisäisessä ohjeistuksessa määritelty päivystäjän ja tilannekuvakoordinaattorin roolit ja vastuut. Taajuushallinnon osalta sisäinen ohjeistus koskettaa tiettyjä nimettyjä henkilöitä. Vastuut Taajuushallinnossa on määritelty yleisellä tasolla. Radiohäiriöiden selvittämiseksi roolien kuvaamista tulisi selkeyttää ja kiinnittää huomioita päätöksenteon kanalta oleellisiin pullonkauluihin. Taajuushallinnon ja Kyberturvallisuuskeskuksen päivystäjien ja tilannekuvakoordinaattoreiden yhteistyötä ja avunantoa nimenomaan vakavissa häiriötapauksissa tulisi kehittää edelleen.

Häiriönhallintaan liittyvää ohjeistusta on saatavilla riittävästi erityisesti Kyberturvallisuuskeskuksessa ja erilaisia poikkeamatilanteita on hyvin runsaasti. Myös Taajuushallinnossa on sisäistä ohjeistusta. Haastattelujen ja kokemuksen pohjalta voidaan arvioida, ettei ohjeiden päivittäminen ja sisäinen koulutus ole vielä riittävällä tasolla. Varsinkin Kyberturvallisuuskeskuksessa tilanteiden monitahoisuus ja kompleksisuus vaatii jatkuvaa arviointia tietoturvahäiriön luokittelusta ja käytännön toimista. Ohjeiden itsenäisellä lukemisella ja kertakoulutuksella ei päästä välttämättä haluttuihin tavoitteisiin, vaan asioiden omaksuminen vaatii harjoittelua ja kertaamista.

Taajuusvalvonnan ryhmäpalaverissa käydään viikoittain läpi mahdolliset hätä- ja turvallisuusradioliikenteeseen liittyneet tapaukset ja arvioidaan niihin liittyviä toimenpiteitä. Tietoa jaetaan hyvin ryhmän sisällä. Epäselväksi haastattelujen pohjalta jää se, miten ja millä tavoin arviointi kehittää sisäistä ohjeistusta ja päivittäistä työtä. Kyberturvallisuuskeskuksessa kerätään kuukausittain ja tarvittaessa useammin merkittävimmät tapaukset yhteiseen arviointiin. Arviointiin voi osallistua koko keskuksen henkilöstö. Kyberturvallisuuskeskuksessa arvioinnin pohjalta kehitetään ohjeistusta, mutta uuden ohjeistuksen kouluttaminen on vain tyydyttävällä tasolla.

Viestintävirasto voi saada virka-apua radiohäiriöiden selvittämiseen Rajavartiolaitokselta tai Puolustusvoimilta. Haastattelujen pohjalta voidaan todeta, että viraston sisäisestä ohjeistuksesta osalta puuttuu selkeä prosessi siitä miten virka-avusta pyytamisestä päätetään.

Taajuushallinnossa on kehitetty sidosryhmätyötä siihen suuntaan, että keskeisillä toimijoilla olisi myös omaa kykyä selvittää radiohäiriöitä. Sidosryhmätyöstä voisi kehittää vielä entisestään kaksisuuntaisempaa muotoon ja tiedottaa yleisesti häiriötilanteista vielä laajemmalle joukolle. Kyberturvallisuuskeskuksen osalta sidosryhmätyö on suunnitelmallista ja hyviä käytäntöjä eri mallien toteuttamisesta olisi hyvä jakaa koko virastonkin osalta.

Tutkimuksen kannalta keskeisiin kysymyksiin Taajuushallinnon ja Kyberturvallisuuskeskuksen häiriönhallintaprosessien yhtenäisyydestä ja häiriönhallinnan laadun ja raportoinnin yhdenmukaisuudesta saatiin selkeä vastaus. Opinnäytetyön tuloksena voidaan todeta, etteivät häiriönhallintaprosessit ole riittävän yhdenmukaisia. Lisäämällä prosessien yhdenmukaisuutta, saadaan tuotettua viraston asiakkaille parempaa palvelua ja laatua. Tämän lisäksi häiriöiden raportointia yhdenmukaistamalla viraston tiedonkulku paranee. Tiedonkulun paraneminen puolestaan sujuvoittaa sisäistä viestintää ja luo samalla asiakkaille vielä paremman mahdollisuuden oikea-aikaiseen ja kohdennettuun viestintään.

