

Kalle Santaharju

**GPS-VASTAANOTTIMEN HARHAUTTAMINEN HEL-  
SINGIN LÄNSISATAMAN SYVÄVÄYLÄN ALUEELLA  
JA SEN VAIKUTUKSET MERENKULKUUN**



JYVÄSKYLÄN YLIOPISTO  
TIETOJENKÄSITTELYTIETEIDEN LAITOS  
2017

## TIIVISTELMÄ

Santaharju, Kalle

GPS-vastaanottimien harhauttaminen Helsingin Länsisataman syväväylän alueella ja sen vaikutukset merenkulkuun

Jyväskylä: Jyväskylän yliopisto, 2017, 75 s.

Kyberturvallisuus, Pro gradu

Ohjaajat: Lehto, Martti

Tutkimuksessa selvitetään teoreettisesta ja laadullisesta näkökulmasta miten haavoittuva ja onnettomuusaltis Helsingin Länsisataman syväväylän alue on satelliittipaikannusjärjestelmään kohdistuvan onnistuneen harhautushyökkäyksen sattuessa. Satelliittipaikannusjärjestelmä, alusten automaattinen tunnistusjärjestelmä ynnä muut navigoinnin järjestelmät on yhdistetty osaksi integroitua merikarttajärjestelmää, mikä herättää kysymyksen siitä, olisiko mahdollista, että harhauttamalla satelliittipaikannusjärjestelmän vastaanotinta kyettäisiin ajatuttamaan alus väärälle suunnalle? Jos alus vastaanottaa harhautettua satelliittipaikannukseen perustuvaa signaalia, voi tämä johtaa hiljalleen aluksen lipumiseen sivuun väylältään kohti onnettomuutta. Tässä tutkimuksessa selvitetään satelliittipaikannukseen perustuvan signaalin harhauttamisen teoriaa sekä pyritään vastaamaan siihen, miten yhteiskuntamme on valmistautunut ja huomionnut yllä esitellyn tilanteen. Tutkimus painottuu suuriin risteilijäaluksiin, joita tutkittavalla alueella liikkuu päivittäin useita vuoden ajankohdasta riippumatta. Kirjallisen teorian lisäksi varmuutta ja todistusaineistoa tutkimukselle on haettu oman alansa asiantuntijoilta tekemällä heille teemahaastattelu, joista saatua tietoa on verrattu alussa kirjallisuuskatsauksella kerättyyn teoriaan.

Tutkimuksen tulokset osoittavat, että alusten ajattaminen onnettomuusalttiiseen tilanteeseen onnistuu vain, jos alus liikkuu täysin automaation varaisesti, ja navigoija ohjailee alustaan vastoin kansallisia ja kansainvälisiä merenkulun lakeja. Navigoija ei tällöin syystä tai toisesta vertaile satelliittipaikannusjärjestelmän tuomaa tietoa visuaaliseen navigoinnin ja tutkan tuomaan tietoon. Aluksen satelliittipaikannusjärjestelmän kautta saatu manipuloitu tieto menee lisäksi alusten automaattisen tunnistusjärjestelmän kautta Helsingin alusliikennepalvelukeskukselle, joka kykenee paljastamaan mahdollisen harhautustilanteen vertailemalla omia tietojaan fuusioidusta tilannekuvamallistaan. Tämä järjestelmä koostuu useista tutkista, kameroista ja alusten automaattisesta tunnistusjärjestelmien lähettämistä tiedoista. Jos alus jostain syystä ajautuisi väärälle suunnalle, Alusliikennepalvelukeskus kykenee näkemään tämän ristiriitatilanteen, koska kaikki nämä tekniset järjestelmät perustuvat eri tekniikalle ja ovat täysin itsenäisiä. Alusliikennepalvelukeskuksissa luotetaan tällaisissa tilanteissa vain tutkan tuomaan tietoon.

Asiasanat: Satelliittipaikannusjärjestelmä, GPS-järjestelmä, satelliittipaikannusharhautus, GPS-harhautus, alusten automaattinen tunnistusjärjestelmä, AIS-järjestelmä, VTS

## ABSTRACT

Santaharju, Kalle

GPS-spoofing in the Helsinki West Harbour sea area and its effects on seafaring  
Jyväskylä: University of Jyväskylä, 2010, 75 p.

Major subject, Cyber Security, Master's Thesis

Supervisor(s): Lehto, Martti

This study examines the risk profile of the Helsinki West Harbour sea area and investigates its susceptibility in the event of a GPS-spoofing attack. The research is conducted from both a theoretical and a qualitative perspective. As a vessel's GPS (Global Positioning System) and AIS (Automatic Identification System) are both connected within the ECDIS (Electronic Chart Display Information System), this raises the question if a vessel could be misdirected to a false course by spoofing the GPS receiver. Were a vessel to receive a spoofed GPS-based signal, the risk of the vessel slowly drifting off course and towards potential collision arises. This study outlines the theories regarding GPS-spoofing, and analyses how Finnish Maritime protocol has taken into account and prepared for the risks involved. The study focuses on large cruise ships several of which operate daily throughout the year in the Helsinki West Harbour area. As a counterpoint to the literature review and theoretical debate the paper introduces interviews with leading experts of the field. These interviews offer new insight and expand upon the discussion presented in the literature review.

The research findings indicate that misguiding vessels into potentially dangerous situations is only possible if the vessel is fully reliant on automation and is, in breach of both national and international Maritime law, not helmed by a navigator. In this scenario, the navigator is for whatever reason failing to compare information provided by the GPS with information from both visual navigation and radar. The manipulated information received by the GPS however is also transmitted through the AIS to the Helsinki Vessel Traffic Service, which can identify potential spoofing by cross-referencing the information received with their own surveillance system. This system compiles information from several radars, cameras and coordinates received by the vessel's GPS. If a vessel were to veer off course the Helsinki Vessel Traffic Service could identify the discrepancies in the navigation information as the technical systems rely on entirely separate technology and are completely independent of one-another. In cases of conflicting information, the Vessel Traffic Service prioritises the information provided by radars.

Keywords: Global Positioning System, GPS, GPS-spoofing, Automatic Identification System, AIS, Vessel Traffic Service

## KUVIOT

KUVIO 1 Tutkimuksen viitekehys .....	10
KUVIO 2 Helsingin syväväylän väyläkortti .....	13
KUVIO 3 Havaitseijan paikan laskeminen GPS-järjestelmässä .....	20
KUVIO 4 GPS-signaalin ja paikan kaappaus.....	23
KUVIO 5 Käytännön GPS-harhautuskoe lennokin ohjaukseen .....	25
KUVIO 6 GPS-simulaattorien paikat. ....	27
KUVIO 7 Aluksen harhautettu paikka .....	28
KUVIO 8 GPS-Simulaattorit.....	29
KUVIO 9 Keskitason GPS-simulaattorin toimintaperiaate .....	30
KUVIO 10 ECDIS-järjestelmään linkitetyt navigaatiojärjestelmät .....	31
KUVIO 11 Mihin kaikkiin järjestelmiin aluksen saamaa GPS-järjestelmää käytetään laivassa ja laivan ulkopuolella.....	37
KUVIO 12. AtoN-järjestelmän toiminta periaate .....	38
KUVIO 13. GPS-tekniikkaan perustuvat järjestelmät .....	39

## TAULUKOT

TAULUKKO 1 GPS-järjestelmän tarkkuus eri paikannustekniikoilla .....	20
--	----

# SISÄLLYS

TIIVISTELMÄ

ABSTRACT

KUVIOT

TAULUKOT

1	JOHDANTO.....	6
1.1	Tutkimusaihe ja -kysymykset .....	7
1.2	Aikaisempi tutkimus, tutkimusmenetelmät, rajaus ja käsitteistö .....	8
2	HELSINGIN SATAMAN MERIALUE JA LIIKENNE.....	11
2.1	Maantieteelliset ominaisuudet ja riskialueet .....	11
2.2	Meriliikenne.....	14
2.3	Merialue eri vuoden aikoina .....	16
3	GPS-JÄRJESTELMÄ JA SEN TOIMINTA PERIAATE .....	18
4	GPS-HARHAUTUS .....	22
4.1	GPS-harhautuksen perusteet ja uhkakuvien kehittyminen .....	24
4.2	GPS-signaalien harhautussimulaattori.....	28
4.3	Mitä onnistunut GPS-signaalien väärentäminen aiheuttaa laivan muille navigointijärjestelmille?.....	31
4.4	GPS-signaalien väärentämisen tuomat uhkakuvat laajemmin meriliikenteelle.....	36
5	TEEMAHAASTATTELUT MERENKULUNASIAANTUNTIJOIDEN KANSSA .....	41
5.1	Liikenneviraston haastattelu.....	42
5.2	Helsinki Vessel Traffic Servicen haastattelu .....	44
5.3	Liikenteen turvallisuusviraston haastattelu .....	47
5.4	Silja Serenaden päällikön haastattelu .....	49
6	TULOKSET JA JOHTOPÄÄTÖKSET .....	52
7	YHTEENVETO .....	55
	LÄHTEET .....	58
	LIITE 1.....	65
	LIITE 2.....	67
	LIITE 3.....	69
	LIITE 4.....	72
	LIITE 5.....	74

# 1 JOHDANTO

Suomalaiset käyttävät tänä päivänä GPS-järjestelmää (Global Positioning System) päivittäin joko itse tietoisesti ja suorittaen sillä jonkinlaisia työ- tai vapaa-ajan suorituksia, tai tietämättään niin, että joku muu käyttää kyseistä järjestelmää heidän puolestaan. Useimmilla meistä voi olla taskussa ns. "älykännyköitä", jotka GPS:n-signaalin ansiosta lähettävät tarkkaa paikkatietoa sijainnistamme (Poutanen, 2016, 34 - 35). Myös ranteessamme voi olla kuntoiluun tarkoitettu kello, joka kertoo lenkkeilijälle tarkan tiedon juostun tai kävellyn lenkin pituudesta. Saatamme myös käyttää autossa GPS-järjestelmään perustuvaa navigaattoria, joka kertoo meille lyhimmän reitin autolla etsimäämme paikkaan. Tämä on tietoista/henkilökohtaista GPS:n käyttöä.

Tietämätöntä tai passiivista päivittäistä GPS:n käyttöä taas voisi olla esimerkiksi sellainen, että tilataan taksi paikasta A paikkaan B ja ryhdytään lukemaan päivän lehteä, kuskin samalla kytkiessä navigaattorin päälle suunnistaessa oikeaan kohteeseen matkustajan nauttiessa matkasta. Vielä mukavampaa olisi lähteä perheen tai ystävien kanssa risteilylle ja nauttia risteilyaluksen henkilökunnan tarjoamasta matkasta aluksen kapteenin ja perämiehien huolehtiessa navigoinnista hyvässä tai huonossa säässä samalla, kun aluksen ohjailijat luottavaisin mielin tarkistavat muun muassa GPS:n avulla aluksen sijaintia ja suuntaa omista navigoimisjärjestelmistään.

Mutta entä, jos joku pääsee muuttamaan GPS-järjestelmän lähettämiä signaaleita tai häiritsemään sitä jollain muulla tavoin niin, että alusten GPS-vastaanottimet saavat väärää tietoa/signaalia? Aiheuttaako tällainen toiminta alusten ajautumista virheelliselle suunnalle? Voidaanko sillä tänä päivänä tai mahdollisesti tulevaisuudessa aiheuttaa vakavia vaaratilanteita meriliikenteessä? Edellä kuvatusta toiminnasta käytetään nimitystä GPS-harhautus (spoofing) tai GPS-juumiuttaminen (jamming) riippuen siitä, minkä tyyppisenä kyseinen isku suoritetaan (Lehtonen, Virtanen ja Askola, 2016, 27).

## 1.1 Tutkimusaihe ja -kysymykset

Kun suuret alukset liikkuvat kapeissa satamiin johtavissa syväväylissä ruuhka-aikoihin, ei virheliikkeille ole sijaa. Tästä syystä tutkimuksessa pyritään tutkimaan mahdollista GPS-harhautuksen uhkakuvaan Helsingin Länsisatamaan vievää syväväylää pitkin. Kyseisen väylän sivustoilla on useita eri luotoja ja kareja, joihin alus voi ajautua, tai alus voi törmätä väylällä toiseen alukseen edellä mainitun kyberiskun takia.

GPS-järjestelmää ei siviilimaailmassa suojata mitenkään, eli se on täysin avoin edellä kuvatuille hyökkäyksille (NASA, 2016). On omituista, että GPS-paikannusjärjestelmä, joka linkittyy käytännössä meidän kaikkien jokapäiväiseen toimintaan, on jäänyt huijausmahdollisuksi niin tieteessä kuin kybermaailmassakin erittäin vähäiselle huomiolle. Varsinkin meriympäristö antaa GPS-signaaleille todella hyvät mahdollisuudet kulkeutua selkeällä kelillä pitkiäkin matkoja verrattuna kumpuileviin maasto- tai kaupunkiolosuhteisiin. Tutkimus suoritetaan lisäksi siitä syystä, että Helsingin satamaan johtavat meriväylät ja sen edustalla olevat meriliikenneväylät ovat todella ruuhkaisia varsinkin kesäkuukausina (Liite 1). Myös Trafi eli Liikenteen turvallisuusvirasto on määrittänyt tämän alueen todella riskialttiiksi alueeksi (Trafi). Mikäli kyberterroristit kykenisivät vaikuttamaan risteily- tai rahtialusten GPS-navigointijärjestelmiin harhautuksen keinoin, antaisi se kyberterroristeille mahdollisuuden saada aikaan valtavia tuhoja niin ihmisten, talouden kuin luonnonkin kannalta.

Tämän tutkimuksen tarkoitus on ensisijaisesti selvittää lukijoille, että kyberturvallisuus on hyvin laaja-alainen tieteenala, jossa myös fyysiset osapuolet ovat aina mukana (Suomen kyberturvallisuusstrategia, 2013, 19). Teoriassa tällaisella kyberiskulla voidaan siis saada mahdollisesti aikaiseksi valtava katastrofi, joka voi olla jotain aivan muutakin kuin esimerkiksi palvelunestohyökkäys pankin sähköisiin palveluihin tai kiristyshaittaohjelma, jolla lukitaan koneesi ja vaaditaan rahaa, jotta koneen saa auki. Mikäli merenkulun toimijoillemme vain jaetaan tämän tyyppistä tietoa ja tutkimusmateriaalia, uskon ja toivon, että tulevaisuudessa kyetään estämään mahdolliset tällaiset hämmentävät ja mahdollisesti jopa lamauttavat tilanteet. Lisäksi tutkimuksella halutaan tuoda meriliikenteen tärkeimmille toimijoille tietoon, että tulevaisuudessa tällaisten GPS-harhautusuhkakuvien muistaminen on entistä tärkeämpää, mikäli meriliikenteessäkin siirrytään kokonaan automatisoituihin laivoihin/laivaliikenteeseen. Tänä päivänä yksittäisen aluksen jo melkein kaikki navigointiin ja liikkumiseen tarkoitetut järjestelmät on kytketty GPS-järjestelmän yhteyteen.

Päätutkimuskysymys tutkielmassani on:

- Millaisia mahdollisia uhkia GPS-harhautukseen saattaa sisältyä meriliikenteessä?

Tähän kysymykseen vastaamiseksi tutkielmassa selvitetään myös seuraavia seikkoja ja pyritään vastaamaan näihin alakysymyksiin:

- Miten GPS-signaali toimii?
- Millaisia haasteita Länsisataman syväväylä asettaa merenkululle?
- Miten kaikki navigointijärjestelmät linkitetään merenkulussa GPS-tekniikkaan?
- Miten GPS-harhauttaminen tapahtuu teoriassa?
- Miten Liikennevirasto, VTS, Trafi ja Silja Serenade -aluksen päällikkö ovat huomioineet tämän mahdollisen uhan ja suhtautuvat siihen?

## **1.2 Aikaisempi tutkimus, tutkimusmenetelmät, raja- ja käsitteistö**

Suomessa ei ole suoritettu aiheesta lainkaan julkista aikaisempaa ja laaja-alaista tutkimusta. Suurin osa GPS-harhauttamisen (spoofing) ja GPS-jumiuttamisen (jamming) termein haettavista hakusanoistakin näyttää keskittyvän enemmän autojen ja lennokkien GPS-järjestelmiin tai itse termistön selventämiseen (Lehtonen, Virtanen ja Askola, 2016, 27). Mutta merenkulusta ei ole vielä löytynyt suomenkielistä laajempaa tutkimusmateriaalia - näin ollen tarvetta tällaiselle tutkimukselle siis on. Englanninkielistä materiaalia tutkimalla löytyy valtavasti tutkimuksia GPS-peräiseen häirintään liittyen, mutta varsinkin merenkulun materiaali ja tutkimus ovat hyvin harvinaista, ja niissä kaikissa on hyvin tekninen näkökulma. Kaikki tutkimukset merenkulussa pohjautuvat lähinnä seuraaviin tutkimuksiin GPS-harhautuksessa: Bhatti, Humpreys, Kerns & Shepard, 2014 ja Humpreys, 2012. Monissa tutkimuksissa on myös yritetty keksiä erilaisia torjunta- ja puolustuskeinoja tätä häirintää vastaan (Johnston, Warner, 2003) ja (Humpreys, Montgomery, 2009). 2010 luvun taitteessa on kansainvälisissä piireissä kyetty todistamaan, että tällainen GPS-harhautus voisi olla potentiaalinen uhkakuva. Mutta vasta vuosina 2013 - 2015 kansainvälisissä piireissä nousi todellinen huoli, kun Humpreyssin tutkimusryhmä suoritti käytännön kokeen Italian edustalla. Tämä koe noteerattiin esimerkiksi Yhdysvaltojen turvallisuusviranomaisien puolella (Proceedings, 2014-2015), tähän turvallisuusalan julkaisuun henkilöt voivat julkaista omia mielipiteitään potentiaalisista uhkakuvista.

Suurin osa yllä mainituista tutkimuksista lähtee aivan eri näkökulmasta kuin tämä tutkimus. Tässä tutkimuksessa katsotaan asiaa sekä aluksen näkökulmasta, että myös Liikenneviraston, VTS:n (Alusliikennepalvelukeskuksen), Tra-



fin (Liikenteen turvallisuusviraston) sekä Silja Serenaden päällikön näkökulmasta, sekä miten he lähettävät ja jakavat tietoa keskenään. Rajaukseen kuuluu vielä tämän lisäksi niin sanottu maantieteellinen aluerajaus, mikä kattaa kaiken sen, mitä Liikenneviraston väyläkortissa on esitetty (Liikennevirasto 2013). (Lisää tietoa kyseisestä alueesta löytyy luvusta 2.1). Tämän lisäksi tutkimuksessa ei oteta huomioon muita satelliittipaikannusjärjestelmiä kuten GLONASS, Galileo, BeiDou, yms., koska näitä järjestelmiä ei ole vielä kokonaan otettu käyttöön, ja se taas vaatisi aivan erilaisia tutkimuksia näkökulmineen. Lisäksi tutkimuksen nimikin jo antaa selvän rajauksen, mitä tässä tutkitaan.

Jotta lukija kykenisi ymmärtämään, mitä tutkimuksessa käytettävällä termistöllä tarkoitetaan, on tähän koottu tärkeimmät termit ja pyritty selventämään niitä. GPS-häirintää voi olla kahdenlaista: jumiuttamista (jamming) tai harhauttamista (spoofing). Tässä tutkimuksessa aihealue rajataan käsittämään vain harhauttamista. GPS-signaalin jumiuttaminen tarkoittaa lähinnä sitä, että samalla taajuudella syötetään vastaanottimelle valtavasti voimakkaampaa lähetyssignaalia, ja heikko GPS-signaali ei kykene pääsemään vastaanottimesta sisään. Näin GPS-järjestelmä ei kykene antamaan merenkulun navigointijärjestelmille paikkatietoa. Harhauttamisessa taas lähetetään vastaanottimelle väärää, niin sanottua manipuloitua tietoa, voimakkaammalla signaalilla, jota vastaanotin ei kykene tunnistamaan vääräksi. Näin alus saadaan harhautetuksi ja pois linjaltaan. Tämä on häirinnän hankalampi ja vaarallisempi muoto. (Lehtonen, Ym., 2016, 27.).

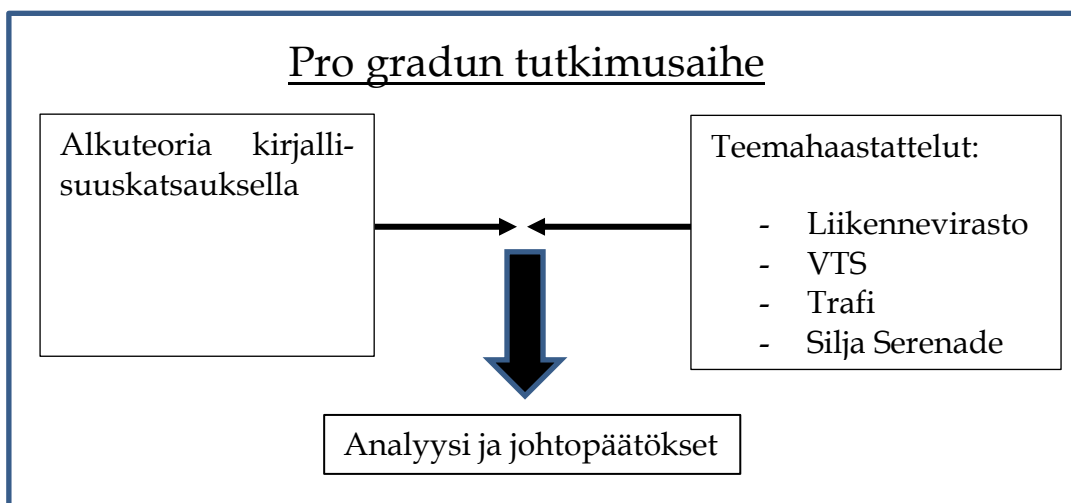
VTS:llä tarkoitetaan Vessel Traffic Service -palvelua, joka suomeksi käännettynä tarkoittaa merenkulun alusliikennepalvelua ja sen toiminnassa olevia keskuksia. Suomessa tätä kaikkea valvoo ja hallinnoi LVM (Liikenne- ja viestintäministeriö), jonka alaisuudessa liikennevirasto ja VTS:t palvelevat. VTS:n toiminnasta säädetään laissa ja asetuksissa (Alusliikennepalvelulaki 623/2005, Valtioneuvoston asetus alusliikennepalveluksesta 763/2005 ja 1798/2009). Näihin samoihin lakeihin ja asetuksiin perustuvat myös kaikki säännöt ja toiminta, niin valtiomme merialueilla kuin myös tutkimallani Helsingin Länsisataman syväväylällä.

AIS-järjestelmällä tarkoitetaan Automatic Identification System -järjestelmää, joka suomeksi on yhtä kuin alusten automaattinen tunnistusjärjestelmä. Tästä eteenpäin tutkimuksessa käytetään järjestelmien kansainvälisiä lyhenteitä. Ainoastaan spoofing ja jamming -termeistä on tästä eteenpäin käytetty suomenkielisiä termejä harhautus tai jumiutus.

Tutkimuksessa asioita käsitellään ja tutkitaan lähinnä Länsisatamassa toimivien suurten alusten näkökulmasta, käsittäen alukset, jotka kykenevät ottamaan kyytiin sadoista aina tuhansiin matkustajia sekä useita autoja. Näitä ovat muun muassa päivittäin alueella operoivat varustamot kuten Tallink Siljan, Eckerö Linen ja St Peter Linen alukset. Tutkimuksessa pyritään luomaan ja kuvailemaan ajatusmaailma suuren risteilijäaluksen ohjailijan/kapteenin kannalta - miten hän mahdollisesti voisi tilanteessa toimia.

Tutkimus on kvalitatiivinen ja sen tarkoituksena on enemmänkin teoreettisesta näkökulmasta kuvailla, minkälaisia uhkia tällaisella harhauttavalla häirintälaitteella voidaan saada aikaan meriliikenteessä. Teknisessä mielessä tätä aihealuetta on jo tutkittu kansainvälisesti jonkin verran, Suomessa taas huomattavasti vähemmän. Tämä tutkimuksen alkuosan tieto on saatu luotettavalla kirjallisuudesta analysoidulla laaja-alaisella kuvailevalla kirjallisuuskatsauksella (Salminen, 2011, 7-8). Tässä ei mennä niinkään meta-analysoivan kirjallisuuskatsauksen kuin systemaattisenkaan kirjallisuuskatsauksen puolelle, vaan pyritään pysymään selvästi kuvailevan kirjallisuuskatsauksen puolella (Salminen, 2011, 7-8). Kyseinen lähdeaineisto on hankittu monesta eri tietolähteestä, koska tutkimuksen aihealueelta ei suoranaisesti löytynyt mitään tutkimusta. Tästä syystä tutkimuksen alkuteoria on jouduttu kasaamaan hyvin monesta lähdemateriaalista ja se muodostuu hyvin laaja-alaiseksi. Tätä alkuteoriaa pyritään vahvistamaan omien alojensa asiantuntijoiden haastatteluilla. Lähdeaineisto koostuu muun muassa aina merikartastoista merenkulkujärjestelmälän kirjallisuuteen, Helsingin sataman ja Liikenneviraston tietokantoihin, kuin myös itse GPS-harhautuksen tutkimusmateriaalit, joihin oleellisesti kuuluu Humpreysin ja Bhattin tutkimukset.

Haastattelut on suoritettu teemahaastatteluperiaatteella (puolistrukturoitu) (Hirsijärvi, Hurme, 1993, 35-37) ja (Saaranen-Kauppanen & Puusniekka, 2006). Haastatteluun on pyydetty merellisen järjestelmätekniikan sekä käytännön navigointialan asiantuntijaa Liikennevirastosta, VTS:stä, Trafista ja Tallink Siljalta. Lopulta tutkimukseen onnistuttiin saamaan jokaisesta organisaatiosta yhden asiantuntijan mielipide haastattelumateriaaliksi. Haastattelu suoritettiin jokaiselle samasta temasta, hieman modifioiduin eri kysymyksin. Näin jokainen kykeni tuomaan julki oman mielipiteensä asiasta. Näitä haastattelumateriaaleja analysoimalla yhdistettiin tulokset ja tehtiin omat johtopäätökset vertailemalla niitä alkuteoriaan (Hirsijärvi & Hurme, 1993, 115-117) (Lisää tietoa luvussa 5.). (Kuvio 1) Viitekehysten kuvassa selvennetään, miten tutkimus on suoritettu.



KUVIO 1 Tutkimuksen viitekehys

## 2 HELSINGIN SATAMAN MERIALUE JA LIIKENNE

Tässä luvussa käydään nopeasti läpi, minkälaisia alueita Helsingin eteläpuolella oleva merialue ja Länsisataman syväväylä ovat, sekä kuinka paljon tutkittavalla alueella liikkuu suuria aluksia. Tämä tehdään sen vuoksi, että jokainen asiaan perehtymätönkin ymmärtää, että kyseessä on kansainvälisesti suuri ja ruuhkainen satamakeskittymä. Helsingin satamalla on jo nyt kapasiteetiltaan suuri ihmisten ja tavaran vienti ja tuonti. Mutta se tulee tulevaisuudessa luultavasti kasvamaan entisestään, ainakin Länsisataman matkustajien osalta, sillä sinne on tämän vuoden keväänä (2017) valmistunut uusi matkustajaterminaali ja uudet laivojen tulo- ja lähtölaiturit (Port of Helsinki, 2017a). Nämä tulevat hyvin suurella todennäköisyydellä lisäämään huomattavasti alusten ja matkustajien vuosittaista määrää.

