Aaro Ijäs

MERENKULUN KYBERTURVALLISUUDEN HAAVOITTUVUUDET

Opinnäytetyö

Tekniikan ammattikorkeakoulututkinto

Kyberturvallisuuden koulutus

2024

Kaakkois-Suomen ammattikorkeakoulu

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Insinööri (AMK)
Tekijä	Aaro Ijäs
Työn nimi	Merenkulun kyberturvallisuuden haavoittuvuudet
Toimeksiantaja	Kaakkois-Suomen ammattikorkeakoulu
Vuosi	2024
Sivut	63 sivua, liitteitä 4 sivua
Työn ohjaajat	Kimmo Kääriäinen, Vesa Kankare

TIIVISTELMÄ

Nykypäivänä merenkulun kyberturvallisuus voi olla osittain puutteellista ja siihen ei ole välttämättä kiinnitetty tarpeeksi huomiota. Tämän seurauksena voi ilmetä kyberturvallisuuden haavoittuvuuksia merenkulussa. Merenkulun kyberturvallisuuden haavoittuvuuksia syntyy erilaisista tekijöistä ja ne voivat mahdollistaa merenkulun kyberhyökkäyksiä. Merenkulussa kuuluisi olla kyberturvallisuuden tietämys hyvällä tasolla, jotta kyberhyökkäyksiin voitaisiin varautua.

Tämä opinnäytetyö oli tapaustutkimus, jossa tutkittiin millä tasolla Xamkin merenkulun opiskelijoiden kyberturvallisuuden tietämys oli. Sen avulla saatiin selville, oliko opiskelijoiden kyberturvallisuuden tietämyksessä parannettavaa, ja mitä näkemyksiä opiskelijoilla oli kyberturvallisuudesta.

Tutkimusotteena käytettiin kvalitatiivisen ja kvantitatiivisen otteen yhdistelmää. Tutkimuksessa kerättiin primääriaineistoa verkkokyselyllä, jonka aiheet liittyivät omaan käyttäytymiseen, kyberhyökkäyksiin, haavoittuvuuksiin ja eri järjestelmiin. Verkkokyselyyn osallistui 33 Xamkin merenkulun opiskelijaa, jossa päästiin kyselyn tavoitemäärään. Tämän lisäksi kerättiin sekundääriaineistoa, joka koostui erilaisista tutkimuksista, tilastoista ja artikkeleista merenkulun kyberturvallisuudesta. Opinnäytetyössä myös selvitettiin miten merenkulun kyberturvallisuuden haavoittuvuudet syntyvät, miksi kyberturvallisuus on tärkeää merenkulussa ja miten merenkulun kyberturvallisuuden haavoittuvuuksia voidaan ennaltaehkäistä.

Tutkimuksen tuloksista saatiin selville, että merenkulun opiskelijoiden kyberturvallisuuden tietämys oli tyydyttävällä tasolla. Opiskelijat osasivat ilmaista kyberturvallisuuden ongelmia merenkulussa ja he ymmärsivät kyberturvallisuuden tärkeyden. Heidän kyberturvallisuutensa tietämys oli kuitenkin osittain puutteellista ja siinä olisi parannettavaa.

Tutkimusta voidaan hyödyntää Xamkin merenkulun koulutuksessa tulosten perusteella. Tämän lisäksi tutkimukselle voidaan tehdä jatkokehitystä myöhempien vuosien merenkulun opiskelijoiden kanssa.

Asiasanat: merenkulku, kyberturvallisuus, haavoittuvuudet, kyberhyökkäykset

South-Eastern Finland University of Applied Sciences

Degree title	Bachelor of Engineering
Author	Aaro Ijäs
Thesis title	Vulnerabilities of maritime cybersecurity
Commissioned by	South-Eastern Finland University of Applied Sciences
Time	2024
Pages	63 pages, 4 pages of appendices
Supervisor	Kimmo Kääriäinen, Vesa Kankare

ABSTRACT

At present time, maritime cybersecurity may be partly deficient and it is not given the attention it necessitates. As a result, cybersecurity vulnerabilities can emerge. Vulnerabilities of maritime cybersecurity originate from different factors, and they can enable cyberattacks against maritime operations. In seafaring, all operations should have a good awareness in cybersecurity so that they could prepare for cyberattacks.

This thesis was a case study which investigated cybersecurity awareness among maritime students in South-Eastern Finland University of Applied Sciences Xamk. The purpose was to identify if there were areas that might require improvement in students' cybersecurity awareness and explore their views on cybersecurity.

The examination used both qualitive and quantitative research methods. Primary data was collected through an online survey that covered topics related to personal behavior, cyberattacks, vulnerabilities and different systems in maritime. In total 33 maritime students participated in the survey and the survey met its target goal. Secondary was gathered from various studies, statistics and articles related to maritime cybersecurity. The thesis examined how vulnerabilities rise and can be mitigated in maritime cybersecurity and why cybersecurity is important in seafaring.

The results revealed that cybersecurity awareness among students was satisfactory. They were able to name cybersecurity issues in maritime operations and understood the importance of cybersecurity. However, their cybersecurity knowledge was partially deficient and there was room for improvement.

The results of this thesis can be used in Xamk's maritime education. Additionally, it serves as a point of reference for a similar study with future maritime students in Xamk.

Keywords: seafaring, cybersecurity, vulnerabilities, cyberattacks

SISÄLLYS

1 JOHDANTO

Merenkulun ala on muuttunut vuosien mittaan uudella teknologialla ja vanhojen järjestelmien päivittämisellä. Uusi teknologia ja vanhojen järjestelmien päivittäminen tuo merenkulun alalle muutoksia ja uudistuksia, jotka luovat mahdollisesti uusia haasteita merenkulun ympäristöön. Merenkulun ympäristö voi olla laaja ja se sisältää monia eri osiota, jotka voi vaikuttaa kyberturvallisuuteen. Kyberturvallisuus alkaa olemaan yhä oleellisempaa merenkulun alalla. Se vaikuttaa moneen eri osa-alueeseen merenkulussa, kuten henkilöstöön, laivaan, yhtiöön ja lastiin. (International Chamber of Shipping 2021, 3.) Merenkulun kyberturvallisuus voi olla osittain puutteellista tai siihen ei ole välttämättä kiinnitetty tarpeeksi huomiota. Tästä voi syntyä ongelmia, jotka luovat mahdollisesti kyberturvallisuuden haavoittuvuuksia tai riskejä. Tämän seurauksena merenkulun kyberturvallisuuden haavoittuvuudet tulevat esille.

Tämä opinnäytetyö on tapaustutkimus, jonka tarkoituksena on kartoittaa merenkulun opiskelijoiden tietämyksen taso merenkulun kyberturvallisuudesta ja sen haavoittuvuuksista. Tutkimusmenetelmiin kuuluvat laadullisen ja määrällisen tutkimuksen ominaisuuksia. Tavoitteena on saada kattavaa ja merkittävää tietoa merenkulun kyberturvallisuuden haavoittuvuuksista opiskelijoiden näkökulmasta. Työn pääpaino keskittyy kyberturvallisuuden tärkeyteen merenkulussa. Tämän avulla saadaan käsitys siitä, miksi kyberturvallisuus on tärkeää merenkulussa ja miten merenkulun kyberturvallisuuden haavoittuvuudet syntyvät. Opinnäytetyön aihe on merenkulussa melko uusi asia ja siksi myös ajankohtainen.

Toimeksiantajana toimii Kaakkois-Suomen ammattikorkeakoulu Xamk. Xamk koostuu neljästä eri kampuksesta, jotka sijaitsevat Kotkassa, Kouvolassa, Mikkelissä ja Savonlinnassa. Opiskelijoita on yhteensä yli 11 500, jotka opiskelevat yli 40:ssä eri amk-koulutuksessa, ja yli 30:ssä eri yamk-koulutuksessa. Merenkulun koulutus koostuu merikapteenin, laivatekniikan insinöörin ja sähkövoimatekniikan insinöörin linjoista. (Kaakkois-Suomen ammattikorkeakoulu Xamk s.a.) Xamk valittiin toimeksiantajaksi, koska opinnäytetyössä luodaan aineistoa, jota voidaan hyödyntää merenkulun koulutuksessa.

2 TUTKIMUSASETELMA

Tutkimusasetelmassa käsitellään opinnäytetyön tutkimusongelma, tutkimusote ja tutkimuskysymykset. Tutkimusongelmalla kerrotaan, miksi tutkimus on tarpeellinen ja miksi tutkimusta tehdään. Tutkimusotteessa käydään tutkimuksen lähestymistapa ja aineistonkeruumenetelmä lävitse. Lähestymistavalla ja aineistonkeruumenetelmällä kerrotaan mistä, miten ja miksi aineistoa kerätään. Tutkimuskysymyksillä vastataan tutkimusongelmaan ja kerrotaan tutkimuskysymyksien tarkoitus.

Opinnäytetyössä tulisi olla riittävä dokumentaatio, jotta tutkimuksen ratkaisut voitaisiin perustella ja arvioida. Riittävällä dokumentaatiolla saadaan luotettavuutta tutkimukseen ja selkeyttä arviointiin. Riittävän dokumentaation lisäksi aineistonkeruu-, analysointi- ja tutkintamenetelmät pitäisi perustella. Menetelmiin tulisi perehtyä etukäteen, jotta vältyttäisiin vääriltä valinnoilta ja virheiltä. (Kananen 2019, 35.) Tämän tutkimuksen aineistonkeruu-, analysointi- ja tutkintamenetelmät ovat valittu niiden soveltuvuuden mukaan.

Opinnäytetyössä pitää ottaa huomioon myös lähteiden luotettavuus. Lähteiden täytyy olla tarpeeksi luotettavia, jotta tutkimuksen reliabiliteetti ja validiteetti pysyy. Tutkimuksen reliabiliteetilla ja validiteetilla varmistetaan, että oikeita asioita tutkitaan ja tulokset ovat pysyviä. (Kananen 2019, 25–30.) Opinnäytetyössä on tärkeää raportoida kaikki tutkimuksen vaiheet perusteellisesti. Perusteellisen raportoinnin avulla saadaan läpinäkyvyyttä tutkijalta ja reliabiliteetin ja validiteetin vahvistusta.

2.1 Tutkimusongelma

Opinnäytetyön tutkimusongelmana on se, että Xamkin merenkulun opiskelijoiden kyberturvallisuuden tietämyksen tasoa ei tiedetä. Tämän takia kuuluisi selvittää millainen on merenkulun opiskelijoiden kyberturvallisuuden tietämyksen taso. Tämän lisäksi voidaan saada näkemyksiä opiskelijoilta merenkulun kyberturvallisuudesta ja sen haavoittuvuuksista. Tutkimuksessa voidaan myös tarvittaessa esittää, millä tasolla kyberturvallisuuden tietämyksen kuuluisi olla. Kyberturvallisuuden tietämys voi olla riittämätöntä tietyillä osa-alueilla. Merenkulussa kuuluisi olla kyberturvallisuuden tietämys hyvällä tasolla, jotta kyberhyökkäyksiin voitaisiin varautua tarpeen mukaan.

Opinnäytetyön aineiston perusteella tutkitaan merenkulun kyberturvallisuuden haavoittuvuuksien merkitystä. Haavoittuvuuksien merkityksellä esitetään, minkälaisia haavoittuvuuksia merenkulun kyberturvallisuudessa on ja miten niitä voitaisiin ennaltaehkäistä. Tähän kuuluu myös mahdolliset ongelmat merenkulun kyberturvallisuudessa. Tässä tutkimuksessa selvitetään, mitä kyberturvallisuuden haavoittuvuuksia merenkulun opiskelijat ovat huomanneet merenkulussa. Tämän tutkimuksen avulla myös havainnollistetaan merenkulun opiskelijoiden oma suhtautumisen ja käyttäytyminen kyberturvallisuuteen.

2.2 Tutkimusote

Tutkimusotteena käytetään kvalitatiivisen ja kvantitatiivisen otteen yhdistelmää. Opinnäytetyö on tapaustutkimus, jonka tarkoituksena on selvittää merenkulun opiskelijoiden kyberturvallisuuden tietämyksen taso verkkokyselyn avulla. Tässä myös tutkitaan mitä näkemyksiä ja mielipiteitä merenkulun opiskelijoilla on kyberturvallisuudesta. Verkkokyselyssä kysytään olennaisia kysymyksiä kyberturvallisuudesta ja sen haavoittuvuuksista. Verkkokyselyn tuloksia analysoidaan ja vertaillaan, jonka lisäksi aineistoa kerätään sekundääriaineistoa erilaisten dokumenttien kautta. Kysely toimii primäärisenä aineistonkeruumenetelmänä ja dokumentit sekundäärisenä aineistonkeruumenetelmänä. (Kananen 2019, 29). Dokumentteihin kuuluu erilaiset tutkimukset, tilastot, artikkelit ja käytännöt.

Tähän tutkimukseen kerätään kattava sekundääriaineisto, jonka jälkeen kootaan primääriaineisto. Sekundääriaineisto koostuu verkossa olevista lähteistä, jotka ovat tarpeeksi luotettavia. Lähteiden luotettavuus arvioidaan siten, että kuka on aineiston laatinut ja mihin tarkoitukseen. Tässä myös tarkastetaan, mitä aineistoa tekijä on aikaisemmin luonut ja kuinka tunnettu tekijä on. Tämän lisäksi katsotaan, mihin aineisto on julkaistu. Sekundääriaineisto koostuu pääosin tutkimuksista, artikkeleista ja käytännöistä. Sekundääriaineiston sisältö liittyy merenkulun kyberturvallisuuteen ja sen haavoittuvuuksiin. Tähän kuuluvat muun muassa merenkulun alusten järjestelmät, merenkulun kyberhyökkäykset ja kyberhyökkäyksien ennaltaehkäisy merenkulussa. Aiheet ovat oleellisia opinnäytetyön kanssa ja aineistoa pyritään etsimään mahdolli-

simman tuoreista lähteistä. Sekundääriaineiston avulla saadaan myös syvempi käsitys aiheesta, ja sekundääriaineistoa hyödynnetään tutkimuskysymyksissä.

Primääriainesto koostuu verkkokyselyn vastauksista ja sen avulla vastataan tutkimusongelmaan. Verkkokyselyn vastauksia analysoidaan vertaamalla sen tuloksia sekundääriaineistoon. Tämän avulla voidaan huomata merenkulun kyberturvallisuuden näkemyksien eroja. Tämän lisäksi voidaan todeta, minkälaisia haavoittuvuuksia ja kyberhyökkäyksiä on huomattu merenkulun alalla opiskelijoiden ja ammattilaisten näkökulmasta.

Tässä tutkimuksessa käytetään määrällisiä ja laadullisia analyysimenetelmiä. Määrällinen analyysimenetelmä perustuu ilmiöiden esiintymiseen tilastojen avulla ja laadullinen analyysimenetelmä perustuu kohteen ymmärtämiseen kokonaisvaltaisesti. (Koppa 2021). Määrällistä analyysimenetelmää käytetään primääriaineiston ja sekundääriaineiston tuloksissa. Tuloksilla esitetään numeroita ja tilastoja, joiden avulla voidaan todeta miten tietyt ilmiöt syntyvät. Laadullista analyysimenetelmää hyödynnetään merenkulun opiskelijoiden ja merenkulun ammattilaisten näkemyksissä. Sillä voidaan todeta merenkulun kyberturvallisuuden haavoittuvuuksien esiintymisympäristö ja merkitys.

Tutkimisotteen yhdistelmä valittiin, koska se soveltuu tapaustutkimukseen ja tutkimusaineisto on monilähteistä. Lisäksi tutkittavien henkilöiden näkökulmat otetaan huomioon ja kyselyssä yleistetään vastauksia. Kyselyn tuloksia ja dokumentteja analysoidaan ja vertaillaan määrällisillä sekä laadullisilla menetelmillä, jotka ovat sisällönanalyysi ja suorat jakaumat. (Kananen 2019, 28, 76.) Tämän tutkimuksen monilähteiseen tutkimusaineistoon kuuluu taulukoita, kuvia, luetteloita, tilastoja ja tekstiä. Monilähteisellä tutkimusaineistolla pyritään dokumentoida tämä tutkimus mahdollisimman perusteellisesti ja tarpeellisesti.

2.3 Tutkimuskysymykset

Tutkimusotteen perusteella kerätään aineisto, jonka avulla vastataan tutkimuskysymyksiin. Tutkimuskysymyksillä avataan aihetta enemmän ja vastataan tutkimusongelmaan. Tutkimuskysymykset ovat laadittu opinnäytetyön kokonaisuuden mukaan. Tutkimuskysymykset ovat listattuna alla olevaan luetteloon:

- Mitkä tekijät luovat merenkulun kyberturvallisuuden haavoittuvuuksia?
- Miksi kyberturvallisuus on tärkeää merenkulussa?
- Miten kyberturvallisuuden haavoittuvuuksia voidaan ennaltaehkäistä merenkulussa?
- Millainen merenkulun opiskelijoiden kyberturvallisuuden tietämyksen taso on?

Merenkulun kyberturvallisuuden haavoittuvuudet syntyvät tekijöistä, joita selvitetään ensimmäisessä tutkimuskysymyksessä. Tässä tutkitaan, mitkä tekijät ovat kyseessä, ja miten ne luovat merenkulun kyberturvallisuuden haavoittuvuuksia. Tekijät voivat olla teknologisia tekijöitä ja inhimillisiä tekijöitä. Teknologiset ja inhimilliset tekijät voivat liittyä paljon toisiinsa kyberturvallisuuden haavoittuvuuksien syntymisessä. Haavoittuvuudet mahdollistavat kyberhyökkäykset merenkulun aluksiin, jonka seuraukset voivat olla kohtalokkaat.

Toisessa tutkimuskysymyksessä vastataan siihen, miksi kyberturvallisuus on tärkeää merenkulussa. Merenkulun kyberturvallisuuden tärkeydellä esitetään asioita, jotka näyttävät sen, miksi kyberturvallisuuteen tarvitsee kiinnittää huomiota merenkulussa. Tässä osiossa esitetään alusten erilaisia järjestelmiä ja niiden käyttötarkoituksia. Niiden avulla kerrotaan, miten laajasti kyberturvallisuus voi ulottua merenkulun aluksissa. Merenkulun kyberhyökkäyksillä voidaan esittää hyökkäysten vaikutuksen merenkulussa. Tähän voi kuulua erilaisten merenkulun kyberhyökkäysten seuraukset ja niiden tilastot. Kyberhyökkäysten esittämisen avulla saadaan kerättyä vaikuttavia hyökkäyksiä merenkulun alalla, jotka näyttävät tilanteen vakavuuden. Näiden mukaan kerrotaan, mitä kyberhyökkäysten tapauksissa voi käydä merenkulussa.

Kolmannessa tutkimuskysymyksessä vastataan siihen, miten merenkulun kyberturvallisuuden haavoittuvuuksia voitaisiin ennaltaehkäistä. Haavoittuvuuksien ennaltaehkäisemisellä esitetään käytäntöjä ja ohjeistuksia, miten kyberhyökkäyksiltä tulisi suojautua merenkulussa. Kyberhyökkäykset voivat olla hyvin vaihtelevia, jolloin käytännöillä pyritään ehkäisemään monia erilaisia hyökkäyksiä.

Viimeisessä tutkimuskysymyksessä selvitetään, millä tasolla merenkulun opiskelijoiden tietämys on kyberturvallisuudesta. Tämän mukaan voidaan selvittää, onko opiskelijoiden kyberturvallisuuden tietämyksessä parannettavaa ja mitä näkemyksiä heillä on merenkulun kyberturvallisuudesta. Tutkimuksen aineiston avulla ja kyselylomakkeen tuloksilla saadaan vastattua tämän tutkimuksen tutkimuskysymyksiin.

3 TEOREETTINEN VIITEKEHYS

Teoreettisessa viitekehyksessä käsitellään kyberturvallisuuden käsitteitä, merenkulun kyberturvallisuutta ja merenkulun kyberturvallisuuden aikaisempia tutkimuksia. Kyberturvallisuuden käsitteissä kerrotaan, mitä käsitteitä opinnäytetyössä käytetään ja mikä kyseisten käsitteiden tarkoitus on. Kyberturvallisuuden käsitteet voivat olla ilmiselviä joillekin, mutta on tärkeää kertoa, mitä kyseiset käsitteet tarkoittavat. Opinnäytetyöhön kerätään erilaisia dokumentteja ja tutkimuksia merenkulun kyberturvallisuudesta. Dokumenttien avulla kerrotaan, mitä aineistoa merenkulun kyberturvallisuudesta on luotu, ja mikä sen merkitys on ollut. Merenkulun kyberturvallisuuden tutkimuksissa selvitetään tutkimusten tarkoitusta ja niiden lopputulosta. Tutkimuksien lopputuloksia verrataan tämän tutkimuksen lopputuloksiin.

Tässä opinnäytetyössä perehdytään olemassa olevaan materiaaliin syvällisesti ja tutkitaan minkälaista materiaalia aiheesta on luotu. Aikaisemmalla materiaalilla ja aineistolla pyritään täydentämään tätä opinnäytetyötä käyttämällä hyödyksi tutkimustuloksia ja teorioita. On tärkeää valita, mitä tutkimuksia ja teorioita ottaa mukaan tähän opinnäytetyöhön. Aikaisempien tutkimusten kuuluisi olla oleellisia tämän opinnäytetyön tutkimusongelman kanssa. (Kananen 2019, 97.)