Tämän lisäksi kyberturvallisuuden varmistaminen-prosessiin saatiin haastattelujen pohjalta parannusehdotuksia sekä tunnistettiin jatkotutkimusaiheita. Häiriönhallintaprosessista voisi

todeta sen, että häiriöilmoitus otetaan virastossa vastaan yhtenäisellä tavalla ja samoin sen dokumentointi tehdään viraston Tapahtumienhallintatietojärjestelmään yhdenmukaisella tavalla. Häiriöilmoituksen vastaanottaja on käytännössä vastuussa häiriön arvioinnista ja ensitoimista. Erityisesti vakavien tapauksien yhdenmukaisessa arvioinnissa, tapausten sisäisessä tiedottamisessa ja häiriötapauksesta oppimisessa tarvitaan selkeästi enemmän yhtenäistämistä. Laadun varmistamisen osalta olisi tärkeää molemmilla toimialoilla jatkaa ja kehittää "lessons learned" yhteisarviointia. Häiriöhallintaan liittyvän ohjeistuksen jatkuva päivittäminen ja ohjeiden koulutus henkilöstölle on myös keskeinen tapa varmistaa, että jokainen häiriötapauksessa vastuussa oleva toimii samalla tavalla.

Tutkimuskysymysten valintaa voidaan pitää varsin onnistuneina, koska opinnäytetyön tulokset kehittävät merkittävästi viraston häiriöhallintaprosessia, yhtenäistävät toimintatapoja, kannustavat yhteistyöhön, parantavat sisäistä tiedonjakamista ja varmistavat laadukkaan palvelun asiakkaalle.

12 Oman työn arviointi

Jo opinnäytetyön suunnitteluvaiheessa vuodenvaihteessa 2015-2016, oli Viestintävirastossa käynnissä ydinprosessin prosessiohjausmallin pilotointi. Viraston sisäisissä keskusteluissa oli havaittavissa tahtotilaa viraston eri toimialarajat ylittävien ydinprosessien kuvaamisesta ja yhtenäistämisestä, jotta päällekkäiseltä työltä vältyttäisiin ja virasto näkyisi asiakaskunnalleen yhtenäisenä Viestintävirastona.

Opinnäytetyön kantavia teemoja ja tutkimuskysymyksiä ovat Viestintäviraston kahden eri toimialan, Kyberturvallisuuskeskus ja Taajuushallinto, häiriöhallinnan toimintamallien suhde ja yhtenäistämisen tarve. Viestintäviraston tulisi tulevaisuudessa vastata entistä paremmin digitalisoituvan yhteiskunnan vaatimukseen sen toiminnan häiriöttömydestä. Tutkimuskysymyksiin vastaaminen osoittautui oletettua vaikeammaksi molempien toimialojen keskeneräisen ohjeistuksen ja puutteellisten prosessikuvausten valossa. Toisaalta vastausten analysointi oman kokemukseen verrattuna valotti minulle mahdollisuuksia, joita erilaisten prosessien yhtenäistäminen tuo tullessaan.

Erityisen hedelmällistä opinnäytetyön laatimisessa oli oman ammattitaidon ja tietämyksen kartuttaminen. Sain opiskella perusteita radiotaajuuksista, niiden käytöstä ja merkityksestä digitaaliselle yhteiskunnalle.

12.1 Luotettavuuden arviointi

Opinnäytetyön tutkimuksen luotettavuus on keskeinen osa työn lopputuloksen arviointia. Tälle opinnäytetyölle asetettiin tavoitteita, joihin on pyritty vastaamaan toiminnallisella ja laadul-

lisellä tutkimuksella. Arvioinnin keskeisiä käsitteitä ovat reliabiliteetti (luotettavuus) ja validiteetti (pätevyys). Luotettavuus ja pätevyys sopivat erinomaisesti määrälliseen tutkimukseen ja on selvää, ettei laadullisen tutkimuksen luotettavuutta voida arvioida samoin tavoin kuin määrällisen. Luotettavuuden arvioinnin osalta voidaan pohtia onko tutkimus johdonmukainen, tuottavatko haastattelukysymykset samantapaisia vastauksia ja ovatko tutkittavat käsitteet olleet riittävän selkeitä sekä tutkijalle että haastateltaville. (Saaranen-Kauppinen, Puusniekka, Kuula, Rissanen & Karvinen 2009, 24-27.)