### 2.1 Maantieteelliset ominaisuudet ja riskialueet

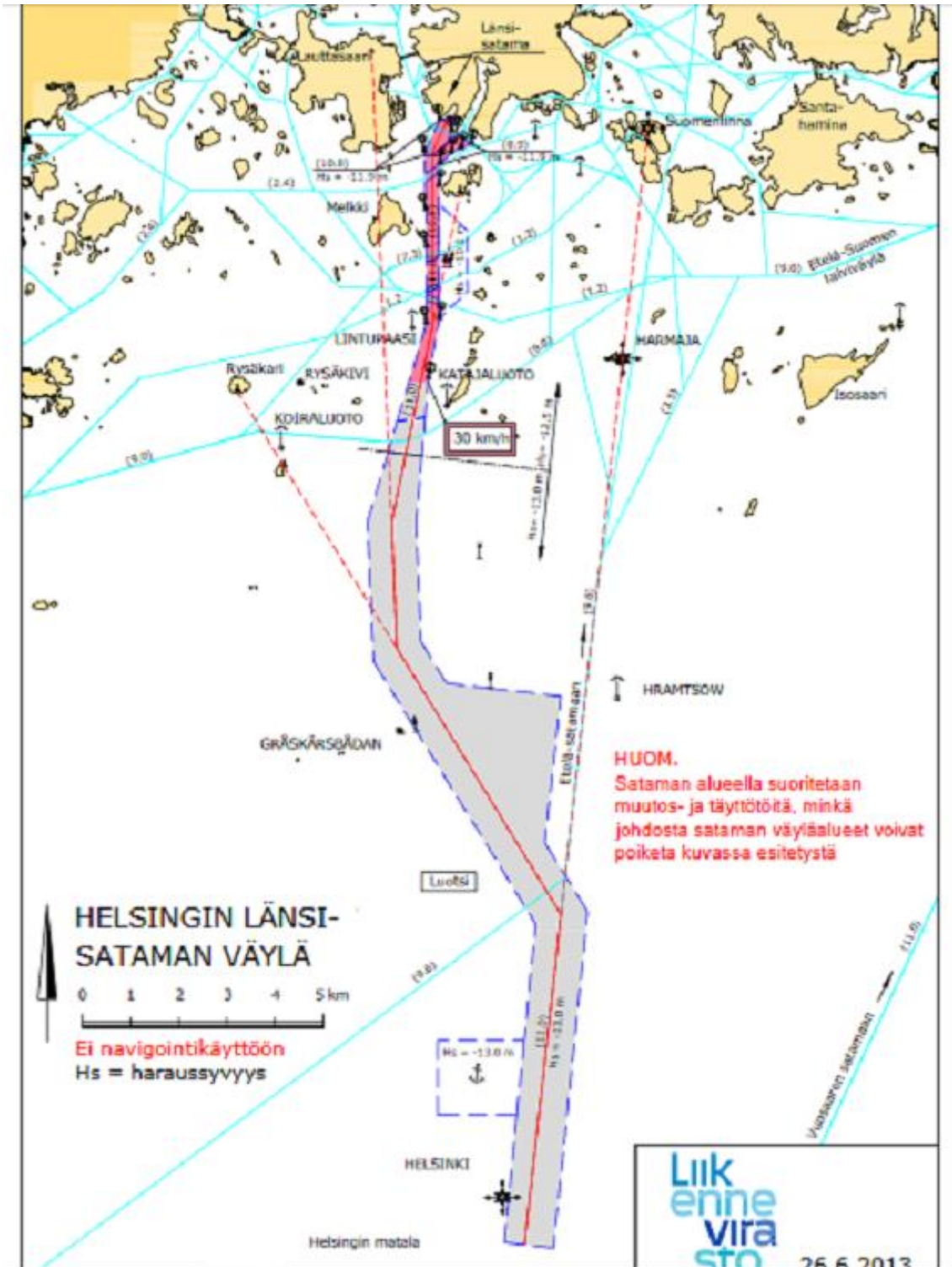
Maantieteellisiltä ominaisuuksilta tutkittava Helsingin Länsisataman syväväylän alue alkaa Helsingin majakan itäpuolelta ja menee luotsipaikan ohi (Läntinen Suomenlahti, 2003), (Helsingin edusta, 2003) ja (Helsingin Länsisataman väyläkortti, 2013). Se kulkee Gråskärsbådanin itäpuolitse, Katajaluotoa länsipuolitse viistäen kohti pohjoista Länsisatamaa. Kaiken kaikkiaan pituutta tällä väylällä on 13 mpk (meripeninkulmaa), mikä on kilometreissä hieman yli 24 kilometriä. Väylän eteläisimmät 4 linjaa on merkitty linjatauluin tai sektoriloistoin, ja pohjoisimmat 3 linjaa Katajaluodosta eteenpäin kardinaalimerkein (Helsingin Länsisataman väyläkortti, 2013).

Väylän takuukulkusyvyvyydeksi annetaan Melkin saarelle asti 11,0 metriä. Melkin saaresta läntisiin ulompiin laitureihin annetaan 10,8 metrin kulkusyvyys ja muun muassa sisempiin Jätkäsaaren laitureihin 8,9 metrin kulkusyvyys. Väylän minimileveydeksi ilmoitetaan vain 247 metriä (Helsingin Länsisataman väyläkortti, 2013).

Väyläkortissa kuuluu myös aina mainita navigoitavuudessa/merenkulussa mahdollisesti asiaa helpottavat tai hankaloittavat tekijät. Helsingin Länsisataman väyläkortissa on merenkulkijoille ilmoitettu seuraavaa: Väylän ulko-osa, mikä tarkoittaa Katajaluodon eteläpuoleista osaa, on käytännössä kokonaan avomerta. Eikä merenpinnan alapuolella ole kovin montaa karikkoa tai matalikkoa. Tästä syystä kyseisellä väyläosuudella merenkulkijat ovat alttiina idän, etelän ja lännen puoleisille tuulille. Katajaluodosta ylöspäin väylää tullessa, taas alusta suojaa tuulilta saaret, luodot, karikot ja matalikot. (Helsingin Länsisataman väyläkortti, 2013). Yllämainitut seikat ovat hyvin tärkeitä ottaa merialuksilla navigoitaessa huomioon, koska tuuli sortaa alusta väylästä sivuun sitä enemmän, mitä enemmän aluksella on tuulipinta-alaa (Forsen, Haavisto, Karlsson, Keränen ja Sivuranta, 2010, 80 – 81).

Helsingin Länsisataman syväväylän väyläkortissa ei anneta kuin yksi rajoitus kaikille kauppaluksille, ja se on nopeusrajoitus. Kyseinen rajoitus alkaa Rysäkiven kohdalta pohjoiseen, ja sen jälkeen maksiminopeus saa olla enää 30 km/h. Kaikki muut liikennettä rajoittavat tekijät ovat vain suosituksia kaupparenkulkijoille. Tuulisuositus on 15m/s ja näkyvyys-suositukseksi sanotaan kaikille aluksille 300 m. Kuitenkin kaikille yli 200 metriä pitkille aluksille suositellaan vähintään yhden mpk:n eli 1,852 kilometrin näkyvyysolosuhteita. (Helsingin Länsisataman väyläkortti, 2013.).

Länsisataman syväväylän riskialueiksi tässä tutkimuksessa kuvitellaan sellaiset alueet, joissa merikartassa ja Helsingin sataman väyläkortissa on esimerkiksi väylää lähellä olevia kareja, luotoja, matalikkoja. Tällaiset riskialueet normaaleissa olosuhteissa hyvällä näkyvyydellä ja kaikkien navigointijärjestelmien toimiessa ovat aina tarkalleen tiedossa. Eivätkä ne tällöin aiheuta riskejä. Länsisatamassa meriliikenne pyörii aamusta yöhön vuoden jokaisena päivänä, ja näihin päiviin mahtuu monia erilaisia navigointikelejä. Merellä navigointi esimerkiksi syysiltaisin on pilkkopimeää. Merellä sumu saattaa yllättää todella nopeasti, ja vesi- tai lumisateen yllättäessä navigointijärjestelmiltä kuin myös aluksen kapteenilta ja vahtiperämiehiltä vaaditaan entistä kovempaa navigointikykyä ja valppautta. Jos esimerkiksi tällöin kyberterroristi suorittaisi GPS-harhautusiskun aluksen ohjailijoiden sitä huomaamatta, muuttuvat nämä mahdolliset meriväylän riskialueet todellisiksi suuriksi uhkakuviksi. (Kuvio 2) on kuvakaappaus Liikenneviraston Internetsivuilta, siellä julkaistusta väyläkortista. Tällä on pyrittävä selventämään lukijoille, minkälaisesta merialueesta on kyse.



KUVIO 2 Helsingin syväväylän väyläkortti, joka paljastaa miten haavoittuva kyseinen alue voi olla. (Liikennevirasto, 2013)

Kun lähdetään tutkimaan väylää etelästä ylöspäin, niin suurin ensimmäinen riskialuerypäs on Katajaluodosta luoteeseen (Helsingin Länsisataman väyläkortti, 2013). Tässä kohtaa on väylän ahtain kohta, ja sen länsipuolelta löytyy laaja kari-alue ja itäpuolelta kari sekä matalikko. Kun tästä mennään eteenpäin kohti pohjoista, jää aivan väylän viereen koirakarin linjaloisto, jonka normaaliolosuhteissa

ei pitäisi aiheuttaa ongelmia. Mutta autopilotilla, huonossa näkyvydessä, toista alusta samaan aikaan väistäessä, voi tilanne muuttua nopeasti toiseksi. Tästä väylää eteenpäin tultaessa ovat kaikki suunnan muutokset, jotka ylittävät väylän rajan satamaan päin mentäessä olla todella vaarallisia, varsinkin Melkin itäpuoli ja Pihlajasaaren luoteispuoli ovat riskialueita. Kaiken tämän lisäksi on riskeiksi tässä vaiheessa hyvä lisätä alusten ohitustilanteet. Helsingin Länsisataman syväväylällä liikkuu useita aluksia saman aikaisesti. Kuinka nopeasti mahdollisesti voidaan kuvitella, että alusta ohjaileva henkilökunta on ymmärtänyt olevansa GPS-harhautuksen alaisena tällaisessa tilanteessa, ja kuinka nopeasti he kykenevät korjaamaan aluksensa tosisuunnalle ja oikealle reitille. Tässä tutkimuksessa oletetaan, että ainoastaan yhdelle alukselle kerrallaan suoritetaan GPS-harhautusta.

## 2.2 Meriliikenne

Länsisatama on mielenkiintoinen tutkimuskohde monessa mielessä. Se on osa suurta Helsingin Sataman kokonaisorganisaatiota ja -infrastruktuuria. Itse Helsingin Satama jakautuu Eteläsatamaan, Katajanokan satamaan, Länsisatamaan, Hernesaaren risteilylaitureihin, Vuosaaren satamaan, Loviisan satamaan (1.1.2017 lähtien), Kantvikin satamaan ja Helsingin hiililaitureihin. Helsingin Satama kokonaisuudessaan on ulkomaankaupan pääsatama, sillä sen kautta kulkee kolmasosa Suomen ulkomaankaupan arvosta. Merikuljetusten arvossa katsottuna Helsingin Sataman kautta kulkee 50 % Suomen merikuljetusten arvosta. Helsingin Satama kokonaisuudessaan on Suomen matkustajaliikenteessä 79 % markkinaosuudellaan ehdoton ykkönen. (Port of Helsinki, 2017b) ja (Liite 1.).

Helsingin Satama jakautuu lähinnä kolmeen vilkkaaseen satamaan matkustajaliikenteellä mitattuna. Katajanokan satamasta matkustetaan Ruotsiin ja Viron, ja Eteläsataman matkustajat lähtevät lähinnä aluksilla Ruotsiin. Kesäisin näihin molempiin saapuu myös ulkomaisia risteilijäaluksia. Länsisatama on näistä kolmesta satamasta kaikkein vilkkain. Vuonna 2015 ainoastaan Länsisataman kautta kulki 6 180 000 Viron, 260 000 Pietarin matkustajaa ja 1 012 000 henkilöautoa (Port of Helsinki, 2017c). Länsisataman suuret matkustajaluvut ovat pääsääntöisesti Viron liikenteen ansiota. Viron liikenne on jatkanut tasaista kasvuaan koko 2000-luvun alun ja 2010-luvun (Suomen satamaliitto, 2016) ja (Tilastokeskus, 2017). Tätä valtaisaan Länsisataman matkustajien kasvun määrää on edesauttanut Länsisatamassa operoivien varustamoiden vuosivuodelta suuremmaksi ja nopeammaksi kasvaneet reittialukset ja niiden lisääntyneet tulo- ja lähtöajat satamasta. Talvella Länsisatamassa tilanne rauhoittuu hyvin paljon, ja liikennekapasiteetti pienenee huomattavasti, kuten jo tilastoista on nähtävillä. Tällä hetkellä esimerkiksi vuoden rauhallisimpaan aikaan, jolla tarkoitetaan syys- ja talvikautta, Länsisatamasta lähtee joka vuorokausi minimissään kahdeksan ja maksimissaan kymmenen suurta, Helsinki-Tallinna välillä liikennöivää matkustaja- ja ajoneuvokuljetukseen erikoistunutta merialusta (Port of Helsinki, 2017d). Vastaavasti Tallinnasta lähtee myös syksyisin ja talvisin joka päivä saman

verran aluksia. Tallinnan päässä operoivilla varustamoilla on käytössä omat satamat laitureineen, jolloin siellä päässä ei synny niin suurta ruuhkaa kuin Länsisatamassa. He voivat siis vapaammin valita alustensa lähtöajat. (Tallink Silja Line, 2017) ja (Eckerö Line, 2017). Tämä puolestaan aiheuttaa normaalisti jo talvikuu-kausinakin Länsisatamassa varsinkin 16:00-18:00 välillä pienimuotoista ruuhkaa. Länsisatamasta alkaa vielä huhtikuussa liikennöimään myös kolmannen laivarustamon alukset Pietarin ja Tallinnan satamiin (St Peter Line, 2017). Joka kevät ja kesä ulkomailta Helsingin Satamaan saapuu Suomeen tulevia loistoristeilyaluksia turisteineen. Näistä ulkomaisista risteilyaluksista suurin osa saapuu juuri Länsisatamaan. Yhteensä esimerkiksi viime vuonna näitä risteilyaluksia saapui suomeen 240 kappaletta ja näissä oli lähes 409 000 matkustajaa (Port of Helsinki, 2017e) ja (Liite 1.) Lisäksi ympäri vuoden Länsisataman merialtaassa, sen lähettyvillä ja sinne johtavalla syväväylällä liikkuu varsinkin kesäisin paljon siviilien huviveneitä, sekalainen määrä viranomaisliikennettä, vesibusseja turisteja varten sekä muutamia pienempiä aluksia, jotka purkavat lastinsa Hernesaareen tai Salmisaaren lähettyville, ja sen takia kulkevat tutkimamme syväväylän kautta.

Länsisatamassa liikennöivät merialukset ja laivat ovat pääsääntöisesti kolmella eri varustamolla hallussa ja tuottavat rahaa heidän kassaan. Nämä ovat Tallink Silja Oy, Eckerö Line Oy ja St Peter Line, joka liikennöi tulevana kautena vain 8.4. - 23.12.2017 (Tallink Silja, 2017), (Eckerö Line, 2017) ja (St Peter Line, 2017). Näiden varustamoiden aluskapasiteetti on hyvin suuri, mikäli sitä tarkastelee yhteismäärällisesti. Se käsittää yhteensä 5 erilaista laivaa jotka ovat pituudeltaan 175 - 212,2 metrin, nopeus 21 - 27 solmun, leveys 27,6 - 32 metrin ja syväys 6,5 - 7,1 metrin väliltä (Eckerö Line, 2017), (Tallink Silja, 2017a) ja (Wikipedia, 2017). Henkilömatkustajia näille aluksille voidaan ottaa parhaimmillaan kerralla 9 973, Ms Anastasian tietoja ei ollut kuitenkaan ilmoitettu. Niin kuin näistä, laivojen niin sanotuista maksimaalisista matkustajien vastaanottokyvyistä kytään jo huomaamaan, mikäli edellä kuvatun kaltainen onnettomuus sattuisi Länsisataman syväväylällä, henkilövahingoissa ei voitaisi tehdä juuri mitään.

Kuten edellä jo todettiin, Länsisatamaan saapuu myös sekalainen määrä ulkomaisia risteilyaluksia, joiden teknisiä tietoja ei ole ilmoitettu. Toisin sanoen joudumme käyttämään tässä vain liitteen 1 tietoa, joka ei kerro aluksien tarkkaa kapasiteettikykyä, kuinka monta matkustajaa mikäkin laiva voi mukaansa ottaa. Tässä vaiheessa voidaan vain todeta, että viime vuonna näiden ulkomaisten turistiristeilijöiden matkustajien kokonaismäärä oli (2016) 408 900. Nyt on arvioitu, että kesällä 2017 päästäisiin myös noin 400 000 matkustajan lukemiin, ja heidät tuotaisiin 283:lla aluksella, joista suurimman matkustajakapasiteettikyky olisi noin 3800 matkustajaa. Keskimääräinen risteilijä toisi tullessaan n. 2000 risteilymatkustajaa. (Visithelsinki.fi).

Tässä tutkimuksessa ei tutkita aiemmin mainittujen pienempien huviveneiden, vesibussien, tai muiden merialusten GPS-järjestelmään kohdistuvaa harhautusta. Tässä tutkimuksessa pyritään keskittymään pääsääntöisesti tämän kappaleen alussa mainittujen ja Länsisatamassa säännöllisesti operoivien varus-

tamoiden alusten laivaliikenteen GPS-vastaanottimien mahdolliseen häiritsemiseen ja harhauttamiseen ja siihen liittyvään toimintaan. Sen takia, että näistä on usean vuoden reittiliikennetilastointitietoa, nämä alukset käyttävät kaikki siviili GPS-järjestelmää ja ovat kooltaan suuria aluksia, mikä mahdollisen onnistuneen GPS-harhautuksen/-kyberiskun jälkeen voi aiheuttaa valtavia lamaannuttavia seurauksia. Mikäli tällä tutkimuksella kyetään teoriassa osoittamaan, että Länsisataman aluksiin kyettäisiin suorittamaan GPS-harhautusta, saadaan tällä tutkimuksella toivottavasti alustemme ja meriliikenteemme turvallisuuden ympärillä työskenteleville henkilöille tiedoksi kyberrikollisten/-terroristien kyky aiheuttaa suuria ja merkittäviä mahdollisia vaaratilanteita.

### 2.3 Merialue eri vuoden aikoina

Kun tutkimme Helsingin syväväylää keväällä, kesällä, syksyllä ja talvella, niin voimme ymmärtää, että mikään vuodenaika ei ole samanlainen toisen kanssa. Tutkittava alueemme sijaitsee Itämerellä, joka on murtovesiallas, ja tämä aiheuttaa kyseiselle alueelle hyvin poikkeuksellisia olosuhteita. Aluetta voisi kuvailla eräänlaiseksi ulkomeren ja sisämeren välimaastoksi tai yhdistelmämereksi, ja se muuttuu yhä enemmän mantereiseksi, mitä enemmän itään päin mennään. Itämereemme vaikuttaa hyvin paljon Golf-virtaus, Skandinavian vuoristo, metsät, suot, järvet, ja tällä alueella paikallinen lämpötila on noin kuusi astetta lämpimämpää kuin 60 -70 astetta leveyspiiriltään sen kuvittelisi olevan. Talvisin taas Siperiasta puhaltava hyytävä viima tuo meille kylmää ilmassaa, jotka aiheuttavat meillä ns. kuivia ja puhaltavia kelejä. (Forsen, Haavisto, Karlsson, Keränen ja Sivuranta, 2010, 223).

Vaikka meillä olisi mantereella suhteellisen hyvät oltavat, niin merellä keväisin Helsingin syväväylä voi olla erittäin sumuinen/merisavuinen. Tämä johtuu pääsääntöisesti siitä, että veden pintalämpötila on huomattavasti kylmempi, kuin vallitseva ilman lämpötila. Tätä ns. kevätsumua/merisumua/-savua esiintyy hyvin tyyninä päivinä, jolloin merellä ei puhalla tuuli ollenkaan. Mutta veden lämpötila saattaisi olla vielä vallitsevaa ilmassaa kylmempää kuin poutapäivänä. Hankalan tästä kaikesta tekee se, että mantereelta ei välttämättä saata nähdä kyseistä sumumassaa ollenkaan, mutta merellä tämä sumu estää näkyvyyden mantereelle päin kokonaan. Keväisin alusten kulkua helpottaa hyvä näkyvyys ja vähentyneet myrskyt. Tosin mahdollisia kevätmyrskyjä saattaa alueella olla. Joka tapauksessa kasvavat sademäärät hankaloittavat tilannetta hyvin paljon. (Forsen, ym., 2010, 226.).

Kesällä meren nopea lämpeneminen edesauttaa tilannetta. Merelle ei jää navigointiin mitään muuta ongelmaa tähän vuoden aikaan kuin sateet ja niiden aiheuttamat huonot näkyvyydet ja etäisyydet. Kesäisin vettä saattaa sataa paljon, mahdollisesti useampi millimetri kerralla, ja mahdolliset paikalliset ukkosmyrskyt voivat luoda myös oman haasteensa tutkittavaan alueeseen. Tällöin alueen aallonkorkeus saattaa nousta yllättävän korkeaksi ja lisäksi alusten suuri tuuli-



pinta-ala asettaa omat haasteensa. Valoisuus lisääntyy kesäkaudella huomattavasti ja saavuttaa Helsingin tasalla juhannuksena melkein 19 tunnin pituuden. (Forsen, ym., 2010, 224 - 226) ja (Ilmatieteen laitos, 2017).

Syksyllä tilanne muuttuu dramaattisesti tutkittavalla alueella. Merivesi alkaa kylmetä, mikä lisää ilman ja sään ennustettavuuden ongelmia ja vaihteluita huomattavasti. Näkyvyys ja tuuliolosuhteet muuttuvat todella paljon, aina todella pitkiksi ajoiksi. Mikäli näkyvyys on heikko sateen tai sumun takia, se aiheuttaa ohjailijalle huomattavia ongelmia. Nämä sateet ja sumut voivat kestää syksyllä useita päiviä peräkkäin. Sateet ja sumut voivat vähäksi aikaa hellittää, ja Helsingin syväväylällä voi olla syksyn takia todella pimeää (Forsen, Ym., 2010, 230). Myös tuuliolosuhteet alkavat lisääntyä ja muuttua hyvinkin laajoiksi myrskyiksi. Kun varsinkin kesällä nämä myrskyt ovat paikallisia myrskyjä, niin syksyllä nämä myrskyt muuttuvat koko Itämeren/Pohjoisen Itämeren alueen kattaviksi myrskyiksi. Näissä myrskyissä aallonkorkeus voi nousta yli neljämetriseksi kovalla tuulella. Itämerellä myrskystä puhutaan, kun tuulen nopeus nousee yli 21 metriä/sekunnissa. Tällöin aallonkorkeus voi nousta yli 7 metrin. (Ilmatieteen laitos, 2017) ja (Forsen, ym., 2010, 231).

Talvella merivesi alkaa kylmentyä entisestään ja se lopulta jäätyy joulukuussa. Sateet muuttuvat aluksi räntäsateeksi ja tämän jälkeen lopulta aina lumisateeksi. Tällaiset sateet aiheuttavat oman ongelmansa navigoijalle, koska näkyvyys huonontuu entisestään, ja voi lopulta muuttua niin, että se on lähes olematon ja lähellä nolaa metriä. Mikäli tähän vielä lisää alueen pimeyden, niin saadaan aikaan melkoinen haaste navigoijalle. (Forsen, ym., 2010, 223 - 224). Hyvänä päivänä ja valoissana ajankohtana voi näkyvyys kuitenkin olla jopa lähelle useaa kymmentä kilometriä. Itse meriveden kylmeneminen aiheuttaa alueella jäätymistä ja myrskyisiä/pärskeisiä aaltoja, mikä johtaa taas kansien vakavaan jäätymistilaan. Tällöin kannella joudutaan kiinnittämään huomiota aluksen vakauksen ja tasapainoon, jottei jää aiheuta tasapainohaittoja. Talvikaudet voivat olla nykyaikana myrskyiltään hyvinkin yleisiä, mikäli tutkitaan ilmatieteen laitoksen tilastoja. Varsinkin marraskuu ja joulukuu kamppailevat hyvinkin tasaisesti tilastollisesti, niin että marraskuussa on ollut keskimäärin 3,5 myrskypäivää ja joulukuussa 3,7 päivää. Tämä tilasto on luotu hyvin pitkän ajan kuluessa vuosilta 1994 - 2017 (alku) (Ilmatieteen laitos, 2017).

### 3 GPS-JÄRJESTELMÄ JA SEN TOIMINTA PERIAATE

Tässä tutkimuksessa GPS (Global Positioning System)-järjestelmällä tarkoitetaan Yhdysvaltojen puolustusministeriön (DoD, Department of Defence) kehittämää navigointijärjestelmäkokonaisuutta, johon tarvitaan satelliitteja sekä monenlaisia vastaanottimia, ja se on suunniteltu käytännössä meri- ja ilmavoimien tarpeisiin. GPS:n todellinen toiminta-aika voidaan katsoa alkaneeksi vuodesta 1978, kun ensimmäinen Navstar-1 -satelliitti laukaistiin avaruuteen, ja liikkuvat vastaanottimet otettiin myös käyttöön. Nykyään GPS:n ylläpito on alistettu Yhdysvaltojen puolustusministeriössä ilmavoimien alaisuuteen (GPS.Gov, 2017a). Jostain syystä tänä päivänä GPS:stä puhuttaessa jopa jotkin tiedemiehet ovat yhdistäneet muut vastaavat satelliitteihin perustuvat navigointijärjestelmät, kuten Venäläisten GLONASS:in, eurooppalaisten Galileon tai esimerkiksi kiinalaisten BeiDoun, saman GPS-termin alle, vaikka näin ei tulisi tehdä. Mikäli esimerkiksi GPS-järjestelmästä, näistä edellä mainituista tai muista järjestelmistä halutaan puhua samanaikaisesti, tulee tällöin yhteisenä paikannusjärjestelmän terminä käyttää joko lyhennettä GNSS tai sen pidempää versiota Global Navigation Satellite Systems (ESA, 2014a). Liekö tällaiseen sekaannukseen syynä useiden edellä mainittujen järjestelmien satelliittien osittain GPS:n kanssa päällekkäin käyttämät signaalien taajuudet tai vastaavat, vaiko jokin muu syy, mutta tässä tutkimuksessa keskitytään vain ja ainoastaan Yhdysvaltojen GPS-järjestelmään.

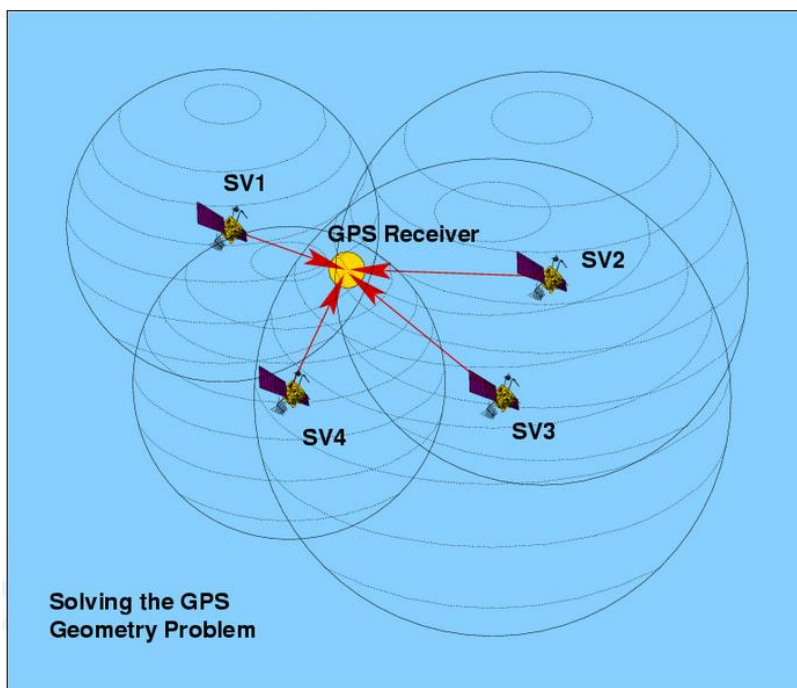
GPS-satelliitteja on avaruudessa kiertämässä yhteensä 32 kappaletta kuu-della eri ratatasolla. Koko GPS:n toiminnan perusidea on ajan laskemisessa. Satelliiteissa on todella tarkat atomikellot, joita Yhdysvaltojen Puolustusviranomaiset valvovat ja tarpeen tullen korjaavat maasta käsin lähettämällä korjauskoodia signaalien valvontakeskuksesta. GPS-järjestelmä voidaan jakaa kolmeen eri ryhmään. Ensimmäiseen ryhmään kuuluvat satelliitit tarkkoine atomikelloineen. Toinen ryhmä on kontrolliverkko, johon kuuluvat päävalvonta-asema ja seuranta-asemat dataa satelliiteille lähettävine antennineen. Kolmanteen ryhmään kuuluvat käyttäjät GPS-vastaanottimineen. Jotta esimerkiksi aluksen GPS-vastaanotin saisi selville paikkansa, täytyy vähintään neljän satelliitin kyetä saada yhteys aluksen vastaanottimeen. Satelliitit lähettävät sekä P-koodia, että C/A-koodia, joko L1, L2 tai L5 -taajuuksilla. P-koodi on sotilasliikenteen käytössä ja C/A koodi on nykyään siviililiikenteen käytössä. Taajuuksista L1 ja L2 kuuluvat vanhempiin satelliitteihin ja L5 taas uudempiin. (GPS.Gov, 2017b) ja (Poutanen, 2016, 19-21.).

Kun satelliitit lähettävät signaaliaan avaruudesta, niin GPS-vastaanotin maan päällä, merellä tai ilmassa - riippuen siitä, minkä tyyppinen se kolmesta vastaanotimesta on - tulkitsee sitä seuraavalla tavalla. Ensimmäisessä vaihtoehdossa vastaanotin mittaa, laskee ja tunnistaa satelliittien lähettämää koodia suhteessa vastaanottimen väliin mahtuvaan etäisyyteen. Tällöin puhutaan koodipaikannuksesta. Perinteisesti siviilialusmerenkulussa käytettiin koodipaikannukseen perustuvaa paikanmäärittystä. Mutta ennen kuin Yhdysvaltojen viranomaiset poistivat C/A-koodista häirintäkoodin, niin tällä paikannusmetodilla ei

päästy tarpeeksi pieniin ja luotettaviin tarkkuuksiin/tuloksiin. Tästä syystä merenkulkijoille luotiin DGPS (Differentiaalinen GPS) -järjestelmä (Hegarty, Kaplan, 2006.). Tämä toimii edellä mainitun periaatteen mukaan, mutta sen lisäksi tässä on kiinteällä pinnalla oleva toinen vastaanotin, jonka paikkaa verrataan liikkuvan vastaanottimen paikkaan. Tieto kiinteällä pinnalla olevasta vastaanottimesta ja sen sijainnista voidaan lähettää liikkuvalla vastaanottimelle esimerkiksi radiolinkeillä, puhelinverkoilla tai internetillä. Näin liikkuva vastaanotin voi tehdä tarkempia etäisyyden laskelmia satelliitteihin nähden ennen oman paikkansa ilmoittamista. Kolmannessa vaihtoehdossa, eli kantoaaltoon/suhteellisuuteen perustuvassa paikannuksessa, on laskea satelliitin signaalin lähettämien aallon pituuksien lukumääriä. Tällä tekniikalla päästään nykyaikana jo huomattavasti tarkempiin paikan määrittäytuloksiin. Nykyaikana on myös käytössä Reaaliaikaisia kinemaattisia mittaus (RTK), sekä Precise Point Positioning (PPP) -tekniikoita, mutta ne eivät toistaiseksi sovellu aluksilla navigointiin. Tämän takia tutkimuksessa ei keskitytä näihin kahteen tekniikkaan. Näistä tekniikoista voi kuitenkin todeta, että niiden hyvänä puolena on se, että paikka pystytään määrittämään todella tarkasti, mutta huonona puolena on tiedonsiirron hitaus. (Poutanen, 2016, 13-16.). Tämän takia ko. paikannustekniikoita (RTK ja PPP) käytetään lähinnä tilanteissa, joissa aikaviiveellä ei ole niin väliä, kuten esimerkiksi maankuoren korkeus ja sivuttaisliikkeet.