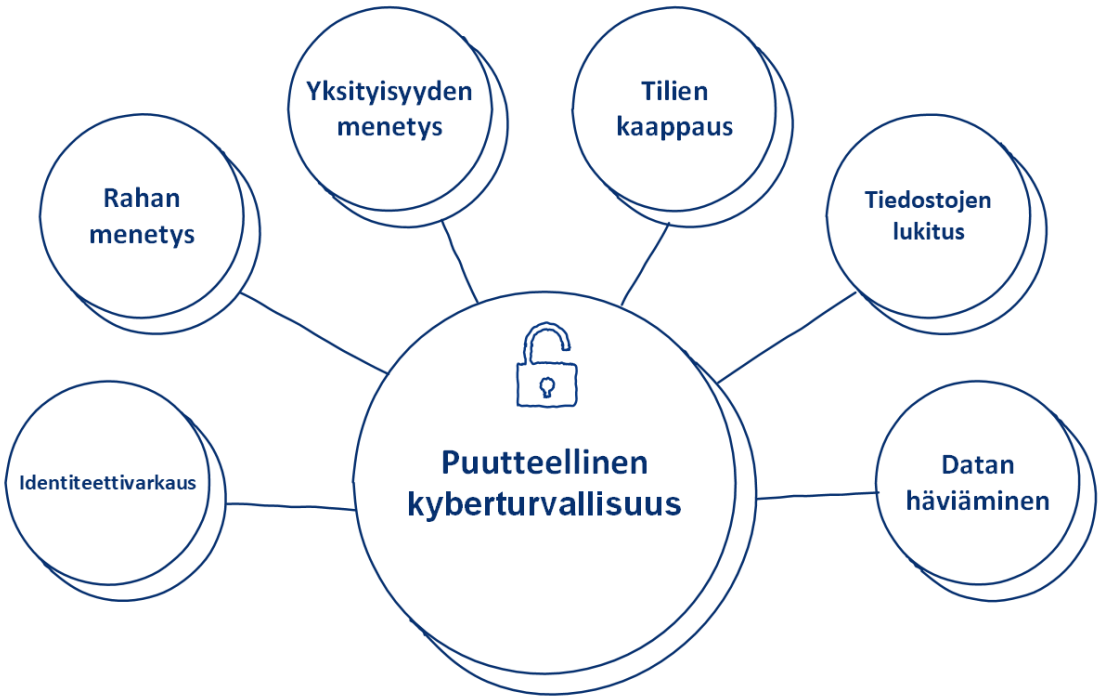
3.1 Kyberturvallisuuden käsitteet

Opinnäytetyössä käytetään tiettyjä kyberturvallisuuden käsitteitä, joiden tarkoitus on tärkeä tietää. Siksi pitää kertoa, mitä kyseisillä käsitteillä tarkoitetaan ja miksi ne ovat oleellisia opinnäytetyössä. Tällä varmistetaan se, että käsitteet eivät jää epäselviksi ja ymmärretään opinnäytetyön kokonaisuus. Käsitteet ovat kyberturvallisuus, haavoittuvuudet, kyberhyökkäykset, riskit ja IT- sekä

OT-järjestelmät. Kyseisiä käsitteitä käytetään runsaasti opinnäytetyössä, ja ne liittyvät paljon toisiinsa.

3.1.1 Kyberturvallisuus

Kyberturvallisuudella tarkoitetaan esimerkiksi laitteiden ja tietojen turvaamista erilaisilla menetelmillä. Menetelmiin kuuluu esimerkiksi virusten torjunta, pääsyoikeuksien hallinta, vahvat salasanat, päivitykset ja turvalliset konfiguroinnit. (F-Secure s.a.) Kyseisillä menetelmillä voidaan suojata tärkeitä tietoja, erilaisia järjestelmiä, päätelaitteita ja verkkoyhteyksiä. Kyberturvallisuus alkaa olemaan entistä tärkeämpää nykypäivänä, kun teknologia kehittyy. Kyberturvallisuuden tulisi olla myös riittävää merenkulussa, jotta eri alusten järjestelmiä pystyttäisiin suojaamaan ja kyberhyökkäyksiin voitaisiin varautua.



Kuva 1 Puutteellisen kyberturvallisuuden mahdolliset vaikutukset (F-secure s.a)

Kuva 1 osoittaa puutteellisen kyberturvallisuuden mahdollisia vaikutuksia. Puutteellisen kyberturvallisuuden seurauksena voidaan menettää monia eri asioita kuten dataa, rahaa ja omaa yksityisyyttä. Puutteellinen kyberturvallisuus voi mahdollistaa muun muassa identiteettivarkauksia, tiedostojen lukituksia ja tilien kaappauksia. (F-Secure s.a.) Merenkulussa puutteellinen kyberturvallisuus voi tulla ilmi merenkulun alusten järjestelmien suojaamattomuudesta tai merenkulun organisaatioiden suhtautumisesta kyberturvallisuuteen.

3.1.2 Haavoittuvuudet

Haavoittuvuudet ovat heikkouksia esimerkiksi järjestelmissä, sovelluksissa, laitteissa ja prosesseissa. Nämä heikkoudet mahdollistavat erilaiset hyökkäykset, jolla voidaan aiheuttaa vahinkoa. (Liikenne- ja viestintävirasto Traficom 2020.) Heikkoukset voivat olla esimerkiksi vanhat käyttöjärjestelmät, vanhat sovellukset, puutteellinen konfigurointi ja heikot salasanat. Kyberturvallisuuden haavoittuvuudet voivat syntyä eri tekijöistä merenkulussa ja niiden vaikutukset voivat olla hyvin laajoja.

Haavoittuvuuksista tulisi ilmoittaa eteenpäin, jos niitä huomataan eri organisaatioissa. Tähän voi kuulua prosesseja ja käytäntöjä, jonka kautta haavoittuvuudet tulisivat tietyille tahoille tietoon. Haavoittuvuuksien ilmoittamiseen voi kuulua erilaisia ilmoitusprosesseja. Ilmoitusprosesseihin kuuluu esimerkiksi bug bounty -ohjelma, vastuullisen julkaisun periaate ja security.txt-tiedosto. Bug bounty -ohjelma voi olla eri organisaatoilla, laitevalmistajilla tai internetsivustoilla käytössä. Bug bounty -ohjelma tarjoaa korvausta niille tahoille, jotka löytävät haavoittuvuuksia ja ilmoittavat niistä eteenpäin ohjelman kautta. Vastuullisen julkaisun periaatteella haavoittuvuus tulisi ilmoittaa virallisen kanavan kautta mahdollisimman ajoissa ja luottamuksellisesti. Organisaatioilla voi olla myös käytössä security.txt-tiedosto, joka voi sisältää yhteistietoja ja ohjeita haavoittuvuuksien ilmoittamisesta. (Liikenne- ja viestintävirasto Traficom 2020a.)

Merenkulun organisaatioissa ilmoitusprosessit voivat vaihdella organisaation mukaan. Voi olla myös mahdollista, että merenkulun organisaatiolla ei ole minkäänlaista ilmoitusprosessia käytössä. Tähän voi olla syynä se, että organisaatio ei ole tietoinen haavoittuvuuksien ilmoittamisesta tai ei näe sitä tarpeellisena.

3.1.3 Kyberhyökkäykset

Kyberhyökkäyksillä tarkoitetaan erilaisia hyökkäyksiä digitaalisessa ympäristössä, kuten tietojen varastaminen ja järjestelmien lamaannuttaminen tai tuhoaminen. (Mäkelä 2022). Kyberhyökkäysten motivaationa voi olla esimerkiksi raha, vahingon luominen, poliittinen vaikutus tai tiedon kerääminen. Näiden

perusteella kyberhyökkäyksiä voi tehdä esimerkiksi yksittäinen henkilö, ryhmä tai valtio. Kyberhyökkäyksen tekijän tunnistaminen voi olla kuitenkin haastavaa, jos tekijä peittää hyvin jälkensä esimerkiksi reitittämällä kyberhyökkäyksen tai tahallaan harhauttamalla (Sisäministeriö s.a). Kyberhyökkäykset voivat kohdistua moneen erilaiseen kohteeseen ja niiden vaikutus voi olla vaihteleva. Merenkulussa kyberhyökkäykset voivat kohdistua esimerkiksi merenkulun alusten eri järjestelmiin. Teknologian kehittyessä kyberhyökkäykset voivat myös mahdollisesti yleistyä.

Kyberhyökkäyksien takana voi olla muun muassa aktivistit, rikolliset, opportunistit tai valtiot. Aktivistien motiivina voi olla maineen tuhoaminen tai tietynlaisen toiminnan keskeyttäminen. Aktivistit pyrkivät mahdollisesti vaikuttamaan organisaation toimintaan. Rikollisten motiivina voi olla rahallinen hyöty tai organisaatioiden vakoilu. Vakoilun myötä voidaan saada esimerkiksi arkaluontoista tietoa organisaatiosta. Opportunistit pyrkivät tunkeutua organisaatioihin haastamalla itseään. Tämä voi olla esimerkiksi erilaisten kyberturvallisuuden haavoittuvuuksien löytäminen. Valtioiden motiivina on usein poliittinen vaikutus tai vakoilu, joka on mahdollisesti kohdistettu toisin valtioihin. (Tuulaniemi 2020, 3.)

3.1.4 Riskit

Riskeillä tarkoitetaan tiettyjen tapahtumien ja niiden seurauksien mahdollisuutta. Nämä ovat yleensä negatiivisia tapahtumia, joista voi syntyä haittaa. Riskit voivat olla myös myönteisiä mahdollisuuksia. (Turvallisuuskomitea 2018, 11.) Riskejä voi syntyä monesta eri syystä kyberturvallisuudessa ja haavoittuvuudet voivat olla yksi syy niiden syntymiseen. Riskejä voi hallita riskienhallintaprosessilla. Tähän kuuluu esimerkiksi riskien tunnistaminen ja riskianalyysi.

Riskienhallinnan ja riskianalyysin avulla pyritään tunnistamaan organisaatioon kohdistuvia uhkia, jotka vaikuttavat mahdollisesti organisaation toimintatapaan. Riskianalyysissa pyritään arvioimaan riskien todennäköisyys ja niiden suuruus. Tämän lisäksi riskianalyysissa tunnistetaan riskien ennaltaehkäisyjen tapoja ja seurataan niiden toteutusta. Riskienhallinnassa käydään myös läpi

se, että miten kuuluisi toimia vahingon sattuessa ja miten vahingoista voidaan toipua. (Luvat ja valvonta s.a.)

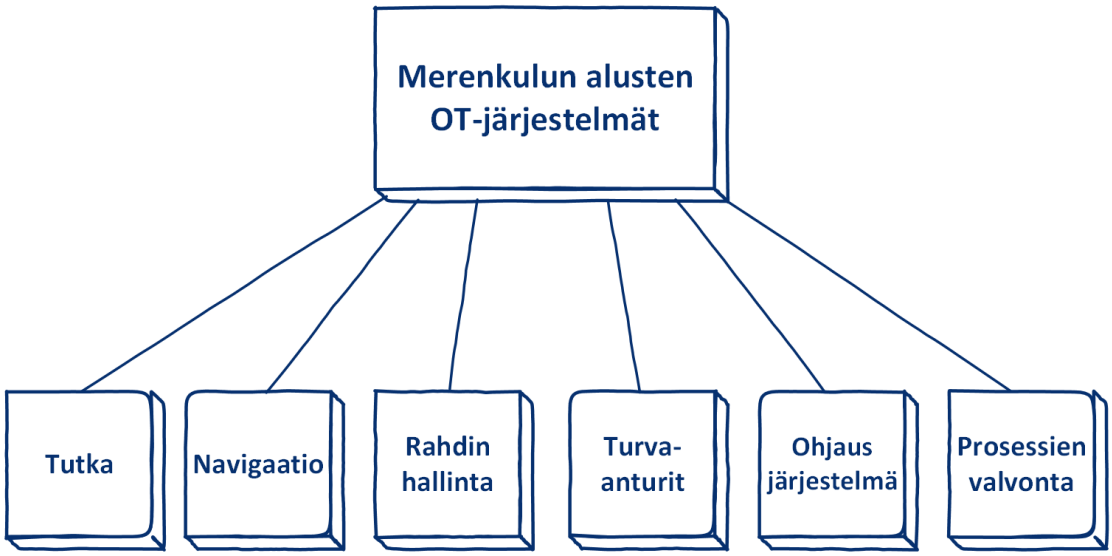
Tapahtuman todennäköisyys	Seurausten vakavuus		
	1. Vähäiset	2. Haitalliset	3. Vakavat
1. Epätodennäköinen	1. Merkityksetön riski	2. Vähäinen riski	3. Kohtalainen riski
2. Mahdollinen	2. Vähäinen riski	3. Kohtalainen riski	4. Merkittävä riski
3. Todennäköinen	3. Kohtalainen riski	4. Merkittävä riski	5. Sietämätön riski

Kuva 2 Esimerkki riskimatriisista (Työturvallisuuspakki s.a.)

Kuva 2 näyttää esimerkin riskimatriisista, jota voidaan hyödyntää riskianalyysissa. Riskimatriisilla pyritään luokittelemaan uhkia niiden todennäköisyyden ja vakavuuden mukaan. Kuvan 2 merkityksetön riski voi olla epätodennäköinen ja sen seuraukset voivat olla vähäiset, kun taas sietämättömällä riskillä tapahtuma voi olla todennäköinen ja sen seuraukset voivat olla vakavat. Riskimatriisin avulla voidaan tunnistaa, minkälaisiin riskeihin kannattaisi kiinnittää huomiota organisaatiossa. Merenkulussa riskimatriisia voidaan esimerkiksi hyödyntää merenkulun organisaatioissa. Riskimatriisin avulla voitaisiin tunnistaa kyberturvallisuuden uhkia aluksissa.

3.1.5 IT- ja OT-järjestelmät

Merenkulussa käytetään monia eri järjestelmiä, jotka kuuluvat tietotekniikan järjestelmiin ja operatiivisen tekniikan järjestelmiin. Tietotekniikalla tarkoitetaan IT-järjestelmiä ja operatiivisella tekniikalla OT-järjestelmiä. IT-järjestelmät ovat sovelluksia ja laitteita, joiden tarkoitus on tuottaa ja käsitellä tietoa eri kanavien kautta. IT-järjestelmiin voi kuulua esimerkiksi tietokoneet, palvelimet, tietokannat ja verkot. OT-järjestelmät hallitsevat alusten laitteita ja sovelluksia, jotka vaikuttavat aluksen toimintaan. (eDOTSolutions 2020, 4–5.)



Kuva 3 Merenkulun aluksiin kuuluvia OT-järjestelmiä (eDOTSolutions, 5)

Kuva 3 osoittaa merenkulun aluksissa olevia OT-järjestelmiä. Kuvasta 3 huomaa, kuinka laajasti OT-järjestelmät vaikuttavat merenkulun aluksissa. Kyseisiä OT-järjestelmiä kuuluisi suojata tarpeen mukaan, jotta kyberhyökkäyksiä voitaisiin ennaltaehkäistä järjestelmissä. OT-järjestelmät eivät ole kuitenkaan välttämättä tarpeeksi suojattuja ja ne voivat käyttää vielä vanhaa teknologiaa. OT-järjestelmissä voi olla myös rajoitteita, jonka takia kyseisiä järjestelmiä ei voida päivittää tai suojata tarpeeksi.

Merenkulussa OT-järjestelmiin tulisi kiinnittää huomiota, koska OT-järjestelmien kyberhyökkäykset uhkaavat fyysistä turvallisuutta ja infrastruktuuria. IT- ja OT-järjestelmien kyberturvallisuuden tarve kasvaa myös kyberhyökkäyksien yleistyessä merenkulussa. Merenkulun ala reagoi kunnollisen kyberturvallisuuden tarpeeseen, mutta ei ole välttämättä valmistautunut kyberturvallisuuden uhkiin. OT-järjestelmien kyberturvallisuuden ongelmat kasvavat, kun OT-järjestelmien hyökkäyspinta laajenee järjestelmien yhteyksien kasvaessa. OT-järjestelmät voivat olla aiempaa enemmän yhdistettynä verkkoon ja muihin järjestelmiin. Tämä tuo ongelmia kuten kyberturvallisuuden haavoittuvuuksien nopeampi leviäminen ja riskien kasvaminen. Merenkulussa voi olla myös tapauksia, joissa organisaatioiden on pakko yhdistää OT-järjestelmiä verkkoon. (DNV 2023, 10, 14, 20.)

3.2 Merenkulun kyberturvallisuus

Tässä luvussa perehdytään siihen, mitä materiaalia merenkulun kyberturvallisuudesta on aikaisemmin luotu, ja miten sitä voidaan hyödyntää tässä opinnäytetyössä. Se on pohja opinnäytetyölle, joka kertoo tarkemmin aineiston merkityksen. Eri tahot ovat luoneet aiheesta dokumentteja, jotka ovat julkaistu vuosina 2020–2023. Kyseisiin tahoihin kuuluu IMO, ICS, DNV ja huoltovarmuusorganisaatio. Dokumentit keskittyvät merenkulun kyberturvallisuuteen, johon kuuluu ohjeita, käytäntöjä ja raportteja.

IMO eli International Maritime Organization on yhdistyneiden kansakuntien luoma järjestö, joka keskittyy kansainvälisen merenkulun turvallisuuteen ja pyrkii estämään alusten tuottamaa saastetta. Siihen kuuluu 175 jäsentä, jotka koostuvat erilaisista organisaatioista ja valtioista. (International Maritime Organization s.a.) International Maritime Organization on päivittänyt vuonna 2022 ohjeet merenkulun kyberturvallisuuden riskienhallinnasta nimellä ”Guidelines on Maritime Cyber Risk Management”. Se on 6-sivuinen dokumentti, jossa listataan suosituksia kyberturvallisuuden riskienhallinnasta merenkulussa. Dokumentissa mainitaan, että riskienhallinta on olennainen osa turvallista ja suojattua merenkulun toimintaa. Kyseisiä suosituksia voidaan integroida olemassa oleviin riskienhallintaprosesseihin ja niillä tähdätään turvallisempaan merenkulun kyberturvallisuuteen. (International Maritime Organization 2022, 1.)

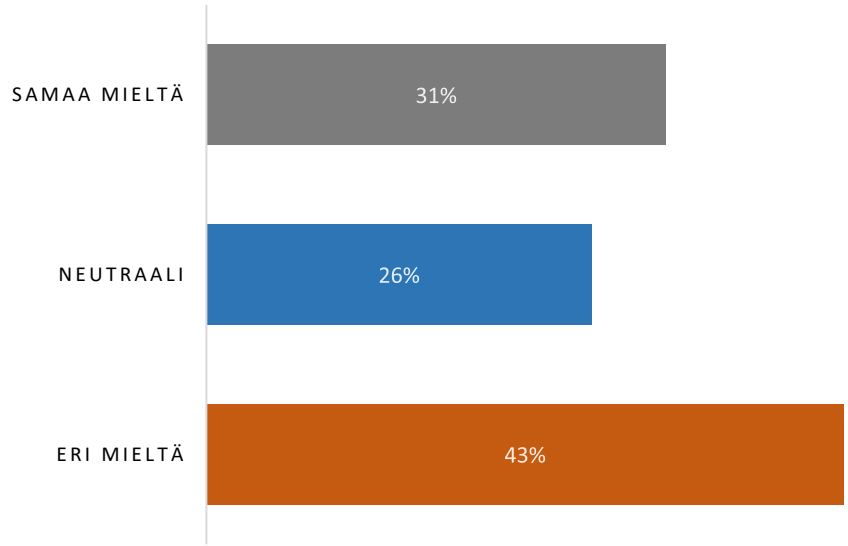
ICS eli International Chamber of Shipping on kansainvälinen kauppayhdistys, joka sisältää jäseniä 40:stä eri maasta. ICS edustaa erilaisia laivanomistajia, johon voi kuulua esimerkiksi matkustajalaivoja, öljytankkereita, konttilaivoja ja rahtilaivoja. ICS on luonut vuonna 2022 dokumentin ‘The guidelines on Cyber Security Onboard Ships’. Tämä dokumentti käy syvällisesti läpi merenkulun kyberturvallisuuden käytäntöjä. Siinä ohjeistetaan miten kyberturvallisuuden riskit tulisi käsitellä ja minkälaisia haavoittuvuuksia on kyseessä. Osa-alueisiin kuuluu muun muassa kyberturvallisuus ja riskienhallinta, uhkien ja haavoittuvuuksien tunnistaminen, riskien arviointi sekä palautuminen kyberhyökkäyksistä. Dokumentti on 61 sivua pitkä ja se on luotu monen eri organisaation ja yhdistyksen avulla. (International Chamber of Shipping. s.a.)

DNV on julkaissut 2023 raportin ‘Maritime Cyber Priority 2023: Staying secure in an era of connectivity’. Raportissa on luotu kysely, jossa on ollut mukana yli 800 merenkulun ammattilaista eri organisaatioista. Tähän on myös kuulunut syvällisiä haastatteluja merenkulun asiantuntijoiden kanssa. (DNV 2023, 2.) Kyselyssä on kysytty erilaisia kysymyksiä merenkulun kyberturvallisuudesta. Näiden tulosten avulla nähdään merenkulun ammattilaisten näkemykset merenkulun kyberturvallisuudesta ja sen puutteista. Merenkulun ammattilaisten näkemyksiä voidaan vertailla Xamkin merenkulun opiskelijoiden näkemysten kanssa. Tämän avulla voidaan huomata mitä eroja merenkulun ammattilaisilla on merenkulun opiskelijoiden kanssa. Merenkulun ammattilaisten tulokset ja kysymykset ovat käännetty suoralla lainauksella DNV:n raportin mukaan.