Pätevydessä on kysymys siitä, onko opinnäytetyö tehty perusteellisesti ja ovatko siinä olevat johtopäätökset "oikeita". Kehittämistavoitteissa ei tyypillisesti ole yhtä oikeaa totuutta tai täydellisyyttä, vaan haetaan menettelytapoja ja ohjeistuksia, jotka elävät muuttuvassa arjessa. (Saaranen-Kauppinen ym. 2009, 25-27.)

Opinnäytetyön haastattelukysymykset esitettiin etukäteen muulla kuin haastateltavalla henkilöstöllä ja kaikki haastattelut nauhoitettiin haastateltavien suostumuksella. Kysymykset koettiin selkeiksi ja ymmärrettäviksi. Nauhoitetut haastattelut aukikirjoitettiin, joten voidaan aikakin todeta, että kysymystenasettelun ymmärrettävyys, käsitteistö ja dokumentointi on ollut luotettavaa. Osin haastattelun tulokset ovat ristiriitaisia, ja näissä tilanteissa on jouduttu miettimään miten moninaiset lausunnot samasta asiasta pitävät paikkansa. Toisaalta tämä tilanne kuvaa hyvin laadullisen tutkimuksen luonnetta.

Tämän opinnäytetyön tavoitteena oli kehittää viraston kyberturvallisuuden varmistamisen prosessia. Työssä esitetyt löydökset ovat päteviä ja niillä kuvataan viraston nykytilaa. Prosessi kehittyy viraston arjessa tapahtuvan oppimisen ja jatkuvan parantamisen kautta. Tämän työn perusteet ovat Viestintävirastoa ohjaavassa lainsäädännössä ja viraston määräyksissä. Tutkittavan asian pätevyys ilmenee paremmin työn tuloksen uskottavuutena ja vakuuttavuutena ja sellaisena kuin se on tutkimustilanteessa työn tekijälle ilmennyt.

12.2 Jatkotutkimusaiheet

Tämä opinnäytetyö osoittaa sen, että tulisi ainakin käynnistää jatkohanke, jossa määriteltäisiin huoltovarmuuden turvaamisen kannalta keskeiset radiotaajuuksien käyttäjät. Nykymallin hätä- ja turvallisuusradioliikenteen määrittelyä ja käyttäjäryhmiä on yritetty yhtenäistää hakemalla esimerkkejä ja toimintatapoja muiden maiden viestintäviranomaisilta. Suomessa laki tietoyhteiskuntakaaresta määrittelee velvollisuuden varautua normaaliolojen häiriötilanteisiin ja poikkeusoloihin. Tietoyhteiskuntakaaren (917/2014, TYK 281 §) mukaan:

"Huoltovarmuuden turvaamisen kannalta keskeisten radiotaajuuksien käyttäjien ja käyttäjäryhmien on huolehdittava radiotaajuuksien riittävän häiriöttömästä ja tehokkaasta käytöstä normaaliolojen häiriötilanteissa ja valmiuslaissa tarkoi-

tetuissa poikkeusoloissa. Liikenne- ja viestintäministeriö päättää keskeisistä radiotaajuuksien käyttäjistä ja käyttäjäryhmistä Huoltovarmuuskeskuksen esityksestä."

Huoltovarmuuden kannalta keskeisten taajuuksien käyttäjien tarkka määrittely on haastavaa, ja vaatii jatkuvaa tarkastelua yhteiskunnan toimintojen ja arvoketjujen muuttuessa. Varautumisen kannalta määrittely on ensiarvoisen tärkeää, koska tällä hetkellä Viestintävirastolta puuttuu selkeä näkemys taajuuksien käyttäjien kriittisyydestä normaaliolojen häiriötilanteissa ja poikkeusoloissa. Viestintäviraston tulisi kyetä myös harjoittelemaan häiriötilanteita yhteiskunnassa oikeilla perusteilla.