Koodipaikannuksessa päästään tänä päivänä perinteisesti vain muutamien metrien tarkkuuksiin, mutta tieto tästä sijainnista tulee nopeasti, ja itse vastaanottimet ovat halpoja. DGPS-järjestelmällä saadaan luotettavaa paikkatietoa ja päästään parhaimmillaan puolen metrin tarkkuuksiin. Kantoaaltoon perustuvalla/suhteellisella paikannuksella päästään parhaimmillaan millimetritarkkuuksiin, mutta haittapuolena on vastaanottimien vaatimat suuret datansiirtomäärät. Tämän takia näiden tieto tarkasta paikasta tulee aina myöhässä, ja vastaanottimien hinnat ovat kalliita. Nämä reunaehdot pätevät vielä tänäkin päivänä, mikäli puhutaan GPS-järjestelmien siviilivastaanottimista. (Poutanen, 2016, 13-16) ja (GPS.Gov, 2017b.).

GPS-järjestelmässä havaittajan paikanmäärittäminen ja lasku perustuvat aikaerojen mittaukseen (Kuvio 3). Signaaliin on moduloitu koodi, josta saadaan selville signaalin kulkuaika, jota nimitetään määreellä  $t$ . Ajassa  $t$  signaali on ehtinyt valonnopeudella SV1-säteisen pallon pinnalle. Samalla lailla, kun SV2-satelliitin etäisyys tunnetaan, tarkentuu paikka SV1 ja SV2 -satelliittien muodostamien etäisyyspallojen leikkausviivoille. Kolmannella satelliitilla SV3 ja edellä mainitulla periaatteella paikka tarkentuu jo kolmen pallon leikkauspisteeseen. Kolmella satelliitilla on kuitenkin vielä pieni kellovirhe, jota varten tarvitaan neljäs satelliitti SV4, joka tarkentaa paikan varmasti mahdollisimman tarkaksi. (Poutanen, 2016, 12-13). Tämän vuoksi on tärkeää, että kontrolliverkko tarkkailee ja korjaa jatkuvasti satelliittien atomikelloja. Mikäli tätä ei tehtäisi, kehittyisi satelliiteille joka päivä noin 10 nanosekunnin virhe. Ajassa se voi tuntua todella pieneltä, mutta pitkillä matkoilla ja valonnopeudella liikuttaessa se tarkoittaa maan päällä päivittäin kolmen metrin virhettä (Askola, Lehtonen & Virtanen, 2016, 24.).



KUVIO 3 Havaintijan paikan laskeminen GPS-järjestelmässä. (Air power Australia)

Markku Poutanen, joka on yksi Suomen johtavia GPS-paikannuksen parissa työskentelevistä tutkijoista, painottaa hyvin vahvasti sitä, että nykyaikana laitevalmistajat antavat liian suuria haavekuvia GPS:n paikannuksen tarkkuudesta. Tästä syystä alla esitettävässä taulukossa oleva karkea perusjako pitää hyvin paikkansa (Taulukko 1):

TAULUKKO 1 GPS-järjestelmän tarkkuus eri paikannustekniikoilla. Koodia käyttämällä päästään metri luokan tarkkuuksiin. Kantoaaltoa käyttämällä päästään jo varmasti desimetrin tarkkuusluokkaan, mikäli apuna käytetään suhteellista mittausta tunnettuun tukiasemaan. Pysyviä asemia pelkästään käyttämällä voidaan päästä millimetrin tarkkuuksiin. (Poutanen, 2016, 16-17).

Havaintosuure	Tarkkuus	Sovellukset
Koodi/koordinaatit	10 m	Navigointi; yksi vastaanotin
	1 m	
Vaihe/Koordinaatit	0,1 m	RTK, tukiasema
	0,01 m	
Vaihe/Muutokset	0,001 m	Pysyvät asemat, PPP

GPS-vastaanottimia on valmistettu monenlaisiksi. Yksitaajuusvastaanottimet vastaanottavat vain GPS-satelliittien lähettämää L1-signaalia ja sitäkin vain yleisesti C/A koodina. Nämä ovat perinteisesti niitä vastaanottimia, joita on käytetty navigointiin ja differentiaalimittauksiin. Joihinkin tällaisiin vastaanottimiin on jo luotu tekniikka, jolla kyetään tallettamaan kantoaallon informaatiota. Tällöin se

soveltuu myös suhteellisiin mittauksiin, mutta vain yhdellä edellä mainitulla taajuudella. Kaksitaajuusvastaanottimet tulkitsevat L1 (1575,42 MHz, aallon pituus 19 cm.) ja L2/L2C (1227,6 MHz, aallon pituus 24 cm.) taajuuden signaaleja. Siviilipuolella vastaanottimet ymmärtävät ainoastaan C/A-koodia, mutta sotilaspuolella nämä vastaanottimet ymmärtävät myös P-koodia. Uusimmissa satelliiteissa, on myös L5-taajuus (1176,45 MHz). Tekniikka on kuitenkin jo kehittynyt niin paljon, että jälkilaskennalla voidaan hankkia myös P-koodin tieto ja näin saada parempaa paikkatietoa. Ongelmana vain on, että vielä tänä päivänäkin kyseinen tieto tulee myöhässä. Monitaajuusvastaanottimista puhuttaessa kyseessä on vastaanotin, joka tulkitsee useiden muiden satelliittien paikkatietojärjestelmää esim. GLONASS tai BeiDou lähettämää signaalia. (Poutanen, 2016, 15-16) ja (ESA, 2014b) ja (GPS.Gov, 2016c.).

Vuoden 2005 jälkeen avaruuteen on lähetetty IIR-M-satelliitteja, jotka kykenevät lähettämään C/A-koodia L1 ja L2 -taajuudella. Samaan aikaan myös L2 lähetystehoja on lisätty. Vuoden 2010 jälkeen avaruuteen on lähetetty IIF satelliitteja, jotka lähettävät dataa yllä mainitulla L5-taajuudella (GPS.Gov, 2016c.).

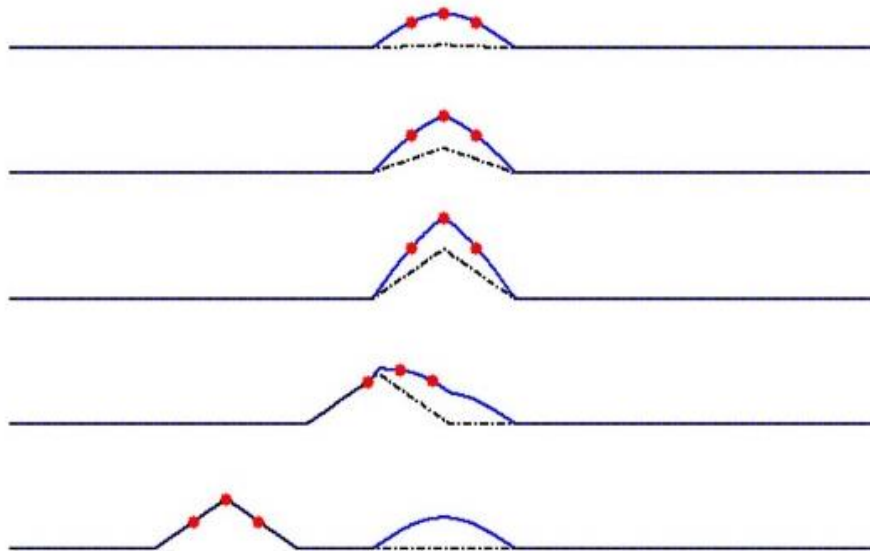
## 4 GPS-HARHAUTUS

Vuoden 2000 toukokuun jälkeen, kun Yhdysvaltojen puolustusvirasto lopetti C/A-koodin (SA = selective availability) tarkoituksellisen huonontamisen, niin GPS-vastaanottimien tarkkuus sekä käyttö on lisääntynyt valtavasti (GPS.Gov, 2012d). Ennen SA-koodin poistoa GPS:n tarkkuutta olisi voitu verrata siihen, että henkilö olisi esimerkiksi Helsingin stadionilla, muttei tiedä, missä hänen oma paikkansa siellä tarkalleen on. Hän voisi olla yhtä hyvin katsomossa, keskellä kenttää tai kentän reunalla. Nyt SA-koodin poistuttua, tämä sama henkilö kykenee tunnistamaan paikkansa sijainnin kyseisellä stadionilla noin 1-10 metrin tarkkuudella. Tämä taas on johtanut siihen, että tänä päivänä yksittäiset lenkkeilijät, autokuskeista kaupallisiin jumbojetteihin käyttävät näitä vastaanottimia yhä enemmän ja enemmän. Samalla lailla näitä vastaanottimia käytetään myös merellä, aina pienistä soutuveneistä suuriin risteilijäaluksiin. GPS paikannuslaitteena ja järjestelmänä on yksi maailman käytetyimmistä ja suosituimmista. Mutta sen suurin heikkous piilee siinä, että sen C/A-koodia, jota siviilipuolella käytetään, ei salata mitenkään (Humphreys, 2012, 2) ja (Poutanen, 2016, 20). Saman aikaisesti tätä kyseistä laitetta ja koodia kuitenkin käytetään päivä päivältä enemmän yllä kuvatulla tavalla aina sunnuntailenkkeilijän matkakellosta viranomaisen navigaattoriin ja öljytankkereiden merenkulun navigoinnin helpottamiseen. (Capkun, Pöpper, Rasmussen & Tippenhauer, 2011, 17 – 21).

Mutta miten merellä käy, jos joku huijaa tai häiritsee GPS-vastaanotinta niin pahasti, että siitä katoaa kokonaan paikkatiedot tai se alkaa salakavalasti ilmoittamaan virheellistä tietoa? Onko sellainen tänä päivänä mahdollista? Lyhyt ja nopea vastaus tähän on, KYLLÄ ja pidempi versio perusteluineen seuraa perässä. Molemmissa sekä jumiuttamisessa, että harhauttamisessa halutaan suorittaa jotain häiriötoimintaa jonkin sorttisille GPS-vastaanottimille. Jälkimmäinen vaihtoehto tuo taas mukanaan huomattavasti vakavammat kyberrikollisten/-terroristien suorittamat teot, joita tässä tutkimuksessa tutkitaan. Tästä syystä monesti tämä termistön ja teknisyiden laajuus kenties luo sekavuutta näiden kahden termin väliin ja yhteiseen sekakäyttöön.

GPS-jumiuttamisella tarkoitetaan suomenkielessä GPS-järjestelmän häiriötoimintaa, jossa tarkoituksena on pyrkiä estämään simulaattorilla (tästä eteenpäin häirintälaitte) GPS-satelliittien heikkoa signaalia pääsemästä perille vastaanottimeen. Häirintälaitteella tullaan ikään kuin tähän väliin suurella häiritsevällä teholla sopivalla GPS:n taajuuskaistalla, ja näin oikea paikka signaali ei pääse perille. Ikävä kyllä kyseisiä häirintälaitteita saa internetistä halvimmillaan 15-280 euron hintaan (Askola, Lehtonen & Virtanen, 2016, 24.). Mikäli tällä keinolla ei kokonaan kyetä estämään GPS-satelliittien signaalia vastaanottimeen, sillä kytetään yleensä ainakin lisäämään huomattavasti häiritsevää signaalien taajuuskohtina, jolloin paikkatiedon luotettavuus pienenee huomattavasti (Kuusniemi, Bhuyian, Kröger, 2013, 3).

GPS-spoofingilla tarkoitetaan GPS-vastaanottimen koordinaattien väärentämistä ja tästä eteenpäin me käytämme termiä GPS-harhauttaminen. Esimerkiksi kyberterroristi käyttää harhauttamiseen suunniteltua simulaattoria ja saa näin halutessaan merialuksen kulkemaan valitsemaansa suuntaan. Hän vastaanottaa oikeita signaaleita satelliiteilta omaan simulaattoriin ja modifioi nämä vääriksi/manipuloiduiksi signaaleiksi. Harhauttaja vain lähettää manipuloidut signaalit oikea-aikaisesti vastaanottajan antenniin, asteittain tehoja lisäten kohti suurempaa tehoa. (Askola, Lehtonen & Virtanen, 2016, 24) ja (Bhatti & Humpreys, 2014, 2-3) lisäksi (kuvio 4). Tällä tavalla harhauttaja kykenee saamaan vastaanottajan GPS-laitteen luulemaan väärää signaalia oikeaksi. GPS-signaalia väärentämällä kyetään saamaan todella suuria riskejä, koska aluksen navigoijan on todella vaikea havaita missä vaiheessa hän on joutunut signaalien väärennöksen uhriksi (Kuusniemi, Ym., 2013, 3). Mikäli navigoija on sokeasti luottanut vain GPS:n tuomaan paikkatietoon, kyetään hänet lopulta huijaamaan uskomaan olevansa eri paikassa, kuin mitä hän oikeasti on.



KUVIO 4 GPS-signaalin ja paikan kaappaus, (Psiaki & Humpreys, 2016).

Kybermaailmalla on kuitenkin kohistu vuodesta 2012 jälkeen, kun tiedemies Todd Humpreys oppilaineen suunnitteli GPS-harhautus simulaattoriin, jolla voitaisiin mahdollisesti johtaa laiva väärälle kurssille. Tällä kyseisellä simulaattorilla hän onnistui suorittamaan käytännön kokeen Italiassa, jossa 65 metriseltä huvijahdilta kyettiin ohjaamohenkilökunnan huomaamatta viemään paikkatiedot ja saattamaan alus väärälle kurssille (Bhatti & Humpreys, 2014, 1-2) ja (UT News, 2013). Palaamme tähän kokeeseen seuraavan luvun loppupuolella, mutta sitä ennen suoritetaan GPS-harhautusteoriakoe ilmasta käsin.

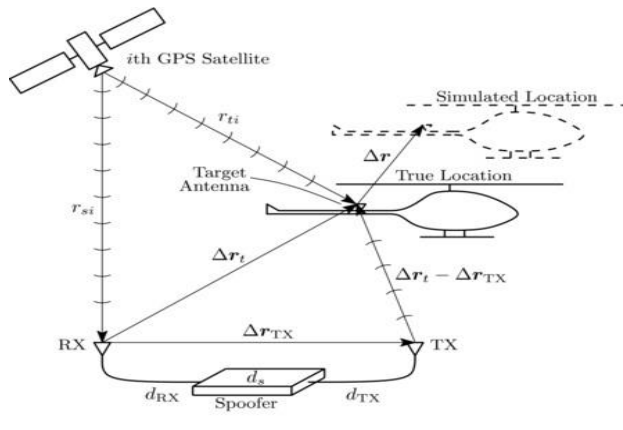
## 4.1 GPS-harhautuksen perusteet ja uhkakuvien kehittyminen

Sen jälkeen, kun SA-koodi poistettiin GPS signaalista, on se lisännyt käyttäjäkuntaa yhteiskunnassamme kansainvälisesti räjähdysmäisesti. Tästä syystä myös useilla tiedemiehillä, on noussut monia riskikuvia sekä mahdollisia uhkamalleja tätä avointa järjestelmää kohtaa. Mutta vain yksi näistä tutkijoista, nousee kirkkaasti esiin muiden joukosta. Kun tänä päivänä lukee GPS-harhautuksesta julkaistuja tieteellisiä artikkeleita, konferenssijulkaisuja tai kirjoja, niin näissä kaikissa viitataan todella vahvasti Texasin Austinin yliopistossa työskenteleviin tiedemiehiin nimeltä Daniel Shepard ja Todd Humpreys. He ovat oivaltaneet heti alusta asti, kuinka suuri uhkakuva nykyinen siviili GPS-järjestelmä yhteiskunnallemme on, mikäli asioiden eteen ei tehdä mitään muutoksia. Tästä syystä he keräsivät joukon parhaimpia opiskelijoitaan, ja suoritti ensimmäisenä käytännön kokeen, jossa tehtiin GPS-harhautus UAV:lle (Unmanned Aerial Vehicles), eli miehittämättömälle lennokille (Shepard, Bhatti & Humpreys 2012).

He rakensivat ensin opiskelijoidensa kanssa tietokonelaboratoriossa simulaattorin, jolla he aikoivat suorittaa kyseisen UAV:n GPS-harhautuksen. He hakivat DHS:ltä (Department of Homeland Security) luvat suorittaa kyseisen käytännön testi, koska GPS:n häirintä Yhdysvalloissa on rangaistava teko. Samalla he hakivat myös luvat testialueeseen. Tämä GPS-järjestelmää käyttävä vastaanotin ja lähetin käsittelivät vain siviilitason C/A, L1-koodia. (Shepard ym., 2012, 2-4.).

Itse käytännön ensimmäinen GPS-harhautustesti suoritettiin White Sandsin ampuma-alueella. Laboratoriossa kehitetty harhautuslaite sijoitettiin puoli mailia testialueen sivuun mäen päälle, itse UAV:n/lennokin lentoalueesta, jossa lennokkia testattiin. Lennokkia alettiin ohjailta noin 16,5 metrin korkeudelta tornista käsin. Käskystä simulaattorilla aloitettiin virheellisen GPS-signaalin heikko lähetys. Tämä huijaussimulaattorin heikko väärän GPS-signaalin lähetys ei vielä tehonnut lennokkiin, mutta testiryhmän lisätessä reilusti lähetystehoja he saivat lennokin otettua haltuunsa GPS-signaaleilla ja huijattua sen tahtomalleen väärälle paikalle. He pystyivät luomaan lennokille kuvitteellisen tilanteen, jossa virheellinen GPS-signaali sai koneen luulemaan olevansa 3,3 jalkaa ylempänä, kuin mitä se oikeasti oli (Kerns, Shepard, Bhatti & Humpreys, 2014) ja (Shepard ym., 2012, 6-8.). Kuviossa 5 pyritään selvittämään, miten lennokki tulkitsee virheellisen korkeuseron.





KUVIO 5 Käytännön GPS-harhautuskoe lennokin ohjaukseen. Kuvassa selvennetään se, kuinka itse tehdyllä GPS-harhautussimulaattorilla kyetään haluttaessa huijaamaan lennokki luulemaan olevansa eri paikassa, kuin missä se oikeasti on (Kerns, Shepard, Bhatti & Humphreys, 2014).

Tällä kokeella kyettiin todistamaan se, että mikäli kyberrikolliset tai -terroristit haluaisivat, vastaavalla toimenpiteellä kyettäisiin tuhoamaan myös miehittämättömiä lennokkeja, mikäli he saisivat käsiinsä tällaisia GPS-huijaussimulaattoreita.

Testiryhmän jäsen, joka oli vastuussa lennokin ohjailusta (hän oli ikään kuin tavanomainen ohjailija, joka ei olisi tiennyt normaalioloissa tästä GPS-huijauksesta) joutui laittamaan manuaaliohjauksen päälle lennokin ollessa enää 3,3 metrin korkeudessa, koska muuten heidän testilennokkinsa olisi romahtanut maankamaralle. Tämä pystyttiin todistamaan useita kertoja, sillä lennokki lähetti lennättäjälle ohjaimen virheellistä tietoa verrattuna siihen, missä se oikeasti oli. Lennokki lensi siis GPS-signaalin harhauttajien mukaan, ei normaalin lentäjän/ohjailijan mukaan. Testi tehtiin myös useamman kerran. Mielenkiintoisinta mielestäni oli se, että tässä kyseisessä kokeessa kaiken muun ohessa onnistuttiin saman tien rakentamaan niin tehokas simulaattori, että sen lähettämä signaaliteho kykeni tekemään tämän kaiken 0,62 kilometrin päästä. Viitteitä siitä, että kyseinen simulaattori olisi toiminut pidempää, olisi mahdollisesti ollut, mutta testissä ei viety sitä pidemmälle. (Shepard ym., 2013, 7-8).

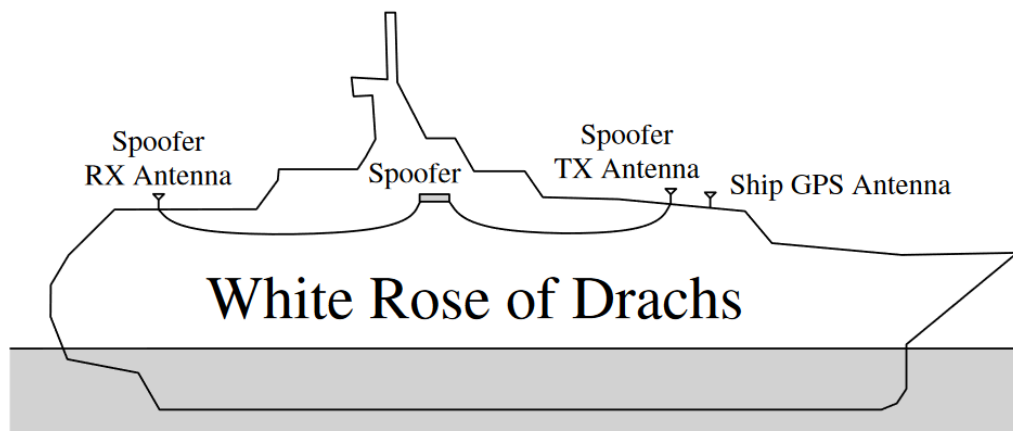
Kun he olivat osoittaneet tiedemaailmalle, että GPS-harhautus ja sen tekniikka ja käytännön tason kaappaus on mahdollista tehdä henkilökohtaisesti, moni tiedemies on ollut ihmeissään, ja varsinkin Yhdysvaltojen viranomaisilla on noussut pahoja ennakkoavistuksia tulevaisuuden varalle. Etenkin Yhdysvaltojen turvallisuusviranomaiset ja puolustusvoimien upseerit ovat alkaneet informoida henkilökuntaansa monin eri tiedotusvälinein kyberterroristien mahdollisista uhkakuvista suorittaa GPS-harhautusta.

Tilanne on kuluneiden vuosien ja myös tulevien vuosien kannalta hieman kaksijakoinen. Samalla kun meidän ja monen muun maan yhteiskunnassa suositetaan liikenteessä entistä enemmän automatiikkaa ja GPS-järjestelmään pohjautuvaa autopilottijärjestelmää, niin mikäli me emme ota huomioon GPS-huijaukseen

pohjautuvaa uhkakuvaa, me luomme tulevaisuutta varten valtavasti uusia riskejä. Varsinkin laivateollisuudessa ja merenkulussa tullaan tulevaisuudessa panostamaan entistä enemmän henkilökunnan vähentämiseen ja useamman asian automatisoimiseen (Rantanen, 2017). Samalla lailla myös laivojen ohjailussa ollaan jo nyt siirrytty autopilottisiin merenkulkuihin mahdollisimman paljon, mutta tulevaisuudessa vielä enemmän. Tähän on monia perusteluita, kuten esimerkiksi aluksen tasaisempi kulkunopeus, optimoidummat käännökset, polttoainekulujen säästyminen, jolloin myös luonto pysyy paremmassa kunnossa. (Alessandri, Donnarumma & Vignolo, 2015, 577-578.). Mutta toisesta näkökulmasta katsottuna ymmärtää hyvin, miksi Yhdysvaltojen rajaviranomaiset ovat maininneet yhdeksi mahdolliseksi tulevaisuuden suurista uhkakuvista jonkin tärkeän tai suuren merialuksen GPS-järjestelmän mahdollisen harhautuksen (Thompson, talvi 2014-2015). Olisiko aluksen harhauttaminen mahdollista, jos se kulkisi vain GPS-järjestelmiin perustuvien navigaatiolaitteiden varassa? Kyettäisiinkö tällä tavalla suorittamaan mahdollinen ja samalla tavalla lamaannuttava terroristi-isku mereltä käsin, kuin vuonna 2001 New Yorkissa WTC-torneihin suoritettiin? Olisiko heidän yhteiskunta mahdollisesti haavoittuva mereltä tuleviin GPS-harhautuksiin?

Myös tästä edellisessä tutkimuksessa ollut Humpreys, halusi ottaa selvää, sekä lisätä keskustelua mahdollisesta GPS-järjestelmään ja meriliikenteeseen tulevaisuudessa kohdistuvasta uhkakuvasta. Hän keräsi ryhmän opiskelijoita, joiden kanssa hän rakensi uuden merialuksen GPS-järjestelmän huijaussimulaattorin, jolla asiaa voisi käytännössä kokeilla. Itse käytännön koe suoritettiin 65 metriä pitkällä White Rose nimisellä superjahdilla Välimerellä Italian eteläpuolella 30:n meripeninkulman päässä rannasta kansainvälisillä merialueilla tutkimusryhmän saatua luvat kaikilta osapuolilta tähän kokeeseen. Humpreys halusi osoittaa ihmisille, kuinka haavoittuva meriliikenteen paikannusjärjestelmä on, ja lisätä keskustelua ihmisten, tiedemiesten ja viranomaisten kesken siitä, miten alus kyetään mahdollisesti kaappaamaan satelliittipaikannusjärjestelmän avulla digitaalisesti. Tähän asti keskustelua aluksen kaappaamisesta/aluksen väkisin ohjailusta oli käyty aina vain sen fyysisessä muodossa, sillä vastaavaa koetta ei ollut vielä kukaan kyennyt tekemään. (Bhatti & Humpreys, 2014, 1-2) ja (UT News, 2013).

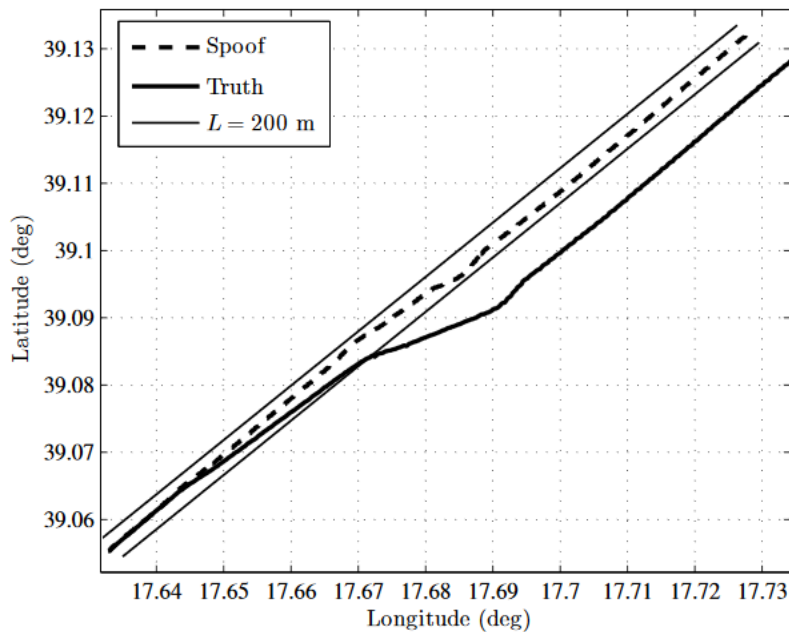
Itse GPS-harhautussimulaattori, josta signaalin lähetystehoja säänneltiin ja lähetettiin, oli noin salkun kokoinen laatikko, ja se sijoitettiin kahden oppilaan kanssa aluksen keskelle sen komentosillalle (Kuvio 6). GPS-huijauslaitteen oma signaalivastaanotin laitettiin aluksen perään ja sen lähettävä osa laivan GPS-vastaanottimen lähelle, jotta koe onnistuisi helpommin. (Bhatti & Humpreys, 2014, 7.).



KUVIO 6 GPS-simulaattorien paikat. Osoittaa Humpreysin ja hänen ryhmänsä sijoittaman GPS-huijaussimulaattorin ja sen vastaanotin- ja lähetinantennien paikat. (Bhatti & Humpreys, 2014, 7).

Koe aloitettiin vasta, kun aluksen kapteeni oli vienyt aluksen turvallisesti sovitulle testipaikalle ja saanut sen pidettyä tasaisesti haluamallaan kulkusuunnalla. Merellä on aina myös jonkin verran tuulia ja virtauksia, jotka pyrkivät kääntämään aluksen kulkusuuntaa, mutta kokenut kapteeni kykenee pitämään aluksen suorassa normaalilla kelillä todella helposti. Tämä aluksen lievä keulan jatkuva suunnanvaihtelu myös helpottaa, niin tutkimuksen suorittajaa kuin myös tosi-paikan tullen kyberrikollista, koska aluksen kapteeni ei niin nopeasti kiinnitä huomioita pieniin heilahduksiin. Lisäksi tässä kokeessa tarkoituksena oli kulkea autopilottiavusteisena niin kuin normaalistikin avomerillä yleensä kuljetaan. Merenkulkuhenkilöstöllä oli siis tarkoituksena ohjailta alusta normaalisti merellä ja koettaa huomata, missä vaiheessa heidät on GPS-harhautettu sivuun sovitulta väyläosuudelta (Kuvio 7). Tutkijaryhmällä taas tarkoituksena oli yrittää kaapata kyseinen alus GPS-harhauttamalla niin hienovaraisesti, ettei ohjaava merihenkilöstö mahdollisesti huomaa sitä. (Bhatti & Humpreys, 2014, 1-2 & 7-8).