Kuva 4 ”Mitkä ovat organisaatiosi kyberturvallisuuden suurimmat haasteet kyberriskien hallitsemisessa (valitse kolme tärkeintä)?” (DNV 2023, 29)

Kuvaan 4 on kerätty DNV:n kyselyn kysymysten tuloksia. Kuvan 4 mukaan huomaa, että merenkulun ammattilaisten mielestä suurimpana haasteena on kyberturvallisuuden riittämätön budjetti ja resurssit. Moni asia voi vaikuttaa toi-

siinsa kyberturvallisuuden haasteissa. Esimerkiksi budjetti voi vaikuttaa koulutukseen ja taitojen puutteeseen miehistössä, sekä tietoturva-asiantuntijoiden puutteeseen. Mainitut haasteet voivat olla myös osallisena haavoittuvuuksien syntymiseen merenkulun kyberturvallisuudessa. Moni näistä haasteista liittyy myös kyberturvallisuuden osaamiseen ja tietämykseen. Kyberturvallisuuden osaaminen ja tietämys voi olla puutteellista monen merenkulun ammattilaisen mielestä.



Kuva 5 ”Minkä verran olet samaa tai eri mieltä lauseen kanssa?”
”Merenkulun organisaatiot jakavat hyvin tietoa ja koulutuksia kyberturvallisuuden riskeistä, uhista ja poikkeamista muiden alan toimijoiden kanssa.” (DNV 2023, 35)

Kuva 5 näyttää, että 43 % vastanneista oli eri mieltä lauseesta ”Merenkulun organisaatiot jakavat hyvin tietoa ja koulutuksia kyberturvallisuuden riskeistä, uhista ja poikkeamista muiden alan toimijoiden kanssa.” Tästä huomaa, että merenkulun organisaatiot eivät välttämättä jaa hyvin tietoa tai koulutuksia osan merenkulun ammattilaisten mielestä. Osuus on melko suuri, joka osoittaa, että kyberturvallisuuden tiedon jakamisessa tai koulutuksissa on mahdollisesti puutteita. Kyberturvallisuuden haasteet voivat myös vaikuttaa tuloksiin ja merenkulun ammattilaisten kokemus.

Huoltovarmuusorganisaatio perustuu huoltovarmuuskeskuksen (HVK) sekä sen hallituksen ja eri toimialojen mukaan. Se pyrkii turvaamaan Suomen huoltovarmuuden sekä sen toimintakyvyn. Huoltovarmuudella tarkoitetaan varautumista erilaisiin kriiseihin ja häiriötilanteisiin. (Huoltovarmuuskeskus. s.a.) Huoltovarmuusorganisaatio on laatinut merenkulun kyberturvallisuudesta alus-

ten parhaat käytännöt, jossa esitetään alusten eri järjestelmät ja niiden kybertuvallisuuden suojauksen. Luvut koostuvat verkkojen segmentoinnista, haittaohjelmien torjunnasta, palomuurien määrittämisestä sekä järjestelmien tietoturvakonfiguroinnista.

Merenkulun kyberturvallisuus on alkanut olemaan tärkeämpi asia, jonka takia kyseisiä käytäntöjä ja ohjeistuksia on luotu. Käytäntöjen ja ohjeiden avulla huomataan, miksi ne on luotu ja mihin tarkoitukseen. Opinnäytetyössä hyödynnetään näitä käytäntöjä ja ohjeita tutustumalla aiheeseen syvemmin, jonka avulla vastataan opinnäytetyön tutkimuskysymyksiin.

3.3 Aikaisemmat tutkimukset

Tässä luvussa tarkastellaan aikaisempia tutkimuksia liittyen merenkulun kyberturvallisuuteen. Tässä esitetään, mitä kyseisissä tutkimuksissa on tutkittu, ja mitä niissä on saatu lopputulokseksi. Näitä tutkimuksia käytetään ulkopuolisina lähteinä. Ulkopuolisten lähteiden avulla olisi tarkoitus samanlaisiin tuloksiin ja hakemaan vahvistusta tähän tutkimukseen (Kananen 2019, 34). Merenkulun kyberturvallisuudesta on luotu tutkimuksia, jotka keskittyvät eri alueisiin. Tähän kuuluu esimerkiksi kyberhyökkäykset, riskit, haavoittuvuudet ja niiden vaikutukset. Tutkimukset ovat julkaistu vuosina 2021–2022.

Vesa Tuomala on julkaissut vuonna 2021 tutkimuksen ”Maritime Cybersecurity. Before the risks turn into attacks”. Tutkimus kuuluu GET READY -projektiin, jossa on selvitetty merenkulun ja logistiikan digitoinnin vaikutuksista. Tuomala (2021, 5) mainitsee, että GET READY -projektin tavoitteena on löytää parhaita käytäntöjä merenkulun alalla, jonka kautta pyritään estämään kyberhyökkäyksiä. Projektissa myös halutaan saada näkyvyyttä kyberturvallisuuteen merenkulun alalla. Tutkimuksessa vastataan kysymykseen ”Mitä tehdä ennen kuin riskit muuttuvat hyökkäyksiksi merenkulun kyberturvallisuudessa?” Kysymykseen vastataan perehtymällä muun muassa kyberturvallisuuden hyökkäyksiin, merenkulun järjestelmin ja kyberturvallisuuden käytäntöihin. Tähän kuuluvat IT-, OT- ja ICS-järjestelmät sekä kyberhyökkäysten ehkäisy erilaisilla menetelmillä. Tutkimuksen lopputuloksena tultiin siihen, että kyberhyökkäykset kasvavat todennäköisesti tulevaisuudessa. Kyberturvallisuu-

den kouluttaminen aluksissa sekä organisaatioissa ehkäisee erilaisia kyberhyökkäyksiä ja haavoittuvuuksia. Sen jälkeen myös todettiin, että tietoturvapoikkeamat ja erilaiset kyberhyökkäykset lisäävät riskejä aluksissa, jolloin ne uhkaavat alusten turvallisuutta ja tietoturvaa. (Tuomala 2021, 30.)

Xamkin merenkulun opiskelijoiden tulisi valmistautua merenkulun kyberhyökkäyksien kasvuun. Merenkulun opiskelijat voisivat hyödyntää Vesa Tuomalan tutkimusta, jonka avulla he voisivat tunnistaa kyberturvallisuuden riskejä merenkulussa. Tämän lisäksi opiskelijoiden olisi hyödyllistä osallistua kyberturvallisuuden koulutuksiin merenkulussa, joiden avulla voitaisiin ehkäistä merenkulun kyberturvallisuuden haavoittuvuuksia tulevaisuudessa.

Meland ym. (2021) ovat tutkineet yksityiskohtaisesti merenkulun kyberhyökkäyksiä vuosina 2010–2020. He ovat luoneet raportin ‘A Retrospective Analysis of Maritime Cyber Security Incidents’. Raportissa tapaukset ovat onnistuneita kyberhyökkäyksiä merenkulussa, joihin ei lasketa pienempiä hyökkäyksiä tai hyökkäysyrityksiä. Nämä ovat vaikuttaneet huomattavasti eri osa-alueisiin merenkulussa. Osa-alueet ovat eri hyökkäyspisteitä aluksissa ja erillisiä ulkopuolisia järjestelmiä. Hyökkäyspisteillä tarkoitetaan kohteita, joita halutaan suojata aluksissa ja sen ulkopuolella. Analyysissa on listattuna kyberhyökkäykset vuoden ja hyökkäyksen mukaan. Tähän kuuluu myös hyökkäyspisteen kohdistuminen. Kyberhyökkäyksiä on kerätty yhteensä 46 kappaletta ympäri maailmaa, jotka ovat hyvin vaihtelevia. Osissa hyökkäyksissä on ollut esimerkiksi kiristyshaittaohjelma osallisena ja toisissa tietojen varastaminen tai paikannusjärjestelmän häiritseminen. Tutkimuksen lopputuloksena he totesivat, että merenkulussa ei ole ollut valtavasti kyberhyökkäyksiä, mutta niillä on ollut hyvin vakavia seurauksia. Kyberhyökkäykset voivat tulla kalliiksi ja aiheesta ei ole tarpeeksi tietoa tai se on puutteellista. (Meland ym. 2021, 520, 528.)

Melandin ym. (2021) koottuja kyberhyökkäyksiä voidaan hyödyntää tässä opinnäytetyössä. Näitä merenkulun kyberhyökkäyksiä voidaan esittää ja kertoa, kuinka erilaisia kyberhyökkäykset voivat olla, ja minkälaisia vaikutuksia hyökkäyksillä on ollut. Tämän lisäksi voidaan tutkia, onko merenkulun kyberhyökkäyksistä tarpeeksi tietoa ja onko se luotettavaa.

Jesse Jaakkola ja Lari Juonala julkaisivat vuonna 2022 opinnäytetyön ”Merenkulun kyberturvallisuus ja kyberhyökkäysten vaikutus kansainväliseen kauppaan”. Opinnäytetyössä tutkittiin, mitä vaikutuksia kyberhyökkäyksillä on kansainvälisessä kaupassa ja kyberturvallisuutta yleisesti merenkulussa. Jaakkola ja Juonala (2022) kertovat, että he haastattelivat kahta merenkulkualan asiantuntijaa. Heidän avullansa selvitettiin, minkälaisia kyberhyökkäyksiä suomalaisiin varustamoihin on tehty ja mitä vaikutuksia sillä on ollut. Haastattelun asiantuntijat olivat osana Finnlines Oyj:tä ja Suomen Varustamot Ry:tä. Heidän lopputuloksenansa oli se, että automaatio lisää riskiä kyberhyökkäyksille ja kyberhyökkäykset kehittyvät vuosien kuluessa. Tämän perusteella he totesivat, että kyberhyökkäykset vaikuttavat suuresti myös kansainväliseen kaupankäyntiin.

Tässä tutkimuksessa voidaan myös vertailla suomalaisten merenkulkualan asiantuntijoiden näkemyksiä Xamkin merenkulun opiskelijoiden kanssa. Lisäksi voidaan tutkia kehittyvätkö kyberhyökkäykset tulevaisuudessa ja miten niihin pitäisi varautua.

4 KYBERTURVALLISUUDEN HAAVOITTUVUUKSIEN SYNTYMINEN

Merenkulun kyberturvallisuuden haavoittuvuuksia voi syntyä monesta eri syystä. Tässä kappaleessa käydään läpi, miten kyberturvallisuuden haavoittuvuudet syntyvät merenkulussa. Haavoittuvuuksia voi syntyä inhimillisistä tekijöistä ja teknologisista tekijöistä. Inhimillisillä tekijöillä tarkoitetaan ihmisten tekemiä virheitä ja teknologiset tekijät ovat järjestelmien sekä laitteiden haavoittuvuuksia.

Merenkulun kyberturvallisuuden haavoittuvuuksien syntymiseen voi vaikuttaa esimerkiksi

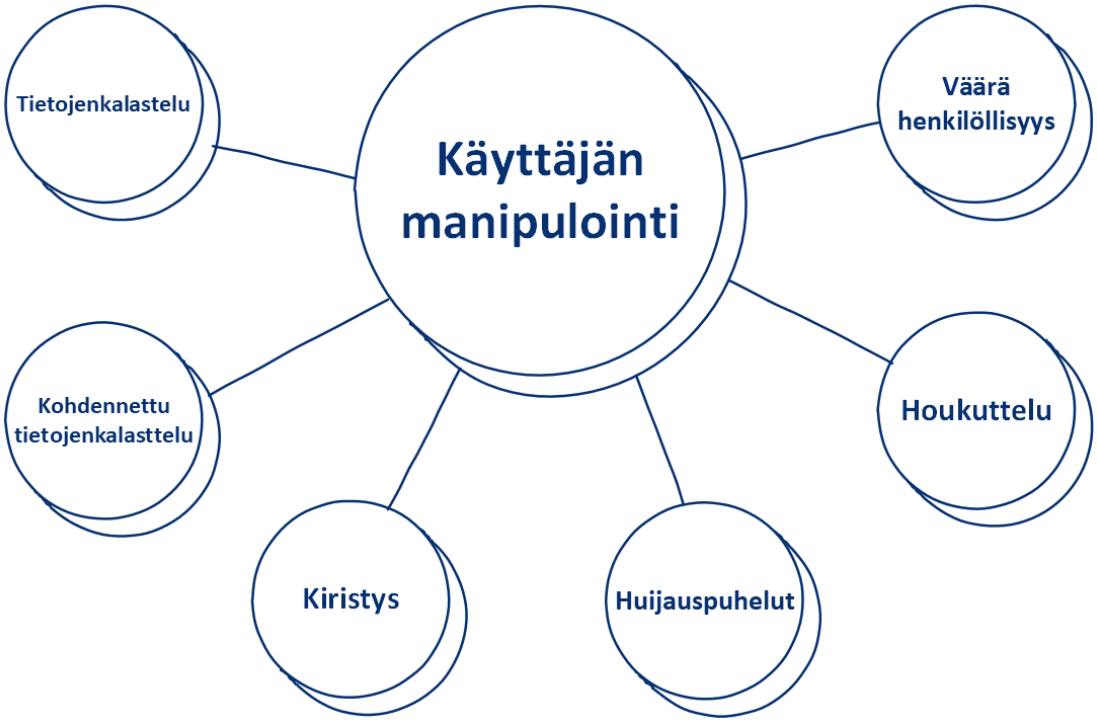
- Vanhentuneet IT- ja OT-järjestelmät, jotka ovat riippuvaisia vanhasta järjestelmästä tai niiden tuki on loppunut
- IT- ja OT-järjestelmien puutteellinen vastuullisuus
- OT-järjestelmät, joita ei pysty päivittämään tai niissä ei voida käyttää virustentorjuntaa
- Kriittisten järjestelmien riittämätön suojaus

- Merenkulun alusten laitteet, joita hallitsevat laitevalmistajat tai laitetuen yritykset
- Kriittisen tiedon jakaminen palveluntarjoajille ja muille merenkulun organisaatioille
- Puutteellinen koulutus kyberriskien hallitsemisessa
  (International Chamber of Shipping 2021, 3.)

4.1 Inhimilliset tekijät

Merenkulun kyberturvallisuuden haavoittuvuuksia voi syntyä inhimillisistä tekijöistä. Inhimilliset tekijät ovat ihmisten luomia haavoittuvuuksia, joita voi olla esimerkiksi puutteellinen kyberturvallisuus ja oma huolimattomuus. Puutteelliseen kyberturvallisuuteen voi vaikuttaa osaamisen ja koulutuksen puute. Osaamisen ja koulutuksen puute voi johtua organisaatioiden asenteesta kyberturvallisuuteen. Tämä voi johtua siitä, että kyberturvallisuutta ei pidetä tarpeeksi tärkeänä organisaatiossa. Organisaatioissa pitäisi olla kyberturvallisuuden koulutus sellaisella tasolla, jossa jokainen ymmärtäisi ja noudattaisi kyberturvallisuuden käytäntöjä. Tämän myötä haavoittuvuuksiin voitaisiin varautua.

Vaikka haavoittuvuuksiin varauduttaisiin ja koulutus olisi hyvällä tasolla, niin ihmiset tekevät virheitä oman huolimattomuuden vuoksi. Virheiden myötä voi syntyä kyberturvallisuuden haavoittuvuuksia merenkulussa. Tämän takia ihmisten omaa huolimattomuutta voidaan käyttää hyväksi kyberhyökkäyksissä esimerkiksi käyttäjän manipuloinnilla. Käyttäjän manipulointi tarkoittaa ihmisten manipulointia, jonka avulla saataisiin luottamuksellista tietoa. (Eurooppaneuvosto 2023). Luottamukselliseen tietoon voi kuulua tunnuksia, salasanoja ja organisaation tietoja.



Kuva 6 Käyttäjän manipuloinnin tavat (Eurooppa-neuvosto 2023)

Kuva 6 osoittaa käyttäjän manipuloinnin eri tapoja. Käyttäjän manipuloinnissa hyökkääjä yleensä esittää olevansa joku muu henkilö, johon voidaan luottaa. Tällä voidaan esittää olevansa esimerkiksi käyttäjän kollega, esimies tai läheinen. Väärällä henkilöllisyydellä voidaan pyrkiä tietojenkalasteluun. Tietojenkalastelulla hyökkääjät tavoittavat käyttäjän vuotamaan luottamuksellista tietoa eri kanavien kautta. Tämä voi olla luotettavan oloiset sähköpostiviestit, viestit, linkit tai puhelut. Tietojenkalastelua voi kohdentaa tiettyyn ryhmään tai kohteeseen kohdennetulla tietojenkalastelulla. Tietoja voi myös pyrkiä saamaan houkuttelun kautta. Houkuttelulla tarkoitetaan käyttäjän houkuttamista tietyillä tarjouksilla, kuten ilmaiset sovellukset, tuotteet tai tilaukset. Hyökkääjä tavoittaa käyttäjän lataamaan haittaohjelmia tai antamaan henkilökohtaisia tietoja houkuttelun avulla. Jos hyökkääjä on saanut luottamukselliset tiedot käsiinsä, niin hyökkääjä voi kiristää käyttäjää paljastamalla luottamuksellisia tietoja. (Eurooppa-neuvosto 2023.)

Käyttäjän manipuloinnin lisäksi hyökkääjät voivat hyödyntää informaatiovaikuttamista. Informaatiovaikuttamisessa pyritään vaikuttamaan ihmisten mielipiteisiin ja käyttäytymiseen esimerkiksi valheellisen tai harhaanjohtavan tiedon jakamisella. Henkilö ei välttämättä tiedä olevansa informaatiovaikuttamisen kohteena ja voi tietämättään jakaa virheellistä tietoa. (Traficom 2020b.) Virheellisten tietojen jakamisella voidaan luoda vahinkoa ihmisille ja organisaatioille.

Virheellisillä tiedoilla organisaatioiden tai ihmisten maineeseen voidaan vaikuttaa negatiivisesti.

Merenkulussa käyttäjän manipulointi ja informaatiovaikuttaminen voi kohdistua keneen tahansa organisaatiossa. Tähän voivat kuulua kokeneet työntekijät tai vasta-aloittaneet harjoittelijat. Olisi tärkeää, että organisaatiossa oltaisiin tietoisia erilaisista käyttäjän manipuloinnin ja informaatiovaikuttamisen keinoista, jotta ei joutuisi itse uhriksi. Hyökkääjät voivat luoda luotettavien tuntuisia verkkosivuja tai sovelluksia, jota merenkulussa käytetään. Näiden kautta voidaan esimerkiksi jakaa haittaohjelmia tai kerätä tunnuksia väärennetyn kirjautumisikkunan kautta. Henkilöä voidaan manipuloida käyttämään kyseisiä verkkosivuja ja sovelluksia. Jos hyökkääjät pääsisivät luottamuksellisiin tietoihin käsiksi, niin tietojen avulla olisi mahdollista hyökätä erilaisiin IT- ja OT-järjestelmiin. Inhimillisillä tekijöillä on paljon merkitystä merenkulun kyberturvallisuuden haavoittuvuuksien syntymisessä. Inhimillisiin tekijöihin täytyisi kiinnittää huomiota ja ymmärtää, miten niitä syntyy ja miten niitä ehkäistään.

4.2 Teknologiset tekijät

Teknologiset tekijät voivat myös aiheuttaa haavoittuvuuksia merenkulussa. Teknologisiin tekijöihin voi kuulua aluksessa olevat erilaiset järjestelmät, ohjelmistot ja sovellukset. Järjestelmät, ohjelmistot ja sovellukset voivat sisältää haavoittuvuuksia, jos niitä ei ole päivitetty tai suojattu. Päivitykset pitäisi olla ajan tasalla, jotta haavoittuvuuksiin voitaisiin varautua. Haavoittuvuuksia voi myös syntyä virheellisistä konfiguroinneista tai sovellusten virheistä. Inhimilliset syyt voivat myös paljon vaikuttaa teknologisten tekijöiden haavoittuvuuksiin.

Järjestelmiin, ohjelmistoihin tai sovelluksiin voi syntyä nollapäivähaavoittuvuuksia. Nollapäivähaavoittuvuuksilla tarkoitetaan haavoittuvuuksia, jotka ovat tunnettuja uusia haavoittuvuuksia, mutta niille ei ole löydetty mitään korjausta. (Turvallisuuskomitea 2018, 15). Korjaus tulisi laatia mahdollisimman nopeasti ja siitä tulisi ilmoittaa julkisesti. Alla olevaan luetteloon on kerätty esimerkkejä nollapäivähaavoittuvuuksista, jotka on ilmoittanut Traficomin kyberturvallisuuskeskus:

- *Microsoftin MSHTML-nollapäivähaavoittuvuus mahdollistaa komentojen suorittamisen etänä. Microsoftilla on tiedossaan haavoittuvuuden hyväksikäyttöyrityksiä. Haavoittuvuuden hyväksikäyttöön riittää dokumentin esikatselu Microsoft Explorer -näkymässä tai haittakoodia sisältävän dokumentin avaaminen.* (Traficom 2021.)