Toisena keskeisenä jatkokehitystyönä voidaan nähdä fyysisten verkkojen tilannekuvan muodostamisen ongelma eli puutteelliset tiedot viranomaisverkko VIRVE:n häiriöistä. Myöskään julkisen hallinnon turvallisuusverkkotoiminnalla (TUVE) ei ole ilmoitusvelvollisuutta Viestintävirastolle. Julkisen hallinnon turvallisuusverkkotoiminnasta säädetyn lain (10/2015, 23 §) mukaan Viestintävirastolla on mahdollisuuksien mukaan velvollisuus antaa virka-apua turvallisuusverkon palvelutuotannon häiriöttömän toiminnan takaamiseksi. VIRVE -verkon osalta Viestintävirasto näkee mahdollisuuksia korjata mainittu puute VIRVE-verkon meneillään olevassa kehitystyössä.

Lähteet

Painetut lähteet

Aaltola, J. & Valli, R. 2001. Ikkunoita tutkimusmetodeihin I: metodin valinta ja aineistonkeruuvirikkeitä aloittelevalla tutkijalla. PS-kustannus: Jyväskylä.

Hirsjärvi, S. & Hurme, H. 2009. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus Helsinki University Press.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2007. Tutki ja kirjoita. 13.-14., osin uudistettu painos. Helsinki: Tammi.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2014. Kehittämistyön menetelmät. 3. uudistettu painos. Helsinki: SanomaPro.

Saaranen-Kauppinen, A., Puusniekka, A., Kuula, A., Rissanen, R. & Karvinen, I. 2009. Toinen vedos. Menetelmäopetuksen tietovaranto. Tampere: Tampereen yliopisto.

Tuomi, J. & Sarajärvi, A. 2002. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Tammi

Tuomi, J. & Sarajärvi, A. 2009. Laadullinen tutkimus ja sisällönanalyysi. 6. uudistettu laitos. Helsinki: Tammi

Sähköiset lähteet

Erillisverkot. 2017. Omistajuus ja hallinto. Viitattu 29.4.2017.
<https://www.erillisverkot.fi/erillisverkot>

Euroopan komissio. 2017. 5G for Europe Action Plan. Viitattu 29.4.2017.
<https://ec.europa.eu/digital-single-market/en/5g-europe-action-plan>

IS. 2015. IoT Pohjoismaissa. Viitattu 18.4.2017.
<http://www.is.fi/digitoday/mobiili/art-2000001867859.html>

ITU. 2015. Report ITU-R M.2370-0. Viitattu 29.4.2017.
https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2370-2015-PDF-E.pdf

Microsoft. 2016. Microsoft Security Intelligence Report. Viitattu 17.4.2017.
<https://www.microsoft.com/security/sir/default.aspx>

Otavan Opisto. 2015. Sähkömagneettisen säteilyn spektri. Viitattu 22.4.2017.
http://opinnot.internetix.fi/fi/muikku2materiaalit/lukio/fy/fy3/4_valo/402?C:D=2079119&m:selres=2079119

RCRWirelessNews. 2017. Viitattu 17.4.2017.
<http://www.rcrwireless.com/20160628/opinion/reality-check-50b-iot-devices-connected-2020-beyond-hype-reality-tag10>

Valtiovarainministeriö. 2016. Pilkahduksia tulevaisuuteen. Viitattu 29.4.2017.
<http://vm.fi/documents/10623/3507992/Pilkahduksia+tulevaisuuteen+%E2%80%93digitalisaation+ja+robotisaation+mahdollisuudet+-raportti/e7154bd3-910a-4f99-89ee-4f9299043d3c>

Viestintävirasto. 2010. Radiotaajuuksien kysyntä tulevaisuudessa. Viitattu 17.4.2017.
https://www.viestintavirasto.fi/attachments/Radiotaajuus_2010_syksy.pdf

Viestintävirasto. 2014a. Määräys 66 teletoiminnan häiriötilanteista. Viitattu 17.4.2017.

<https://www.viestintavirasto.fi/ohjausjavalvonta/laitmaarayksetpaatokset/maaraykset/maaraykset66teletoiminnanhairiotilanteista.html>

Viestintävirasto. 2014b. Määräys 67 teletoiminnan tietoturvasta. Viitattu 17.4.2017.
<https://www.viestintavirasto.fi/ohjausjavalvonta/laitmaarayksetpaatokset/maaraykset/maaraykset67teletoiminnantietoturvasta.html>

Viestintävirasto. 2014c. Kyberturvallisuuskeskuksen tietoturvapalvelut. Viitattu 29.4.2017.
<https://www.viestintavirasto.fi/kyberturvallisuus/viestintavirastontietoturvapalvelut.html>