GPS-huijausta testaavat tutkijat aloittivat aluksen väärennetylle suunnalle huijaamisen aluksi rauhallisesti ja maltilla, niin että alus eteni sivusuunnassa vain 0,5m/s. Itse alus eteni samaan aikaan 15 solmun vauhdilla eteenpäin. Kun oltiin varmistuttu, että aluksen järjestelmät eivät hälytä poikkeavista GPS-signaaleista ja aluksen ohjailusta vastaava henkilöstö ei ollut huomannut vielä mitään, aluksen loittonemisvauhdiksi alkuperäisestä kapteenin haluamasta suunnasta lisättiin 2m/s. Lopulta alus käännettiin saman suuntaiseksi, kuin alun perinkin se oli ennen GPS-huijauksen alkua. Näin ollen tutkimuksessa oli onnistuttu siirtämään laiva hieman yli 200 metriä linjasta sivuun kuin missä sen piti kapteenin mukaan alun perin olla. Eikä laivan navigointivälineet tai navigoinnista vastaava merihenkilöstö ollut huomannut kyseistä tapausta. (Bhatti & Humpreys, 2014, 8).



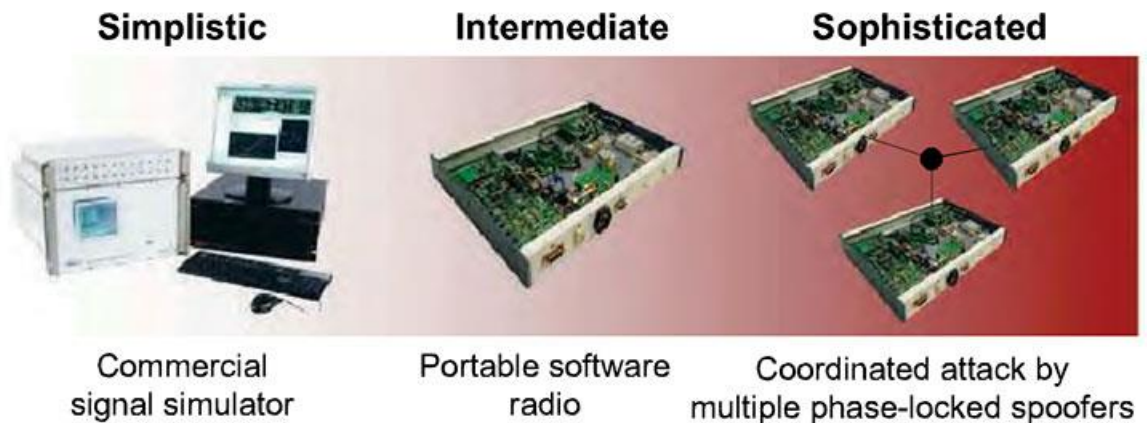
KUVIO 7 Aluksen harhautettu paikka. Katkoviiva osoittaa navigointihenkilöstön luuleman laivan paikan ja suunnan. Tummennettu paksumpi viiva osoittaa aluksen tutkimuksessa kulkeman todellisen paikan ja suunnan. Suorat ohuet viivat ilmoittavat väärennetyn paikan vaihteluvälin. (Bhatti & Humpreys, 2014, 8).

Suurempaan aluksen GPS-järjestelmien ja merihenkilöstön harhauttamiseen tässä tutkimuksessa ei menty. Katsottiin, että jo tällä oltiin kyetty osoittamaan, kuinka navigointijärjestelmät ovat haavoittuvia. Kokeella oli myös kyetty saattamaan alus eri koordinaateille kapteenin huomaamatta, vaikka oltiin avomerellä ja sivusuuntainen siirtymä oli ehkä näin ollen hankala huomata perinteisillä navigointijärjestelmillä. Kokeella haluttiin kuitenkin ensisijaisesti kokeilla, kyetäänkö GPS-huijausta ylipäättänsä tekemään, niin että navigointijärjestelmät eivät huomautta mitään, ja huomaako henkilöstöstä kukaan mitään. (Bhatti & Humpreys, 2014, 8.). Lisäksi näinkin pieni sivuttaissuunnan siirtymä on jo kohtalokas esimerkiksi rannikon ja sataman lähetyvillä muun muassa sumun aikaan. Lisäksi Helsingin edustalla on liikenteen ruuhkaisuuden vuoksi vähän aikaa toimia.

## 4.2 GPS-signaalien harhautussimulaattori

GPS-signaalilähettimet voivat olla hyvin halpoja rakentaa ja tehdä, kun puhutaan siviilitason simulaattoreista. Tässä vaiheessa on syytä kertoa, mitä harhautussimulaattorilla tarkoitetaan. Harhautussimulaattorilla tarkoitetaan GPS-harhautukseen kykenevää ja sitä varten rakennettua lähetintä. Itse asiassa näitä on

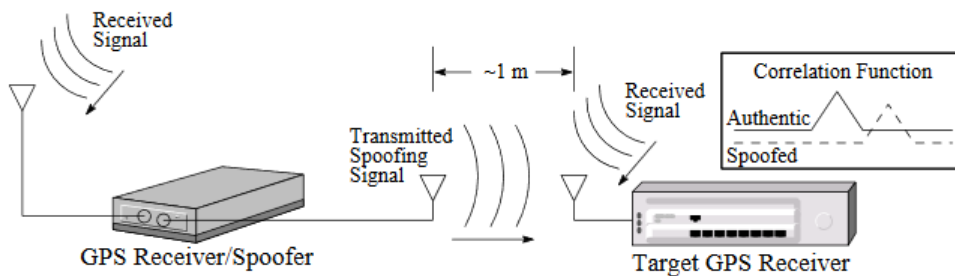
rakennettu myös siviilikäyttöön koulutusta varten. Kuitenkin näiden joutuessa rikollisten käsiin, ne muuttuvat hyvin vaarallisiksi välineiksi ja ovat hyvin oivallisia välineitä GPS-järjestelmien huijaamiseen ja väärentämiseen. Tutkijat jakavat GPS-simulaattorit/-lähettimet kolmeen eri luokkaan (Kuvio 8). Nämä kolme luokkaa ovat: simplistinen/liian pelkistetty (simplistic), keskitason simulaattorikone (intermediate) ja monimutkainen/kehittynyt (sophisticated) (Sathyamoorthy, 2013, 45-46) ja (Humphreys, ym., 2008, 3-4.).



KUVIO 8 GPS-Simulaattorit (Sathyamoorthy, 2013, 45).

Simplistinen lähetin toimii yksin ilman muita ominaisuuksia ja GPS-järjestelmiä. Tämän tyyppisessä väärennösiskussa ei kyseessä ole yhteistoimintasygnäalin ja doberilmiön tyyppisestä yhteistyöstä, vaan simulaattori toimii itsenäisesti lähettäen omaa dataa aluksen vastaanottimeen. Laivan/aluksen GPS-paikannin voi mahdollisesti kadottaa väliaikaisesti oman paikkansa joutuessaan tällaiseen iskuun, ja parhaimmassa tapauksessa voidaan kyetä tunnistamaan, että se on joutunut väärennöksen alaiseksi, sillä tällaisessa tapauksessa GPS-paikannin jumiuntuu 100 nanosekunniksi. (Humphreys, ym., 2008, 3.). Tosin niin kuin ymmärretään, niin käytännössä tuo 100 nanosekunnin viive on hyvin lyhyt. Tällöin voidaan ajatella, että sen voi tunnistaa/paljastaa teoriassa, mutta käytännössä ei. Valitettavasti nykyisissä laivoissa ja niiden vastaanottimissa ei ole vielä sellaista tekniikkaa, joissa kyetään tunnistamaan, että alus on joutunut manipuloidun GPS-signaalin alaiseksi. Tällaisissa tilanteissa laivan paikka ja aika ovat muuttuneet oleellisesti, sen oikeista tiedoista ajoista ja paikoista. Tämän takia kaikki siviili GPS-järjestelmää käyttävät laivat ovat haavoittuvia, jopa yksinkertaisille GPS-signaalien väärennösyökkäyksille (Sathyamoorthy, 2013, 45-46). Tämän tyyppiset pelkistetyt lähettimet voivat painaa hyvin paljon ja näillä on hyvin heikko teho. Lisäksi nämä simplistiset lähettimet maksavat myös huomattavia määriä, mikä voidaan katsoa näiden epäeduksi (Humphreys, ym., 2008, 3). Tosin tekniikka ja kehitys kehittyvät päivä päivältä kovaa vauhtia, ja tämä kyseinen Humphreysin-raportti oli laadittu vuonna 2008, eli noin kymmenen vuotta sitten. Näin ollen voimme sanoa, että kyseiset laitteet ovat jo mahdollisesti historiaa tai ainakin kehittyneet huomattavasti.

Intermediate-tyyppinen, eli keskitason lähettin toimii aivan eri tavalla. Se on niin pieni ja kevyt, että se kyetään laittamaan GPS-vastaanottimen viereen hyvin lähelle, mahdollisesti jopa yhden metrin etäisyydelle, josta se kykenee lähettämään väärennettyä dataa (signaalin paikkatietoa). Ajan kanssa se arvioi oikeat toimenpiteet vastaanottimelle ennen kuin se aloittaa GPS-signaalin väärennös-hyökkäyksen, milloin sen tunnistaminen vaikeutuu huomattavasti (Kuvio 9).



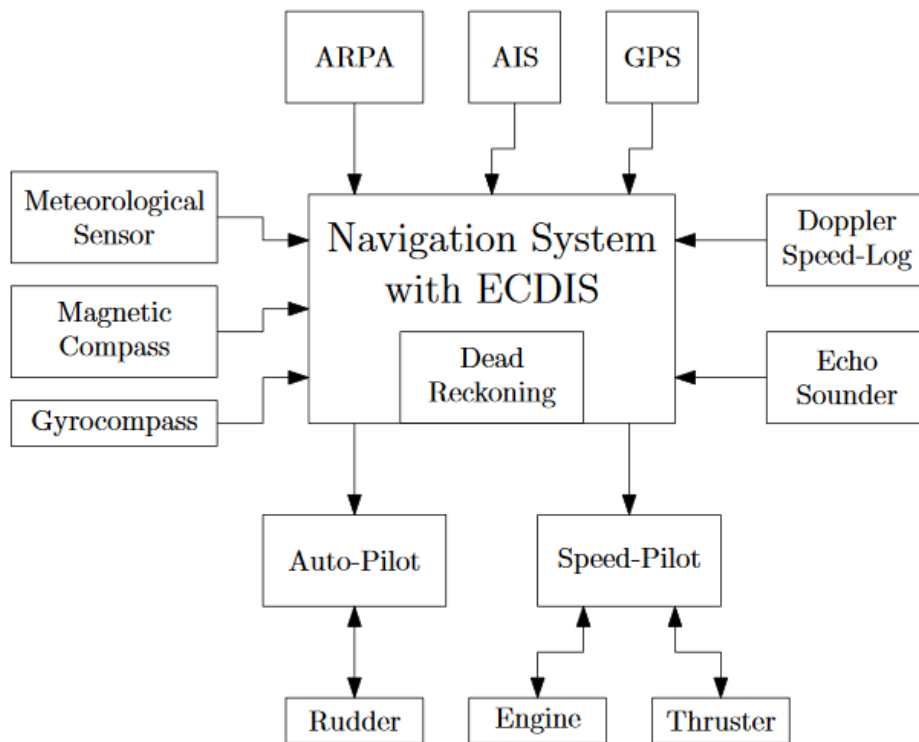
KUVIO 9 Keskitason GPS-simulaattorin toimintaperiaate, (Humphreys, ym., 2008, 3).

Keskitason GPS-signaalin väärennysisku voidaan tehdä pikkuhiljaa signaalin tehoa lisäämällä, niin että lopuksi laivan GPS-vastaanotin on kaapattu kokonaan haltuun, eikä sen ohjailija ole huomannut yhtään mitään. Hyökkääjä kykenee lisäämään vähitellen lähettimen tehoa ajan kuluessa, niin että kyseinen lähettin voi olla vastaanottimen vieressä useita tunteja, jopa päiväkausia peräjälkeen. (Sathyamoorthy, 2013, 45-46) ja (Humphreys, ym., 2008, 3-4.). Tämän tyyppisen lähettimen paikantaminen on jo hyvin hankalaa, mutta se kyetään tekemään useammalla paikantamisantennilla. Yksittäisellä paikantamisantennilla lähettimen paikantaminen on käytännössä mahdotonta.

Sophisticated-tyyppinen eli monimutkainen/kehittynyt GPS-järjestelmään perustuva signaalin väärennösisku on selvästi kaikkein vaikein paikallistaa, voisi jopa väittää, että se on mahdotonta. Tässä kyseisessä iskutyypissä on huomattavasti kehittyneemmät välineet kuin kahdessa aiemmassa esitellyssä vaihtoehdossa. Tämä kehittynyt signaalilähettin on hyvin pienikokoinen, ja niitä voi olla tilanteesta riippuen useita. Tällainen useamman laitteen isku, voi olla hyvin vaikea havainnoida ja tunnistaa hyökkääjää (Sathyamoorthy, 2013, 52) ja (Humphreys, ym., 2008, 4.). Tämä lähettin/nämä lähettimet kykenevät jo itsenäiseen toimintaan hyökkäysalueellaan, ja voivat luoda sinne hyvin hankalasti tunnistettavan olosuhteen jolloin siviilivastaanottimet eivät kykene havaitsemaan sitä/niitä juuri millään tavoin. Tämän jälkeen ainoaksi tavaksi sen torjumiseksi ja estämiseksi omiin järjestelmiin ja vastaanottimiin jää lähinnä salaustamiseksi. (Sathyamoorthy, 2013, 52).

### 4.3 Mitä onnistunut GPS-signaalien väärentäminen aiheuttaa laivan muille navigointijärjestelmille?

GPS-vastaanotin oli aiemmin vuosia sitten laivojen komentosilloilla erillään oleva laite, jonka rikkoutuinen tai joutuminen häiriötilanteisiin ei vaikuttanut niin vahvasti muihin aluksen toimintoihin. Nykyisten laivojen komentosiltojen navigointijärjestelmät toimivat digitaalisesti elektroniikalla ja ne ovat integroitu yhteen ECDIS-järjestelmäksi (ECDIS = Electronic Chart Display and Information System), (Kuvio 10). Tästä syystä seuraavaksi selvitetään, miten GPS-signaalien väärentäminen vaikuttaa muihin ECDIS-järjestelmään integroituihin navigointijärjestelmiin, kuten erilaisiin kompasseihin sekä ARPA, AIS, DR ja autopilotti-järjestelmiin.



KUVIO 10 ECDIS-järjestelmään linkitetyt navigaatiojärjestelmät. Kertoo hyvin, mitkä kaikki aluksen järjestelmät on integroitu ECDIS-navigointijärjestelmään, ja miten nämä järjestelmät ovat riippuvuussuhteessa GPS:n kanssa. (Bhatti & Humphreys, 2014, 31.).

Kuten aiemmissa luvuissa on jo mainittu, GPS-jumiuttamisella (jamming) estetään esimerkiksi aluksen GPS-vastaanotinta saamasta signaalia. Tällöin GPS-vastaanotin selvästi ilmoittaa niin suurta virhelukemaa paikassa, että kokenut aluksen navigoija tai ohjailija luultavasti huomaa nopeasti olevansa hyökkäyksen kohteena eikä tällöin suurempia ongelmia muihin ECDIS-järjestelmän ominaisuuksiin pääse syntymään (Tucci, 2015, 49.). GPS-signaalien harhauttaminen taas voi olla todella petollinen kyberisku, koska se voi tulla navigointihenkilös-

tön huomaamatta asiaa, aivan kuten Humpreysin suorittamassa käytännön ko-  
keessa pääsi tapahtumaan. Mikäli aluksen navigoija ei suorita paikan tarkistuk-  
sia perinteisillä paikanmäärittämismetodeilla, voi alus joutua todella uhkaaviin ti-  
lanteisiin.

Jokaisessa aluksessa on perinteinen magneetti- ja hyrräkompassi, jotka ei-  
vät häiriinny väärennetyistä GPS-signaaleista. Mutta niillä saatava paikkatieto  
on huomattavasti epätarkempi, kuin normaalissa tilanteessa olevan GPS-vas-  
taanottimen ilmoittama paikka. Satelliittikompassi taas ilmoittaa todella tarkkaa  
aluksen paikkaa merikartalle. Mutta valitettavasti myös tämä on onnistuneen  
GPS-signaaleja väärentävän iskun myötä ilmoittamassa väärää paikkaa. Tosin  
Humpreys mainitsee, että satelliittikompassista voisi olla myös hyötyä hyök-  
käyksen sattuessa, koska se ottaa tietoja aluksen muista kolmesta akselikulman  
liikkeestä ja satelliittitiedot se kerää kahdella antennilla. Nämä kaksi antennia on  
asennettu kölisuuntaisesti erilleen toisistaan. Kun antennit ovat eri kohdassa nii-  
den saamasta signaalierosta voidaan laskea aluksen kulkema suunta (Bhatti &  
Humpreys, 2014, 3), (Sperry Marine, 2017) ja (Kiljala, 2011, 40.).

ARPA-tutka (Automatic Radar Plotting Aid) on alun perin kehitetty meren-  
kulkijoille estämään laivojen törmäyksiä toisiinsa. Kyseinen tutka laskee muiden  
alusten kulkemat suunnat ja nopeudet oman laivan suhteen. Tähän järjestelmään  
syötetään kompassitiedot, GPS- ja lokitiedot, jotka se yhdistää omiin tutkakaikui-  
hin ja lähettää ne ECDIS-järjestelmään. Mikäli alukselle tulee väärää GPS-signaa-  
lia, voi se aiheuttaa vaarallisia riskitilanteita, koska tutkan saama oma ns. ” raa-  
kakaiku”, joka tulee laivoista ja rannoista on totta. Esimerkiksi ulkomerellä, jossa  
etäisyydet ovat pitkiä ja samoja suuntia pidetään kauan, voidaan joutua todella  
hankaliin tilanteisiin, koska aluksen oma kompassisuunta ja paikkatieto ovat  
väärä (mikäli ollaan vain satelliittikompassin varassa), ja ARPA-tutka saattaa il-  
moittaa todella riskialttiita ohitustilanteita. Jos hyökkäyksen alkaessa tutkasta  
katsottaisiin vain raakakaikua, niin ARPA-tutkan avulla säästyttäisiin monelta  
tulevaisuuden onnettomuudelta. Mikäli GPS-signaalin ominaisuudet poistetaan  
kaikista navigointilaitteista, ARPA-tutka ei kuitenkaan kykene ilmoittamaan  
muuta kuin näkemänsä maalit oman laivan keulasuunnassa ja merimerkit ja ran-  
nikon muodot. Mitään liikevektoreita se ei tällöin kykene ilmoittamaan (Bhatti &  
Humpreys, 2014, 2-3.).

AIS-järjestelmä (Automated Identification Systems) on pakollinen kaikissa  
bruttovetoisuudeltaan yli 300 GT aluksissa ja kaikissa matkustajalaivoissa koosta  
riippumatta. Jokaisessa yllämainitut kriteerit täyttävässä laivassa on yksi AIS-  
koodia lähettävä kone, johon on asennettu aluksen kansainvälinen tunnistenu-  
mero. Jokaiseen laitteeseen linkitetään/merkitään aluksen tiedot, kuten esimer-  
kiksi identiteetti, tyyppi, paikka, kurssi, nopeus, navigointistatus ja tarvittavat  
turvallisuustiedotteet. Tähän voidaan liittää myös lähtö- ja tulosatamat (IMO,  
2017a). Kun nämä alusten AIS-tiedot lähetetään automaattisesti ECDIS-järjestel-  
mään, jossa ne yhdistetään elektronisten merikarttojen päälle ja lähetetään myös  
ARPA-tutkaan, on alusten helppo tunnistaa toisensa ja tarpeen tullen ottaa toi-  
siinsa yhteyttä VHF-radioliikenteelle määrätyillä radiokanavilla, jotta merilii-



kenne menisi turvallisesti eteenpäin. Samaa AIS-järjestelmää käyttää tänä päivänä Liikenneviraston Vessel Traffic Service (Alusliikennepalvelu). Tilanne muuttuu kuitenkin hankalaksi tämänkin järjestelmän kannalta, kun laiva joutuu GPS-signaalien harhautuksen kohteeksi. AIS-järjestelmä ottaa paikkansa pääsääntöisesti suoraan GPS-vastaanottimelta. Mikäli tämä vastaanotin ilmoittaa, että ollaan paikassa X, joka on väärä, niin AIS-järjestelmä ilmoittaa myös muille aluksille tämän saman paikan X manipuloidut tiedot. (Bhatti & Humpreys, 2014, 2). Kaikki muut alukset näin ollen näkevät omilla komentosilloillaan kyseisen harhautetun laivan merikartoillaan väärässä paikassa, ja luultavasti vielä luottavat tähän tietoon. Tällöin voidaan joutua hankaliin tilanteisiin, jos molemmille aluksen navigoijalle tulee esimerkiksi ohitus- tai risteämistilanteita, jotka tulevat äkkiiarvaamatta ja yllättäen.

Dead Reckoning System eli (DR)-järjestelmä perustuu samalle periaatteelle, jota merenkulussa on tehty jo satoja vuosia. Nyt saman asian tekee vain kone huomattavasti tehokkaammin ja useimpia järjestelmiä saman aikaisesti hyväksi käyttäen. DR-järjestelmä laskee mahdollisimman varman paikan gyroskoopilla inertiaalinavigointivälineitä hyödyksi käyttäen ja halutuun aikajaksoon. Se merkitsee tämän hetken paikan merikartalle ja huomioi muiden navigointijärjestelmien ECDIS-järjestelmään lähettämiä tietoja, kuten esimerkiksi tuulen nopeuden, suunnan, aluksen kulkeman nopeuden jne. DR-järjestelmä auttaa ohjailijaa näkemään kulkemansa matkan ja tekemään mahdollisia tulevaisuuden reittivalintoja ja ohituksia. Laivan tulee merkitä paikkansa vähintään kerran tunnissa ja joka kerta, mikäli paikkatiedot muuttuvat oleellisesti edellisestä paikasta ja suunnasta. Tällä tarkoitetaan sitä, että oltaisiin ajauduttu sivuun alkuperäiseltä reitiltä. (Maritime Safety Information, 2017) ja (Britannica, 2017). Nykyaikana ko. järjestelmä ottaa paikkatietonsa melkein jatkuvalla syötöllä GPS-järjestelmästä, koska se on nähty tähän asti hyvin luotettavaksi järjestelmäksi. Tämän lisäksi kulloiseenkin paikkatietoon lisätään vallitsevat sääolosuhteet, nopeus yms., jolloin saadaan normaalioloissa hyvin varma ja luotettava paikkatieto tulevaisuutta varten. Näin tiedettäisiin, missä oltaisiin aluksella esimerkiksi samoilla olosuhteilla ja nopeuksilla kuuden minuutin kuluttua.

Valitettavasti laivan kapteeni/ohjailija ei voi käyttää käsittelemässämme GPS-signaalien ongelmatilanteessa saman tien hyödyksi DR-järjestelmää, koska kyseinen järjestelmä on saanut koordinaattitiedot GPS-järjestelmästä. Tämä GPS-järjestelmä taas on tällä hetkellä väärennettyjen GPS-signaalien alaisena, jolloin se on valmis antamaan ainoastaan näitä paikkatietoja eteenpäin (Bhatti & Humpreys, 2014, 2). Jos aluksen ohjailusta vastaava henkilö huomaa olevansa tällaisen hyökkäyksen alaisena, hänen tulisi ensin nopeasti hankkia nykyisen paikan tiedot perinteisemmillä navigointivälineillä, sekä aktiivisemmin pyrkiä määrittämään paikkaansa visuaalisesti esimerkiksi kiinteitä merimerkkejä ja linjatauluja hyväksi käyttäen, mikäli niitä on vain nähtävissä. Tosin Norjassa on tutkittu INS:n (Inertiaalinavigointijärjestelmän) kehittämistä yhdistettynä laivojen tekniikkiin kaikuluoteihin, mikä voisi helpottaa tarkan paikan määrittämisessä. Mikäli

merenpohjista saadaan tehtyä kunnon kartat, niin nykyisillä 3D-kaikuluotitukilla on kyetty saamaan todella tarkkoja ja luotettavia paikkatuloksia (Hagen, Skaugen, Ånensen, 2013, 7.).

ECDIS (Electronic Chart Display and Information System) on tietokoneeseen asennettu sähköinen merikarttaohjelma, joka yhdistää kuviossa 10 mainittujen järjestelmien sille lähettämät tiedot. Tämä tietokone ja siihen asennettu ohjelma on suunniteltu helpottamaan merenkulkijoiden ja laivojen liikkumista merellä. Siihen asennetaan halutut merikartat, joihin merenkulkijat suunnittelevat reittinsä haluamallaan tavalla. Tähän samaan järjestelmään on myös tallennettu aluksen käännössäteet halutuilla nopeuksilla. Ohjelma tunnistaa myös turvalliset ja vaaralliset merialueet, eli reittiä suunnitellessa ohjelma hälyttää/varoittaa, jos reitti on suunniteltu liian matalien tai karikkoisten kohtien kautta (Orädd, 2010, 19-20.). Näihin elektronisiin merikarttoihin ECDIS-järjestelmälle tuodaan tiedot muun muassa AIS-, GPS-, DR-, ynnä muista järjestelmistä. ECDIS kokoaa nämä kaikki yhdeksi kokonaisuudeksi ja tuo nämä tiedot visuaaliseen muotoon elektroniselle kartalle. Nämä kaikki tiedot voidaan yhtä lailla viedä ARPA-tutkan näyttöruudulle, jos ohjailija niin haluaa. Kuten aiemmin ollaan jo käsitelty, GPS-signaalien väärentäminen ilmaisee näillä järjestelmillä väärää paikkaa, jolloin aluksen paikka ilmestyy myös elektronisella kartalla väärässä paikassa. Jatkotutkimusaiheen ongelmineen ja kysymyksineen, miten merenkulkijat käyttäytyvät tilanteessa, jossa GPS-signaalit ovat väärennettyjä. Huomaavatko he esimerkiksi ARPA-tutkan kanssa rannikkoalueella, että tutkan ilmoittamat etäisyydet eivät täsmää GPS:n ilmoittamien koordinaattien kanssa?

Laivan autopilotti on se ensimmäinen ns. itsenäinen toimija, joka tulisi kytkeä pois päältä, kun GPS-vastaanottiin saapuu vääriä signaaleja kyberrikollisen/-terroristin toimesta. Autopilotti saa ohjeita ja tietoa ECDIS-järjestelmästä, johon tiedot ovat tulleet monilta eri järjestelmiltä. ECDIS-järjestelmä vain kasaa nämä kaikki tiedot ja lähettää ne edelleen autopilotille, joka toimii näiden ohjeiden ja tietojen mukaan. Sovituissa reittipisteissä se kääntää alusta sopivalla kääntösäteellä analysoiden nopeutta ja peräsinkulmaa sekä aluksen kulloistakin lastikapasiteettia. Se lukee/seuraa jatkuvasti ECDIS-järjestelmälle merkittyä reittiä ja pitää laivan kelistä huolimatta sovitulla reitillä ja oikeilla GPS-reittipisteillä. (Bhatti & Humpreys, 2014, 2.) ja (Orädd, 2010, 19-20.). Myös tässä järjestelmässä piilee sama ongelma kuin aiemmissakin järjestelmissä. Kun kyseessä on väsymätön automaattinen kone, joka jatkuvasti on ohjelmoitu noudattamaan saamiaan GPS-signaalien koordinaatteja, se ei huomaa taitavasti tehtyä GPS-signaalien väärentämishyökkäystä, vaan lähtee hiljalleen lipumaan reitiltä sivuun. (Bhatti & Humpreys, 2014, 2 & 8.). Valitettava tosiasia on, ettei näitä väärennettyjen GPS-signaalien hyökkäyksiä kykene huomaamaan aina aluksen ohjailijatkaan, aivan kuten Humpreysin tutkimuksessa kävi ilmi.