- *Microsoft Support Diagnostic Tool -diagnostiikkatyökalusta on paljastunut nollapäivähaavoittuvuus, joka mahdollistaa komentojen suorittamisen etänä haitallisten Microsoft Word -dokumenttien avulla. Microsoft julkaisi 14.6. päivityksen haavoittuvuuteen, joka on syytä asentaa viipymättä.* (Traficom 2022.)

- *Vuoden 2023 lopulla SMTP-protokollan useisiin toteutuksiin julkaistiin nollapäivähaavoittuvuus. Haavoittuvuutta hyödyntämällä uhkatoimijat voivat väärinkäyttää haavoittuvia SMTP-palvelimia maailmanlaajuisesti lähettääkseen haitallisia sähköposteja mielivaltaisista sähköpostiosoitteista, mikä mahdollistaa mm. kohdistettuja tietojenkalasteluhyökkäyksiä.* (Traficom 2024.)

Yllä olevat esimerkit näyttävät, minkälaisia nollapäivähaavoittuvuuksia voi olla kyseessä. Kyseiset nollapäivähaavoittuvuudet vaikuttivat merenkulussa mahdollisesti sähköposteihin ja Windows-järjestelmiin. Nollapäivähaavoittuvuudet ovat haastavia siinä mielessä, että hyökkääjä voi hyödyntää nollapäivähaavoittuvuuksia kyberhyökkäyksissä ja nollapäivähaavoittuvuuksiin ei tule välttämättä korjauksia ajallaan.

Nollapäivähaavoittuvuuksien lisäksi järjestelmissä, ohjelmistoissa tai sovelluksissa voi olla RCE Remote Code Execution -haavoittuvuuksia. RCE-haavoittuvuudella tarkoitetaan haavoittuvuutta, joka mahdollistaa haitallisen koodin suorittamisen etänä. Haitallisen koodin suorittamisessa voidaan hyödyntää myös nollapäivähaavoittuvuuksia. Hyökkääjä on päässyt käyttäjän järjestelmään käsiksi esimerkiksi käyttöjärjestelmän, palvelimen tai sovelluksen haavoittuvuuksien kautta. Tämän avulla hyökkääjä pystyy esimerkiksi hallita järjestelmän eri ominaisuuksia sekä kerätä arkaluontoista tietoa. (Sheps 2023.)

Merenkulussa voi olla myös käytössä vanhentuneita käyttöjärjestelmiä kuten Windows 7 tai Windows XP. Jotkut merenkulun alusten järjestelmät voivat käyttää vielä kyseisiä käyttöjärjestelmiä. Tämä voi johtua siitä, että järjestelmä voi olla riippuvainen käyttöjärjestelmästä ja sitä ei päivitetä ollenkaan. Windows 7- ja Windows XP-käyttöjärjestelmien tuki on lakkautunut kokonaan, ja

niihin ei tule enää tietoturvapäivityksiä. Kun käyttöjärjestelmien tuki on lakkautunut kokonaan, niin se mahdollistaa useampia kyberhyökkäyksiä. Tämä vaikuttaa merenkulun kyberturvallisuuden haavoittuvuuksien syntymiseen.

Teknologisiin tekijöihin vaikuttaa myös merenkulun alusten digitalisointi. Merenkulun alusten digitalisointi kasvattaa saatavilla olevaa tietoa ja edistää mahdollista hyökkäyspintaa. Hyökkäyspinnalla tarkoitetaan sitä, kuinka laajasti haavoittuvuuksia on ja kuinka todennäköisesti kyberhyökkäys voidaan tehdä tietyn haavoittuvuuden kautta. Merenkulun organisaatioiden tavoitteena tulisi pitää hyökkäyspinta mahdollisimman pienenä ja ennaltaehkäistä kyberhyökkäyksiä.

5 KYBERTURVALLISUUDEN MERKITTÄVYYS MERENKULUSSA

Kyberturvallisuuden merkittävyys alkaa kasvamaan merenkulussa digitalisaation yhteydessä. Kyberturvallisuuden tietoisuus merenkulussa on kohtuullisen uusi asia, joka pitäisi ottaa vakavasti katastrofien ehkäisemiseksi. (eDOTSolutions 2020.) Tässä kappaleessa tutustutaan siihen, miksi kyberturvallisuus on tärkeää merenkulussa. Kyberturvallisuuden tärkeyttä voidaan osoittaa merenkulun alan järjestelmillä ja merenkulkuun kohdistuvilla kyberhyökkäyksillä. Merenkulun alan järjestelmiin on koottu alusten järjestelmiä, joiden kautta kyberhyökkäyksiä on mahdollista tehdä. Merenkulun kyberhyökkäyksiin on koottu esimerkkejä kyberhyökkäyksistä merenkulun alalla.

International Maritime Organization julkaisi vuonna 2017 säännöksen merenkulun kyberriskien hallinnasta nimeltä ’Resolution MSC.428(98)’. Kyseisessä säännöksessä nostetaan huomioon kyberturvallisuuden tärkeys ja sen implementointi merenkulun alalla. Tämä säännös painostaa kaikkien merenkulun alan organisaatioita ja toimijoita ymmärtämään kyberriskien uhat ja haavoittuvuudet turvallista merenkulkua varten. Organisaatioita ja muita merenkulun alan toimijoita kehotettiin noudattamaan ja ottamaan käyttöön säännökset vuoteen 2021 mennessä. Tämän lisäksi organisaatioita ja toimijoita kehotettiin implementoimaan käytäntöjä ohjeistuksesta ’Guidelines on maritime cyber risk management’. (International Maritime Organization 2017.) Kyseinen säännös oli luotu, koska International Maritime Organizationin mielestä merenkulussa täytyisi keskittyä enemmän kyberriskien hallitsemiseen. International Maritime

Organization näki tarpeellisena luoda säännöksen vuoden 2017 merenkulun kyberturvallisuuden tason mukaan.

5.1 Alusten järjestelmät

Tässä luvussa tutustutaan merenkulun alusten IT- ja OT-järjestelmiin, jotka voivat sisältää kyberturvallisuuden haavoittuvuuksia. Järjestelmät ovat koottu niiden merkittävyyden ja mahdollisten hyökkäysten mukaan. Muidenkin merenkulun järjestelmien kautta on kuitenkin mahdollista tehdä kyberhyökkäyksiä. Alusten järjestelmiin kuuluu AIS, GNSS ja ECDIS. Kyseiset järjestelmät ovat oleellisia järjestelmiä merenkulussa, jota käytetään paikantamiseen, navigointiin ja tiedon jakamiseen.

5.1.1 GNSS

GNSS (Global Navigation Satellite System) paikantaa käyttäjän sijainnin satelliittien avulla koko maailman mittakaavassa. GNSS toimii samalla tavalla kuin GPS (Global Position System), mutta suuremmalla mittakaavalla. GNSS ei paljasta käyttäjän sijaintia, mutta sijainti voidaan jakaa muuta kautta. Sijainti voidaan jakaa esimerkiksi pilvipalveluiden tai laitevalmistajan sovelluksien kautta. GNSS-paikannuksessa voi olla kuitenkin epätarkkuuksia ja se voi sisältää virheitä. Paikannukseen voi vaikuttaa satelliittisignaalien voimakkuus ja oma sijainti. Näiden lisäksi muut signaalit voivat häiritä paikannusta, joka voi olla tahallista tai tahatonta. On erittäin tärkeää, että paikannus on mahdollisimman tarkka, koska paikannusvirheet luovat turvallisuusriskejä. Paikannusvirheet voivat luoda vaaratilanteita tai onnettomuuksia esimerkiksi navigoinnissa. (Maanmittauslaitos s.a.) Merenkulussa GNSS on äärimmäisen tärkeä navigoinnin suhteen. Se vahvistaa merenkulun turvallisuutta ja ennaltaehkäisee vaaratilanteita. GNSS on kuitenkin haavoittuvainen kyberhyökkäyksille, kuten signaalienhäirinnälle ja väärennetylle sijainnille.

5.1.2 AIS

AIS eli Automatic Identification System -järjestelmää käytetään merenkulun alusten informaation jakamiseen. AIS-järjestelmän avulla ilmoitetaan missä alus liikkuu, kuinka nopeasti alus liikkuu ja minkälainen alus on kyseessä.

Tieto kulkee lähettyvillä oleville aluksille ja rannikkoasemille, joissa on AIS-järjestelmä käytössä. Tämä tieto lähetetään säännöllisin väliajoin VHF-taajuusalueella ja siinä käytetään hyödyksi aluksen GNSS-järjestelmää. Lähetettävään tietoon kuuluu muun muassa MMSI-numero, ISO-numero, aluksen nimi sekä kutsumerkki, aluksen pituus sekä leveys ja aluksen sijainti. AIS-järjestelmän kattavuusalue voi olla 20–350 mpk eli noin 37–648 km. Keskiarvoltaan kattavuusalue on noin 40 mpk eli 74 km. Kattavuusalue riippuu paljon säästä ja aluksesta. AIS-järjestelmän kuuluisi olla aina päällä, jotta merenkulun alusten toimintaa voitaisiin seurata ja alusten tietoa voitaisiin käyttää hyödyksi. AIS-järjestelmä parantaa merenkulun turvallisuutta ja tietoisuutta. Harvoissa tapauksissa AIS-järjestelmä voidaan ottaa oikeutetusti pois päältä. Tämän syynä voi kuitenkin olla laittoman toiminnan peittäminen. (North Atlantic Treaty Organization, 2021.)

AIS-järjestelmän oleellisiin ominaisuuksiin kuuluu merenkulun alusten törmäyksien estäminen. Tämä on erittäin tärkeää silloin, kun ei ole rannikkoasemia lähettyvillä. AIS-järjestelmä tarkastaa aluksien suunnan sekä nopeuden ja tietyt järjestelmät hälyttävät siitä, jos alukset ovat törmäyskurssilla. Tämän kanssa voi tulla ongelmia, jos AIS-dataa on muokattu. Muokatun AIS-datan seurauksena voi tulla vääriä hälytyksiä AIS-järjestelmään sekä se voi luoda vaaratilanteita. (Balduzzi ym 2014, 7.)

5.1.3 ECDIS

ECDIS eli Electronic Chart Display Information System -järjestelmä digitalisoi perinteisen merenkulun navigoinnin. ECDIS-järjestelmän avulla saadaan luettua ja päivitettyä merikarttaa. Merikarttaa voidaan päivittää verkon välityksellä, joka voi tuoda kuitenkin ongelmia kyberturvallisuuden suhteen. Tämä lisää altistusta kyberturvallisuuden haavoittuvuuksiin. ECDIS-järjestelmä käyttää yleisesti vanhoja käyttöjärjestelmiä, joka voi tuoda lisää ongelmia. ECDIS-järjestelmä saa myös tietoa muista alusten järjestelmistä kuten tutkasta ja AIS-järjestelmästä. (eDOTsolutions 2020, 7.)

Svilicic ym (2019) tutkivat ECDIS-järjestelmän haavoittuvuuksia ”Raising Awareness on cyber Security of ECDIS” -raportissaan. He skannasivat haavoittuvuuksia Nessus Professional haavoittuvuusanalyysi ohjelmalla Transas Navi-

Sailor 4000 ECDIS -järjestelmästä. Tämä tapahtui simulaatiotilassa, jossa oli 6 ECDIS-järjestelmää, joissa oli käytössä Windows 7-käyttöjärjestelmä. Kaikissa ECDIS-järjestelmissä oli saman verran haavoittuvuuksia, joista löytyi yhteensä 1 kriittinen haavoittuvuus, 7 suurta haavoittuvuutta, 15 keskikokoista haavoittuvuutta ja 1 alhainen haavoittuvuus. Alla olevaan taulukkoon on kerätty ECDIS-järjestelmän haavoittuvuuksia raportin perusteella.

Taulukko 1 Windows 7-käyttöjärjestelmän haavoittuvuuksia, jotka olivat käytössä ECDIS-järjestelmissä (Sycilic ym 2019, 234)

Palvelu	Haavoittuvuus	Vakavuus
SMB (Server Message Block)	SMB v1 -versio sisältää RCE -haavoittuvuuksia ja tietojen paljastamisen haavoittuvuuksia	Kriittinen
RDP (Remote Desktop Protocol)	RDP-palvelu sisältää RCE-haavoittuvuuden ECDIS-järjestelmässä	Suuri
Terminaali	Terminaalipalvelu on haavoittuvainen man-in-the-middle-hyökkäyksille, jolla hyökkääjä voi päästä arkaluontoisiin tietoihin käsiksi	Keskikokoinen
SAM (Security Account Manager) ja LSA (Local Security Authority)	SAM- ja LSA-palvelut sisältävät haavoittuvuuden, joka mahdollistaa käyttöoikeuksien korottamisen	Keskikokoinen
SMB	ECDIS-järjestelmän SMB-palvelimeen ei vaadittu kirjautumista	Keskikokoinen
Terminaali	Terminaalipalvelun konfigurointi käyttää alhaista salaustasoa	Alhainen

Taulukko 1 näyttää erilaiset Windows 7 -käyttöjärjestelmän haavoittuvuudet, joita tutkittiin ECDIS-järjestelmissä. Vakavin haavoittuvuus oli SMB-protokollassa. SMB-protokollan avulla saadaan jaettua ja muokattua tiedostoja tietokoneiden välillä verkossa. (Microsoft s.a). SMB-protokolla sisälsi RCE-haavoittuvuuksia, joka mahdollistaa haitallisen koodin suorittamisen etänä. Tämän lisäksi arkaluontoisten tietojen paljastuminen oli myös mahdollista ja SMB-palvelimeen ei vaadittu kirjautumista. Taulukon RDP-palvelu mahdollisti myös haitallisen koodin suorittamisen. RDP-palvelua käytetään laitteiden etähallintaan kuten tietokoneet ja palvelimet. (Microsoft s.a). Terminaalipalvelu oli taas haavoittuvainen man-in-the-middle-hyökkäykselle ja terminaalipalvelun konfigurointi käytti alhaista salaustasoa. Man-in-the-middle-hyökkäyksellä tarkoitetaan hyökkäystä, jossa hyökkääjä tulee kahden osapuolen väliin salakuuntelemaan ja keräämään tietoa, joka voi olla esimerkiksi uhrin ja palvelimen väli verkossa. (Microsoft 2021.)

SAM- ja LSA-palvelut sisälsivät haavoittuvuuden, jolla voitiin korottaa käyttäjän käyttöoikeuksia. Käyttöoikeuksien korotuksella hyökkääjä pyrkii korottamaan omia oikeuksiaan järjestelmässä, kuten järjestelmänvalvojan oikeuksiin. SAM-palvelu hallinnoi paikallisia käyttäjätilejä sekä niiden salasanoja paikallisessa tietokoneessa ja LSA-palvelu vastaa paikallisten käyttäjien todennuksesta ja käyttöoikeuksista. (Microsoft 2009).

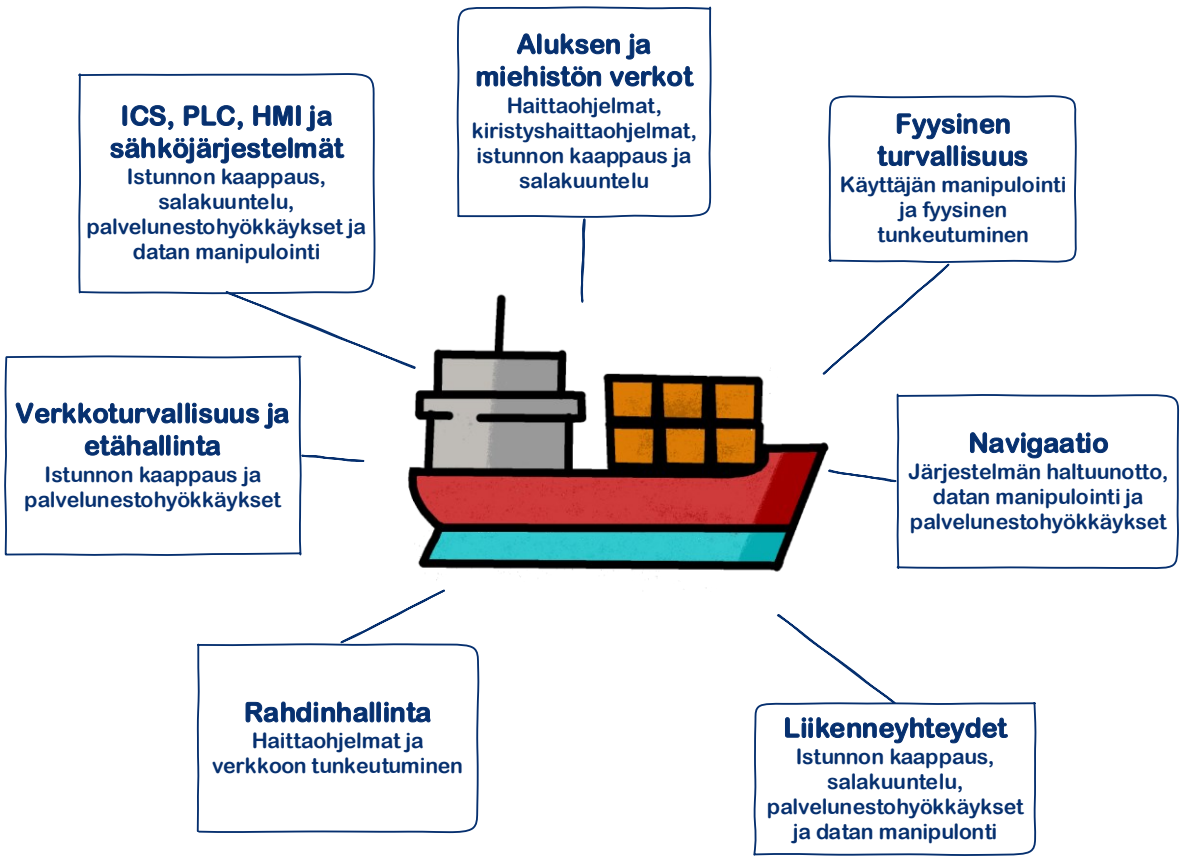
Taulukon 1 haavoittuvuuksien lisäksi ECDIS-järjestelmistä löytyi Apache Web-palvelimen ja VNC eli Virtual Network Computing -palvelimen haavoittuvuuksia. ECDIS-järjestelmien Apache Web -palvelin oli vanhentunut, joka mahdollistaa muun muassa palvelunestohyökkäykset, hyökkääjän pääsyn arkaluontaisiin tietoihin, ECDIS-järjestelmän kaatumisen ja haitallisen koodin suorittamisen. Lisäksi ECDIS-järjestelmän VNC-palvelimessa ei ollut autentikointia käytössä, joka mahdollistaa hyökkääjän yhdistämään ECDIS-järjestelmään. (Sycilic ym 2019, 234.)

5.2 Merenkulun kyberhyökkäykset

Vuosien mittaan merenkulkuun on kohdistunut eri laajuisia kyberhyökkäyksiä. Tässä luvussa käsitellään vaikuttavia kyberhyökkäyksiä merenkulun alalla. Näiden kyberhyökkäyksien avulla huomataan, kuinka tärkeää kyberturvallisuus

on merenkulussa ja minkälaisia vaikutuksia kyberhyökkäyksillä on ollut. Merenkulun kyberhyökkäykset voivat ulottua laajasti eri järjestelmiin, joita aiemmassa luvussa käsiteltiin. Merenkulun kyberhyökkäyksien tiedon saatavuus vaihtelee hyvin paljon, jonka takia tietyistä kyberhyökkäyksistä on enemmän tietoa kuin toisista. Tiedon saatavuus riippuu kyberhyökkäysten merkittävyydestä ja siitä, kuinka paljon asiaa on tutkittu ja minkälaisia kyberhyökkäyksiä on ilmoitettu.

Vuosina 2017–2019 merenkulun kyberhyökkäykset OT-järjestelmiin olivat nousseet huomattavasti. Hyökkäyksiä oli ollut yhteensä 480 ja ne ovat kasvaneet jopa 900 % vuodesta 2017 vuoteen 2019. (The Maritime Executive 2020.) Tähän pitää ottaa myös huomioon ne kyberhyökkäykset OT-järjestelmiin, joista ei ole ilmoitettu. Ilmoittamattomien kyberhyökkäysten määrää on vaikea arvioida, koska niihin voi vaikuttaa esimerkiksi hyökkäysten suuruus tai inhimilliset tekijät.



Kuva 7 Rahtialuksen ympäristö (Huoltovarmuusorganisaatio 2021, 5)

Kuva 7 osoittaa rahtialuksen ympäristön sekä siihen kohdistuvia kyberhyökkäyksiä. Kyberhyökkäykset ovat vaihtelevia ja niitä voi tehdä monen eri kana-

van kautta. Rahtialuksen hyökkäyspinta voi olla laaja, jos kyseisessä ympäristössä löytyy paljon haavoittuvuuksia. Kyberhyökkäyksiin voi sisältyä haittaohjelmien levittämistä, istunnon kaappausta, salakuuntelua, palvelunestohyökkäyksiä ja datan manipulointia. Istunnon kaappauksessa hyökkääjä pyrkii ottamaan aktiivisen käyttäjän istunnon haltuunsa järjestelmässä tai sovelluksessa. Tämä voi tapahtua tunnistetietojen väärentämisenä tai kaappauksena. (OWASP s.a.) Palvelunestohyökkäyksillä taas pyritään estämään tiettyjä palveluita tai järjestelmiä kuormittamalla niitä. Tämä voi tapahtua esimerkiksi lähettämällä erittäin suuren määrän liikennettä palvelimeen. Salakuuntelulla pyritään saamaan luottamuksellista tietoa, jota voidaan hyödyntää kyberhyökkäyksissä kuten datan manipuloinnissa, jossa hyökkääjä muokkaa järjestelmän tai sovelluksen tietoja omiin tarkoituksiinsa.