Viestintävirasto. 2015a. Toimialakatsaus 4/2015. Viitattu 17.4.2015.
https://www.viestintavirasto.fi/attachments/Viestintaviraston_toimintaymparistokatsaus_2015.pdf

Viestintävirasto. 2015b. Määräykset 66 ja 67. Viitattu 19.4.2017.
https://www.viestintavirasto.fi/attachments/esitykset/Uudet_M66_ja_M67.pdf

Viestintävirasto. 2016a. Tilastot ja vertailut. Viitattu 29.4.2017.
<https://www.viestintavirasto.fi/tilastotjatutkimukset/tilastot.html>

Viestintävirasto. 2016b. Ilmoitus radiohäiriöstä. Viitattu 20.4.2017.
<https://www.viestintavirasto.fi/asioikanssamme/ilmoituksetjambuutlomakkeet/tietoturvailmoituksetja-hakemukset/ilmoitusradiohairioista.html>

Viestintävirasto. 2017a. Tietoturvan vuosi 2016. Viitattu 17.4.2017.
https://www.viestintavirasto.fi/attachments/tietoturva/Tietoturvan-vuosi_2016_ViVi_29-11-2017_L.pdf

Viestintävirasto. 2017b. viestintäviraston organisaatio. Viitattu 29.4.2017.
<https://www.viestintavirasto.fi/viestintavirasto/virastonesittelyjatehtavat/organisaatio.html>

Viestintävirasto. 2017c. Viestintäviraston toimialat. Viitattu 29.4.2017.
<https://www.viestintavirasto.fi/viestintavirasto/virastonesittelyjatehtavat/toimialat.html>

Viestintävirasto. 2017d. Radiotaajuusmääräys 4. Viitattu 18.4.2017.
<https://www.viestintavirasto.fi/ohjausjavalvonta/laitmaarayksetpaatokset/maaraykset/radiotaajuusmaarays4.html>

Viestintävirasto. 2017e. Liikenne- ja viestintäministeriön ja Viestintäviraston välinen tulossopimus vuodelle 2017. Viitattu 21.4.2017.
https://www.viestintavirasto.fi/attachments/Liikenne-_ja_viestintaministerion_ja_Viestintaviraston_valinen_tulossopimus_vuodelle_2017.pdf

Yhteisverkko. 2017. Suomen Yhteisverkko. Viitattu 29.4.2017.
<http://yhteisverkko.fi/suomen-yhteisverkko/>

Äänipää. 2005. Äänen taajuus. Viitattu 29.4.2017.
http://www.aanipaa.tamk.fi/taajuu_1.htm

Julkaisemattomat lähteet

Haastattelu A. 2016. haastattelu 26.5.2016. Viitattu 22.4.2017.

Haastattelu B. 2016. haastattelu 30.5.2016. Viitattu 23.4.2017.

Haastattelu C. 2016. haastattelu 27.6.2016. Viitattu 23.4.2017.

Haastattelu D. 2016. haastattelu 27.6.2016. Viitattu 23.4.2017.

Viestintävirasto. 2017. Sisäinen ohje A. Viitattu 29.4.2017.

Viestintävirasto. 2017. Sisäinen ohje B. Viitattu 29.4.2017.

Virallislähteet

HE 80/2001 vp. Hallituksen esitys eduskunnalle radiolaiksi sekä laeiksi televisio- ja radiotoiminnasta annetun lain ja yksityisyyden suojasta televiestinnässä ja teletoinnin tietoturvas- ta annetun lain 4 §:n muuttamisesta

Kansainvälisen televiestintäliiton (engl. ITU International Telecommunication Union) Radio- ohjesääntöön

Laki julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015)

Laki kansainvälisistä tietoturvaluvelvoitteista (588/2004)

Laki tietoturvaluveluuden arviointilaitoksista (1405/2011)

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009)

Laki viestintähallinnosta (625/2001)

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvaluveluuden arvi- oinnista (1406/2011)

Tietoyhteiskuntakaari (917/2014)

Turvaluveluusselvityslaki (726/2014)