Näiden edellä mainittujen laitteiden ja järjestelmien lisäksi GPS-järjestelmä voidaan kytkeä vielä joihinkin muihin aluksen laitteisiin (Kuvio 11) ja (Tucci, 2015, 49). Nämä laitteet/järjestelmät eivät suoranaisesti ole vaikuttamassa tämän hetken ohjailuun, vaan ovat enemmän turvaamassa aluksen ja henkilöstön tilannetta onnettomuuden sattuessa. DSC (Digital Selective Calling) on merihädässä

olevien alusten pelastusjärjestelmä, joka toimii VHF-radiokanavataajuuksilla. DSC:llä lähetetään hätäkutsu kanavalla 70 samanaikaisesti viranomaisille ja lähimmille aluksille. Kaikilla kaupallisilla suuremmilla aluksilla tähän järjestelmään on linkitetty myös GPS-järjestelmä, jolloin se kykenee lähettämään muille viestin saajille saman tien laivan tarkka paikan (Viestintävirasto, 2012). Jos laiva on joutunut väärin GPS-signaalien johdosta onnettomuuteen tai vaaratilanteeseen, niin laivan GPS-vastaanottimen oikeaksi paikaksi luulema väärä koordinaattipaikka lähtee muille aluksille eteenpäin tiedoksi. Kaikki hätäkutsun saaneet merkitsevät elektronisiin merikarttoihin hädässä olevan laivan väärään paikkaan ja lähtevät kohti tuota pistettä auttamaan hädässä olevaa laivaa. Jos väärillä GPS-signaaleilla olisi ajettu laiva vain muutama sata metriä sivuun väylästä, niin se ei vielä tällaisessa tapauksessa pahemmin haittaisi pelastajia löytäjästä pulassa olevaa laivaa. Mutta pidemmällä ulkomerien väylillä pimeässä, saateella tai sumukelillä tilanne voisikin olla jo toinen. Varsinkin, jos kyberterroristi olisi jo suorittanut kyseistä toimintaa useista tunneista muutamiin päiviin, ja näin kyennyt ajattamaan laivan linjalta kauas sivuun.

DP (Dynamic Positioning)-järjestelmää eli dynaamista paikannusjärjestelmää käytetään enemmän laivoissa, jotka työskentelevät esimerkiksi tutkimus ja öljynporauslauttojen kiinnitystehtävissä, joissa täytyy pysyä mahdollisimman tarkasti samalla paikalla merta kovassa tuulessa ja merenkäynnissä. Kyseessä on oma tietokone ohjelmajärjestelmineen, joka inertiaalinavigointijärjestelmäperiaatteen mukaan pitää sen paikan, joka GPS-järjestelmällä on sille käsketty (Holvik, 1998, 1-10) ja (Palola, 2011, 23-25). Vaikka GPS-järjestelmä on yksi tärkeimmistä vaikuttavista tekijöistä Dynamic Positioning -järjestelmässä, tätä ei käsitellä nyt tarkemmin, koska tämä liittyy lähinnä aluksiin, jotka eivät tällä hetkellä liiku Helsingin Länsisataman syväväylällä. Tässä tutkimuksessa käsitellään vain satamien välillä liikkuvia aluksia eikä stabiilissa työssä pysyviä aluksia.

VDR (Tuccin Kuvio 11, jostain syystä Vessel Data Recorder, yleisemmin käytetään nimitystä Voyage Data Recorder.) on suomeksi ”mustalaatikko”, joka tallentaa aluksen kulkemaa matkaa GPS-pisteineen ja muun muassa laivan teknistä dataa (Huang & Ren, 2010, 181-183.). Valitettavasti myös tämä laite alkaa tallentaa väärää GPS-signaalin muodostamaa koordinaattipaikkaa sillä hetkellä, kun kyseinen onnistunut kyberhyökkäys on alkanut (Tucci, 2015, 49). Eli mikäli jonain päivänä tällaisen GPS-kyberhyökkäyksen johdosta tapahtuisi onnettomuus, onnettomuuden selvittävä tutkimuslautakunta joutuu mahdollisesti todella hankalan tehtävän eteen yrittäessään selvittää, milloin väärän signaalin aloitus on alkanut ja siihen liittyviä syitä.

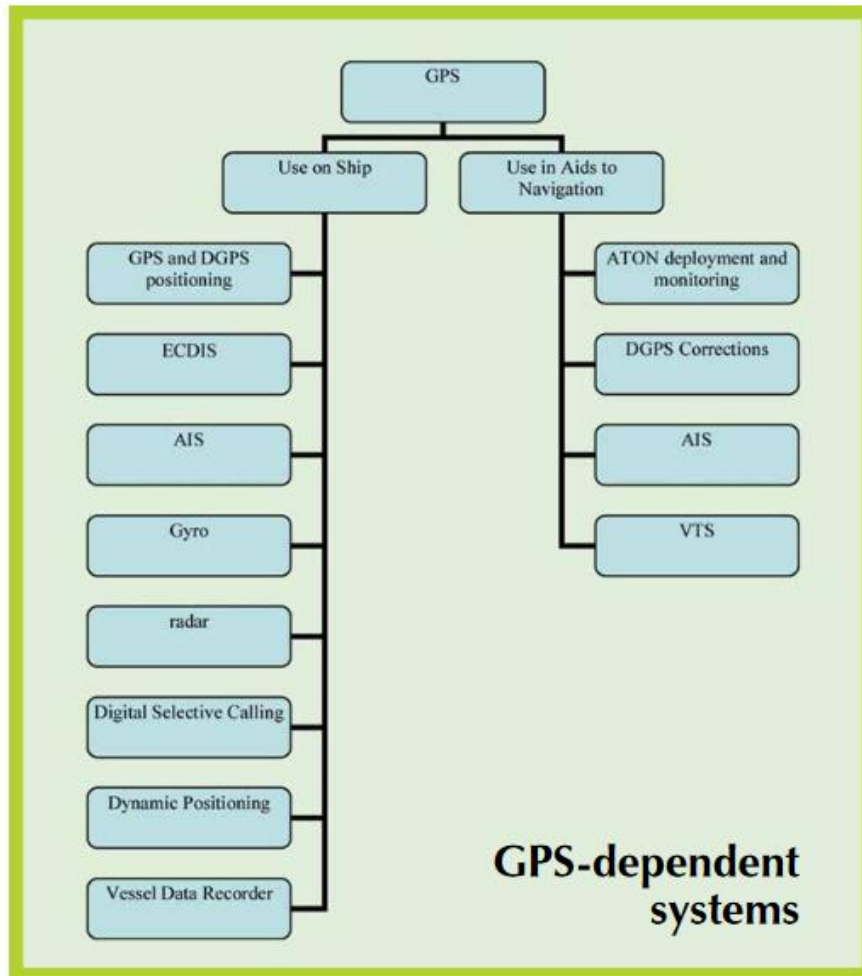
Jos vedetään yhteen edellä esitettyjä asioita, voidaan todeta, että laiva ei siis ole mikään muu kuin jatkuvasti GPS-tietoa pyörittävä tietokone, joka käsittelee kaikenlaista dataa ympäristöstään (esim. tuuli, paikka, nopeus, sorto). Laivan eri järjestelmät tuottavat tämän informaation ECDIS-järjestelmälle, joka muodostaa siitä kokonaisen informaatioympäristön tai tilannekuvakartan. Tällä tiedolla päivitetään mm. elektronista merikarttaa, josta navigoija kykenee näkemään oman paikkansa merenkulussa. Valitettavasti tämä paikannussignaali on täysin avoin/salaamatonta. Sitä käyttävät myös kaikki suuret valtiomme ja ulkomaiset

risteilijäalukset, joissa kyseinen tieto integroidaan heidän aluksen ECDIS-järjestelmään. Vain pienellä, hetken kestäväällä kyberiskulla kyetään ajatuttamaan suuret alukset kohti onnettomuutta tai mahdollista vaaratilannetta. Riskinä on laivojen ajautuminen karille laivan saatua virheellistä GPS-signaalitietoa ”harhauttajilta”/hakkereilta, jotka syöttävät sille jatkuvasti väärää dataa lähettimillään. Aluksesta puuttuvat kokonaan hälyttimet ja varoitimet tällaisen tilanteen varalta. Aluksilla kyllä on hälyttimet GPS-signaalin katoamiseen liittyen, mutta harhauttamisessa tämä signaali ei katoa mihinkään. Näin ollen siis hälyttimet eivät myöskään noteeraa mahdollista uhkakuva/ onnettomuutta. Tässä uhkakuva oletetaan siis, että aluksen kapteeni/ohjailija ei kykene tiedostamaan visuaalisin keinoin, missä hän liikkuu.

Kun GPS-signaalin harhautusta tarkastellaan yksittäistä alusta laajemmassa mittakaavassa, niin asia ei merenkulussa olekaan enää niin pieni ja ongelmaton kuin, mitä sen olisi luullut olevan. Tätä väärennettyä GPS-signaalia voitaisiin käyttää monessa muussakin järjestelmässä, kuten seuraavassa neljässä palvelussa: ATON (Aids to Navigation), DGPS (Differentiaali-GPS), AIS (Automatic identification systems), ja VTS (Vessel Traffic Service). Näitä asioita käsitellään tarkemmin seuraavassa luvussa.

#### **4.4 GPS-signaalien väärentämisen tuomat uhkakuvat laajemmin meriliikenteelle**

AtoN (Aids-to-Navigation) -palvelu tarkoittaa laajemmassa mittakaavassa navigoijia/merenkulkijoita varten ja heidän matkantekoa helpottamaan keksittyjä erilaisia poijuja, sektoriloistoja, majakoita ja vastaavia apuvälineitä. Tässä tutkimuksessa AtoN-palvelulla tarkoitetaan virtuaalisia merenkulkijoiden palveluita, niin sanottuja älypoijuja tai vastaavia virtuaalisia merimerkkejä. Nämä saavat tietonsa GPS-järjestelmästä, eli kyseessä on siis GPS-tekniikkaan perustuva paikanninjärjestelmä. Nämä tiedot siirretään elektroniselle merikartalle eli ECDIS-järjestelmälle. Aluksen navigoija määrittää aluksen sijainnin niin oman GPS-järjestelmän kuin myös AtoN-järjestelmän merkkejä hyväksi käyttäen. (Basker, 2006) ja (Tamaru & Tassedda, 2008, 119 - 200.).



KUVIO 11 Mihin kaikkiin järjestelmiin aluksen saamaa GPS-järjestelmää käytetään laivassa ja laivan ulkopuolella (Tucci, 2015, Proceedings, 49.).

Jatkossa tässä tutkielmassa puhuttaessa AtoN-palvelusta tarkoitetaan tällä erityisesti virtuaalista AtoN-palvelua. Se kykenee ilmaisemaan aluksen kaikki tiedot elektroniselle merikartalle. Tämän perusteella navigoija kykenee paikantamaan paikan virtuaalisten poijujen tai monien muidenkin välissä sekä niin sanotut hankalat tai vaaralliset paikatkin.

AtoN-järjestelmä perustuu aivan samaan tekniikkaan kuin AIS-järjestelmä. Tällä pyritään luomaan aluksen ohjailijalle vain varmuutta ja turvallisuutta paikantamiseen, sekä pyritään ennalta ehkäisemään aluksen onnettomuuksien sattumista tulevaisuudessa. AtoN jaetaan kolmen tyyppisiin kategorioihin: virtual-, synthetic-, ja real-. Real tarkoittaa sellaista merimerkkiä, jonka navigoija kykenee itse omin silmin näkemään, ja mikäli siihen liitetään synthetic- ominaisuus, niin silloin tämä kyseinen merimerkki, esim. poiju, kykenee lähettämään myös tietoa siitä, onko mahdollisesti valosammunut tai mikä on paikallinen aallon- tai vedenkorkeus. Jos merimerkkiä ei voi nähdä omin silmin, mutta se näkyy esim. AIS-järjestelmän välityksellä, niin silloin kyseessä on virtual-versio. Näitä käytetään yleensä talvikaudella, kun meri on jäässä tai hylkyjen yms. väliaikaisten ratkaisujen tilalla. Tämä kaikki tieto lähetetään yleensä maa-asemalle, joka taas lähettää

sen tarvisijoille AIS-järjestelmällä. Jokainen ns. tavallinen ja virtuaalinen GPS-/AIS-tekniikkaan perustuva merimerkki näkyy elektronisella merikartalla omalla esitysmerkillään, joten niitä ei voi sekoittaa keskenään. Jos GPS-signaalia häiritään tai manipuloidaan, niin myös virtual-AtoN -tieto on manipuloitua, koska sekä AtoN että AIS-järjestelmä perustuvat käytännössä sataprosenttisesti GPS-tekniikkaan. Toisin sanoen GPS-pohjaiset merimerkit eivät siis ole luotettavia.

Elektronisella merikartalla näkyy nämä poijut, kardinaalimerkit, sektoriloistot jne., joihin yhdistetään laivan liikevektori kyseisiin kohteisiin. Näin meriliikenne ja sen turvallisuus paranevat normaaliolosuhteissa huomattavasti (Basker, 2006). AtoN palvelu helpottaa alusten turvallisuutta ja onnistuu vähentämään törmäyksiä ja läheltä piti tilanteita todella paljon, koska laivan jatkuva etäisyyden arviointi perustuu kyseisessä palvelussa näihin liikevektoreihin ja ajan mahdolliseen arvioimiseen keskenään. (Tamaru & Tassedra, 2008, 199 – 200.). Kyseessä on siis aivan samanlainen palvelu, kuin ARPA-tutkan luoma virtuaalimaailma, jossa yhdistyy useat eri aikaan ja nopeuteen perustuvat turvallisuuskriteerit ja ilmiöt (Kuvio 12).

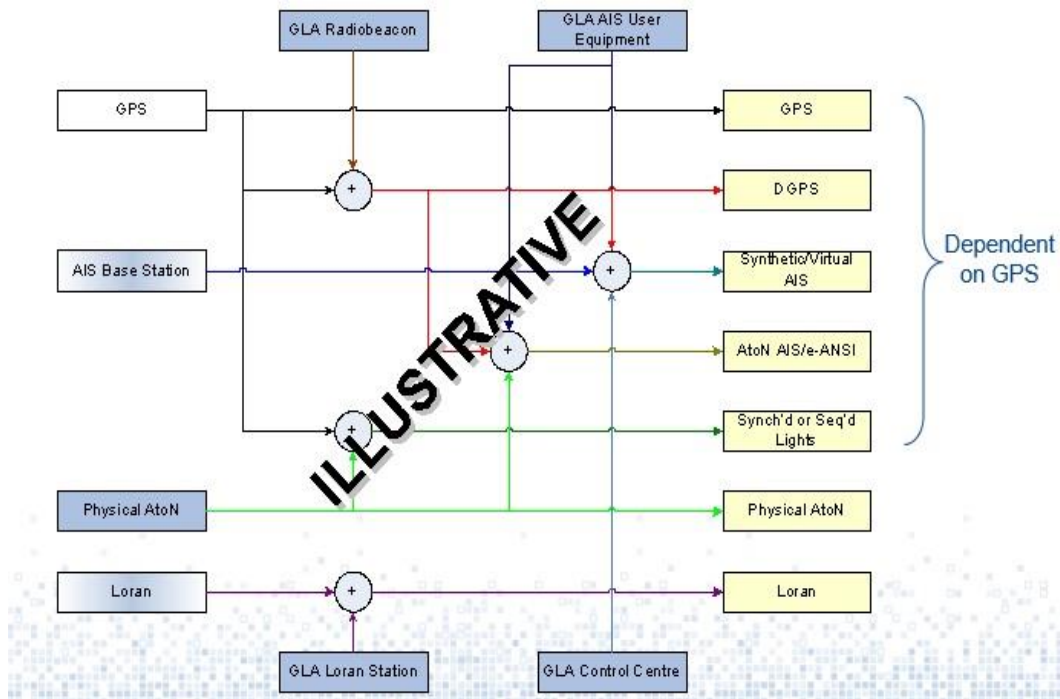


KUVIO 12. AtoN-järjestelmän toiminta periaate. Kertoo, miten virtuaalinen-ATON toimii käytännössä. (Subsea Worlnews, 2016)

Kuviossa 12 esitetään Vesper Marinen luoma ratkaisu Long Islandin kaapelin turvaksi. Kyseisellä alueella ei saa ankkuroida ollenkaan katkoviivojen sisäpuolella. Mikäli laiva päättää ankkuroida tällä alueella, järjestelmä havaitsee sen liikkeen hidastumisesta ja AtoN-palvelu lähettää saman tien hälytyskäskyn eteenpäin (Subsea Worlnews, 2017).

Mutta mitä aluksen kapteeni voi tehdä, jos hän joutuu tällaisen hyökkäyksen kohteeksi? Kapteeni ei kykene saamaan luotettavaa GPS-sijaintia ja siihen liittyvää tietoa tai tämä tieto on manipuloitua, jolloin aluksen GPS-sijainti on aivan väärä, ja se taas vaikuttaa moneen muuhun aluksen navigoinninja järjestelmään. Aluksen lähettämä oma AIS-tieto on myös yhtä väärä kuin GPS-tieto ja tämä tieto taas lähtee eteenpäin VTS:lle ja heidän muodostamalleen tilannekuvakartalleen. Jos kyberterroristi suorittaa GPS-harhautusta aluksen ulkopuolella tarkoituksenaan väärentää esim. näiden virtuaal-

listen AtoN-merkkien paikkatietoa ja onnistuu siinä, niin myös näiden harhautussimulaattorin signaalien sisään ulottuvat laivat ja AtoN-merkit menettävät oman paikkansa. Tämä johtuu siitä syystä, että virtuaalinen AtoN-tekniikka perustuu lähes samaan periaatteeseen kuin AIS-järjestelmän tekniikka, joka on täysin GPS-tekniikasta riippuvainen. Tätä sekavuutta on pyritty selventämään (Kuvio 13).



KUVIO 13. GPS-tekniikkaan perustuvat järjestelmät, (Basker, 2006).

Tällaisessa tilanteessa aluksen kapteeni voisi käyttää myös ARPA-tutkan normaalia versiota ilman GPS-paikannusta, jos vain tiedostaa olevansa väärässä paikassa. Suurena apuna tällaisessa tilanteessa on se, että kapteeni kykenee saamaan radioyhteyden VTS-keskukseen, josta hän saa lisäapua. Vaikka VTS-keskus on saanut aluksen väärän AIS-paikan tiedon aluksen GPS-perusteisen AIS-järjestelmän kautta, VTS kuitenkin kykenee määrittämään aluksen tarkan sijainnin oman tilannekuvansa ansiosta. Tästä sekä tiedonsiirrosta aluksen ja VTS-keskuksen välillä kerrotaan tarkemmin luvussa viisi.

Tällaisessa tilanteessa VTS voisi mahdollisesti jakaa neuvoja tai ohjeita, miten tilanteessa tulisi toimia. Tulisiko tällaisessa tilanteessa laskea ankkuri pohjaan ja jäädä odottamaan kyseisen hyökkäyksen loppumista? Vai tulisiko pyrkiä aktiivisesti kohti laituria riskeistä huolimatta, jos vain ollaan tarpeeksi lähellä laituria? Tulisiko viranomaiset pyytää apuun VTS-keskuksen pyytämänä, lähettää ne laivalle tai luodolle ja odottaa, että he saavat tämän harhauttajan kiinni? Tällöin puolustusvoimien tai rajavartioston boarding-ryhmä hoitaisi haitallisen ongelman. Vai voisiko hinaajista saada nopeasti apua?

Mutta mitä käy, mikäli kapteeni ei huomaa joutuneensa GPS-signaalin väärennyksen uhriksi? Luvussa viisi on pyritty selvittämään näitä vaihtoehtoja. Lisäksi tarkastellaan, kauanko laiva seilaisi tutkittavalla alueella ilman VTS:n yhteydenottoa, jos tällainen GPS-harhautus tapahtuisi? Mikä on VTS:n kyky huomata laivan tai useamman laivan joutuminen GPS-signaalin väärennyksen uhriksi? Onko merenkulkuumme luotu mahdollisia "turvaverkkoja", jos aluksen kapteeni ei jostain syystä tiedosta olevansa väärässä paikassa?



## 5 TEEMAHAASTATTELUT MERENKULUNASIAN-TUNTIJOIDEN KANSSA

Tässä luvussa aiemmin esitetty teoria kytketään osaksi käytännön asiantunte-  
musta, minkä vuoksi on suoritettu teemahaastatteluja Liikennevirastossa Kaisu  
Heikosen, Meriliikennekeskuksen päällikön Samu Kosken, Trafin Jami Metsärin-  
teen ja Silja Serenade -aluksen kapteenin, Martin Björkellin kanssa, aikavälillä 18.  
4. - 8.5.2017. Teemahaastatteluilla on pyritty selvittämään näiden toimijoiden  
mielipiteet ja näkemykset tutkittavasta aiheesta. Koska he toimivat ja vaihtavat  
tällä alueella tietoa keskenään valtavasti, heillä on pätevä ja luotettava tietotaito  
tutkittavaan aiheeseen. He ovat niitä, jotka vastaavat meidän jokapäiväisestä tur-  
vallisuudesta ja kuuluvat samaan palveluja tarjoavaan yhteisöön kyseisellä Hel-  
singin Länsisataman syväväylällä. Haastatteluiden ulkopuolelle on rajattu muut  
METO (merelliset toimijat) -osapuolet, joita edellä lueteltujen lisäksi ovat esimer-  
kiksi Puolustusvoimat ja Rajavartiolaitos. Tutkimuksen haastattelujen ulkopuo-  
lelle on myös rajattu Viestintäviraston Kyberturvallisuuskeskus ynnä muut vas-  
taavat toimijat, koska tutkittava aihealue koetaan Suomessa hyvin arkaluon-  
toiseksi, ja jos asiaa olisi lähdetty tiedustelemaan näiltä instansseilta, olisi se voi-  
nut nostaa turvaluokituksen tasoa, eikä tutkimus olisi enää ollut julkista materi-  
aalia. Haastattelukysymykset on pyritty pitämään puhtaasti teoreettisella tasolla  
ja asiaa on yritetty katsoa ”astetta kauempaa”, menemättä erityisen yksityiskohtai-  
seen ja tekniseen tietoon. Kuitenkin haastatteluissa oli aistittavissa hetkiä tai  
tilanteita, jolloin vastauksia ei vain syystä tai toisesta, mahdollisesti salassapitoon  
liittyvistä seikoista johtuen, kyetty antamaan.

Teemahaastattelu suoritettiin seuraavalla tavalla: Jokaista asiantuntijaa  
haastateltiin reilusta tunnista puoleentoista tuntiin, ja jokainen haastattelu nau-  
hoitettiin, johon haastateltavilta pyydettiin lupa. Aiheemme pyöri saman teeman  
ympärillä, mutta jokaiselle toimijalle oli modifioitua kysymykset, siten että asi-  
antuntija kykeni tuomaan oman mielipiteensä esille GPS-järjestelmästä, meren-  
kulusta Helsingin ympäristössä, GPS-harhautuksesta ja siihen liittyvistä näke-  
mistään uhkakuvista, mahdollisesta tulevaisuuden näkökulmista/suunnitel-  
mista, yms. Tämän jälkeen haastattelumateriaali on litteroitu ja lähetty kyseiselle  
haastatellulle asiantuntijalle takaisin, ja annettu hänelle mahdollisuus muut-  
taa/poistaa/lisätä haastattelumateriaalia. Näin kyettiin välttämään mahdolliset  
tulevat akateemiset/tutkimuksen vastaiset väitteet ja toimet. Nämä haastattelu-  
rungot kysymyksineen löytyvät tutkimuksen liitteistä. Kysymykset on myös lit-  
teroidessa pyritty pitämään käytännössä siinä muodossa, kuin ne keskustelussa  
käytiin.

Näillä käytännön teemahaastatteluilla haluttiin hakea ennen kaikkea evi-  
denssiä tutkimukselle, mutta myös yhtä lailla varmistaa teorian pätevyys. Haas-  
tatteluiden avulla haluttiin lisäksi löytää mahdollisia yhtymäkohtia ja poik-  
keavuuksia kansainvälisten tutkimusten kanssa, eli ovatko meidän haastatellut  
virastot/osapuolet samaa mieltä tästä nousevasta GPS-harhautuksen uhkaku-  
vasta kuin esimerkiksi muut länsimaat, ja miten tämä tutkimusaihe asettuu

osaksi yhteiskuntaamme ja Helsingin edustaa. Seuraavissa alaluvuissa esitetään tiivistettyinä jokaisen asiantuntijan oma näkemys kyseisestä aiheesta tutkimuksen kannalta tärkeimpine kohtineen. Jokainen alaluku perustuu tutkijan ja haastateltavan väliseen kahdenkeskiseen keskusteluun.

Mikäli asiaa haluaa tutkia vielä laajemmin, haastatteluiden litteroitu materiaali löytyy tutkijalta ja se on saatavissa. Kyseinen materiaali siis ei ole liitetty vastauksineen tutkimukseen, vaan liiteluettelosta on löydettävissä luvun otsikonimensä mukaan käyty haastattelurunko. Ainoastaan suorat lainaukset on merkitty tutkimuksen yhteyteen tarkasti. Kaikki muu materiaali on referoitu kokonaisuutta haastattelusta, ja siitä on pyritty muodostamaan tiivis kokonaisuus 2 – 3 sivulle.

## 5.1 Liikenneviraston haastattelu

Koska Liikennevirasto hallinnoi ja on vastuussa vesiväyliemme kehittämisestä ja valvomisesta, oli selvää, että tästä organisaatiosta täytyi saada asiantuntija haastateltavaksi. Haastateltava oli diplomi-insinööri Kaisu Heikonen. Liikenneviraston alaisuuteen kuuluvat myös paikalliset VTS-keskukset, jotka toimivat käytännön alusten liikenteen ohjauksessa ja turvaamassa onnettomuuksia merialueillamme.

Heikosen mielestä GPS-järjestelmän heikkoudet ja ongelmakohdat ovat nimenomaan järjestelmän avoimuudessa. Tämä mahdollistaa sen, että voitaisiin valmistaa virheellinen lähetin, joka voisi voimakkaammalla teholla kyetä kaappaamaan signaalin itselleen, mikäli sekä lähetin että vastaanotin käyttävät samaa signaalia. Tämä mahdollinen uhkakuva on heidän organisaatiossa tiedostettu jo vuosia sitten. Hän myös mainitsee, että GPS-järjestelmä voi olla väärässä tai toimia väärin ilman, että sitä edes häiritään, ja tästä syystä Liikennevirasto pyrkii löytämään merenkulkuun ylimääräisiä paikannuskeinoja. Liikennevirastossa on tiedostettu, että liian monet aluksen järjestelmät perustuvat tänä päivänä GPS-tekniikkaan, mutta heillä oli se linjaus, että Trafissa vastataan kaikesta mikä sijoittuu aluksen sisäpuolella olevaan tekniikkaan, ja aluksen päälliköllä taas on vastuu aluksen ohjailusta ja navigoinnista. Kysymykseen siitä, onko Liikennevirastolla tänä päivänä olemassa jokin raja, missä risteilijän tai vastaavan kokoluokan aluksen tulee kytkeä autopilotti pois päältä saapuessaan Länsisatamaan, Heikonen vastasi, että nykytekniikalla voidaan tulla autopilotilla melkein satamaan asti perille, mikäli ohjailija/kapteeni vain on valppaana, tiedostaa missä ollaan ja kuittaa ja hyväksyy jokaisen manööveri- sekä ennakkokäänöspisteen.

Teemahaastattelussa selvisi, että merenkulussa aluksen ulkopuolisesta GPS-tekniikasta ja siihen liittyvistä uhkakuvista esiin näytti nousevan kaksi yhdistävää tekijää aivan kuten tutkimuksen teoriassakin. Nämä yhdistävät tekijät ovat AtoN- ja AIS-järjestelmä. AtoN-merimerkkejä/-poijuja ja vastaavia on kuulemma olemassa myös Suomessa, mutta tarkkoja paikkoja ei kyetty haastattelussa selvittämään. Varmaa kuitenkin on, että niitä ei ole tutkimuksen käsittä-

vällä alueella. AIS-järjestelmä nähdään Liikennevirastossa enemmänkin raportointivälineenä kuin navigointivälineenä. Kyseessä on siis järjestelmä, jolla alus raportoi omaa paikkatietoaan aluksen sisäisiin järjestelmiin ja ulkoisiin organisaatioihin, kuten esimerkiksi VTS-keskukseen, ja näistä monien alusten lähettämistä AIS-tiedoista voidaan luoda tilannekuvaa VTS-keskuksessa.

Liikennevirastossa koetaan, että nimenomaan VTS on heillä se ainoa paikka, joka kykenee huomaamaan, jos alus lähtee luisumaan pois sovitulta reitiltä, koska heidän tieto perustuu ennakoivaan keinoon paljastaa passiivisin havainnointijärjestelmin mahdolliset onnettomuustilanteet. Eli se perustuu sekä tutkatietoon, AIS-järjestelmään että kameran tuomaan yhdistettyyn tietoon. Mikään näistä järjestelmistä ei ole riippuvainen toisen tekniikasta, ja jos esimerkiksi AIS-järjestelmän ja tutkan tieto ilmoittaisivat ristiriitaa keskenään, niin VTS luottaisi puhtaasti tutkajärjestelmään. Toisin sanoen, jos alus ei jostain syystä itse tiedosta olevansa väärässä paikassa, vaan lähettää AIS-järjestelmällään manipuloitua tietoa, niin VTS:ssä kyllä kyetään se näkemään ja ottamaan alukseen yhteyttä esim. meriVHF-radiolla. Koska tutkimani alue on aivan Liikenneviraston ”fokusaluetta”, heillä on luotu todella kattava tutkapeitto tälle Helsingin Länsisataman syväväylän alueelle. Tämä tutkapeittoalue kykenisi toimimaan ja paljastamaan edellä kuvatut tilanteet myös siinä tapauksessa, että joku tutkista olisi epäkunnossa tai sitä korjattaisiin.