Alla olevaan luetteloon on kerätty merenkulun kyberhyökkäyksiä ”A Retrospective Analysis of Maritime Cyber Security Incidents” -raportista. Kyberhyökkäykset ovat lueteltuna niiden vuoden mukaan:

- International Maritime Organizationin verkkosivut ja intranet estettiin kokonaan käytöstä palvelunestohyökkäyksellä. (2020)
- Iranilainen Shadid Rajaeen satama lamaannutettiin kokonaan pois käytöstä palvelunestohyökkäyksellä, josta syytettiin Israelia. (2020)
- Carnival Corporation & plc -varustamoon hyökättiin kahdesti kiristyshaittaohjelmalla, joka mahdollisesti keräsi asiakkaiden ja työntekijöiden yksityistietoja ja luottokorttitietoja. (2019–2020)
- Hurtigruten-varustamoon levitettiin kiristyshaittaohjelma, joka sulki organisaation järjestelmiä useaksi päiväksi. Asiakkaiden passitietoja pääsi mahdollisesti hyökkääjien käsiin. (2020)
- COSCO-varustamo kärsi kiristyshaittaohjelmasta, joka sulki sähköpostin sekä puhelinverkon viideksi päiväksi (2018)
- Austal-laivarakennusketjun suunnittelumalleja ja työntekijöiden tietoja varastettiin, joita myytiin eteenpäin pimeässä verkossa (2018)
- Etelä-Korean alueella 280 merenkulun alusta joutui takaisin satamaan, kun alusten navigointia oli häiritty kyseisellä alueella. (2016)
- Tanskan viranomainen Danish Maritime Authority koki tietojenkalastelu-hyökkäyksen, jossa varastettiin verkon topologian dokumentteja. (2012)

- Antwerpin sataman rahdinhallintajärjestelmä joutui haittaohjelman uhriksi, joka mahdollisti huumeiden ja aseiden salakuljettamisen. Huumeet ja aseet olivat merkattuina banaaneiksi rahdinhallintajärjestelmässä pari vuotta huomaamatta. (2011–2013)

  (Meland ym 2020, 522–524.)

Luettelosta huomaa, kuinka erilaisia kyberhyökkäykset voivat olla merenkulun alalla. Hyökkäyksistä suuri osa oli kiristyshaittaohjelmia. Tähän voi vaikuttaa se, että hyökkäyksien motivaationa voi olla raha. Kiristyshaittaohjelmat ovat myös levinneet hyvin laajasti, jonka takia niitä on kerättynä enemmän raporttiin.

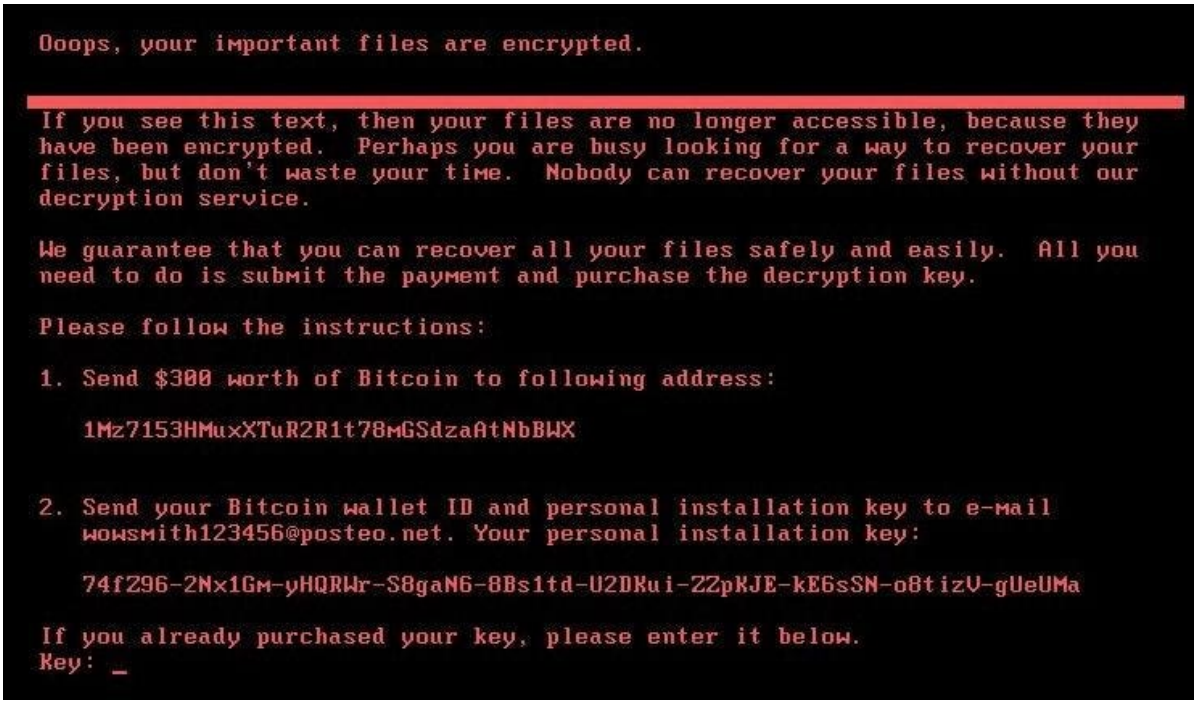
5.2.1 Kiristyshaittaohjelmat

Kiristyshaittaohjelmat ovat alkaneet olla yleinen ongelma merenkulussa. (CyberOwl 2022, 12). Kiristyshaittaohjelmilla tarkoitetaan haittaohjelmia, joiden tarkoitus on kiristää käyttäjää erilaisilla tavoilla. Hyökkääjä pyrkii jakamaan kiristyshaittaohjelman käyttäjän laitteelle, jolloin sillä voidaan tehdä vahinkoa. Kiristyshaittaohjelma voidaan levittää esimerkiksi sähköpostien tai verkkosivujen kautta. Kiristyshaittaohjelma voi lukita tietokoneessa olevia tiedostoja erilaisilla salausmenetelmällä. Nämä tiedostot voivat olla esimerkiksi kuvia, tekstitiedostoja, taulukkotiedostoja, sovelluksien tiedostoja ja järjestelmän tiedostoja. Kun tiedostot ovat lukittuna, niin hyökkääjä yleensä vaatii lunnaita, jolloin tiedostojen lukitus voitaisiin avata. Tiedostojen lukituksen avaaminen ei ole kuitenkaan varmaa, vaikka lunnaat maksettaisiin. Kiristyshaittaohjelma on erittäin haitallinen, jos se on kyennyt lukitsemaan tärkeitä tiedostoja, joilla ei ole varmuuskopioita. Ilman varmuuskopiota tiedostojen palautus voi olla mahdotonta, joka voi johtaa suuriin menetyksiin.

Merenkulun alan tunnetuimpia kyberyökkäyksiä on NotPetya-kiristyshaittaohjelma, joka levisi laajasti eri organisaatioissa vuonna 2017. Kiristyshaittaohjelma oli venäjältä peräisin ja kohteena olivat ukrainalaiset yritykset. Kiristyshaittaohjelma levisi tuolloin laajimpaan tanskalaiseen merenkulun organisaatioon A. P. Møller-Mærskiin. Maersk sisälsi tuolloin yli 75 000 työntekijää yli 130:tä maasta ja se on vieläkin maailman suurin rahtilaivavarustamo. NotPetya päätyi Intellect Service -nimiseen ukrainalaiseen ohjelmistoyritykseen. Intellect Service oli luonut M.E.Doc nimisen-sovelluksen, jota käytettiin verojen

maksamiseen Ukrainassa. NotPetya levisi M.E.Doc -sovellukseen, kun hyökkääjä oli saanut työntekijän salasanan haltuunsa. Tämän takia kaikki organisaatiot, jotka käyttivät kyseistä sovellusta, joutuivat mahdollisesti kiristyshaittaohjelman uhriksi. (Columbia University 2022, 2–3.)

Maerskilla oli käytössä M.E.Doc -sovellus Ukrainassa ja osa Maerskin palvelimista käytti Windows 2000 -järjestelmää. Windows 2000 -järjestelmä ei saanut enää päivityksiä ja se sisälsi useita haavoittuvuuksia. Maerskissa oli myös huomautettu, että organisaatio käytti vanhentuneita käyttöjärjestelmiä ja verkon segmentoinnissa oli puutteita. Näiden syiden takia NotPetya päätyi Maerskiin ja teki valtavaa tuhoa. NotPetya levisi nopeasti eri satamiin, jonka takia siihen ei pystytty reagoimaan. NotPetya lukitsi järjestelmät kokonaan ja pyysi lunnaita. Tiedostoja ei saanut kuitenkaan mitenkään takaisin, vaikka lunnaat maksettaisiin. (Columbia University 2022, 3–4.)



Kuva 8 NotPetyan kiristysviesti (Forbes 2017)

17 Maerskin satamaa ja Maerskin varausjärjestelmä meni kokonaan käyttökelvottomaksi moneksi päiväksi. Nostureita ei pystynyt käyttämään satamissa, jolloin alukset eivät saaneet lastia ollenkaan. Maerskin verkkoa ei ollut kunnolla segmentoitu, joka tarkoitti sitä, että verkkoa ei ollut jaettu pienempiin aliverkkoihin. Maersk sulki kokonaan verkkonsa, jotta kiristyshaittaohjelma ei levisi enää pidemmälle. 150 Maerskin palvelinta oli kuitenkin menetetty kokonaan, kun hyökkäykseen ei ollut varauduttu. Maerskin 4 000 palvelinta ja 45

000 tietokonetta saatiin kymmenessä päivässä takaisin, mutta koko organisaation jälleenrakentamisessa meni noin kaksi kuukautta. Maersk menetti arvioltaan noin 250–300 miljoonaa dollaria NotPetyan takia, mutta arvioidut menetykset voivat olla vielä paljon suuremmat. Monet muut organisaatiot menettivät kaiken kaikkiaan yhteensä 10 miljardia dollaria hyökkäyksen takia. (Columbia University 2022, 5–6.)

Maerskin tapauksessa kiristyshaittaohjelmiin ei ollut kunnolla varauduttu, vaikka organisaatiolta olisi löytynyt resursseja siihen. Maerskin kyberturvallisuuden budjetilla voi olla tähän vaikutusta ja myös sillä, että merenkulun alalla ei ole aikaisemmin ollut näin suurta kyberhyökkäystä. Kyberhyökkäyksiä voidaan olla vähätelty ja nopeasti leviävää kiristyshaittaohjelmaa ei olla pidetty uhkana tai suurena mahdollisuutena.

5.2.2 GNSS-signaalien häirintä

GNSS-signaalia voidaan häiritä eri keinoilla. GNSS-signaalien häirintä voi olla signaalien estämistä ja signaalien väärentämistä. Signaalien estämisessä hyökkääjä pyrkii vaikuttamaan GNSS-signaalien radiotaajuuteen. Tämä voi tapahtua signaalien estämiseen tarkoitetuilla laitteilla. Laitteiden avulla voidaan luoda vahvempia signaaleja samalla radiotaajuudella, jotka peittävät GNSS-signaalit. Kun GNSS-signaalit ovat peitettynä, niin käyttäjän sijaintia ei voida vahvistaa liiallisten signaalien seurauksena. (Intertanko 2019, 3.)

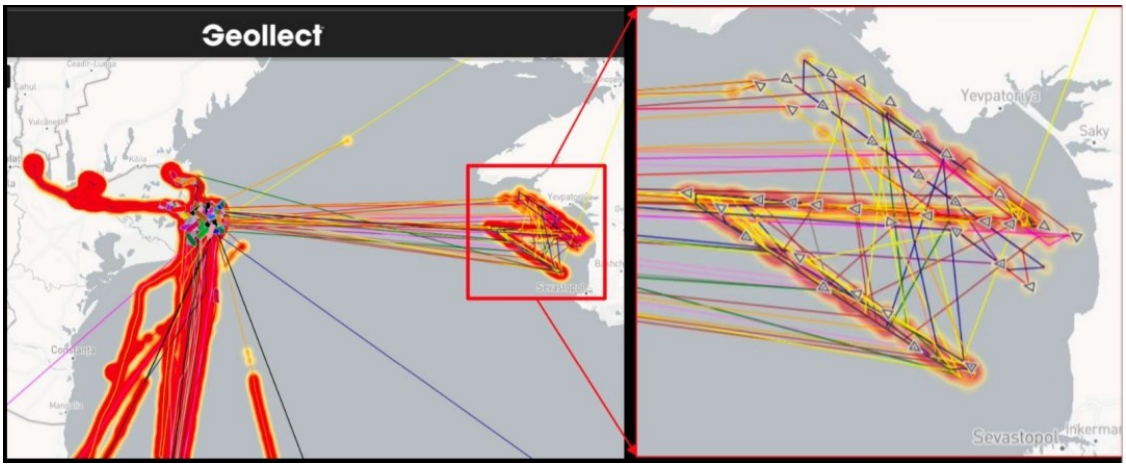
GNSS-signaalien väärentämisessä hyökkääjä pyrkii väärentämään käyttäjän sijaintia. Väärentäminen tapahtuu lähettämällä vääränlaisia GNSS-signaaleja, jotka yritetään näyttämään oikeilta GNSS-signaaleilta. Tämän seurauksena käyttäjä voi luulla olevansa eri paikassa missä sijaitsee. Signaalien väärentämisessä on myös mahdollista vaihtaa käyttäjän sijaintia määritetyn ajan päästä. Yhtenä GNSS-signaalien väärentämisen keinona hyökkääjä lähettää oikeita signaaleja ja ajan mittaan väärentää oikeat signaalit vääränlaisiksi. GNSS-signaalien estäminen on todennäköisempää kuin niiden väärentäminen. Tämä johtuu siitä, koska signaalien estäminen on paljon helpompaa ja yleisempää kuin signaalien väärentäminen. Signaalien väärentäminen on monimutkainen hyökkäys, jossa hyökkäyksen lähde voidaan mahdollisesti paikantaa. (Intertanko 2019, 4.)

Center for Advanced Defense Studies tutki GPS-järjestelmien väärentämistä Venäjällä ja Syyrialla ”Above Us Only Stars” -raportissaan. Raportissa tutkittiin merenkulun GNSS-signaalien väärentämistä, joissa vaikutettiin monen merenkulun alusten sijaintiin ja navigointiin. GNSS-signaalien väärentämiset sijoittuivat yhteensä kymmeneen sijaintiin Venäjälle, Krimille ja Syyriaan. GNSS-signaalien väärentämistapauksia oli yhteensä 9 883, ja ne vaikuttivat yhteensä 1311 merenkulun alukseen. Väärentämiset tapahtuivat tammikuun 2016 ja marraskuun 2018 välisenä aikana. 94 % GNSS-signaalien väärentämisistä sijoittuivat Gelendžikin, Sotšin ja Pietarin lähettyville. Tämä voi kuitenkin johtua siitä, että alueilla oli satamia, jotka tunnistivat GNSS-signaalien väärentämisiä tarkemmin. (Center for Advanced Defense Studies 2019, 20–21.)

5.2.3 AIS-datan manipulointi

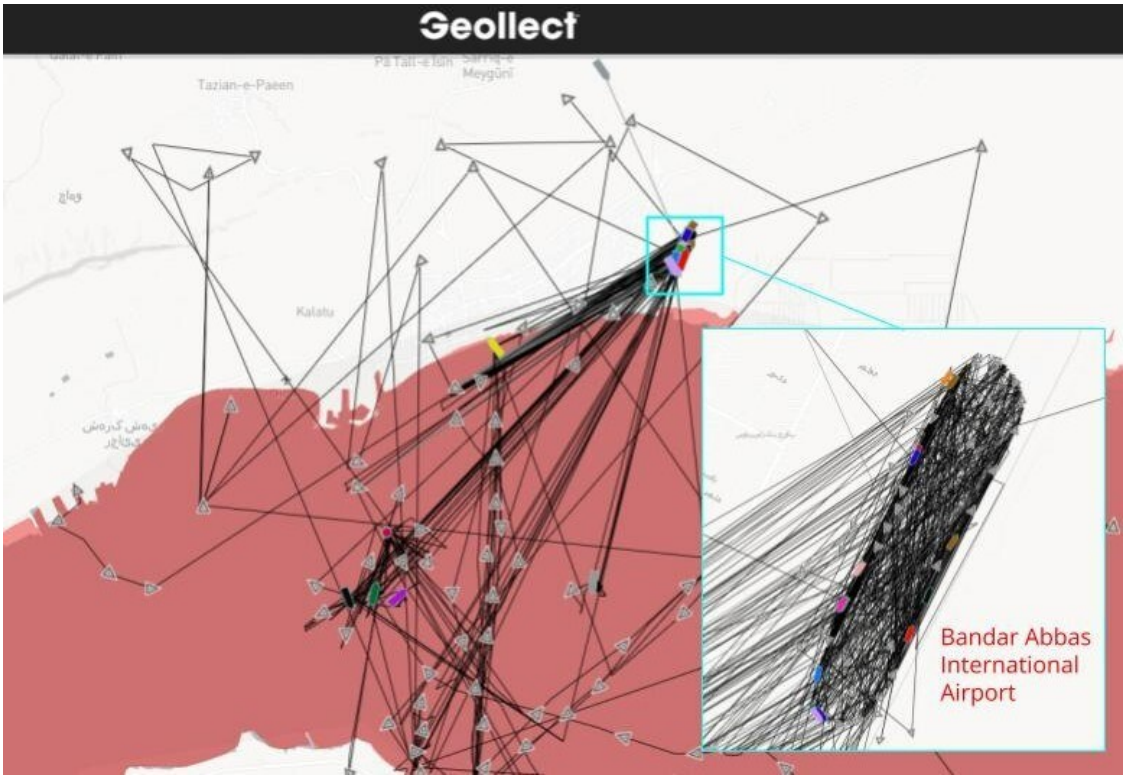
AIS-järjestelmä sisältää kriittisiä haavoittuvuuksia, joka mahdollistaa AIS-järjestelmän datan muokkauksen. Tätä kutsutaan AIS-datan manipuloinniksi. AIS-datan manipuloinnissa voidaan muokata merenkulun alusten sijaintia ja identiteettiä. Tähän voi kuulua esimerkiksi alusten hävittämistä ja luontia AIS-järjestelmään sekä alusten tietojen muokkaamista. Tieto voi olla harhaanjohtavaa tai väärennettyä. Alusten identiteettiä ei voida varmistaa mitenkään, jonka takia AIS-data ei voi olla täysin varmaa. (Windward 2014, 2–5.) AIS-datan manipulointi tuo ongelmia merenkulkuun kuten AIS-datan luotettavuuden menettäminen ja vaaratilanteet. AIS-datan tulisi olla luotettavaa, jotta merenkulku olisi turvallisempaa. AIS-datan manipulointi on uutta merenkulussa, joka voi alkaa yleistyä enemmän.

AIS-datan manipulointiin voi kuulua SART-tiedon muokkaus. SART on laite, jonka avulla voidaan paikantaa aluksia ja ihmisiä hätätilanteissa. SART-laite lähettää hätäsignaalin, kun se tulee kosketukseen veden kanssa. SART-tiedon muokkauksessa voidaan luoda väärennettyjä hätäsignaaleja haluttuun paikkaan. Alusten on pakko reagoida hätäsignaaleihin ja auttaa hädässä olevia. Väärennetyt hätäsignaalit luovat kumminkin ongelmia ja aiheuttavat resurssien kulutusta. Hyökkääjät voivat käyttää hätäsignaaleja hyödykseen ja tuoda esimerkiksi aluksia vaarallisille alueille. Vaarallisiin alueisiin voi kuulua alueet, joissa on piratismia. (Balduzzi ym 2014, 7-9.)



Kuva 9 AIS-datan manipuloinnin avulla alukset on väärennetty näyttämään ’Z’ kirjaimelta (Geocollect 2023a)

Kuva 9 osoittaa AIS-datan manipulointia, jossa on väärennetty aluksia näyttämään venäjän hyökkäyssodan ”Z” -kirjaimen tunnusmerkiltä. AIS-datan manipulointi näkyi AIS-järjestelmissä 14.5.2023 Mustallamerellä. Tunnusmerkki oli 65 km pitkä ja alukset näyttivät liikkuvan noin 102 solmua eli 188 km/h, joka varmisti AIS-datan manipuloinnin. Manipuloinnin syynä hyökkääjät todennäköisesti pyrkivät nostamaan Venäjän moraalia, jossa myös hyödynnettiin informaatiovaikuttamista. Tämä kyseinen AIS-datan manipulointi vaaransi alueen merenkulkua, koska se lisäsi riskiä alusten törmäyksiin ja onnettomuuksiin. Kyseessä oli sodan lähellä oleva alue ja väärennetyt alukset estivät näkyvyyttä AIS-järjestelmässä. (Geollect 2023a.)