Viestintäviraston radiotaajuusmääräys 4V/2016 M

Viestintäviraston määräys teletoinnin häiriötilanteista 66/2014 M

Viestintäviraston määräys teletoinnin tietoturvaluveluudesta 67A/2015 M

Kuviot

Kuvio 1: Sähkömagneettinen spektri (Otavan opisto 2015)	10
Kuvio 2: Yleiskuva taajuuksien käytöstä Suomessa (Viestintävirasto 2009)	11
Kuvio 3: Viestintäviraston organisaatio (Viestintävirasto 2017)	14
Kuvio 4: Viestintäviraston ydinprosessit (Viestintävirasto 2015)	15
Kuvio 5: Laadun varmistaminen (Viestintävirasto 2015)	16
Kuvio 6: Microsoftin 21:n Security Intelligence Report tilastoja (Viestintävirasto 2016)	17
Kuvio 7: Kiireellisten hätä- ja turvallisuusradioliikenteen käsittely.....	23
Kuvio 8: Varoituksen tasot	26
Kuvio 9: Tapauksen arviointi ja käsittely.....	27
Kuvio 10: Tiedonkulku Kyberturvallisuuskeskuksessa.....	28

Liitteet

Liite 1: Taajuushallinnon henkilöstön haastattelukysymykset	45
---	----

Liite 1: Taajuushallinnon henkilöstön haastattelukysymykset

1. Hätä- ja turvallisuusliikenteen määrittely
 - Miten määrittely on tehty ja miten häiriötilanteet priorisoidaan?
 - Mikä/mitkä ovat pääasialliset asiakasryhmät?
 - Onko kaikki asiakkaat priorisoitu selkeästi?
 - Onko tavoite LVM tulossopimusmallissa riittävän selkeä?
 - "Hätäliikenteen radiohäiriöt selvitetään tehokkaasti. Häiriön selvittämiseen enintään kuluva aika, (16) tuntia virka-aikana"
2. Radiohäiriön vastaanotto
 - Mitä kanavia pitkin ja kenelle/keille tieto radiohäiriöstä saapuu virastoon?
 - Miten asiakkaita on neuvottu olemaan yhteydessä?
 - Miten tieto jaetaan toimialalla? Onko sovittuja pelisääntöjä tai vastuutahoja?
 - Kenestä tulee tapauksen omistaja?
 - Mitä ensitietoa häiriötapauksesta tarvitaan?
 - Onko olemassa valmista "sapluunaa" tarvittavista teknisistä tiedoista?
3. Radiohäiriön tapausarviointi
 - Miten tapauksen vaikuttavuusarviointi tehdään?
 - Arvioidaanko laajemmat vaikutukset?
 - Informoidaanko muita sidosryhmiä? Miten pidetään yllä sidosryhmäverkostoa?
 - Kuka/ketkä tekevät päätöksen häiriöselvitykseen lähtemisestä?
 - Mitkä ovat häiriöselvitystyöhön kuuluvien roolit?
4. Radiohäiriöiden selvittäminen
 - Jaetaanko johdolle tilannekuvatietoa, minkälaista ja missä vaiheessa?
 - Miten asianomistajaa ohjeistetaan (asianomistajan omat toimet)
 - Vastuukysymykset (omaisuuden/henkien menetyt?)
 - Kun oma kyky ei riitä, kuka esim. tekee päätöksen virka-avusta?
 - Mistä muualta voidaan pyytää apua, verkostot?
5. Häiriöiden selvittäjien turvallisuuskysymykset
 - Vaaralliset työtilanteet jne.
6. Raportointi
 - Millä tavoin häiriöiden selvitys raportoidaan (matkalla? Tehdäänkö mittauksia?)
 - Mitä ohjeistusta on saatavilla raportoinnista?
 - Onko määritelty raportin valmistumisaikaa (esim. 2vrk kuluessa?)
 - Miten raportit käsitellään?, esitelläänkö kollegoille/ esimiehelle? Koostetaanko yhteen?
 - Miten arvioidaan tapausten selvittämisen onnistuminen?

- Lessons learned
- Muuttaako häiriöiden selvittely omaa teknistä häiriöselvitykseen kuuluvaa toimintaa?
- Muuttaako ohjeistusta asiakkaille tai viraston määräyksiä tai suosituksia?
- Tarvitaanko viraston tiedotusta asiasta?
- Miten palaute kerätään asiakaskunnalta?
- Jaetaanko tieto tapauksesta ja sen selviämisestä asianomistajalla ja miten, jos jaetaan?
- Onko muita tavoitteita kuin aikatavoite 16h?