VTS-keskuksen järjestelmiin on myös luotu tiettyjä raja-arvoja useille maaleille. Jos jokin näistä maaleista poikkeaisi esim. nopeuden tai maantieteellisen paikan osalta tai vain myöhästyy, vaikka oletetusta väylän käännoispisteestä, niin tällöin hälytysjärjestelmät ilmoittavat mahdollisesta vaaratilanteesta. Näin kytetään luomaan operaattorin ja aluksen väliin mahdollisimman pieni aikaviive, jotta tilanne saataisiin hetimiten korjattua, koska tutkittavalla alueella on hyvin vähän tilaa. Jos aluksella suoritettaisiin GPS-harhautusta, niin VTS näkisi sen käytännössä reaaliaikaisesti ja kykenisi ilmoittamaan alukselle, että heidän (VTS)tutka- ja AIS-järjestelmissään on ristiriitaa keskenään, eli aluksen virtuaalipaikka on eri kuin sen fyysinen paikka.

Heikosen mielipide GPS-järjestelmään ja siihen linkitettyihin järjestelmiin oli seuraava:

”Ei meriliikenne siihen pysähdy, jos GPS katoaa. Ongelmat ovat ehkä enemmän vaikiintuneissa toimintatavoissa, jotka nykyisin tukeutuvat paljon satelliittinavigointiin (koska se tuottaa tietoa helposti). Kyllä meidän väylästä ja liikenteenohjaus toimivat ihan mainiosti myös ilman GPS-järjestelmää. Meillähän turvallinen väylällä liikkuminen perustuu visuaaliseen merkintään ja aluksen omaan tutkanavigointiin.” (Heikonen, haastattelu, 20.4.2017).

Heikosen näkemys on se, että meriliikenteessä aluksen kipparilla on vastuu laivastaan ja päätäntävalta sen suunnasta. Mikäli jotain ikävää kävisi, niin Liikennevirasto on juuri tätä varten suunnitellut ja kehitellyt niin sanottuja ”turvaverkkoja”, eli järjestelmiä merenkulkuun, jotka edesauttaisivat estämään mahdollisen onnettomuuden tutkittavalla alueella. Muun muassa tätä varten he ovat luoneet

sekä Länsisataman syväväylälle, että koko kansalliselle merialueellemme lukuisia tutkaheijasteita ja -majakoita, jotta alus kykenisi paikantamaan itsensä paikassa kuin paikassa. Liikennevirastossa myös oletetaan, että alusten ohjailijat kykenisivät paikantamaan alustensa sijainnin visuaalisesti olosuhteista riippumatta.

Heikonen on kuitenkin sitä mieltä, että vaikka tämä GPS-harhautus ei ole mikään yleinen tai todennäköinen tilanne, niin sitä on kuitenkin syytä tutkia ja viranomaisten kiinnittää asiaan huomiota, koska jo pelkkä sen tapahtumisen mahdollisuus voi aiheuttaa aluksella todella paljon hämmennystä, jos ikään kuin lukkiudutaan vain tuijottamaan hälyttäviä järjestelmiä eikä katsella ikkunasta ulos valvoen merellistä liikennettä.

Mieltäessä mahdollisia keinoja tai teknisiä järjestelmiä, jolla kyettäisiin havainnoimaan tai puolustautumaan tällaista uhkaa vastaan, lukuun ottamatta tutkaa ja visuaalista navigointia, Heikonen kertoi, että tulevaisuudessa on tulossa niin sanottu "multi-task-receiver". Tämä tarkoittaisi käytännössä järjestelmää, joka kykenisi toimimaan ja käsittelemään monia eri merenkululle jo luotuja taajuusalueita samanaikaisesti ja jatkuvasti vertailemaan niitä keskenään. Näitä voisi olla esimerkiksi GPS-satelliittien lisäksi jo nyt käytössä olevat muut satelliittijärjestelmät kuten Venäjän GLONASS, Galileo, BeiDou ynnä muut. Näiden lisäksi referensseinä voitaisiin käyttää mahdollisesti radiomajakkataajuuksia. Näitä mahdollisia jo olemassa olevia taajuuksia on muun muassa esimerkiksi seuraavat taajuudet: 100kHz, 300kHz, 500kHz ja 160MHz. Näin kyseinen järjestelmä kykenisi vertailemaan useampaa jo olemassa olevaa järjestelmää ja sen tuottaa tietoa keskenään sekä jatkuvasti päivittämään paikkaansa. Jos joku paikkatieto tai siihen perustuva tekniikka antaa virheellistä dataa kyseiselle "multi-task-receiverille", niin se kykenisi hylkäämään tämän järjestelmän väliaikaisesti pois käytöstä. Näin alusten päälliköille kyettäisiin antamaan lisää varmuutta paikantamiseen.

## 5.2 Helsinki Vessel Traffic Servicen haastattelu

Tämän luvun lähteenä on käytetty haastattelua, joka on suoritettu Helsingin meripelastuskeskuksessa, johon kuuluvat sekä Helsinki VTS 1 ja VTS 2. Kyseisen haastattelussa käydyn runko löytyy liitteestä kolme. Helsinki Vessel Traffic Service (VTS = Alusliikennepalvelukeskus) on osa Liikennevirastoa ja se koostuu sekä Helsinki VTS yhdestä ja kahdesta. Nämä taas ovat osa Suomenlahden meripelastuskeskuksia. VTS:n tehtävinä on ennaltaehkäistä alusten onnettomuuksia ja niistä syntyviä ympäristökatastrofeja. Tähän päivittäiseen työhön kuuluu esimerkiksi alusten ja yhteistyökumppaneiden kanssa informaation vaihtoa eri viestijärjestelmillä. Alusliikennettä voidaan myös monesti porrastaa ja ohjata, ja aluksille voidaan myös antaa navigointiapua, mikäli he vain sitä haluavat tai tarvitsevat. Tämän lisäksi viranomaisten kanssa voidaan tehdä useita viranomais-tehtäviä.

Teemahaastattelussa keskusteltaessa GPS-järjestelmän ongelmakohdista meriliikennekeskuksen päällikkö Samu Koski myönsi, että kyseessä on siviili- puolella täysin avoin järjestelmä, jota kykenee käyttämään jokainen henkilö. Tämä taas antaa tälle järjestelmälle sen mahdollisuuden, että se on täysin avoin kaiken tasoiselle häirinnälle niin GPS-jumiuttamisesta aina GPS-harhautukseen. Tämän lisäksi merenkulkuun on luotu valtavan laajamittainen integroidun navigoinnin järjestelmä, joka perustuu kokonaan tähän tekniikkaan. Jos joku kykenisi harhauttamaan aluksen väärälle kurssille, vaikuttaisi se tätä kautta myös VTS:n toimintaan, koska GPS-tekniikkaan pohjautuva AIS-järjestelmä lähettää tietoa VTS:lle.

Koska aluksen päälliköllä on aina laivastaan lain määräämä vastuu, perustuu VTS:n toimintaidea niin sanottuun proaktiiviseen valvontaan. VTS-keskus saa aluksilta meri-VHF-radiolla AIS-tietoa, jossa on muun muassa aluksen kansainvälinen tunnusnumero, nimi, koko, yms. Tämä sama järjestelmä lisäksi ilmoittaa niin sanotussa normaalitilanteessa oman tarkkan paikansa VTS:n tilannekuvakartalla, koska se on myös sidottu kiinni GPS-järjestelmään. Jos taas kuvitellusti alus joutuisi GPS-harhautuksen alaiseksi. Liikkuisi sen GPS-järjestelmään perustuva paikkatieto hienosti tilannekuvakartalla viivaa pitkin, mutta tutkan tuoma tieto kertoisi aluksen kulkeutuvan väärällä kurssilla. VTS kykenee paljastamaan tämän mahdollisen ongelma- tai ristiriitatilanteen sillä, että heillä on tälle alueelle todella kattava tutkaverkko. Tällä kattavalla tutkaverkolla kyetään näkemään ja todistamaan se, että mahdollinen vaaratilanne olisi syntymässä. VTS siis kykenevät näkemään aluksen sen todellisessa fyysisessä paikassaan ilman AIS-järjestelmää. Kysyessä Samu Koskelta haastattelussa kumman järjestelmän, AIS:n vai tutkan, tuomaa tietoa he uskovat tai kumpaan he luottavat valvoessaan meriliikennettä, hän kertoi, että fuusioudussa valvontajärjestelmässä ilman muuta tutkan tuomaa tietoa, koska se on aina nopeampi ja luotettavampi kuin GPS-pohjaisen järjestelmän tuoma tieto. AIS-järjestelmä antaa/raportoi heille minimissään kohteen tunnustiedot, jotta alusta voidaan kutsua oikealla nimellä, mikäli tällaisia ongelmatilanteita pääsisi syntymään. Heille AIS-järjestelmä on vain yksi sensorilähde muiden joukossa.

Koska kyseessä on täysin julkinen työ, tässä tutkimuksessa ei haluttu selvittää tutkien tarkkaa lukumäärää. Tutkimuksessa haluttiin kuitenkin selvittää, kyetäänkö nykyisillä tutkien määrillä turvaamaan kattava tutkapeitto, jos jokin tutka on esimerkiksi huollossa tai vain muuten poissa käytöstä. Tähän kysymykseen Kosken vastaus oli seuraava:

*”Kappalemäärää en voi sanoa, mutta niitä on huomattava määrä. Jäljellä olevat kyllä pystyvät korvaamaan toisiaan ja niillä kyetään määrittämään, mikä jäljittää ja mikä piirtää. Näillä kyetään kuitenkin antamaan luotettavaa paikkatietoa, mikäli aluksen AIS-järjestelmä antaisi meille manipuloitua paikkatietoa ja jokin tutka olisi pois käytöstä esim. huollon vuoksi. Eli AIS-järjestelmä on vain yksi sensorilähteistä.” (Koski, haastattelu, 28.4.2017).*

Jos alusta uhkaisi vaaratilanne, on VTS velvoitettu ottamaan alukseen välittömästi yhteyttä, esimerkiksi meri-VHF:llä, ja kysymään mahdollisia lisätietoja

alukselta. Varsinkin tällä tutkittavalla alueella on jo aikaviiveidenkin takia saatava kyseinen tieto mahdollisimman nopeasti.

VTS:ssä on useampi alusliikenneohjaaja, joka kykenee samanaikaisesti kattamaan laajan alueen, johon voi kuulua useampi alusmaali. Tosiasia on, että tämä yksittäinen alusliikenneohjaaja kykenee näkemään näiden maalien todellisen fyysisen paikan VTS:n fuusiomaalijärjestelmän ansiosta. Nämä maalien tiedot kerätään eri sensorijärjestelmistä kuten tutkista, AIS-järjestelmistä ja kameroista. Fuusiojärjestelmä antaa valvojalle mahdollisuuden vertailla sensorien tuomaa tietoa keskenään ja tarpeen tullen myös tiputtaa jokin näistä pois. Nämä kaikki ovat täysin eri tekniikkaan perustuvia järjestelmiä ja niillä ikään kuin luodaan "turvaverkkoja" merenkulkuun juuri edellä kuvatun kaltaisia tilanteita varten. Tämän lisäksi alusliikenneohjaaja kykenee luomaan ja simuloimaan eri kokoisille, nopeuksille ja painoisille aluksille sekä maantieteellisille ominaisuuksille niin sanottuja turvarajoja oletetuille kulkureiteille. Jos nopeus on esimerkiksi liian luja tai ennakkokäännöspiste näyttäisi myöhästyvän tai kyseisellä suunnalla kaksi alusta tulee törmäämään, niin aluksiin voidaan ottaa hyvissä ajoin yhteyttä ja kysyä, ovatko kyseiset laivat mahdollisesti huomioineet tilanteen. Riippuen alueesta tai väyläosuudesta, VTS pyrkii jatkuvasti ennakoimaan ja kuvittelemaan, mitä mahdollisesti tällä suunnalla ja nopeudella mahtaisi arviolta tapahtua aika-haarukalla kuudesta minuutista aina kolmeenkymmeneen minuuttiin. Mikäli suunta tai nopeus voisi osoittaa mahdollisuutta onnettomuuteen, on syytä ottaa laivaan yhteyttä. Jos taas alusliikenneohjaaja ei itse tätä huomaa, niin järjestelmässä on tällaista tilannetta varten edellä kuvatut hälytysrajat. Kun alus ylittää hälytysrajat, järjestelmä hälyttää, ja alusliikenneohjailija kykenee kohdistamaan katseensa tähän mahdollisesti syntyvässä olevaan ongelmatilanteeseen.

Kosken mukaan, tutkittavalla alueella ei ole vielä älypöijuja, eikä virtuaalisia älyväyliä (AtoN). Hänen mukaansa kaikki toistaiseksi käytössä olleet älypöijut tai -väylät ovat painottuneet joko Vuosaaren, Porvoon edustalle tai Länsirannikollemme.

Haastattelussa Kosken mielipiteensä tästä tutkittavan alueen vaarallisuudesta kohteineen, ei valitettavasti kyetty saamaan mitään pätevää yksittäistä paikkaa. Mutta kaiken kaikkiaan hänen vastauksensa oli tiivistettynä tämän alueen ruuhkaisuudessa ja valtavassa merenkulun liikenteessä. Jos tällä alueella jostain sattuisi, olisi se hänen mielestään hyvin "halvaannuttavaa".

Kaiken kaikkiaan VTS:ssä lähdetään siitä perusajatuksesta, että laivan kipparin tulee jatkuvasti tiedostaa, missä hänen aluksensa liikkuu reaali maailmassa, merellisessä ympäristössä, ja mihin aluksen liikevektori on milläkin hetkellä suunnattu. Mikäli tämä kyky pettää esimerkiksi todella rankan räntäsateen tai vastaavan takia siten, ettei kapteeni kykene näkemään ohjaamon ikkunasta ulos eikä saamaan tutkaltaan luotettavaa tulosta, niin tällaista tilannetta varten on olemassa VTS. Se turvaa meriliikennettä ja yrittää estää onnettomuuksia syntyästä.

Jokainen VTS:n työntekijä on entinen merimies, jotta he kykenisivät ymmärtämään alusten käyttäytymisen merellä eri olosuhteissa. Samu Koski halusi tähdentää seuraavaa asiaa:

”Vielä tänä päivänäkin merenkulkijan tärkein ominaisuus on visuaalinen havainnointikyky. Ammattitaitoinen merimies vertaa jatkuvasti saamaansa visuaalista tietoa tutkakuvaansa ja esimerkiksi GPS-järjestelmään ja muodostaa näistä omaan tilannekuvakartan omaan päähänsä. Mikäli jostain syystä näiden kesken tulee poikkeamaa/ristiriitaa, tulee aina uskoa omia silmiä ja niiden tuomaa merenkulun tietoa.” (Koski, haastattelu, 28.4.2017).

### 5.3 Liikenteen turvallisuusviraston haastattelu

Trafin eli Liikenteen turvallisuusviraston tehtävänä on ylläpitää, myöntää, valvoa ja päivittää merialusten sertifiikaatteja ja henkilöstön pätevyksiä. Näihin kaikkiin kuuluu muun muassa tutkittava GPS-järjestelmä ja merenkulkijoiden oma pätevyys. Lisäksi Trafi on yksi METO-ryhmään kuuluvista organisaatioista ja se pitää jatkuvasti yhteyttä satamiin ja aluksiin kansainvälisiin aluksista aina tavallisiin veneilijöihin asti. Trafissa pohditaan jatkuvasti, miten järvi- ja merialueemme saataisiin entistä turvallisemmaksi ja kyettäisiin estämään ihmisiä tekemästä virheitä. Teemahaastattelu suoritettiin Trafin erikoistutkijan Jami Metsärinteen kanssa.

Keskusteltaessa GPS-järjestelmän ongelmakohdista Metsärinne täsmensi, että heillä ei ole organisaatiossa mitään yhteistä linjaa asiaan, mutta hänen henkilökohtainen mielipiteensä on, että nykyaikana liian useat järjestelmät perustuvat navigoinnissa GPS-paikannukseen tai ovat siitä riippuvaisia. Tämä herättää ajatuksen siitä, että jos joku kykenisi aiheuttamaan kyseiseen järjestelmään jotain poikkeavaa, koska merenkulussa useat valvovat seurantajärjestelmät sekä satamassa että maalla perustuvat samaan tekniikkaan. Itse laivallahan näitä järjestelmiä on lukuisia.

”Täytyy kyllä sanoa, että länsimaisten alusten kaikki paikannus on GPS-perusteista ja näin ollen se tarkoittaa sitä, että GPS-tieto jaetaan lähes kaikkiin ”brykan” laitteisiin, kaiuista, VHF-DSC-laitteisiin. Myös satelliitti-järjestelmistä inmarsatit käyttävät samaa GPS-signaalia, jopa uudet EPIRB-pojut hyödyntävät GPS:ää. Eli myös hätälaitteistossakin ollaan GPS:n varassa yhä enemmän ja enemmän. Kaikki AIS-pohjaisen teknologian paikannusmenetelmät perustuvat myös GPS-järjestelmään.” (Metsärinne, haastattelu, 25.4.2017).

Metsärinne myöntää sen, että GPS-harhautus Länsisataman edustalla olisi todella hämmäntävä ja ongelmallinen, koska siellä jo pelkästään etäisyydet ovat todella pieniä, liikennettä on paljon ja aikaa ei ole hukattavaksi, varsinkaan kesällä, kun on ns. turistikausi ja kyseinen alue on aivan täynnä monia erilaisia ja eritasoisia merenkulkijoita. Jos tähän vielä lisätään se hämmäntävä tosiasia, kun aluksen kapteeni ymmärtää, että hänen aluksensa todellinen paikka ei ole siellä, missä sen kuuluisi olla, voi olla todella halvaannuttava kokemus. Tällaisessa tilanteessa hänen mielestään navigoijan kuuluisi mahdollisimman nopeasti päästä tilanteesta irti ja lopettaa GPS-pohjaisiin järjestelmiin uskomisen. Navigoijan tulisi uskoa vain ja ainoastaan silmien ja tutkan tuomaa tietoa navigoinnissa. Trafi

on luonut omille Internet-sivuilleen Suomenlahden tilannekuvakartan, jossa tutkittava alue on luokiteltu hankalimmaksi/onnettomuusaltteimmaksi. Liekö syynä juuri se, että tälle pienelle alueelle on varsinkin kesällä tungettu kaikki alukset veneilijöistä suuriin ulkomaisiin risteilijäaluksiin. Kun kaikki vielä tukeutuvat näihin GPS-tekniisiin järjestelmiin, se pikkuhiljaa nakertaa meiltä perinteistä merenkulutaikaa pois, eikä enää tiedetä, kuka on väistämisvelvollinen missäkin tilanteessa.

Lisäksi Metsärinne painottaa GPS-järjestelmän ja siihen pohjautuvien järjestelmien kuten ECDIS-järjestelmän jatkuvaa mielessään kyseenalaistamista merenkulussa. Hänen mielestään pätevän ammattimerenkulkijan tulisi syväväylällä huomata linjasta poikkeaminen viimeistään siinä vaiheessa, kun ollaan tulossa sisään Länsisataman syväväylälle (tarkoitetaan eteläpäätä). Mikäli keula näyttää tässä vaiheessa, että ollaan linjatauista sivussa tai menossa poijun väärältä puolelta, niin silloin suuntaa tulee vaihtaa. Vielä tässäkin vaiheessa kyseinen poikkeama kyetään korjaamaan. Hänen mielestään paljon suurempi uhkakuva voisi olla vastaavan tilanteen tapahtuminen ulkomerellä, kun kaksi suurta öljytankkeriala seilaa pitkin Suomenlahtea. Näin voitaisiin saada aikaan suuri öljykatastrofi.

Myös Metsärinne myöntää, että tutkittavalle alueelle on luotu kattava tutkaverkko suurten alusten turvaksi METO-hengessä (rakentanut VTS, Puolustusvoimat ja Rajavartiolaitos). Nämä tutkaverkon luojat voivat itse käyttää toistensa tutkia, joko samanaikaisesti päällekkäin tai valikoiden joitain tutkia pois päältä tai käytettäviksi, mikäli ongelmia ilmaantuu. Näin kyetään saamaan muun muassa risteilijöille lisää turvallisuutta. Jos merenkulussa ilmenisi jotain poikkeavaa, esimerkiksi aluksen omassa kulussa AIS-maali ja tutkamaali ilmoittavat ristiriitaa keskenään, niin siihen voidaan ottaa yhteyttä usein eri keinoin. Yleisin kuitenkin on meriVHF-taajuus. Näiden tutkien tarkkaa kokonaismäärää ei selvitetty kattavasti, vaan siitä pyrittiin saada arvio. Metsärinteen mukaan näitä tutkia on kyllä riittävästi, ja näillä tulisi kyetä toimia kaikissa olosuhteissa ilman poikkeuksia. Hänen mukaansa tulisi kyllä olla todella huono tuuri, mikäli jotain ikävää pääsisi sattumaan näiden järjestelmien epäkunnon takia. Trafissa oletetaan myös, että VTS kykenee huomaamaan ja tunnistamaan poikkeavuudet AIS- ja tutkamaalin kesken. Eli mikäli näiden järjestelmien osalta tulee ristiriitaa, niin tutkaa uskotaan.

Trafissakin ollaan tiedostettu GPS-järjestelmään liittyvät uhkakuvat ja sen takia myös Metsärinne toteaa, että nyt on kehitteillä "Multi-task-receiver"-järjestelmä. Kaikki siihen liittyvät tekniikat ovat jo olemassa, mutta nyt vain odotellaan sitä, että jokin valmistaja ryhtyy suunnittelemaan ja valmistamaan kyseistä laitetta/vastaanotinta laajamittaisesti yleiseen käyttöön.

Trafi on myös hyvin peloissaan ja huolestunut tästä GPS-harhautukseen liittyvästä uhkakuvasta, mutta he ovat pyrkineet huomioimaan kaikissa omissa riskianalyyseissaan nämä nousevat haasteet ja uhat. He ovat sitä mieltä, että niin kauan, kun laivalta löytyy ohjailija, joka osaa kyseenalaistaa GPS:n tuomat tiedot omiin visuaalisiin sekä tutkan tuomiin navigointitietoihin verrattuna, niin mitään ikävää ei pääse käymään.



## 5.4 Silja Serenaden päällikön haastattelu

Tämä luku perustuu tutkijan ja Silja Serenade -aluksen päällikön Martin Björkelin väliseen nauhoitettuun teemahaastatteluun, jonka sisältämät tutkimuskysymykset on löydettävissä tutkimusliitteessä 5. Silja Serenade ei liiku Länsisataman syväväylää pitkin, vaan Tukholmasta päin tullessa Helsingin matalalle, sieltä Harmajan ohitse ja Kustaanmiekan kautta Eteläsatamaan. Suurten alusten päälliköistä hän oli ainoa, joka antoi teemahaastattelulle mahdollisuuden ja hän on toiminut jo vuosia suurilla aluksilla kuin myös Silja Serenadella. Lisäksi häneltä löytyy käytännön näkemystä ja kokemusta aiheeseen suuren risteilijän päällikönä.

Björkelillä on hieman erilainen näkemys tutkittavaan aiheeseen kuin edellä esitetyillä instansseilla, koska Silja Serenade on vain yksittäinen yksikkö, joka kulkee merellä. Aluksella he kokevat GPS-järjestelmän ongelmat olevan lähinnä antennin vastaanottimien fyysisten seikkojen kanssa. Eli heillä on jouduttu uusiimaan useita vastaanottimia laitevikojen takia. Itse GPS-järjestelmän avoimuus ei heidän mielestään ole ongelma, enemmänkin päinvastoin jopa etu, jotta he kykenevät saamaan tarkkaa paikkaa muiden yhteistyökumppaneiden kanssa.

Selvitettäessä Björkelliltä GPS-järjestelmään kytketyistä järjestelmistä, hän myönsi, että tänä päivänä lähes jokainen navigointiin perustuva laite tai järjestelmä kytkeytyy GPS:ään jollain lailla. Mutta on eri asia, kuinka nopeasti kapteeni kykenee huomaamaan joutuneensa GPS-harhautuksen alaiseksi, ja kuinka moni näistä järjestelmistä on GPS:stä riippuvainen. Keskustelussa navigoinnista ja täysin GPS:stä riippuvaisesta integroidusta elektronisesta merikartasta (ECDIS) ja muista itsenäisistä järjestelmistä hän kertoi minulle seuraavaa:

”Mikäli virheellinen GPS-signaali on manipuloitu ja tieto pääsee läpi, niin silloin myös karttapaikankin tieto siirtyy. Tämän kuitenkin kykenee huomaamaan siitä, että maakohteet eivät siirry, eli itsenäisen tutkan signaalien avulla kyetään paljastamaan GPS-harhautus (mikäli virhe on suuri). Tutka ei siis ikinä näytä väärin, vaan näyttää sen hetken maakohteiden suhteellista sijaintia.” (Björkell, haastattelu, 8.5.2017).

Näyttäisi siis siltä, että kaikki aiemmissa luvuissa esitetty teoria on aivan oikeassa, eli aluksen ohjailijan visuaalinen navigointikokemus yhdistettynä tutkan tuomaan tietoon kykenee taistelemaan ja puolustamaan alusta GPS-harhautuksen uhkaa vastaan ja juuri niin kuin kansalliset ja kansainväliset merilait vaativat. Björkell myönsi, että aluksen päällikkö on aina vastuussa aluksensa turvallisuudesta ja se ei siirry kenellekään muulle.

Serenadella on kuulemma useampi tutka, ja niitä toimii myös eri taajuuksilla. Kertaakaan ei historian aikana ole käynyt vielä niin, etteikö kyseinen tutkajärjestelmä, olisi kyennyt antamaan luotettavaa tietoa säässä kuin säässä. Mikäli heidän aluksensa joutuu GPS-harhautuksen alaiseksi, he kyllä lähettävät eteenpäin esim. AIS-järjestelmällä virheellistä paikkatietoa niin muille aluksille kuin

VTS:lle, mutta alukset kyllä oletettavasti kykenevät tunnistamaan omilla tutkilaan ja visuaalisella navigointikyvyllään kyseisen tiedon olevan virheellistä. Mikäli muut alukset joutuvat vastaavasti GPS-harhautuksen alaiseksi ja lähettävät AIS-järjestelmällä manipuloitua tietoa Serenadelle, niin Serenadella kyetään tähän samaan. Aivan samalla tavalla toimii myös VTS. Eli AIS-järjestelmä on siis vain raportointijärjestelmä, joka perustuu GPS-järjestelmään.

Jos Serenade joutuisi jotenkin GPS-harhautuksen uhriksi ja he kykenisivät vain tiedostamaan mahdollisen edessä piilevän onnettomuuden vaaran (visuaalinen navigointikyky tai tutka paljastaisi aluksen paikan vääräksi, VTS ottaisi yhteyttä), se vaatisi vain muutaman sekunnin, kun kaikki GPS:stä riippuvat navigointijärjestelmät kyettäisiin kytkemään irti GPS-järjestelmästä ja saamaan alus turvallisuudelle paikalle tai takaisin linjalle. Björkell kertoi seuraavaa:

”Tosin hyvin epämiellyttävään se olisi ajaa laivaa ilman paikkatietoa, tosin karttaa pystytään kyllä käyttämään ilman paikkatietoakin, mutta tällöin kartan joutuu manuaalisesti kohdistamaan aika ajoin. Mutta kaikkeen kyllä pystytään. Eli GPS ei ole meille mikään kriittinen järjestelmä. Tosin en lähtisi tässä vähättelemään sen tärkeyttä.” (Björkell, haastattelu, 8.5.2017).

Björkellin mielestä GPS-järjestelmä on se, joka tänä päivänä normaalissa merenkulussa ensimmäiseksi pettää ilman harhautuksia. Erityisesti antennien vastaanottimet ovat heikoimpia lenkkejä ja niitä joudutaan uusimaan usein. On myös mahdollista, että rankassa lumisateessa korjaussignaali katoaa väliaikaisesti.

Kysyessäni varustamoiden suhtautumista autopilotin käyttöön Björkell täsmensi, että tämä niin sanottu autopilotti on aivan eri asia kuin track pilot. Heidän track pilot käsittää neljä eri tasoa, joista alin on täysin manuaali ja ylin on vasta itsenäisesti alusta GPS-koordinaattien perusteella ohjaileva tekninen järjestelmäkokonaisuus, joka on GPS:stä riippuvainen. Heidän aluksessaan tällaista ylintä tasoa käytetään vasta ulkomerellä. Helpommin sanottuna jako menee lähinnä niin, että mitä helpommat keliolosuhteet ja helpompi alue, sen enemmän automatiikkaa. Tämän lisäksi myös jokaisen laivan työkulttuuri ja alustekniikka voi luoda aivan erilaiset käyttöolosuhteet. Jos jotain ongelmia ilmenisi, he voisivat vain yhdellä napinpainalluksella siirtyä manuaaliohjaukseen.

Björkell on täysin samaa mieltä jo aiemmin tutkimuksessa luvussa 5.2 selvitettyyn VTS:n tilannekuvan muodostamiseen ja meriturvallisuuden valvomiin. Mutta hän itse on sitä mieltä, että tällaiset mahdolliset GPS-harhautuksen takia väylältä sivuun luisumiset tulisi kyllä huomioida laivalla ensin. Jos jostain syystä se ei auta, niin vasta tämän jälkeen VTS:n kuuluisi antaa mahdollista neuvontaa tai huomauttaa.