Kuva 10 Yli 60 merenkulun alusta siirretty AIS-datan manipuloinnilla (Geollect 2023b)

Kuva 10 näyttää yli 60 merenkulun aluksen liikkumisen Iranin kansainvälisen lentokentän Bandar Abbasin alueella. Tämä tapahtui 26.4-8.6.2023 välisenä aikana ja osa aluksista näyttivät liikkuvan noin 50 solmua eli 93 km/h. Alukset liikkuivat lentokentän yläpuolella kuukausien ajan. Tekijästä tai motiivista ei ollut selvää, mutta tapaus varmistettiin AIS-datan manipuloinniksi. Irania epäiltiin tekijäksi, kun Iran on aikaisemmin manipuloinut AIS-dataa merenkulussa. (Geollect 2023b.) Kyseisellä AIS-datan manipuloinnin motivaationa on voinut olla lentokentän näkyvyyden peittäminen tai hyökkäyksen testaaminen. Motivaatiosta ei kuitenkaan ollut selvää, jolloin hyökkäyksestä voidaan vain arvioida, mikä on voinut olla sen motivaationa.

5.3 Merenkulun kyberhyökkäyksien ennaltaehkäisy

Merenkulun kyberhyökkäyksiin voidaan varautua niiden ennaltaehkäisyllä. Ennaltaehkäisyllä pyritään estämään kyberriskejä ja haavoittuvuuksia syntymästä. Jotta kyberhyökkäyksiä voitaisiin ennaltaehkäistä merenkulussa, niin pitäisi merenkulun organisaatioissa olla suhtautuminen kyberturvallisuuteen kohdallaan. Organisaatioissa tulisi olla asiallinen kyberturvallisuuskoulutus, jotta ymmärrettäisiin kyberturvallisuuden riskit ja haavoittuvuudet. Kyberturval-

lisuuskoulutuksella voidaan mahdollisesti estää käyttäjän manipuloinnin hyökkäyksiä. Käyttäjän manipuloinnin eri keinot tulisi tietää, jotta organisaatioissa ei jouduttaisi käyttäjän manipuloinnin uhriksi. Merenkulun organisaatioissa tulisi olla myös järjestelmät suojattuna kyberhyökkäyksiltä. Järjestelmät kuuluisivat olla säännöllisesti päivitettynä ja niissä täytyisi käyttää turvallisia ja monimutkaisia salasanoja. Salasanat eivät kuuluisi olla myöskään missään näkyvillä ja oletussalasanoja ei kuuluisi olla lainkaan.

Merenkulun organisaatioissa pitäisi olla myös verkot segmentoituna eri verkkoihin, jotta mahdolliset kyberhyökkäykset voitaisiin rajoittaa. Verkot voidaan jakaa eri osioihin, johon voi kuulua esimerkiksi miehistöverkot, koneistoverkot, matkustajaverkot ja hallinnolliset verkot. Verkkojen segmentoinnin lisäksi palomuurit tulisi määrittää, jolla suodatettaisiin verkkoliikenne. Olisi myös tärkeää tunnistaa kolmannet osapuolet ja valvoa heidän toimintaansa verkossa tai järjestelmissä. Valvonnassa kannattaa ottaa huomioon myös mahdolliset haittaohjelmat. Haittaohjelmat voivat levitä esimerkiksi verkon tai muistitikkujen kautta. Tuntemattomien muistitikkujen sisältöä ei kuuluisi katsoa ja haittaohjelmia varten täytyisi olla virustentorjuntaohjelma käytössä. Joihinkin järjestelmiin virustentorjuntaa ei voida asentaa, jolloin tiukkoja käyttöoikeuksia ja verkon segmentointia voidaan käyttää hyödyksi. Tämän kaiken lisäksi järjestelmiä kuuluisi monitoroida ja ottaa lokienhallintajärjestelmä käyttöön. Monitoroinnilla ja lokituksella voidaan havaita kyberhyökkäyksiä ja tarkastella poikkeamatietoja. (Huoltovarmuusorganisaatio 2021, 8–15.)

GNSS-signaalien häiritsemisen ja väärentämisen ennaltaehkäisyssä navigoinnin järjestelmissä kuuluisi olla hälytys, kun sijainti on muuttunut tai hävinnyt. Joillain merenkulun organisaatioilla voi olla kuitenkin käytössä vielä vanhempia navigoinnin järjestelmiä, joissa ei ole hälytystä käytössä. ECDIS-järjestelmän avulla voidaan myös havaita sijainnin muutosta. Sijainti kuuluisi vahvistaa säännöllisin väliajoin, jotta merenkulku olisi turvallisempaa. Tämän lisäksi olisi tärkeää järjestää harjoituksia tilanteisiin, jossa GNSS-signaaleja häiritään tai väärennetään. (Intertanko 2019, 6–7.)

6 TUTKIMUKSEN VERKKOKYSELY

Merenkulun opiskelijoille laadittiin kysely, joka sisälsi kysymyksiä merenkulun kyberturvallisuudesta ja sen haavoittuvuuksista. Kysely luotiin Google Formsin avulla, ja se sisälsi 29 kysymystä. Tavoitteena oli kartoittaa merenkulun opiskelijoiden kyberturvallisuuden tietämyksen taso. Tärkeää oli, että kysymykset olivat selkeitä ja ne eivät johdatellut johonkin tiettyyn vastaukseen. Kyselyssä pyrittiin saamaan rehellisiä vastauksia opiskelijoilta ja heidän tietämyksestään aiheesta. Kysymykset olivat suurimmaksi osaksi monivalintakysymyksiä. Tämä johtuu siitä, että monivalintakysymyksiin pystyy usein helpommin vastaamaan kuin esimerkiksi avoimiin kysymyksiin. Kysely myös sisälsi valintaruutuja ja lineaarisia asteikkoja. Valintaruutujen avulla saatiin useampi vastaus kysymyksestä ja lineaarisella asteikolla kerättiin vastaajan arvio kysymyksestä.

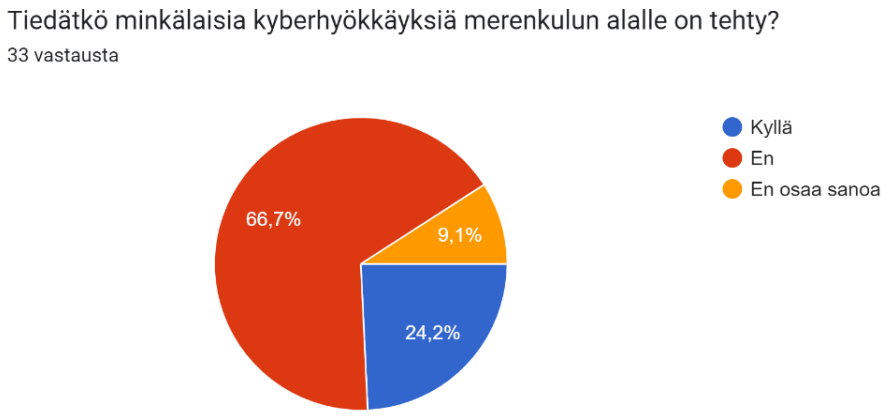
Kyselyn ensivaikutelma on tärkeä, jotta herätettäisiin vastaajien mielenkiinto ja luottamus. Piti myös huomioida, että kaikkea kysytään tarkasti ja kysely oli sopivan pituinen. Sopivan pituisella kyselyllä vastaajat pyrkisivät vastaamaan kaikkiin kysymyksiin ja tekemään kyselyn loppuun. Liian pitkään tai monimutkaiseen kyselyyn ei välttämättä vastata loppuun asti. Joihinkin kysymyksiin käytettiin myös Likert-asteikkoa, jossa kysyttiin minkä verran on samaa mieltä lauseen kanssa. Tämän avulla kerättiin vastaajien näkemyksiä tietyistä lauseista. (Tietoarkisto s.a.)

Kyselyä varten kirjoitettiin saatekirje, joka jaettiin toimeksiantajan kautta jokaiselle merenkulun opiskelijalle Learn-alustalle. Tavoitteena oli, että mahdollisimman moni merenkulun opiskelija vastaisi kyselyyn. Pyrkimyksenä oli saada ainakin 25 vastausta kahden viikon aikana. Kyselyyn pystyi vastaamaan 29.1.2024-12.2.2024 välillä. Kyselyyn piti saada tarpeeksi vastaajia, jotta saataisiin onnistunut tutkimus ja tarkemmat tutkimustulokset. Kysely oli jaettu eri aiheisiin, kuten omaan käyttäytymiseen, kyberhyökkäyksiin, haavoittuvuuksiin ja järjestelmiin. Aiheiden kysymykset oli luotu sellaisiksi, johon suuri osa opiskelijoista pystyisi vastaamaan. Oli myös tärkeää, että kysymykset olivat loogisessa järjestyksessä ja kysyttiin oleellisia kysymyksiä, joka varmistaa kyselyn tasapainoisuuden, kattavuuden ja selkeyden. (Tietoarkisto s.a).

Kaikkiin kysymyksiin ei ollut pakko vastata, mutta se oli suositeltavaa. Kysely alkoi kysymyksillä, johon oli helppo vastata. Jos ei osannut vastata kysymykseen, niin useaan vaihtoehtoon oli lisätty ”en osaa sanoa” -vastaus. Sen avulla saadaan myös selville, kuinka paljon vastaajat tietävät aiheesta ja kysymyksistä. Kyberturvallisuuden käsite oli selitetty kyselyn alussa, jotta ymmärrettiin sen tarkoitus. Tämän jälkeen kysyttiin tiedetäänkö, mitä kyberturvallisuus tarkoittaa. Tällä varmistettiin se, että vastaaja ymmärtää aiheen kokonaisuuden ja pystyi vastaamaan kysymyksiin.

Tutkimuksessa tarkastetaan minkälaisia vastauksia oli saatu kyselystä ja kuinka moni oli vastannut mihinkin kysymykseen. Vastaukset ovat valittu niiden olennaisuuden ja tärkeyden mukaan. Tämän tutkimuksen kyselyn vastauksia käydään myös tarkemmin tutkimuksen tuloksissa ja johtopäätöksissä läpi. 71 merenkulun opiskelijaa oli kirjautunut Learn-alustalle kyselyn vastausaikana. Kyselyyn vastasi yhteensä 33 merenkulun opiskelijaa, jolloin vastausten tavoitteeseen päästiin. Learn-alustalla oli kuitenkin 315 merenkulun opiskelijaa lisättynä. Osa merenkulun opiskelijoista oli mahdollisesti myös harjoittelussa tai töissä kyselylomakkeen vastausaikana, jolloin opiskelija ei ole välttämättä avannut Learn-alustaa. Kyselyn vastaamiseen voi vaikuttaa myös opiskelijoiden aktiivisuus.

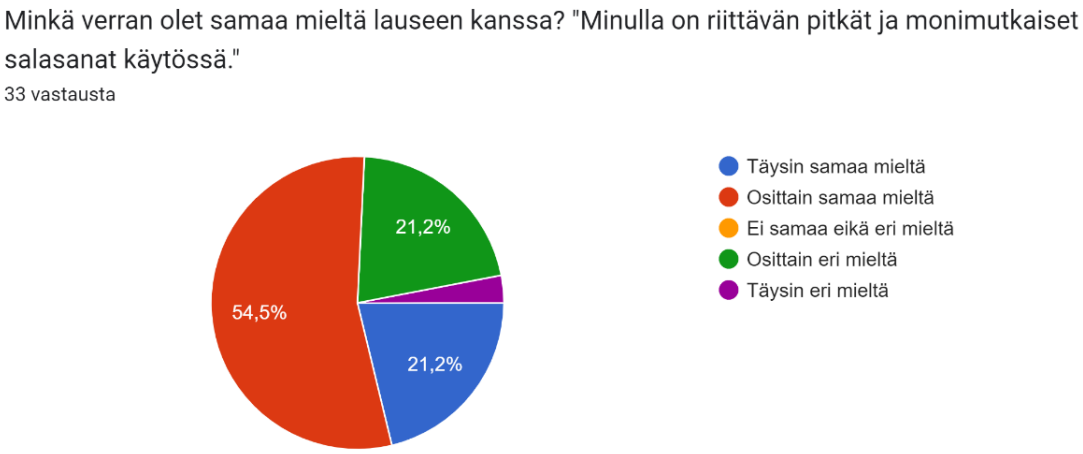
Opiskelijat olivat eri vuoden merenkulun opiskelijoita, mikä vaikutti vastausten vaihtelevuuteen. Ensimmäisen vuoden opiskelijoita vastasi 9, toisen vuoden opiskelijoita 8, kolmannen vuoden opiskelijoita 7, neljännen vuoden opiskelijoita 5 ja muita opiskelijoita 4. Muihin opiskelijoihin kuului esimerkiksi viidennen vuoden opiskelijoita ja tyhjiä ”muu opiskelija” vastauksia. Noin 60 % opiskelijoista on ollut harjoittelussa merellä olevalla aluksessa ja noin 33 % on ollut töissä ja harjoittelussa merellä olevalla aluksessa. Opiskelijoilla oli ollut kokemusta itse merenkulusta ja sen ympäristöstä.



Kuva 11 Merenkulun kyberhyökkäykset

Kuva 11 kertoo, että suurin osa opiskelijoista ei ollut tietoisia minkälaisia kyberhyökkäyksiä merenkulun alalle on tehty. 22 opiskelijaa (66,7 %) vastasi, että he eivät olleet tietoisia merenkulun kyberhyökkäyksistä. 3 opiskelijaa (9,1 %) vastasi, että ei osaa sanoa. Loput 8 opiskelijaa (24,2%) olivat tietoisia siitä, minkälaisia kyberhyökkäyksiä merenkulun alalle oli tehty. Vastauksiin voi vaikuttaa se, että merenkulun kyberhyökkäykset eivät ole tulleet esille opintojen aikana tai aiheeseen ei olla perehdytty. Merenkulun kyberhyökkäyksistä olisi tärkeää tietää, jotta tunnistettaisiin hyökkäysten vaikutus merenkulussa. Sen lisäksi voidaan varautua myös erilaisiin kyberhyökkäyksiin. Vastaus tuli yllätyksenä, kun ”en”-vastauksien määrä oli niin suuri. Esimerkiksi NotPetya-haittaohjelma on erittäin tunnettu kyberhyökkäys merenkulun alalla, mutta suuri osa merenkulun opiskelijoista ei tiennyt siitäkään.

Meland ym. (2020, 528) mainitsevat, että merenkulun alalla ei ole ollut eniten kyberhyökkäyksiä, mutta niillä on ollut kaikista vakavimpia seurauksia. Tämän lisäksi he kertoivat, että merenkulun kyberhyökkäyksien tietämyksessä on puutteita ja siitä ei ole välttämättä tarpeeksi tietoa.



Kuva 12 Salasanojen monimutkaisuus

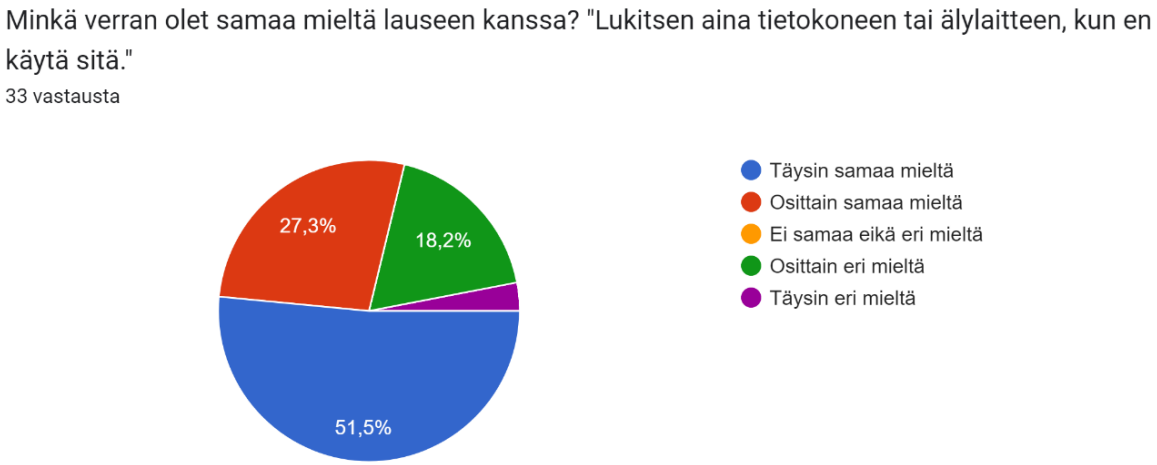
Kuvan 12 mukaan 18 opiskelijaa (54,5 %) oli osittain sitä mieltä, että heillä on riittävän pitkät ja monimutkaiset salasanat käytössä. 7 opiskelijaa (21,2 %) oli täysin samaa mieltä ja sama määrä osittain eri mieltä. 1 opiskelija oli täysin eri mieltä lauseen kanssa. Monella voi olla myös erilainen käsitys riittävästä ja pitkästä salasanasta. Kysymyksen olisi voinut muotoilla myös eri tavalla ja antaa esimerkin riittävän pitkästä ja monimutkaisesta salasanasta. Tähän kysymykseen olisi voinut antaa esimerkin, että monimutkainen salasana on ainakin 12 merkkiä pitkä ja se sisältää erikoismerkkejä, numeroita ja isoja sekä pieniä kirjaimia. Vastauksista kuitenkin suuri osa käytti omasta mielestään riittävän pitkiä ja monimutkaisia salasanoja.

Kuva 13 IT- ja OT-järjestelmien tietämys

Kuva 13 näyttää, että 14 opiskelijaa (42,4 %) tiesi mitä IT- ja OT-järjestelmät tarkoittivat. Toiset 14 opiskelijaa (42,4 %) vastasivat, että eivät ole tietoisia IT-

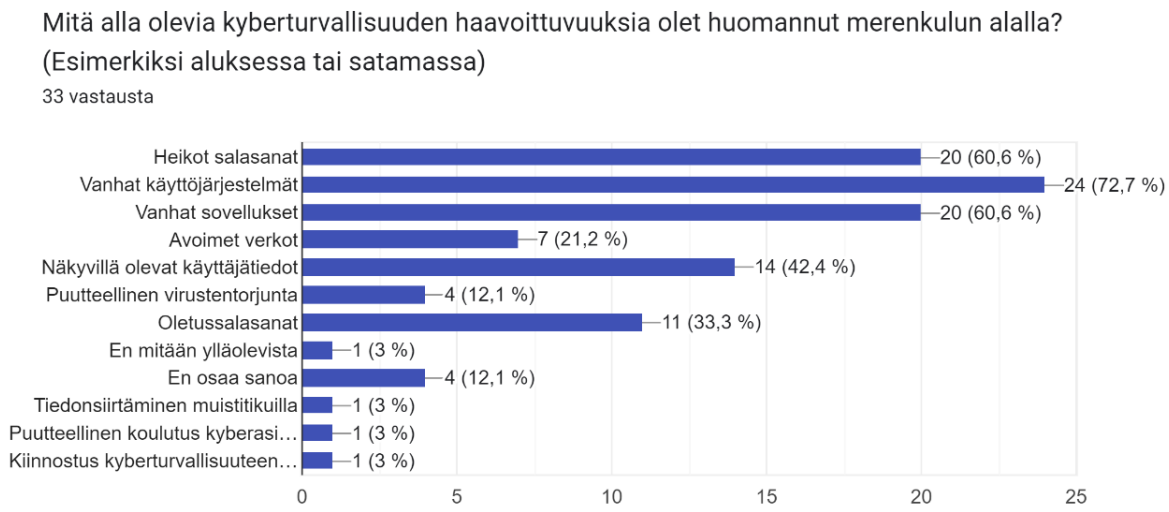
ja OT-järjestelmistä. 5 opiskelijaa (15,2 %) vastasi ”En osaa sanoa”. ”En osaa sanoa” -vastauksista voidaan todeta, että vastaajat eivät tienneet mitä kyseiset järjestelmät tarkoittavat. ”’En osaa sanoa” -vastauksia oli lisätty, jotta kysymysten vastaaminen tuntui helpommalta vastaajille. Tämän kysymyksen vastauksiin voi vaikuttaa myös eri vuoden merenkulun opiskelijat. Suuri osa vastaajista oli ensimmäisen vuoden ja toisen vuoden merenkulun opiskelijoita. IT- ja OT-järjestelmien tietämys on kuitenkin tärkeää merenkulun kyberturvallisuudessa.

Meland ym. (2020, 519) mainitsevat, että merenkulussa IT- ja OT-järjestelmien uhat kasvavat, jonka takia voi syntyä vakavia taloudellisia seurauksia ja maineen haittaa. Merenkulun opiskelijoiden tulisi tietää IT- ja OT-järjestelmistä, sekä niiden haavoittuvuuksista.