Teoreettisesti ajateltuna Björkell näkee, että GPS-harhautus voisi onnistua mahdollisesti tilanteessa, jossa ollaan alueella, missä ei ole kuin matalia luotoja, joista ei voi saada tarpeeksi luotettavaa ja tarkkaa tutkatietoa, jos tällaisissa olosuhteissa jouduttaisiin vielä koviin merenkäynnin olosuhteisiin, niin silloin tämän tyyppinen harhautus saattaisi onnistuakin. Mutta jos keskitymme tutkittavaan Helsingin Länsisataman syväväylän alueeseen, on siellä useampia varmoja

tutkaheijasteita ja kaikukohteita. Björkell on myös sitä mieltä, että kukaan ei käytännössä viitsi tulla tarpeeksi lähelle antennia, jotta tällainen harhautusisku onnistuisi. Kyseiset antennit näet sijaitsevat rajatulla alueella. Jos tilanne olisi mahdollista suorittaa kotoa käsin, niin silloin näkökulma voisi olla aivan toisenlainen.

Myös Björkell toivoi, että tulevaisuudessa kyettäisiin keksimään jokin laite tai järjestelmä, jolla voisimme saada jotain redundanssia merenkulun paikan määrittämiseen. Näin voisimme mahdollisesti vertailla ja varmistaa oman paikkatietomme useampaan navigointijärjestelmään perustuen ja kykenisimme saamaan lisää evidenssiä.

## 6 TULOKSET JA JOHTOPÄÄTÖKSET

Koska Länsisataman syväväylä on maamme yksi ruuhkaisimmista meriväylistämme, jonka käyttökapasiteetti on vuosien varrella lisääntynyt valtavasti ja tulee oletettavasti myös lisääntymään, kuuluu merialueemme myös niin sanottuun todennäköisimpään riskialueeseen, jossa on sattunut ja voi vuosien varrella satua huomattavan paljon onnettomuuksia myös tulevaisuudessa. Eli useat merellä toimivat organisaatiomme joutuvat valvomaan ja kiinnittämään näihin asioihin erittäin paljon aikaa ja huolta jokaisessa päätöksessään. Myös Länsisataman kapeikot ja minimaaliset käänösalueet suurille risteilyaluksille antavat oman haasteensa kyseiselle alueelle varsinkin kesäkausina, kun alueella lisäntyy normaalin liikenteen lisäksi myös turismiliikenne. Lisäksi haasteelliset ja nopeasti vaihtelevat sääolosuhteet koettiin haastatteluihin osallistuneiden asiantuntijoiden parissa tämän alueen suurimmiksi ja todennäköisimmiksi riskitekijöiksi.

Tänä päivänä lähes kaikki merialusten navigointiin perustuvat järjestelmät ovat täysin riippuvaisia GPS-järjestelmästä ECDIS-järjestelmän kautta. GPS-järjestelmä taas on täysin avoin ja salaamaton kaikelle pahantahtoiselle toiminnalle, muun muassa GPS-jumiuttamiselle ja -harhauttamiselle. Jos tällainen pahantahainen toiminta onnistuisi, niin se kykenisi sekoittamaan meriliikenteemme tällaisella alueella aivan sekaisin, koska muun muassa samaa aluksen saamaa harhautettua GPS-tietoa saavat useat toimijat esimerkiksi AIS-järjestelmän kautta omille tilannekuvakartoilleen, ja näin myös heillä voi teoriassa tilannekuva sekoittua. Muun muassa näistä syistä tässä tutkimuksessa haluttiin lähteä tutkimaan teorian kannalta, millaisia mahdollisia uhkia GPS-harhautukseen saattaisi sisältyä meriliikenteessä, jos tällainen harhautustoiminta onnistuisi Helsingin Länsisataman syväväylällä.

GPS-harhautus on jopa suoritettu käytännön olosuhteissa aivan Italian eteläisellä merialueella muutama vuosi sitten. Tosin tämä suoritettiin aivan ulkomerellä ja autopilotilla (track-pilot-mode), joka on täysin GPS-järjestelmästä riippuvainen. Koe kyettiin suorittamaan ja alus harhauttamaan väylästään sivuun lisäämällä manipuloitua tehoa, eikä aluksen päällikkö henkilökuntineen tai hälytysjärjestelmät kyenneet tunnistamaan virheellistä dataa oikeasta. Tämä perustui siihen, että GPS-signaali on hyvin heikko, ja lisäämällä voimakkaampaa, mutta virheellistä/manipuloitua paikkatietoa oikea-aikaisesti, ei vastaanotin kykene tunnistamaan oikeaa väärästä, vaan uskoo ja luulee manipuloitua signaalia oikeaksi paikkatiedoksi ja seuraa sitä orjamaisesti. Teoriassa GPS-harhautus on siis mahdollista, mutta kykenisikö se vaikuttamaan meidän meriliikenteeseemme jotenkin ”lamaanuttavasti/halvaannuttavasti”.

Meidän merialueillamme aluspalvelulaki määrittää, että aluksen päällikkö on aina vastuussa aluksestaan kaikissa olosuhteissa, ja tämä vastuu siirtyy häneltä pois vasta siinä tilanteessa, kun joku muu on valmis vastaanottamaan häneltä päällikön tehtävät. Päällikölle on opetettu jo merikoulussa, että omat silmät eivät petä koskaan ja niitä tulee aina uskoa navigoinnissa. Paikan varmistukseen

paras apuväline on tutka ja vasta tämän jälkeen GPS. Vaikka tarkkuuden optimoinnissa voidaan asia normaalioloissa nähdä toisinpäin.

Jos alus jostain syystä joutuu GPS-harhautuksen uhriksi, lähtee alukselta saman tien AIS-järjestelmällä kyseinen manipuloitu tieto VTS:lle. Koska VTS:n valvontajärjestelmä perustuu ns. fuusioituun malliin, jossa voidaan yhdistää useat tutkat, kamerat ja AIS-järjestelmän tiedot, he kykenevät huomaamaan heti ristiriitaa näiden järjestelmien kesken ja ottamaan alukseen yhteyttä. Riippuen siitä, missä päin väylää ollaan ja kuinka paljon matkaa on vaaralliseen onnettomuuteen, VTS voi toimia joko heti, tai antaa laivan mahdollisesti itse korjata tilanteen, jos alus on vain alueella, jossa tilaa on siihen riittävästi. AIS-järjestelmä ja sen tuoma paikkatieto ei ole VTS:lle mikään kriittinen tieto, vaan AIS-järjestelmä on heille enemmänkin raportointijärjestelmä, mikä vain vahvistaa tutkan tuomaa paikkatietoa ja antaa heille lisätietoa aluksesta. VTS pyrkii siis proaktiivisesti valvomaan ja täten estämään mahdolliset onnettomuustilanteet.

Liikennevirasto, VTS ja Trafi olivat kaikki tiedostaneet tämän GPS-järjestelmän potentiaalisen uhkakuvan ja heikkouden, mutta juuri sitä varten merialueillamme alukset seilaavat asetustemme ja lakiemme mukaan, ja viranomaiset voivat luoda erilaisia ”turvaverkkoja/-keinoja” auttaakseen aluksia. Tätä varten Liikennevirasto on luonut tutkittavalle väyläosuudelle alusten kulkua varten, niin päivä- kuin yöajaksi, kattavan, visuaalisen navigointiin perustuvan merimerkistön aina kardinaalimerkeistä linjatauluihin sekä kattavan tutkaheijasteisiin perustuvan maalimerkistön. Mentiin kyseistä linjaa kumpaan suuntaan tahansa, niin aina tulisi kyetä näkemään edes joitain merenkulun merkkejä. Jos on aivan täysin olematon näkyvyys esimerkiksi sumun aikaan, niin tällöin kyetään tunnistamaan vähintäänkin tutkamaaleja. Jos jostain syystä tämäkään ei ole mahdollista, niin VTS antaa navigointiapua esim. radioteitse. Asia voidaan myös katsoa siitä näkökulmasta, että alukset ovat merialueellamme vastuullisia seilaamaan merilain ja sääntöjen mukaan. Eli nämä ovat niin sanottuja operoivia yksiköitä, joiden kuuluisi tällä alueella kyllä kyetä huomaamaan mahdollinen GPS-harhautusyritys. VTS:n tehtävänä on valvoa, että alukset kulkevat sääntöjen mukaan ja tarpeen tullen kyetä varoittamaan ja estää mahdolliset onnettomuudet keinoin, jotka heille on suotu. VTS on siis luotu näkemään mahdolliset vaaratilanteet proaktiivisesti, ja he ovat merten valvova viranomainen. VTS on osa Liikennevirastoa, jolle se raportoi ja jonka kanssa se tekee yhteistyötä. Liikenneviraston tehtävä on hallinnoida merialueitamme ja suunnitella niitä entistä turvallisemmaksi. Trafi taas on merenkulussa organisaatio, jonka työntehtävänkuvaaan kuuluu vastata turvallisuudesta aluksen reelingin sisäpuoleisista asioista lähtien sekä suunnitella ja keksiä keinoja, joilla merenkulun järjestelmistä kyettäisiin saamaan entistä turvallisempia.

Kukaan haastattemistani organisaation edustajista ei pitänyt GPS-harhautusta todennäköisenä uhkana. Mutta jos jostain syystä se tapahtuisi ja onnistuisi, niin seuraukset voisivat olla todella huolestuttavia tai lamaannuttavia. Onnistuakseen se kuitenkin vaatisi nykyjärjestelmillä lukuisten seikkojen toteutumista. Ensinnäkin GPS-harhautusta suunnittelevan henkilön tulisi päästä jollakin keinoin aluksen GPS-antennien vastaanottimen luo. Tämä alue on rajattu. Jos tälle

alueelle kuitenkin onnistuttaisiin jotenkin pääsemään, niin hänen tulisi operoida oletetusti kannelta, että signaali kykenee pääsemään laivan vastaanottimeen. Jos aluksen henkilökunta jossain vaiheessa huomaa henkilön operoivan jotain pahantahtoista, niin hänet otetaan totta kai kiinni ja ilmoitetaan viranomaisille. Mikäli tämä henkilö jostain syystä onnistuisi suorittamaan toimensa, onnistunut GPS-harhautus vaatisi myös sen, että aluksessa tulisi olla autopilotin Track-Pilot päällä, joka kytketään vasta ulkomerellä. Jos se kuitenkin olisi kytketty jostain syystä päälle, niin kolmanneksi aluksen päällikön tulisi katsella jonnekin aivan muualle, kuin ulos ikkunasta tai tutkan ruudulle. Tämänkin jälkeen alukseen otettaisiin yhteyttä vielä VTS:stä useampaan otteeseen varoittaen potentiaalisesta vaaratilanteesta ja pyytäen suunnan ja nopeuden muutosta. Jos aluksen päällikkö ei noteeraisi näitäkään kutsuja missään vaiheessa, niin vasta tämän jälkeen onnettomuus voisi tapahtua. Tästä syystä tutkimuksen lopputuloksena voidaan pitää sitä, että onnistuneen GPS-harhautuksen todennäköisyys tutkittavalla alueella on todella pieni.

## 7 YHTEENVETO

GPS-vastaanottimien tarkkuus sekä käyttö on lisääntynyt valtavasti vuoden 2000 toukokuun jälkeen, kun Yhdysvaltojen Puolustusvirasto lopetti C/A-koodin tarkoituksellisen huonontamisen SA-koodilla. Tämän jälkeen GPS-järjestelmää on voitu pitää täysin avoimena kaikille käyttäjille. Tämä on herättänyt tutkijoissa ajatuksen siitä, voisiko joku sen avulla päästä harhauttamaan meriliikennettä ja aiheuttamaan mahdollisen kyberterroristisen teon.

Koska GPS-signaalin teho on heikko ja sitä ei siviilipuolella salata mitenkään, oivalsivat Humpreys ja Bhatti tukijaryhmineen mahdollisen uhkakuvan: Olisiko mahdollista rakentaa ns. harhautussimulaattori, joka saisi GPS-vastaanottimen luulemaan vahvempaa tehoa oikeaksi? He halusivat suorittaa kyseisen GPS-harhautuksen ensin miehittämättömälle lennokilleen vuoden 2010 alussa. Kun tämä koe oli onnistunut ja oli näytetty toteen, että GPS-harhautus on mahdollista, he halusivat suorittaa sen myös laivalle Italian eteläpuolella. Tässä koeksessa aluksessa oli aluksen kapteeni miehistöineen mukana, mutta itse alus oli kulkemassa GPS-reittipisteiden mukaan automaattisesti, aivan niin kuin normaalistikin ulkomerellä tehtäisiin. Tutkimusryhmä onnistui harhauttamaan aluksen sivuun reitiltään, ja aluksen henkilökunta ei ollut kyennyt huomaamaan sitä mitenkään. Tämän jälkeen eri alan viranomaiset noteerasivat tämän kauhukuvan tosissaan ja alkoivat pohtia asiaa aivan toisesta näkökulmasta. Esimerkiksi risteilijöiden ajattaminen karille, rantaan tai öljytankkereiden törmäyttämiset Manhattanin satamaan olisivat valtavia katastrofeja tämän päivän merenkulussa.

Koska aluksen navigaatiojärjestelmät, pois lukien ohjailijan visuaalinen kyky ja tutkat, perustuvat tänä päivänä suurilla aluksilla melkein kokonaan GPS-tekniikkaan, myös tässä tutkimuksessa haluttiin lähteä samasta näkökulmasta liikkeelle ja tutkia, onnistutaanko tänä päivänä teoriassa suorittamaan mahdollinen vaaratilanne merenkulussa Helsingin Länsisataman syväväylällä risteilyaluksen GPS-vastaanottiin kohdistettavalla hyökkäyksellä. GPS:n tuoma tieto linkitetään ECDIS-järjestelmään, johon tulevat myös muut aluksen järjestelmien tiedot. Tämä on erinomainen keino saada alus kulkemaan automaattisesti GPS-koordinaattien mukaisesti paikasta toiseen ns. normaalitilanteessa. Tässä kaikki järjestelmät keskustelevat ja vaihtavat tietoa keskenään aina aluksen työntövoimaan liittyvistä järjestelmistä aluksen paikanmäärittäjiin ja navigaatiojärjestelmiin. Tämän lisäksi ECDIS-järjestelmään on liitetty AIS-järjestelmä, joka lähettää aluksen omat tiedot muille aluksille ja VTS-keskukselle. Jos GPS-harhauttaja onnistuu tehtävässään ja onnistuu harhauttamaan aluksen väärälle suunnalle antamalla sille ns. väärää paikkatietoa, niin aluksen hälytysjärjestelmät eivät kykene huomaamaan asiaa mitenkään. Tällöin tutkittavalla alueella on teoriassa mahdollista sattua onnettomuustilanne. Jos aluksen ohjailija/kapteeni taas on valppaana ja on valmis jatkuvasti vertailemaan GPS-järjestelmän, tutkansa sekä visuaalisen navigoinnin tuomaa tietoa keskenään, niin hän on aina tietoinen, missä päin syväväylää milloinkin liikutaan ja onnettomuus kyetään mahdollisesti estämään.

Länsisatama on Helsingin ruuhkaisin ja käyttökapasiteetiltaan suurin alue, jossa liikkuu tutkittavia suuria risteilyaluksia päivittäin 8-10 kappaletta molempiin suuntiin. Tämän lisäksi siellä liikkuu sekalainen määrä muuta liikennettä, ja liikenne kasvaa kesää kohti mennessä ja laskee puolestaan talveksi. Tutkimus suoritettiin peilaamalla teoriaa asiantuntijoiden teemahaastatteluihin. Varsinkin tämän väylän ruuhkaisuus koettiin kaikkien haastatteluun osallistuneiden osapuolien mukaan potentiaalisesti vaaratekijäksi. Lisäksi vuodenaikojen erilaiset sääominaisuudet ja vaihtelut tekevät alueesta haasteellisen navigoinnille.

Itse GPS-harhautusta ei ole Helsingin Länsisataman syväväylällä vielä kertaakaan tapahtunut, koska merenkulun ja lakiemme mukaan aluksen navigointi tulee suorittaa aina visuaalisesti ja käyttäen navigoinnissa apuna tutkaan ja GPS:n perustuvia järjestelmiä. Eli navigoinnissa tärkeysjärjestys on aina visuaalinen navigointikyky, tutkan tuoma tieto ja vasta sitten GPS:n tieto. Haastateltujen toimijoiden mukaan tällaisissa tilanteissa huomiointi kuuluisi mennä niin, että aluksella kyettäisiin itse huomaamaan tällaiset harhautustoimenpiteet ja tarpeen tullen toimimaan tarvittavalla tavalla, jotta onnettomuus kyettäisiin estämään. VTS on myös perustettu turvaamaan aluksia juuri tämän tai vastaavan tyyppisiä onnettomuustilanteita varten, ja tarpeen tullen he voivat puuttua tilanteeseen antamalla navigointiapua estääkseen syntyvän katastrofin. Kaikki haastatteluihin osallistuneet henkilöt pitivät onnistuneen GPS-harhautuksen todennäköisyyttä hyvin pienenä uhkatekijänä. Kuitenkin näiden uhkien varalta Liikennevirasto ja Trafi suunnittelevat ns. "turvaverkkoja", jotka voisivat mahdollisesti tehdä meriliikenteestämme vieläkin turvallisemman.

Liikennevirasto ja Trafi, jotka ovat muun muassa merellisten toimijoiden päävastuuorganisaatioita ja tulevaisuuden kehittäjiä, ovat yhteistyössä eri ulkomaisten organisaatioiden kanssa alkaneet kehittää "turvaverkkona" GPS:n tilalle mahdollisia redundanssijärjestelmiä. Muun muassa yksi tällainen mahdollinen järjestelmä voisi olla "Multi-Task-Receiver", joka kykenisi GPS:n lisäksi vastaanottamaan muitakin merenkulun taajuuksille varattuja radiosignaaleja sekä yhdistämään niitä muihin satelliittijärjestelmiin. Monen järjestelmän päällekkäisyydellä tutkimani GPS-harhautus tehtäisiin mahdottomaksi. Vastaanotin kykenisi vertailemalla tunnistamaan GPS-harhautuksen signaalin poikkeukselliseksi suhteessa muiden tuomaan dataan. Tosin tämä on vasta tulevaisuutta ja sen toimivuus kyetään todistamaan vasta sitten, kun ensimmäiset laitteet tulevat käyttöön ja myyntiin.

Ennen tätä hetkeä olisi hienoa päästä suorittamaan rauhallisemmalla testi-alueella, tai miksei myös tutkimallani alueella, käytännön koe. Tässä tämä teoreettinen tilanne tuotaisiin osaksi reaali maailmaa. Eli helpommin sanottuna simuloitaisiin samanlainen tilanne rannikkoalueillamme kuin Humpreysin tutkimuksessa Italian eteläpuolella ja katsottaisiin, miten käy. Otettaisiin esimerkiksi 5-10 eri alusta ja annettaisiin heille ohjeiksi navigoida aivan normaalilla tavalla rannikko-olosuhteissa. Tämän jälkeen samat alukset vietäisiin ulkomerelle ja toistettaisiin koe aivan samaan tyyliin. Tutkimuksissa pyrittäisiin selvittämään a) Onnistuuko GPS-harhautus käytännössä? b) Miten kauan menee, että aluksen henkilökunta kykenee huomaamaan kyseisen harhautuksen? c) Paljonko alusta



saadaan ajatutettua linjasta sivuun? ja d) Kauan kestää, että alus on palannut takaisin väylälleen? Tämän lisäksi vielä vertailtaisiin alusten tuloksia keskenään ja toimivuutta VTS:n kanssa.

Toinen huomattava tutkimisen aihe voisi olla myös se, tuleeko GPS-harhautuksen riski kasvamaan tulevaisuudessa, kun meriliikenteessä tulee kulkemaan enemmän autonomisia aluksia. Kyetäänkö uusilla kehitettävillä järjestelmillä takaamaan autonomisten alusten turvallinen kulku, ja miten autonomiset alukset pystyvät huomioimaan muut merellä liikkujat, kuten vapaa-ajan pienet alukset, sekä miten nämä pienet alukset toimisivat mahdollisen vaaratilanteen uhatessa. Autonomiset aluksethan oletettavasti liikkuisivat paikasta toiseen ilman häiriötä, mutta miten ihmiset kykenevät niihin reagoimaan mahdollisissa kiireellisissä ja vaaratilanteissa, kun aikaa ei ole hukattavaksi.

## LÄHTEET

### Tieteelliset julkaisut :

#### Artikkelit :

- Air Power Australia, haettu 22.5.2017,  
<https://image.slidesharecdn.com/presentation1-150112054741-conversion-gate01/95/adapive-missile-guidance-using-gps-15-638.jpg?cb=1421041751>
- Alessandri, A., Donnarumma, S., & Vignolo, S., (2015), *System control design of autopilot and speedpilot for a patrol vessel by using LMIs*, Towards Greenmarine Technology and Transports, ISBN : 978-1-138-02887-6, 577-588, haettu 2.2.2017 sivulta,  
[https://books.google.fi/books?hl=fi&lr=&id=pcB5CgAAQBAJ&oi=fnd&pg=PP1&dq=balticsea+autopilot&ots=Ae-fbMobns&sig=2v\\_iSiWQnZDOXS7KIT1ZzmXozTA&redir\\_esc=y#v=onepage&q=autopilot&f=false](https://books.google.fi/books?hl=fi&lr=&id=pcB5CgAAQBAJ&oi=fnd&pg=PP1&dq=balticsea+autopilot&ots=Ae-fbMobns&sig=2v_iSiWQnZDOXS7KIT1ZzmXozTA&redir_esc=y#v=onepage&q=autopilot&f=false)
- Alusliikennepalvelulaki, 623/5.8.2005, haettu 20.1.2017 sivulta,  
<http://www.finlex.fi/fi/laki/ajantasa/2005/20050623>
- Askola, H., Lehtonen, S. & Virtanen A., (2016), *Liikenteen sähköisten palveluiden tietoturva – niihin kohdistuvat tietoturvariskit ja häirintämenetelmät sekä näiden vaikutukset ja ennaltaehkäisy*, Teknologian tutkimuskeskus VTT Oy, ISBN 978-951-38-8406-2. haettu 8.2.2017 sivulta,  
<http://www.vtt.fi/inf/pdf/technology/2016/T253.pdf>
- Basker, S., (2006), *The Role of GNSS in the GLAs' Future Service Provision*, Research and Navigation, General Lighthouse Authorities, Power point diat 1-22, haettu 17.3.2017 sivulta  
[www.gps.gov/cgsic/international/2006/manchester/basker.ppt](http://www.gps.gov/cgsic/international/2006/manchester/basker.ppt)
- Bhatti, J., & Humphreys, T., (2014), *Covert Control of Surface Vessels via Counterfeit Civil GPS Signals*, The University of Texas at Austin, 1-10, haettu 2.2.2017, sivulta,  
<https://pdfs.semanticscholar.org/6f20/450b32b71f2454e63292acb632d3619ee8ef.pdf>
- Britannica, (2017), *Dead Reckoning, Modern Navigation*, Ensyklopedia Britannica, haettu 9.2.2017 sivulta  
<https://global.britannica.com/technology/navigation-technology/Modern-navigation#toc61194>
- Cao, K, Cheng, X, Li, B & Xu, J, (2009), *Analysis of Forgery Patterns for GPS Civil Spoofing Signals*, Computer Sciences and Convergence Information Technology, 24 – 26 November, IEEE, 353-356, haettu 6.2.2017 sivulta  
<http://ieeexplore.ieee.org/abstract/document/5367927/?part=1>
- Capkun, S., Pöpper, C., Rasmussen, K. & Tippenhauer, N. (2011), *On the requirements for successful GPS attacks*, Proceedings of the 18th ACM conference on Computer and communications security, october 17 – 21, ISBN: 978-1-4503-0948-6, 75-85, haettu 6.2.2017 sivulta

- <http://dl.acm.org/citation.cfm?id=2046719>
- Eckerö Line, (2017), *Aikataulut & hinnat*, Eckerö Line, haettu 30.1.2017 sivulta, [https://www.eckeroline.fi/webapp/wcs/stores/servlet/Content\\_10151\\_10001\\_-77?page=index.php%3Foption%3Dcom\\_content%26view%3Darticle%26id%3D180%26lang%3Dfi-FI&smi=131&menuid=143&storeId=10151](https://www.eckeroline.fi/webapp/wcs/stores/servlet/Content_10151_10001_-77?page=index.php%3Foption%3Dcom_content%26view%3Darticle%26id%3D180%26lang%3Dfi-FI&smi=131&menuid=143&storeId=10151)
- ESA, (2014a), *What is GNSS*, European Space Agency, Navipedia, Haettu 30.1.2017 sivulta, <http://navipedia.net/index.php/GNSS>
- ESA, (2014b), *GPS signal Plan*, European Space Agency, Navipedia, haettu 1.2.2017 sivulta, [http://navipedia.net/index.php/GPS\\_Signal\\_Plan](http://navipedia.net/index.php/GPS_Signal_Plan)
- Forsen, M., Haavisto, J., Karlsson, S., Keränen, K., Sivuranta, T., (2010), *Merenkulun perusteet, rannikolta avomerelle*, Opetushallitus, 3. painos, ISBN 978-952-13-4571-5
- GPS.Gov, (2017a), *The Global Positioning System*, What is GPS, United States Government, haettu 31.1.2017 sivulta, <http://www.gps.gov/systems/gps/>
- GPS.Gov, (2017b), *How does GPS work, Frequently Asked Question*, United States Government, haettu 31.1.2017 sivulta, <http://www.gps.gov/support/faq/#howgpsworks>
- GPS.Gov, (2016c), *New Civil Signals, Modernization*, United States Government, haettu 1.2.2017 sivulta, <http://www.gps.gov/systems/gps/modernization/civilsignals/>
- GPS.Gov, (2016d), *Selective Availability*, haettu, haettu 24.5.2017 sivulta <http://www.gps.gov/systems/gps/modernization/sa/>
- Hagen, O, Skaugen, A & Ånensen, K, (2013), *Robust Surface Vessel Navigation Using Terrain Navigation*, Norwegian Defence Research Establishmen, IEEE, haettu, 10.2.2017 sivulta <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6608055>
- Hegarty, C. & Kaplan, E., (2006), *Understanding GPS, Principles and Applications*, Artech House, London, ISBN: 1-58053-894-0, Second edition, haettu, 7.2.2017 sivulta, [http://d1.amobbs.com/bbs\\_upload782111/files\\_33/ourdev\\_584835O21W59.pdf](http://d1.amobbs.com/bbs_upload782111/files_33/ourdev_584835O21W59.pdf)
- Helsingin edusta, (2003), INT 1250 FI18, Liikennevirasto, ISBN 978-952-255-711-1
- Helsingin Länsisataman väylä, (2013) *Väyläkortit*, Liikennevirasto, (haettu 25.1.17) [http://www.liikennevirasto.fi/documents/20473/134114/Vaylakortti\\_Helsingin\\_Lansisataman\\_vayla\\_fi\\_0.pdf/754f02c0-8826-4016-b386-a3b16d6be60d](http://www.liikennevirasto.fi/documents/20473/134114/Vaylakortti_Helsingin_Lansisataman_vayla_fi_0.pdf/754f02c0-8826-4016-b386-a3b16d6be60d)
- Hirsijärvi, S., Hurme, H., (1993), *Teemahaastattelu*, Yliopistopaino, Helsinki, 1993
- Holvik, J., (1998), *Basics of Dynamic Positioning*, DP Conference, Houston, 1-10, haettu, 10.2.2017 sivulta

- <http://www.dynamic-positioning.com/proceedings/dp1998/BHolvik.PDF>
- Huang, J. & Ren, Z., (2010), *The Information Reconstruction System of VDR & AIS Data Fusion*, Navigation Institute, IEEE, 181-183, haettu 10.2.2017 sivulta  
<http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5551504>
- Humphreys, T., (2012), *Statement on the Vulnerability of Civil Unmanned Aerial Vehicles and Other Systems to Civil GPS Spoofing*, The University of Texas at Austin, 1-16, haettu 2.2.2017 sivulta  
<http://rnl.ae.utexas.edu/images/stories/files/papers/Testimony-Humphreys.pdf>
- Humphreys, T., Kintner, P., Ledvina, B., O'Hanlon, B. & Psiaki, M., (2008), *Assessing the Spoofing Threat : Development of a Portable GPS Civilian Spoofer*, ION GNSS Conference Savannah, GA, septemper, 16-19, haettu 6.2.2017 sivulta  
[https://gps.mae.cornell.edu/humphreys\\_etal\\_iongnss2008.pdf](https://gps.mae.cornell.edu/humphreys_etal_iongnss2008.pdf)
- Humphreys, T., Montgomery, P., (2009), *Receiver-autonomous spoofing detection: Experimental results of a multiantenna receiver defence against a portable civil GPS spoofer*, University of Texas at Austin, Proceedings of the ION, 124-130, haettu 5.2.17 sivulta,  
[http://rnl.ae.utexas.edu/images/stories/files/papers/multi\\_antenna\\_defense\\_montgomery.pdf](http://rnl.ae.utexas.edu/images/stories/files/papers/multi_antenna_defense_montgomery.pdf)
- Ilmatieteen laitos, (2017), *Suomen nykyilmasto ja tilastot*, haettu 17.3.2017 sivulta,  
<http://ilmatieteenlaitos.fi/ilmasto>
- IMO, (2017a). *AIS Transponders*, International Maritime Organization, haettu 9.2.2017 sivulta,  
<http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx>
- IMO, (2017b) *Vessel Traffic Service*, International Maritime Organization, haettu 11.4.2017 sivulta,  
<http://www.imo.org/en/OurWork/Safety/Navigation/Pages/VesselTrafficServices.aspx>
- Johnston, R. & Warner, J., (2003), *GPS Spoofing Countermeasures, Vulnerability Assessment Team*, Homeland Security Journal, haettu 6.2.2017 sivulta,  
<http://lewisperdue.com/DieByWire/GPS-Vulnerability-LosAlamos.pdf>
- Kerns, A., Shepard, D., Bhatti, J., & Humphreys, T., (2014), *Unmanned Aircraft Capture and Control Via GPS Spoofing*, Journal of Field Robotics, Volume 31, Issue 4, 617-636, haettu 2.2.2017 sivulta  
<http://onlinelibrary.wiley.com/doi/10.1002/rob.21513/full>
- Kiljala, M., (2011), *Navigoinnin elektroniset apuvälineet, Tutka, AIS ja GPS-järjestelmä*, Lahden Ammattikorkeakoulu, s. 40, haettu 9.2.2017 sivulta  
<http://www.sperrymarine.com/news/ng-introduces-new-technology-satellite-compass-system>
- Kotiranta, E, (2008) *Alusliikennepalvelun kehittäminen*, Selvitystyö, Liikenne ja Viestintäministeriö, ISBN 978-952-201-742-0, haettu 11.4.2017 sivulta,  
<https://www.lvm.fi/documents/20181/819315/2308.pdf/969da8d9-8b74-4f1f-be9d-a01e3f6d2cd4?version=1.0>