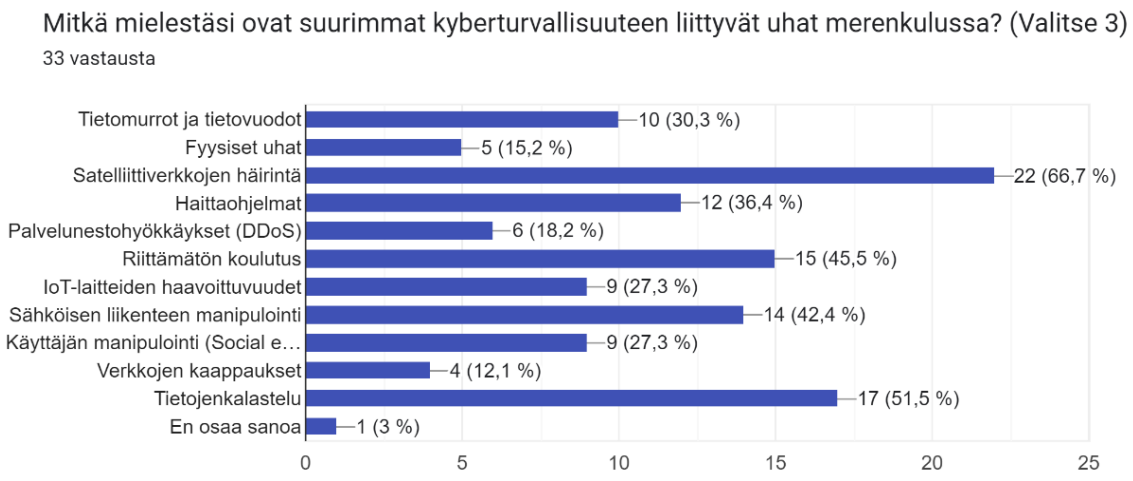
Kuva 14 Tietokoneen ja älylaitteiden lukitus

17 opiskelijaa (51,5 %) kertoi lukitsevansa tietokoneen tai älylaitteen aina kun ei käytä sitä kuvan 14 mukaan. 9 opiskelijaa (27,3 %) oli osittain samaa mieltä ja 6 opiskelijaa (18,2 %) osittain eri mieltä. 1 opiskelija oli taas täysin eri mieltä lauseen kanssa. Tietokoneen ja älylaitteen lukitus on tärkeää, koska lukitsematon älylaite tai tietokone voi päästä muiden tahojen käsiin. Lukitsematon tietokone tai älylaite luo turhia riskejä, jolta voidaan helposti välttyä. Vastausten perusteella voidaan todeta, että enemmistö opiskelijoista lukitsee aina tietokoneen tai älylaitteen, kun ei käytä sitä.



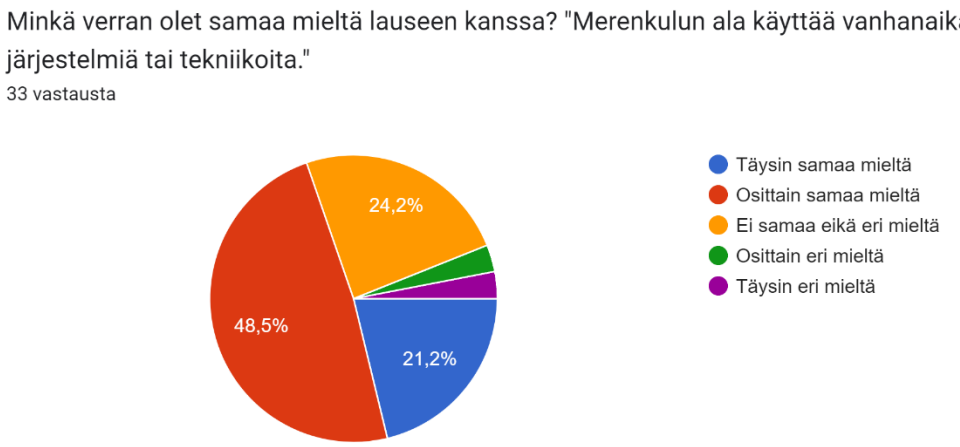
Kuva 15 Kyberturvallisuuden haavoittuvuudet merenkulussa

Merenkulun opiskelijoilta kysyttiin, mitä haavoittuvuuksia he ovat nähneet merenkulun alalla kuvan 15 mukaan. Merenkulun alalla tarkoitettiin kyberturvallisuuden haavoittuvuuksia esimerkiksi aluksissa tai satamissa. Tähän voi kuulua harjoittelut ja työpaikat. Kuva 15 osoittaa, että merenkulun opiskelijat ovat huomanneet eniten vanhoja käyttöjärjestelmiä, heikkoja salasanoja sekä vanhoja sovelluksia. 24 opiskelijaa (72,7 %) vastasi ”Vanhat käyttöjärjestelmät” ja 20 opiskelijaa (60,6 %) vastasi ”Heikot salasanat” ja ”Vanhat sovellukset”. Opiskelijat olivat lisänneet myös omia vastauksia kuten ”Tiedonsiirtäminen muistitikulla”, ”Puuttellinen koulutus kyberasioissa” ja ”Kiinnostus kyberturvallisuuteen heikko”. Vastauksista tuli ilmi, että opiskelijat ovat huomanneet hyvin paljon vanhaa teknologiaa. Oletussalasanojen määrä yllätti myös sen suuren määrän takia. Oletussalasanoja ei tulisi olla ollenkaan käytössä, koska se mahdollistaa helpon murtautumisen. Onko merenkulun organisaatioissa huomattu, että he käyttävät oletussalasanoja vai eikö sen vaihtamista pidetä tarpeellisena?



Kuva 16 Kyberturvallisuuden uhat merenkulussa

Merenkulun opiskelijoiden mielestä suurimpia uhkia merenkulun kyberturvallisuudessa ovat satelliittiverkkojen häirintä, tietojenkalastelu ja riittämätön koulutus kuvan 16 mukaan. 22 opiskelijaa (66,7 %) vastasi satelliittiverkkojen häirintä, 17 opiskelijaa (51,5 %) vastasi tietojenkalastelu ja 15 opiskelijaa (45,5 %) vastasi riittämätön koulutus. Kysymykseen oli rajattu 3 vastausta, jotta saataisiin tarkempia tuloksia. Satelliittiverkkojen häirinnän määrä oli yllättävän suuri, kun oletettiin, että tietojenkalastelu, riittämätön koulutus tai käyttäjän manipulointi olisi ollut suurempana uhkana. Tästä voidaan myös todeta, tiesivätkö merenkulun opiskelijat mitä tietyt kyberturvallisuuden uhat tarkoittavat? Voi olla mahdollista, että käyttäjän manipulointi ei ole tullut aikaisemmin vastaan tai esimerkiksi palvelunestohyökkäysten tarkoitusta ei tiedetty. Tämä lisäksi tiettyjen kyberturvallisuuden uhkien laajuutta tai vaikutusta ei välttämättä ole ollut tiedossa. Vastauksiin voi vaikuttaa myös merenkulun opiskelijoiden omat kokemukset tai ulkoiset tekijät.



Kuva 17 Merenkulun alan järjestelmät

Kuvan 17 mukaan 16 opiskelijaa (48,5 %) oli osittain samaa mieltä, että merenkulun ala käyttää vanhanaikaisia järjestelmiä tai tekniikoita. 7 opiskelijaa (21,2 %) oli täysin samaa mieltä lauseen kanssa ja 8 opiskelijaa (24,2 %) ei ollut samaa eikä eri mieltä. 1 opiskelija oli osittain eri mieltä ja 1 muu opiskelija oli täysin eri mieltä. Opiskelijat olivat huomanneet merenkulun alalla paljon vanhoja käyttöjärjestelmä sekä sovelluksia. Tämän lisäksi heikkoja salasanoja ja näkyvillä olevia käyttäjätietoja oli huomattu myös runsaasti. Suuri osa kyselyn vastaajista oli ensimmäisen ja toisen vuoden merenkulun opiskelijoita. Heillä ei välttämättä ole paljon kokemusta merenkulusta, mutta he ovat todennäköisesti käyneet laivaharjoittelua Xamkissa. Se on mahdollista, että Xamkin laivaharjoittelu on vaikuttanut kyselyn vastauksiin ja opiskelijoiden näkemyksiin. Onko Xamkin laivaharjoittelussa vanhaa teknologiaa käytössä? Suuri osa kuvan 17 vastauksista on kuitenkin myönteisiä lauseen kanssa.

7 YHTEENVETO

Yhteenvedossa läpikäydään tämän tutkimuksen tulokset ja sen johtopäätökset. Tulokset vastaavat tutkimuskysymyksiin, jotka olivat mitkä tekijät luovat merenkulun kyberturvallisuuden haavoittuvuuksia, miksi kyberturvallisuus on tärkeää merenkulussa, miten kyberturvallisuuden haavoittuvuuksia voidaan ennaltaehkäistä merenkulussa ja millainen merenkulun opiskelijoiden kyberturvallisuuden taso on. Tämän lisäksi pohdinnassa läpikäydään tutkimuksen onnistuminen ja sen luotettavuus. Luotettavuudella tarkoitetaan tutkimuksen

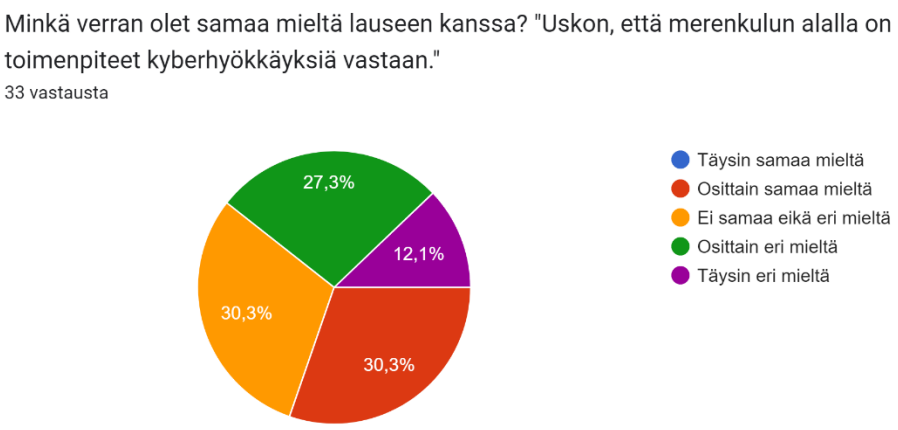
reliabiliteettia ja validiteettia. Reliabiliteetin ja validiteetin tulisi olla riittävä, jotta tutkimus voitaisiin luokitella luotettavaksi.

7.1 Tutkimuksen tulokset

Tutkimuksen tuloksilla vastataan tutkimuskysymyksiin aineiston perusteella. Kyselyn vastauksia analysoidaan vielä tarkemmin ja tässä esitetään merenkulun opiskelijoiden näkemykset ja heidän kyberturvallisuuden tietämyksen taso. Kyberturvallisuuden tietämyksen tasossa on otettu huomioon oppilaiden kokemus merenkulussa ja kyselyn vastauksien vaihtelevuus.

Kuva 18 Kyberhyökkäysten kasvu merenkulussa

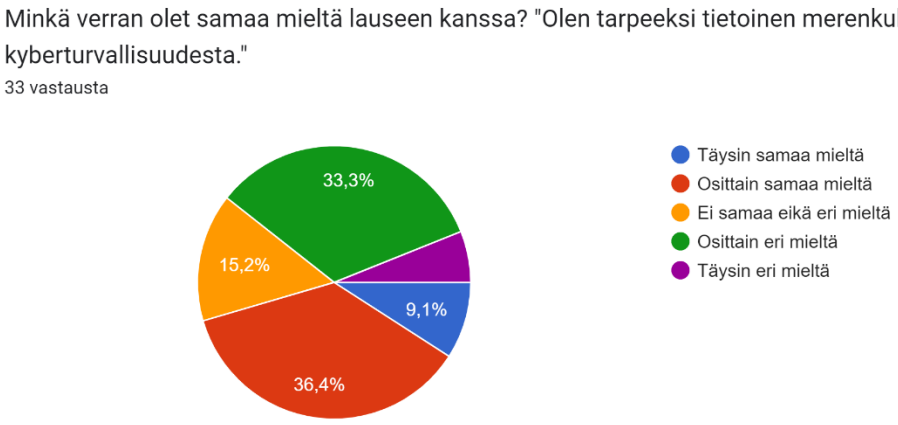
Kuva 18 näyttää, että merenkulun opiskelijoiden mielestä kyberhyökkäykset tulevat kasvamaan tulevaisuudessa. 31 opiskelijaa (93,9 %) vastasi ”Kyllä” ja 2 opiskelijaa (6,1 %) vastasi ”En”. Kukaan opiskelijoista ei vastannut ”En osaa sanoa” eli vastaukset olivat varmoja. Vesa Tuomalan tutkimuksen lopputuloksissa mainittiin, että kyberhyökkäykset tulevat kasvamaan todennäköisesti tulevaisuudessa (Tuomala 2021, 30). Opiskelijoilla oli myös sama näkemys merenkulun kyberhyökkäyksien kasvusta. Merenkulun kyberhyökkäyksien kasvuun voi liittyä monta tekijää ja Xamkin merenkulun opiskelijoiden tulisi varautua kyberhyökkäyksien kasvuun merenkulun alalla.



Kuva 19 Kyberhyökkäysten ennaltaehkäisy merenkulussa

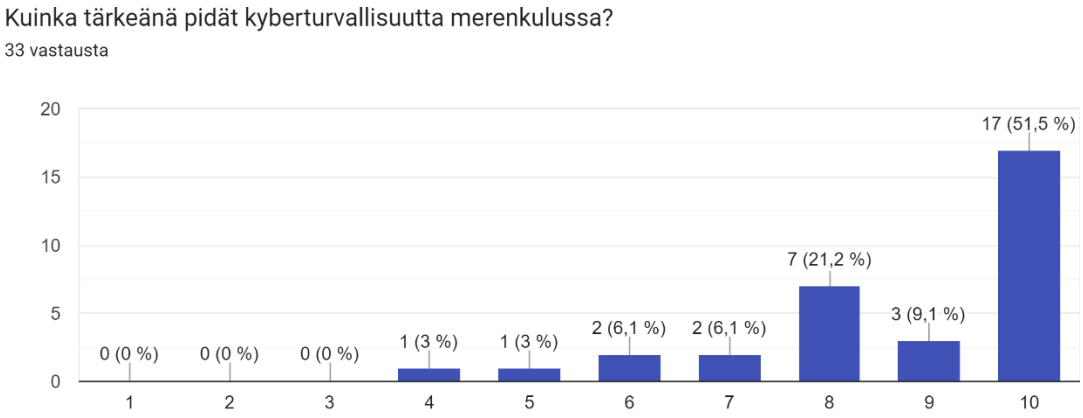
Merenkulun opiskelijoilta kysyttiin kuvan 19 mukaan, onko merenkulun alalla riittävät toimenpiteet kyberhyökkäyksiä vastaan. 4 opiskelijaa (12,1 %) oli täysin eri mieltä, 9 opiskelijaa (27,3 %) oli osittain eri mieltä, 10 opiskelijaa (30,3 %) oli ei samaa eikä eri mieltä ja 10 opiskelijaa (30,3 %) oli osittain samaa mieltä. Vastauksista kukaan ei ollut täysin samaa mieltä lauseen kanssa. Merenkulun opiskelijoilla ei ollut paljon luottamusta siihen, että heidän alallaan olisi riittävät toimenpiteet kyberhyökkäyksiä vastaan.

DNV:n laatimassa kyselyssä 71 % merenkulun ammattilaista oli sitä mieltä, että heidän organisaatiossansa OT-järjestelmissä on riittävät toimenpiteet kyberhyökkäyksiä vastaan. (DNV 2023, 22) Merenkulun ammattilaisilla voi olla enemmän luottamusta merenkulun organisaatioihin heidän tietämyksensä ja kokemuksen perusteella. Xamkin merenkulun opiskelijoilla ei ole välttämättä tarpeeksi kokemusta merenkulusta ja heidän kyberturvallisuutensa tietämyksessä voi olla paljon eroja merenkulun ammattilaisten kanssa. Erona on myös se, että merenkulun ammattilaiset olivat monesta merenkulun organisaatiosta ympäri maailmaa ja kyselyssä oli yli 800 merenkulun ammattilaista. 800 merenkulun ammattilaisen ja 33 Xamkin merenkulun opiskelijan välillä on hyvin suuri ero. On kuitenkin tärkeää tutkia ammattilaisten ja opiskelijoiden välisiä näkemyksiä.



Kuva 20 Tietoisuus kyberturvallisuudesta

Merenkulun opiskelijoilta kysyttiin heidän kyberturvallisuuden tietoisuudestaan kuvan 20 mukaan. Kysymys jakoi vastauksia, jolloin 3 opiskelijaa (9,1 %) oli täysin samaa mieltä ja 11 opiskelijaa (36,4 %) oli osittain samaa mieltä. 5 opiskelijaa (15,2 %) vastasi ei samaa eikä eri mieltä ja 12 opiskelijaa (33,3 %) vastasi osittain eri mieltä. 2 opiskelijaa oli täysin samaa mieltä. Merenkulun opiskelijat tiesivät vaihtelevasti merenkulun kyberturvallisuudesta omasta mielestään. Suuri osa vastaajista eivät olleet täysin varmoja, joka osoittaa sen, että merenkulun opiskelijoiden kyberturvallisuuden tietoisuus voisi olla paremmalla tasolla. Kyberturvallisuuden tietoisuuteen voidaan vaikuttaa esimerkiksi kyberturvallisuuden koulutuksella, ja merenkulun opiskelijat voisivat osallistua myös eri kyberturvallisuuden tapahtumiin.



Kuva 21 Merenkulun kyberturvallisuuden tärkeys

Yli puolet merenkulun opiskelijoista pitivät kyberturvallisuutta erittäin tärkeänä kuvan 21 mukaan. Kysymykseen pystyi vastaamaan asteikolla 0–10 kyberturvallisuuden tärkeydestä. ”0” -vastaus tarkoitti, että kyberturvallisuus ei ole lainkaan tärkeää merenkulussa ja ”10” -vastaus tarkoitti, että kyberturvallisuus on erittäin tärkeää merenkulussa. Kyberturvallisuuden tärkeyteen voi vaikuttaa se, että opiskelijat ovat huomanneet paljon vanhoja käyttöjärjestelmiä ja sovelluksia merenkulussa. Tämän lisäksi he olivat huomanneet vanhoja salasanoja ja oletussalasanoja. Heidän kokemuksensa perusteella kyberturvallisuus on ollut puutteellista merenkulussa, joka voi luoda ajatuksen siitä, että merenkulun kyberturvallisuudessa olisi parannettavaa. Tämän takia merenkulun opiskelijat voivat pitää kyberturvallisuutta erittäin tärkeänä merenkulussa.

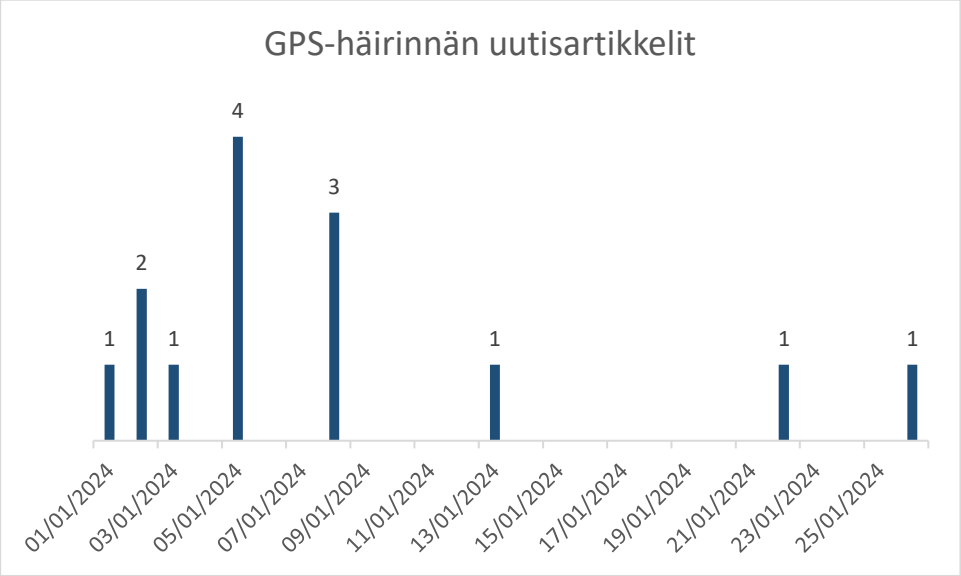
Merenkulun opiskelijoilta kysyttiin että ”Onko mielestäsi merenkulun alalla jotain kehitettävää kyberturvallisuuden suhteen?”. Kysymykseen pystyi vastaamaan vapaamuotoisesti. Alla olevaan luetteloon on kerätty kysymyksien vastauksia suoralla lainauksella:

- ” Järjestelmien verkottumisen hallinta”
- ”Koulutus”
- ” Kaikki laitteet, jotka yhteydessä internettiin, voisi olla paremmin suojattuja”
- ” Ennakoiva koulutus, suljettu verkko, riittävä verkkoturva”
- ” Kyberturvallisuuteen liittyvät koulutusmateriaalit ovat usein aika raskaita ja vaikeasti ymmärrettäviä/lähestyttäviä tietopaketteja, jos kyberturvallisuus ei ole aiheena entuudestaan kovin tuttu.”
- ” Vanha viisaus koskien kaikkea digitaalista toimintaa: Mikä on luotu 0/1 järjestelmällä voidaan muuttaa 0/1 järjestelmällä.”
- ” Paljon vanhanaikaisia sovelluksia käytössä. Merenkulun rahtien liikkuvuudesta vastaavien järjestelmien tulisi olla todella hyvin suojattu, sillä niiden murtaminen ja tekeminen käyttökelvottomaksi johtaisi pahimmillaan siihen, että ei tiedetä mihin pitäisi mennä, mitä lastia on tulossa ja mihin se pitäisi viedä.”