- Kuusniemi, H., Bhuiyan, M., Kröger T., (2013), *Signal Quality Indicators and Reliability Testing for Spoof-Resistant GNSS Receivers*, Finnish Geodetic Institute, Department of Navigation and Positioning, Finland, haettu 8.2.2017 sivulta, [https://www.researchgate.net/publication/236343778\\_Signal\\_Quality\\_Indicators\\_and\\_Reliability\\_Testing\\_for\\_Spoof-Resistant\\_GNSS\\_Receivers](https://www.researchgate.net/publication/236343778_Signal_Quality_Indicators_and_Reliability_Testing_for_Spoof-Resistant_GNSS_Receivers)
- Liikennevirasto, (2017) *Helsinki VTS Master's Guide, Ammattimerenkulku*, haettu 11.4.2017 sivulta, <http://www.liikennevirasto.fi/ammattimerenkulku/meriliikenteen-ohjaus/vts/helsinki#.WOyuzKL-vIU>
- Liikennevirasto, (2013), *Helsingin Länsisataman väylä, väyläkortti*, haettu 4.5.2017 sivulta, <http://www.liikennevirasto.fi/ammattimerenkulku/liikukuminen-vesivaylilla/vaylakortit#.WQreFsb-vIV>
- Läntinen Suomenlahti, (2003), FI 952, Liikennevirasto, ISBN 978-952-255-773-5
- Maritime Safety Information, (2017), *Dead Reckoning*, National Geospatial Intelligence Agency, 99-104, haettu 9.2.2017 sivulta, [http://msi.nga.mil/MSISiteContent/StaticFiles/NAV\\_PUBS/APN/Chapter-07.pdf](http://msi.nga.mil/MSISiteContent/StaticFiles/NAV_PUBS/APN/Chapter-07.pdf)
- NASA, (2016) *How do Global Positioning systems, or GPS, work?*, haettu 9.3.2017 sivulta, [https://www.nasa.gov/audience/foreducators/topnav/materials/listbytype/How\\_Do\\_Global\\_Positioning\\_Systems.html](https://www.nasa.gov/audience/foreducators/topnav/materials/listbytype/How_Do_Global_Positioning_Systems.html)
- Orädd, P., (2010), *Integroidut komentosiltaratkaisut ja niiden kehittyminen*, Kymenlaakson Ammattikorkeakoulu, s. 19 - 24, haettu 9.2.2017, sivulta [https://www.theseus.fi/bitstream/handle/10024/12302/oradd\\_panu.pdf?sequence=1](https://www.theseus.fi/bitstream/handle/10024/12302/oradd_panu.pdf?sequence=1)
- Palola, J., (2011), *Dynaamisen paikannuksen käsikirja*, Satakunnan ammattikorkeakoulu, s. 23-25, haettu 10.2.2017 sivulta [https://www.theseus.fi/bitstream/handle/10024/36649/Palola\\_Juha.pdf;sequence=1](https://www.theseus.fi/bitstream/handle/10024/36649/Palola_Juha.pdf;sequence=1)
- Port of Helsinki, (2017), *Traffic in the Port of Helsinki 2010-2016 (LIITE1 tilasto)*
- Port of Helsinki, (2017a), *Uudistamme satamaa, Länsisataman kehittäminen*, Port of Helsinki, haettu 25.1.2017 sivulta, <http://www.portofhelsinki.fi/uudistamme-satamaa/lansisataman-kehittaminen>
- Port of Helsinki, (2017b), *Helsingin Satama, Suomen ulkomaankaupan ja matkustajaliikenteen pääsatama*, haettu 30.1.2017 sivulta <http://www.portofhelsinki.fi/helsingin-satama>
- Port of Helsinki, (2017c), *Länsisatama uudistuu, Forward together*, haettu 30.1.2017 sivulta <http://www.portofhelsinki.fi/sites/default/files/attachments/lansisatama-uudistuu.pdf>
- Port of Helsinki, (2017d), *Saapuvat ja lähtevät laivat, Länsiterminaali, Port of Helsinki*, haettu 30.1.2017 sivulta, <http://www.portofhelsinki.fi/matkustajille/saapuvat-ja-lahtevat-laivat>

- Port of Helsinki, (2017e), *Julkaisut ja tilastot, Helsingin sataman liikenne tilastot*, Port of Helsinki, haettu 30.1.2017 sivulta,  
<http://www.portofhelsinki.fi/helsingin-satama/julkaisut-ja-tilastot>
- Poutanen, M., (2016), *Sateelliittipaikannus*, Tähtitieteellinen yhdistys Ursa, Ursan julkaisuja Nro. 152, Helsinki
- Rantanen, K., (2017), *Aavelaiivat valtaavat meriä*, Helsingin Sanomat julkaisupäivä 1.2.2017, sivut B8-B9
- Saaranen-Kauppinen, A. & Puusniekka, A. 2006. *KvaliMOTV - Menetelmäopetuksen tietovaranto*, Tampere: Yhteiskuntatieteellinen tietoarkisto, haettu 9.3.2017 sivulta  
<http://www.fsd.uta.fi/menetelmaopetus>
- Salminen, A. (2011), *Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin*, Vaasan Yliopiston julkaisuja, ope-  
tusjulkaisuja 62, sivut 7-8
- Sathyamoorthy, D., (2013), *Global navigation satellite system (GNSS) spoofing: A review of growing risks and mitigation steps*, Defence S&T Tech. Bull, 47-67, Haettu 13.3.2017 sivulta,  
[https://www.researchgate.net/profile/Dinesh\\_Sathyamoorthy/publication/259465910\\_Global\\_navigation\\_satellite\\_system\\_GNSS\\_spoofing\\_A\\_review\\_of\\_growing\\_risks\\_and\\_mitigation\\_steps/links/00b4952bdc288d6301000000/Global-navigation-satellite-system-GNSS-spoofing-A-review-of-growing-risks-and-mitigation-steps.pdf](https://www.researchgate.net/profile/Dinesh_Sathyamoorthy/publication/259465910_Global_navigation_satellite_system_GNSS_spoofing_A_review_of_growing_risks_and_mitigation_steps/links/00b4952bdc288d6301000000/Global-navigation-satellite-system-GNSS-spoofing-A-review-of-growing-risks-and-mitigation-steps.pdf)
- Shepard, D., Bhatti, J., Humpreys, T., (2012), *Evaluation Of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks*, The University of Texas at Austin, haettu 24.5.2017 sivulta,  
<http://rnl.ae.utexas.edu/images/stories/files/papers/PMUAndUAVSpoofingION2012.pdf>
- Sperry Marine, (2017) *NG Introduces New Technology Satellite Compass System*, Northrop Grumman, haettu 9.2.2017 sivulta,  
<http://www.sperrymarine.com/news/ng-introduces-new-technology-satellite-compass-system>
- Suomen Kyberturvallisuusstrategia, (2013), *Valtioneuvoston periaatepäätös*, ISBN: 978-951-25-2433-4, s. 19
- Suomen Satamaliitto, (2016), *Vuositilastoja*, matkustajaliikenne, haettu 30.1.2017 sivulta,  
<http://www.satamaliitto.fi/fin/tilastot/vuositilastoja/>
- St Peter Line, (2017), *Aikataulut*, St. Peter Line, haettu 30.1.2017 sivulta,  
<http://www.stpeterline.fi/aikataulut>
- Subsea Worldnews, (2016), *Vesper Marine Solution for Long Island Sound Cable Protection*, haettu 22.3.2017 sivulta,  
<http://subseaworldnews.com/2016/08/02/vesper-marine-solution-for-long-island-sound-cable-protection/>
- Tallink silja Line, (2017), *Aikataulut Helsinki-Tallinna*, Tallink Silja Line, haettu 30.1.2017 sivulta,  
<https://www.tallinksilja.fi/aikataulut-helsinki-tallinna>

- Tallink Silja Line, (2017a), *Tallinkin LNG-uuden aluksen nimeksi Megastar*, haettu 24.5.2017, sivulta, <https://www.tallinksilja.fi/22.01.2016-tallinkin-uuden-Ing-aluksen-nimeksi-megastar>
- Tamaru, E. & Tassedda, H., (2008), *A Study on a Dynamic Traffic management System based on Virtual and Synthetic AtoN AIS System*, Japan Institute of Navigation, haettu 17.3.2017 sivulta [http://ci.nii.ac.jp/els/110007045530.pdf?id=ART0008972763&type=pdf&lang=en&host=cinii&order\\_no=&ppv\\_type=0&lang\\_sw=&no=1489751930&cp=](http://ci.nii.ac.jp/els/110007045530.pdf?id=ART0008972763&type=pdf&lang=en&host=cinii&order_no=&ppv_type=0&lang_sw=&no=1489751930&cp=)
- Thompson, B., *GPS-Spoofing and Jamming: A global concern for all vessels*, *Proceedings of the Marine Safety & Security Council*, vol. 71, number 4, 50-52, haettu 2.2.2017 sivulta [http://www.uscg.mil/proceedings/archive/2014/Vol71\\_No4\\_Wint2014.pdf](http://www.uscg.mil/proceedings/archive/2014/Vol71_No4_Wint2014.pdf)
- Tilastokeskus, (2017), *Matkustajaliikenne Suomen ja ulkomaiden välillä satamittain ja maittain 2000-2016*, haettu 30.1.2017 sivulta, [http://pxnet2.stat.fi/PXWeb/pxweb/fi/StatFin/StatFin\\_lii\\_uvliik/060\\_uvliik\\_tau\\_106.px/?rxid=f137171b-168d-4bb1-aec4-55221bbe9c61](http://pxnet2.stat.fi/PXWeb/pxweb/fi/StatFin/StatFin_lii_uvliik/060_uvliik_tau_106.px/?rxid=f137171b-168d-4bb1-aec4-55221bbe9c61)
- Trafi, (2015) *Merenkulun riskialueet kartalla*, haettu 4.5.2017 sivulta, [https://www.trafi.fi/merenkulku/merenkulun\\_riskialueet\\_kartalla](https://www.trafi.fi/merenkulku/merenkulun_riskialueet_kartalla)
- Tucci, A, (2015), *Dial "C" for Cyber Attack, How marine system vulnerabilities can increase cyber risk*, *Proceedings of the Marine Safety & Security Council*, Volume 72, Number 2, 48-51, Haettu 8.2.2017 sivulta, [http://www.uscg.mil/proceedings/archive/2015/Vol72\\_No2\\_Sum2015.pdf](http://www.uscg.mil/proceedings/archive/2015/Vol72_No2_Sum2015.pdf)
- Ut News, (2013), *Ut Austin Researchers succesfully Spoof an \$80 million Yacht at Sea*, *The University of Texas at Austin*, haettu 1.2.17, <https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea>
- Valtioneuvoston asetus alusliikennepalvelusta, 763/2005, haettu 20.1.2017 sivulta, <http://www.finlex.fi/fi/laki/alkup/2005/20050763>
- Valtioneuvoston asetus alusliikennepalvelusta, 1798/2009, haettu 20,1,2017 sivulta, <http://www.finlex.fi/fi/laki/alkup/2009/20091798>
- Viestintävirasto, (2012), *Rannikkolaivurin VHF-radioliikenneopas*, haettu 10.2.2017 sivulta, [https://www.viestintavirasto.fi/attachments/Rannikkolaivurin\\_radioliikenneopas.pdf](https://www.viestintavirasto.fi/attachments/Rannikkolaivurin_radioliikenneopas.pdf)
- Wikipedia.org
- Visithelsinki.fi, (2017), *Helsinkiin odotetaan vilkasta Risteilykesää*, haettu 17.5.2017 sivulta <http://www.visithelsinki.fi/fi/ammattilainen/miksi-helsinki/ajankohtaista/helsinkiin-odotetaan-vilkasta-risteilykesaa>





## LIITE 1



17.5.2017

## TRAFFIC IN THE PORT OF HELSINKI

<b>CARGO TRAFFIC</b>	<b>2010 tons</b>	<b>2011 tons</b>	<b>2012 tons</b>	<b>2013 tons</b>	<b>2014 tons</b>	<b>2015 tons</b>	<b>2016 tons</b>
UNITISED GOODS							
Imports and exports							
import	5 022 870	5 270 026	4 965 574	4 750 849	4 790 403	4 836 633	5 018 520
export	4 786 119	4 903 144	4 818 436	4 894 163	5 244 651	5 562 929	5 546 514
<b>UNITISED GOODS</b>	<b>9 808 989</b>	<b>10 173 170</b>	<b>9 784 010</b>	<b>9 645 012</b>	<b>10 035 054</b>	<b>10 399 562</b>	<b>10 565 033</b>
BULK CARGO							
Import	794 275	900 826	903 863	795 151	655 263	773 208	818 294
Export	238 527	241	144	400	3 638	6 621	10 901
<b>BULK CARGO TOTAL</b>	<b>1 032 802</b>	<b>901 067</b>	<b>904 007</b>	<b>795 551</b>	<b>658 901</b>	<b>779 829</b>	<b>829 195</b>
<b>TOTAL FOREIGN CARGO</b>	<b>10 841 791</b>	<b>11 074 237</b>	<b>10 688 017</b>	<b>10 440 563</b>	<b>10 693 955</b>	<b>11 179 391</b>	<b>11 394 228</b>
<b>COASTAL TRAFFIC</b>	<b>89 707</b>	<b>151 585</b>	<b>143 242</b>	<b>108 226</b>	<b>134 313</b>	<b>230 810</b>	<b>226 691</b>

<b>TOTAL CARGO TRAFFIC</b>	10 931 498	11 225 822	10 831 259	10 548 789	10 828 268	11 410 201	11 620 918
----------------------------	------------	------------	------------	------------	------------	------------	------------

---

**UNITISED CARGO TRAFFIC**

Loaded and empty containers, TEU	392 828	393 619	404 895	406 085	400 510	430 427	451 263
Lorries and semitrailers, pcs.	482 429	513 959	494 136	479 392	497 246	511 776	525 337

---

**PASSENGER TRAFFIC**

Passengers	9 769 321	10 259 986	10 597 712	10 715 735	10 900 619	11 168 976	11 524 203
Cruise passengers	343 933	385 541	368 276	420 000	419 690	436 500	408 900
Buses, passenger cars and vans	1 141 979	1 217 049	1 268 771	1 292 505	1 360 650	1 412 226	1 499 088

---

**VESSEL TRAFFIC**

Vessel calls	8 453	8 776	8 733	8 126	7 968	8 413	8 469
	100 996	103 693	106 756	115 851	114 415		118 473
Vessels, net tons	100	538	746	524	054	113 601 848	587

source: Port of Helsinki

## LIITE 2

Liikenneviraston haastattelu 20.4.17

Haastattelija: Kalle Santaharju

Haastateltava: Kaisu Heikonen

Paikka: Liikennevirasto

**Mitkä ovat Liikenneviraston tehtävät merenkulussa?**

**Mainitse GPS järjestelmän ongelmakohdat?**

**Onko historiassa viitteitä GPS-harhautuksesta tai sen yrityksestä meriliikenteessä?**

**Tehän kuulutte VTS:n yläpuolelle?**

**Miten meriliikenteessä kyetään turvaamaan/takaamaan alusten ja henkilökunnan turvallisuus kaikissa olosuhteissa (kamerat, tutkat, radio jne.)?**

**VTS:n tutkajärjestelmä ei ole missään yhteydessä GPS-järjestelmään, eli se on täysin itsenäinen?**

**Entä jos puhutaan Helsingin Länsisataman Syväväylästä tai Helsingin edustasta, niin kuinka monta tutkaa siellä on? Pystytkö yhtään selventämään enempää?**

**Eli Länsisataman syväväylä on niin Strategisesti kriittisesti tärkeimmistä väyläalueista?**

**Entä jos GPS-harhautus iskuyritys yllättää, tuleeeko siitä teille tietoa? Vai meneekö se suoraan VTS:ään?**

**Onko VTS:llä muita järjestelmiä olemassa kuin tutkat ja AIS-järjestelmä, mitkä tulevat laivalta, millä se muodostaa tilannekuvaa ja pystyisi valvomaan?**

**Onko VTS samanlainen valtuuksiltaan verrattuna ilmavalvontaan vai onko se matalammalla tasolla?**

**Mitkä järjestelmät perustuvat GPS-tekniikkaan?**

Jos mennään reelingin ulkopuolelle, niin onko siellä jotain järjestelmiä, mitkä perustuvat GPS-tekniikkaan?

Puhutaanko näissä nyt Electronic Aids to Navigation- järjestelmistä? Mikä pohjautuu aivan samaan tekniikkaan kuin GPS ja AIS järjestelmiin?

Entä mitkä järjestelmät valvonnassa eivät perustu GPS-tekniikkaan?

Koet siis, että ollaan ilman GPS tekniikkaakin turvallisella pohjalla?

Miten GPS-harhautusta vastaan kyettäisiin taistelemaan tai luomaan jotain välineistöä?

Koetko, että GPS harhautuksia olisi jo tapahtunut Suomessa tai niitä tulisi tapahtumaan?

Kuinka pitkälle satama-alueelle laivat saa/niillä on oikeudet tulla autopilotilla, ennen kuin se täytyy kytkeä pois päältä.

Lähinnä ajattelin, että GPS-tekniikkaan perustuva autopilotti kykenisi tarpeen tullen viemään aluksen vaaralliselle alueelle, eli tätä mä ajattelin?

Ottaako VTS laivaan minkälaisella aikaviiveellä yhteyttä, mikäli se lähtee luisumaan sivuun suunnaltaan?

Tähänkin tulee kyetä, mikäli AIS-järjestelmän tiedot poikkeaisivat tutkan ilmoittamista tiedoista? Eli mikäli laiva itse raportoi AIS-järjestelmällään oikeasta paikasta, mutta VTS:n tutkat havaitsevat poikkeavuuden?

Tuleeko teiltä enemmän apupyynnöjä VTS:lle vai tuleeko sieltä enemmän tännepäin, näihin GPS-harhautuksiin liittyen?

Eli periaatteessa te luotte niitä turvakeinoja tulevaisuutta varten, eli ette ole siinä tällä hetkellä?

Onko jotain muuta, jota haluat vielä sanoa aiheeseen liittyen?

### LIITE 3

VTS-haastattelu 28.4.2017

Haastattelija: Kalle Santaharju

Haastateltava: Samu Koski Meriliikennekeskuksen päällikkö (Helsinki)

Paikka: Vilhovuorenkatu 2 - 4

**Mitkä ovat VTS:n tehtävät ja vastuut?**

**Miten toimitte yhteistyössä Liikenneviraston kanssa ja miten sijoitutte kyseiseen organisaatiohierarkiaan?**

**Miten toimitte yhteistyössä muiden valtion toimijoiden kanssa?**

**Miten saatte tietoa laivoilta ja millä teknisillä järjestelmillä?**

**Mainitse GPS järjestelmän ongelmakohdat?**

**Mitkä merenkulun järjestelmät perustuvat laivalla GPS-tekniikkaan?**

**Eli mikäli laivan GPS-järjestelmää kyetään harhauttamaan ja antamaan sille virheellistä tietoa, niin se lähettää kyseisen tiedon teille AIS-järjestelmälleen?**

**Mitkä merenkulun järjestelmät perustuvat laivan ulkopuolella GPS-tekniikkaan?**

**Onko historiassa viitteitä GPS-harhautuksesta tai sen yrityksestä, Länsisataman Syväväylällä?**

**Miten meriliikenteessä kyetään turvaamaan/takaamaan alusten ja henkilökunnan turvallisuus kaikissa olosuhteissa (kamerat, tutkat, radio jne.)?**

**Te voitte asettaa eri väylille ja maaleille erilaisia rajoja ja mikäli tämä kyseinen maali ne jostain syystä ylittäisi, niin teillä alkaa saman tien järjestelmät hälyyttämään? Tähän samaan kyetään, vaikka operaattorilla olisi seurattavana useampi maali samanaikaisesti?**

**Eli kykenette ottamaan laivaan yhteyttä esim. VHF:llä mikäli vaaratilanne uhkaisi?**

**Onko laivan kapteeni itse vastuussa laivasta?**

**Kykenettekö näkemään kameroilla kaikki Länsisataman Syväväylän linjaosuudet ja onko niissä pimeänäkökyky?**

**Kuinka useita näitä tutkia ja kameroita tällä alueella on?**

**Entä jos GPS-harhautus isku yritys yllättää, mihin järjestelmiin se vaikuttaa?**

**Miten GPS-harhautusta vastaan kyettäisiin puolustautumaan?**

**Onko Helsingin Länsisataman Syväväylällä eAton(electronic Aids to navigation)-välineistöä, mikä liitettäisiin ECDIS-järjestelmään?**

**Kyetäänkö näitä GPS-harhautuksia havaitsemaan mahdollisesti millään lailla?**

**Entä millaisella aikaviiveellä?**

**Jos alus alkaa lipua pois sovitulta reitiltä, niin kuinka nopeasti te otatte siihen yhteyttä?**

**Miten mahdollisena pidät, että tällaista mahdollista GPS-harhautusta olisi jo tapahtunut Länsisataman Syväväylällä tai merialueillamme?**

**Miten pitkälle laivat voivat seilata/kulkea autopilotilla tullessaan kohti satamaa?**

**Miten VTS valvoo meriliikennettä Helsingin edustalla ja vastaa siitä, että alukset pääsevät turvallisesti perille Länsisatamaan?**

**Miten VTS yhdistää alukselta samansa AIS-tiedon omiin tilannekuviinsa, joissa yhdistyy tutka ja kamera tiedot? Eli kykeneekö VTS erottamaan aluksen sivuun luisumisen, mikäli se saa väärää AIS-tietoa laivalta?**

**Nimeä vaarallisimmat Länsisataman Syväväylän kohteet?**

**Jos mennään historiassa taaksepäin, niin onko tällä väylällä sattunut paljon onnettomuuksia?**

**Onko VTS:llä huomioitu, tämä tulevaisuudessa perustettava Itämeren testi-alue tuleville laivoille ja miten?**

**Onko tulevaisuuden varalle kehitetty mitään varajärjestelmiä, mikäli laivat seilaavat automaattisesti kauko-ohjauksen avulla?**

**Onko jotain muuta vielä, mitä haluat tuoda ilmi/julki asiaan liittyen?**

## LIITE 4

Trafin haastattelu 25.4.2017

Haastattelija: Kalle Santaharju

Haastateltava: Jami Metsärinne/erityisasiantuntija

Paikka: Trafi, Kumpulantie 9, Helsinki

**Mitä Trafin tehtäviin kuuluu merellisestä näkökulmasta?**

**Miten toimitte yhteistyössä Liikenneviraston kanssa?**

**Miten toimitte yhteistyössä laivojen kanssa?**

**Mainitse GPS järjestelmän ongelmakohdat?**

**Mitkä järjestelmät perustuvat GPS-tekniikkaan?**

**Onko historiassa viitteitä GPS-harhautuksesta tai sen yrityksestä, Länsisataman Syväväylällä?**

**Miten meriliikenteessä kyetään turvaamaan/takaamaan alusten ja henkilökunnan turvallisuus kaikissa olosuhteissa (kamerat, tutkat, radio jne.)?**

**Onko tällä alueella VTS:n tutkia, kameroita tai luotu muita "turvaverkkoja"?**

**Kuinka useita näitä tutkia ja kameroita tällä alueella on?**

**Kyetäänkö niillä saamaan luotettava paikannustieto?**

**Jos tutkamaalin ja AIS-maalin kesken tulee ristiriitaa, niin kumpaa uskotaan?**

**Entä jos GPS-harhautus iskuyritys yllättää, mihin järjestelmiin se vaikuttaa?**

**Miten GPS-harhautusta vastaan kyettäisiin puolustautumaan?**

**Onko Helsingin Länsisataman Syväväylällä eAton (electronic Aids to navigation)-välineistöä? ja onko sitä mahdollisesti jossain muualla?**

**Kyetäänkö näitä GPS-harhautuksia havaitsemaan mahdollisesti millään lailla?**



Entä jos asiaa katsotaan laivan sisäisesti, eli ajatellaan alusta omana yksikönä ja sen sisällä toimii ns. kyberterroristi, joka saa jollain keinolla X alukselle luotua väärän/harhautetun GPS-signaalin ja täten sen pois reitiltään?

Entä millaisella aikaviiveellä?

Miten pitkälle laivat voivat seilata/kulkea autopilotilla tullessaan kohti satamaa?

Miten Trafi vastaa siitä, että alukset pääsevät turvallisesti perille Länsisataman edustalla?

Ottaako kyseinen alusliikennepalvelu saman tien laivaan yhteyttä, mikäli sen suunta alkaa mennä pois sovitulta suunnalta/väylältä?

Nimeä vaarallisimmat Länsisataman Syväväylän kohteet?

Kävin tuossa muutama päivä aikaisemmin katsomassa teidän sivuja, kun mietin mitä teiltä kysyisin ja silmiini osui Trafian tilannekuva kartta Suomenlahdelta, jossa mielenkiinnolla huomasin, että Helsingin alue oli väriltään aivan punainen (luokiteltu riskialueeksi), kun muu Suomenlahden alue oli suhteellisen neutraalin sininen (alue, missä ei juuri vahinkoja pääse syntymään).

Onko Trafilla huomioitu tämä Itämeren testialue tuleville laivoille ja miten?

Onko tulevaisuuden varalle kehitetty mitään varajärjestelmiä, mikäli laivat seilaavat automaattisesti kauko-ohjauksella?

Onko jotain muuta vielä, mitä haluat tuoda ilmi/julki asiaan liittyen?

## LIITE 5

Aika: 8.5.2017

Haastattelija: Kalle Santaharju

Haastateltava: Martin Björkell, Silja Serenaden päällikkö

Paikka: Silja Serenaden ohjaamo

**Mainitse GPS-järjestelmän ongelmakohdat?**

**Mitkä merenkulun järjestelmät on linkitetty laivalla GPS-tekniikkaan?**

**Mitkä näistä järjestelmistä on suoraa yhteydessä ohjaukseen/navigointiin?**

**Mitkä merenkulun järjestelmät perustuvat laivan ulkopuolella GPS-tekniikkaan?**

**Miten saatte tietoa muilta laivoilta ja millä teknisillä järjestelmillä?**

**Entä mitkä järjestelmät eivät perustu GPS-tekniikkaan?**

**Miten GPS-harhautusta vastaan kyettäisiin puolustautumaan?**

**Onko Helsingin Länsisataman Syväväylällä eAton (electronic Aids to navigation)-välineistöä, mikä liitettäisiin ECDIS-järjestelmään?**

**Kyetäänkö näitä GPS-harhautuksia havaitsemaan mahdollisesti millään lailla?**

**Entä millaisella aikaviiveellä?**

**Miten mahdollisena pidät, että tällaista mahdollista GPS-harhautusta olisi jo tapahtunut Länsisataman Syväväylällä tai merialueillamme?**

**Onko historiassa viitteitä GPS-harhautuksesta tai sen yrityksestä, Länsisataman Syväväylällä?**

**Onko historiassa kertaakaan käynyt niin, että Länsisataman Syväväylän tapaisella alueella oltaisiin oltu pelkästään GPS:n varassa meriliikenteessä?**

**Miten pitkälle laivat voivat seilata/kulkea autopilotilla tullessaan kohti satamaa?**

**Kuinka nopeasti kykenette kytkemään aluksen täysin manuaaliseen ohjaukseen, missä kaikki järjestelmät ovat täysin itsenäisiä ja riippumattomia GPS-järjestelmästä?**

**Miten VTS valvoo meriliikennettä Helsingin edustalla ja vastaa siitä, että alukset pääsevät turvallisesti perille Länsisatamaan? tai ylipäättänsä laituriin?**

**Ottaako kyseinen alusliikennepalvelu saman tien laivaan yhteyttä, mikäli sen suunta alkaa mennä pois sovitulta suunnalta/väylältä?**

**Miten VTS yhdistää alukselta samansa AIS-tiedon omiin tilannekuviinsa, joissa yhdistyy tutka ja kamera tiedot? Eli kykeneekö VTS erottamaan aluksen sivuun luisumisen, mikäli se saa väärää AIS-tietoa laivalta?**

**Nimeä vaarallisimmat Länsisataman Syväväylän kohteet (perusteluineen)?**

**Onko tulevaisuuden varalle kehitetty mitään varajärjestelmiä, mikäli laivat seilaavat automaattisesti kauko-ohjauksen avulla?**

**Miten merkittävänä/huolestuttavana uhkana pidät GPS-harhautusta?**

**Onko jotain muuta vielä, mitä haluat tuoda ilmi/julki asiaan liittyen?**