- ” Ice järjestelmä näkyy kaikkialla. Antaa tietoa kaikille joilla on ice laivojen liikkeistä.”

- ”Järjestelmien modernisointi sekä suurempi huomio kyberturvallisuuteen palomuurejen yms kanssa.”

Merenkulun opiskelijoiden vastaukset koostuivat pääosin kyberturvallisuuden koulutuksesta, verkon suojauksesta ja järjestelmien kyberturvallisuudesta. Merenkulun ammattilaisten mielestä toiseksi suurimpaan kyberturvallisuuden haasteeseen kuului koulutuksen puute kyberturvallisuudessa DNV:n kyselyn mukaan. (DNV 2023, 28). Tämä on yhteinen asia, joka tuli ilmi merenkulun opiskelijoiden ja merenkulun ammattilaisten vastausten perusteella. Merenkulun kyberturvallisuuden koulutuksessa olisi siis parannettavia asioita. Kyberturvallisuuden koulutus tulisi olla myös ymmärrettävää jokaiselle.



Kuva 22 GPS-häirinnän uutisartikkeleiden määrä

Opiskelijat pitivät suurimpana merenkulun kyberturvallisuuden uhkana satelliittiverkkojen häirintää kyselyn vastausten arvioinnissa. Opiskelijoiden vastauksiin on voinut myös vaikuttaa kyselyn ja GPS-häirinnän uutisoinnin ajankohta. GPS-signaalien häirinnästä uutisoitiin tammikuussa 2024 runsaasti ja kysely toteutettiin 29.1.2024–12.2.2024 välisenä aikana. Tätä varten kerättiin uutisartikkeleita ”GPS-häirintä” google haun avulla. Uutisartikkelit kerättiin verkon kautta, jonka aikaväliksi laitettiin 1.1–12.2.2024. Tämän jälkeen löytyi yhteensä 14 uutisartikkelia GPS-häirinnästä kuvan 22 mukaan. Uutiset koostui-

vat Ylen, HS:n, Ilta-Sanomien, Demokraatti.fi:n, Tekniikka & talouden, Iltalehden ja Verkkouutisten artikkeleista. Uutisartikkelit liittyivät Venäjän GPS-häirintään Itämerellä ja GPS-häirinnän vaikutuksiin. Kysely oli luotu uutisten jälkeen samassa kuussa, jonka takia kyselyn vastauksiin on voinut hyvin paljon vaikuttaa GPS-häirinnän uutisointi. Uutisointi on voinut vaikuttaa opiskelijoiden vastauksiin, kun aihe on ollut hyvin ajankohtainen asia.

7.2 Tutkimuskysymyksiin vastaaminen

Tässä luvussa vastataan opinnäytetyön tutkimuskysymyksiin, jotka ovat listattuna alla oleviin luetteloihin. Tutkimuskysymyksiin vastataan opinnäytetyön tuloksien perusteella.

- Mitkä tekijät luovat merenkulun kyberturvallisuuden haavoittuvuuksia?

Ensimmäiseen tutkimuskysymykseen vastattiin kertomalla, että merenkulun kyberturvallisuuden haavoittuvuuksia syntyy inhimillisistä ja teknologisista tekijöistä. Inhimilliset tekijät voivat olla esimerkiksi puutteellinen kyberturvallisuus ja oma huolimattomuus. Nämä ovat siis ihmisten luomia haavoittuvuuksia, jota voidaan hyödyntää muun muassa käyttäjän manipuloinnilla ja informaatiovaikuttamisella. Teknologiset tekijät ovat järjestelmien, ohjelmistojen ja sovelluksien riittämätön suojaus tai päivitys. Tähän voi kuulua esimerkiksi nollapäivähaavoittuvuudet, vanhat käyttöjärjestelmät ja alusten digitalisoinnin vaikutus.

- Miksi kyberturvallisuus on tärkeää merenkulussa?

Kyberturvallisuus on tärkeää merenkulussa, koska kyberhyökkäykset voivat levitä eri järjestelmiin ja tehdä valtavaa vahinkoa. GNSS-, AIS- ja ECDIS-järjestelmät ovat esimerkiksi haavoittuvuuksia kyberhyökkäyksille. ECDIS-järjestelmässä haavoittuvuuksista huomattiin, että merenkulun alusten järjestelmät voivat sisältää paljon erilaisia haavoittuvuuksia. NotPetya -kiristyshaittaohjelma on myös hyvä esimerkki siitä, miten voi käydä pahimmassa tapauksessa kyberhyökkäysten suhteen. Kiristyshaittaohjelmat alkavat olemaan myös suurempi ongelma merenkulussa ja kyberhyökkäykset tulevat todennäköisesti kasvamaan tulevaisuudessa.

- Miten kyberturvallisuuden haavoittuvuuksia voidaan ennaltaehkäistä merenkulussa?

Merenkulun kyberturvallisuuden haavoittuvuuksia voidaan ennaltaehkäistä kyberturvallisuuskoulutuksella ja kyberhyökkäyksiin varautumisella. Kyberhyökkäysten varautumiseen kuuluu järjestelmien kovennus kuten verkkojen segmentointi, virustentorjunta, monitorointi ja lokitus. Salasanojen kuuluisi olla myös turvalliset ja monimutkaiset eikä oletussalasanoja kuuluisi olla lainkaan käytössä. Navigoinnin järjestelmissä kuuluisi olla myös käytössä hälytys, joka hälyttää sijainnin muuttumisesta tai katoamisesta.

- Millainen merenkulun opiskelijoiden kyberturvallisuuden tietämyksen taso on?

Merenkulun opiskelijoiden kyberturvallisuuden tietämyksen taso oli tyydyttävällä tasolla. Merenkulun opiskelijat osasivat ilmaista ongelmia merenkulun kyberturvallisuudessa ja he suhtautuivat kyberturvallisuuteen vakavasti. Lisäksi opiskelijat ymmärsivät kyberturvallisuuden merkityksen merenkulussa, ja osa oppilaista olivat myös lisänneet omia vastauksia kyselyn kysymyksiin. Valtaosa opiskelijoista käyttivät omasta mielestä riittävän pitkiä ja monimutkaisia salasanoja sekä päivittivät säännöllisesti sovelluksia ja järjestelmiä, joita he käyttivät.

Opiskelijat pitivät kyberturvallisuutta tärkeänä merenkulussa, mutta suuri osa merenkulun opiskelijoista ei kuitenkaan tiennyt minkälaisia kyberhyökkäyksiä merenkulun alalle on tehty. Merenkulun alan opiskelijoiden kuuluisi tietää minkälaisia kyberhyökkäyksiä merenkulun alalle on tehty, jotta he ymmärtäisivät kyberturvallisuuden riskeistä ja haavoittuvuuksista merenkulussa. IT- ja OT-järjestelmät olivat myös tuntemattomia suurelle osalle opiskelijoista. IT- ja OT-järjestelmät ovat tärkeä osa merenkulun kyberturvallisuutta, jotka opiskelijoiden kuuluisivat tietää. Tähän voi kuitenkin vaikuttaa eri vuoden opiskelijat, jotka ei välttämättä tiedä vielä järjestelmien tarkoituksesta. Lisäksi suuri osa merenkulun opiskelijoista ei ollut täysin varmoja siitä, että he ovat tarpeeksi tietoisia merenkulun kyberturvallisuudesta. Tämä osoitti sen, että heidän kyberturvallisuutensa tietämyksessä olisi vielä parannettavaa.

7.3 Johtopäätökset

Tutkimusongelmana oli se, että Xamkin merenkulun opiskelijoiden kyberturvallisuuden tietämyksen tasoa ei tiedetty. Opiskelijoiden kyberturvallisuuden tietämyksen taso oli tyydyttävällä tasolla, koska opiskelijat ymmärsivät kyberturvallisuuden tärkeyden, mutta kyberturvallisuuden tietämyksessä oli puutteita. Opiskelijoiden kyberturvallisuuden tietoisuus voisi olla siis paremmalla tasolla. Opiskelijoiden vastauksiin vaikutti heidän kokemuksensa merenkulusta ja mahdollisesti GPS-häirinnän uutisointi. Merenkulun kyberturvallisuuden koulutuksessa olisi myös parannettavia asioita merenkulun opiskelijoiden ja merenkulun ammattilaisten mielestä. Riittämättömän kyberturvallisuuden koulutuksen takia voi syntyä kyberturvallisuuden haavoittuvuuksia merenkulussa.

Tarpeenmukaisella kyberturvallisuuden koulutuksella voidaan ennaltaehkäistä kyberturvallisuuden haavoittuvuuksia ja merenkulun kyberhyökkäyksiä. Kyberturvallisuuden koulutus tulisi olla myös ymmärrettävää jokaiselle. Tämän lisäksi merenkulun kyberhyökkäykset kasvavat todennäköisesti tulevaisuudessa ja merenkulun opiskelijoiden pitäisi varautua niihin asianmukaisesti. Merenkulun opiskelijoiden olisi hyvä tietää merenkulun kyberhyökkäyksistä, jotta voitaisiin ymmärtää, minkälaisia kyberhyökkäyksiä merenkulkuun on mahdollista tehdä, ja mitä ne voivat luoda aikaan. Xamkin merenkulun opiskelijoiden tulisi siis varautua tulevaisuuteen tutustumalla kyberturvallisuuteen syvällisemmin.

7.4 Pohdinta

Opinnäytetyö oli pääsääntöisesti onnistunut tutkimus, koska kyselyyn osallistui tarpeeksi vastaajia ja vastaajilta saatiin tarpeellista tietoa aiheesta. Tutkimuksen luotettavuuteen vaikutti myös moni asia. Esimerkiksi kaikkiin tutkimuskysymyksiin vastattiin perusteellisesti ja opinnäytetyössä tutkittiin oleellisia asioita. Näiden lisäksi dokumentaatiota oli tehty riittävästi ja tulokset johdettiin aineiston perusteella. Lopputuloksena päästiin samankaltaisiin tuloksiin kuin teoreettisen viitekehyksen tutkimuksissa. Toimeksiantajan kautta saatiin myös jaettua kysely mahdollisimman monelle Xamkin merenkulun opiskelijalle.

Suuri osa tämän tutkimuksen kyselyn kysymyksistä oli olennaisia kysymyksiä, mutta osa kysymyksistä olisi voineet muotoilla eri tavalla. Kysely olisi voinut olla myös lyhyempi, koska tietyt kysymykset tuntuivat tarpeettomilta. Kysely saattoi tuntua pitkältä, kun siinä oli 29 kysymystä ja kyselyn olisi voinut myös rajata toisen vuoden opiskelijoista ylöspäin. Ensimmäisen vuoden opiskelijoilla ei välttämättä ole tarpeeksi kokemusta merenkulusta, vaikka olisivat olleet jo harjoittelussa.

Opinnäytetyön luonnissa oli kuitenkin ongelmia, koska aineistonkeruu ja tutkimuksen lopputulos oli puutteellista suunnitteluvaiheessa. Tämän takia opinnäytetyön tekeminen oli epävarmaa ja hankalaa suunnitteluvaiheen aikana. Opinnäytetyöhön tuli paljon muutoksia, jolloin aikataulussa ei pysytty alkuperäisen suunnitelman mukaan. Alun perin haluttiin laatia opinnäytetyö merenkulun kyberturvallisuuden haavoittuvuuksista, koska se oli hyvin kiinnostava aihe. Aihe oli kuitenkin laaja ja opinnäytetyössä ei ollut tarpeeksi suunniteltu sitä, minkälaisen tutkimuksen aiheesta voisi tehdä. Kyselylomaketta ei ollut vielä suunnitteluvaiheessa myöskään laadittu. Näiden syiden takia tutkimuksen luotettavuus kärsi. Opinnäytetyön aikana saatiin kuitenkin palautetta ohjaajilta. Palautteen myötä tehtiin muutoksia, jolloin saatiin selkeämpi tutkimus ja järkevä lopputulos opinnäytetyöhön. Opinnäytetyö olisi ollut aikataulun mukaan valmis, jos suunnitteluvaiheessa olisi tehty tarpeelliset muutokset aikaisemmin.

Opinnäytetyössä tutkittiin merenkulun kyberturvallisuuden haavoittuvuuksia aineiston avulla. Aineistosta löytyi eroavasti tietoa eri aiheista. Esimerkiksi merenkulun alusten eri järjestelmien kyberturvallisuudesta ei löytynyt paljon luotettavaa materiaalia tai siinä oli puutteita. NotPetya -kyberhyökkäyksestä ja kyberturvallisuuden käytännöistä löytyi taas valtavasti tietoa. Aineistolla vastattiin kaikkiin tutkimuskysymyksiin. Tutkimuskysymyksiin vastattiin kertomalla millä tasolla opiskelijoiden kyberturvallisuuden tietämyksen taso oli ja esittämällä miksi kyberturvallisuus on tärkeää merenkulussa. Merenkulun kyberturvallisuuksien haavoittuvuuksien syntyminen ja ennaltaehkäisy käytiin myös lävitse opinnäytetyössä. Opinnäytetyötä tehtiin kuitenkin satunnaisesti ja sen tekemisessä ei ollut aina rutiinia. Tämän takia jotkut opinnäytetyön osiot voivat olla sekalaisempia kuin toiset. Opinnäytetyön luomisessa joutui myös oppimaan paljon uusia asioita, johon meni myös huomattavasti aikaa. Vaikka työn

tekeminen oli ajoittain hankalaa ja parannettavaa olisi tietyissä osioissa, niin opinnäytetyön lopputulokseen ollaan kuitenkin tyytyväisiä.

Tutkimukselle voidaan tehdä jatkokehitystä laatimalla kysely myöhempien vuosien merenkulun opiskelijoille. Sen jälkeen voidaan vertailla tämän tutkimuksen kyselyn tuloksia myöhempien vuosien merenkulun opiskelijoiden kanssa. Vertailussa voidaan tutkia mihin suuntaan merenkulun opiskelijoiden kyberturvallisuuden tietämyksen taso on mennyt ja miten sitä voitaisiin mahdollisesti kehittää. Tätä voidaan myös laajentaa laatimalla kysely suomalaisten merenkulun organisaatioille tai merenkulun ammattilaisille. Tästä voidaan huomata mitä eroja kyberturvallisuuden näkemyksessä on Xamkin merenkulun opiskelijoiden ja suomalaisten merenkulun ammattilaisten välillä.

LÄHTEET

About ICS. s.a. International Chamber of Shipping. WWW-dokumentti. Saatavissa: https://www.ics-shipping.org/about-ics/ [viitattu 7.9.2023].

About ISO. s.a. International Organization for Standardization. WWW-dokumentti. Saatavissa: https://www.iso.org/about-us.html [viitattu 10.9.2023].

Above Us Only Stars. 2019. Center for Advanced Defence Studies. PDF-dokumentti. Saatavissa: https://c4ads.org/reports/above-us-only-stars/ [viitattu 20.3.2024].

AIS (Automatic Identification System) overview. 2021. North Atlantic Treaty organization. WWW-dokumentti. Saatavissa: https://shipping.nato.int/nsc/operations/news/2021/ais-automatic-identification-system-overview [viitattu 4.3.2024].

Balduzzi M, Pasta A & Wilhoit K. 2014. A Security Evaluation of AIS. PDF-dokumentti. Saatavissa: https://documents.trendmicro.com/assets/white_papers/wp-a-security-evaluation-of-ais.pdf [viitattu 13.3.2024].

Cyber Security & Ships. 2020. eDOTSolutions. PDF-dokumentti. Saatavissa: https://www.edot-solutions.com/Brochure/eDOT-CyberSecurityAndShips-WhitepaperVer6Oct2020.pdf [viitattu 21.2.2024].

Frequently Asked Questions. s.a. International Maritime Organization. WWW-dokumentti. Saatavissa: https://www.imo.org/en/About/Pages/FAQs.aspx [viitattu 1.9.2023].

Geollect AIS spoofing analysis featured by UKRINFORM. 2023a. Geollect. WWW-dokumentti. Saatavissa: https://www.geollect.com/news/geollect-ais-analysis-featured-by-ukrinform/ [viitattu 5.3.2024].

Geollect featured by TradeWInds – AIS data spoofed to move 60 ships to Iran's Bandar Abbas airport. 2023b. Geollect. WWW-dokumentti. Saatavissa: https://www.geollect.com/news/geollect-featured-by-tradewinds-ais-data-spoofed-to-move-60-ships-to-irans-bandar-abbas-airport/ [viitattu 5.3.2024].

Guidelines on maritime cyber risk management. 2022. International Maritime Organization. PDF-Dokumentti. Saatavissa: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf [viitattu 10.8.2023].

Haavoittuvuudet – miten niistä ilmoitetaan oikein. 2020a. Liikenne- ja viestintävirasto Traficom. WWW-dokumentti. Päivitetty 23.03.2023. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuudet-miten-niista-ilmoitetaan-oikein [viitattu 13.9.2023].

Haavoittuvuus SMTP-protokollan toteutuksissa useissa eri sähköpostiohjelmistoissa. 2024. Liikenne- ja viestintävirasto Traficom. WWW-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_10/2022 [viitattu 28.2.2024].

Huoltovarmuusorganisaatio. s.a. Huoltovarmuuskeskus. WWW-dokumentti. Saatavissa: https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio [viitattu 12.9.2023].

Jaakkoja J & Juonala L. 2022. Merenkulun kyberturvallisuus ja kyberhyökkäysten vaikutus kansainväliseen kauppaan. LAB-ammattikorkeakoulu. Opinnäytetyö. PDF-dokumentti. Saatavissa: https://urn.fi/URN:NBN:fi:amk-202201251667 [viitattu 15.10.2023].

Jamming and Spoofing of Global Navigation satellite Systems (GNSS). 2019. INTERTANKO. PDF-dokumentti. Saatavissa: https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf [viitattu 5.3.2024].

Kananen J. 2019. Opinnäytetyön ja pro gradun pikaopas. Avain opinnäytetyön ja pro gradun kirjoittamiseen. Jyväskylä: Jyväskylän ammattikorkeakoulu. E-kirja. Saatavissa: https://kaakkuri.finna.fi/Record/kaakkuri.225239?sid=3072261111. [viitattu 13.8.2023].

Kyberturvallisuuden sanasto. 2018. Turvallisuuskomitea. PDF-dokumentti. Saatavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf [viitattu 18.10.2023].

Kyberturvallisuus. s.a. Sisäministeriö. WWW-dokumentti. Saatavissa: https://intermin.fi/kansallinen-turvallisuus/kyberturvallisuus [viitattu 25.4.2024].

Kyberturvallisuus: käyttäjän manipulointi. 2023. Eurooppa-neuvosto. Euroopan unionin neuvosto. WWW-dokumentti. Saatavissa: https://www.consilium.europa.eu/fi/policies/cybersecurity/cybersecurity-social-engineering/ [viitattu 7.2.2024].

Kyselylomakkeen laatiminen. s.a. Tietoarkisto. WWW-dokumentti. Saatavissa: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvanti/kyselylomake/laatiminen/ [viitattu 16.1.2024].

Man in the Middle. 2021. Microsoft. WWW-dokumentti. Saatavissa: https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-sstp/4a6778bc-a4a9-46c6-9120-7493c61f95e5 [viitattu 18.3.2024].

Maritime Cyber Priority. 2023. DNV. PDF-dokumentti. Saatavissa: https://www.dnv.com/cybersecurity/cyber-insights/maritime-cyber-priority-2023.html [viitattu 28.9.2023].

Meland P.H., Bernsmed K, Wille E, Rødseth Ø.J. & Nesheim D.A. 2021. A Retrospective Analysis of Maritime Cyber Security Incidents.t PDF-dokumentti. Saatavissa: https://www.transnav.eu/Article_A_Retrospective_Analysis_of_Maritime_Cyber_Security_Incidents_Meland,59,1144.html [viitattu 10.8.2023].

Merenkulun Kyberturvallisuus –Alusten parhaat käytännöt. 2021. Huoltovarmuusorganisaatio, Vesikuljetuspooli. PDF-dokumentti. Saatavissa:

https://www.huoltovarmuuskeskus.fi/files/a3512a9ae47541a92f002c60c6fa3030dc5327d3/kyberturvallisuus-parhaat-kaytannot-aluksille.pdf [viitattu 6.4.2024].

Microsoftin MSHTML-nollapäivähaavoittuvuus mahdollistaa komentojen suorittamisen etänä. 2021. Liikenne- ja viestintävirasto Traficom. WWW-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_26/2021 [viitattu 28.2.2024].

Mitä on kyberturvallisuus? s.a. F-Secure. WWW-dokumentti. Saatavissa: https://www.f-secure.com/fi/articles/what-is-cyber-security [viitattu 13.9.2023].

Merenkulku ja logistiikka. s.a. Kaakkois-Suomen ammattikorkeakoulu Xamk. WWW-dokumentti. Saatavissa: https://www.xamk.fi/koulutus/merenkulkujalogistiikka/ [viitattu 18.9.2023].

Mäkelä, T. 2022. Varaudu kyberhyökkäykseen – kyse ei ole jos, vaan milloin. Elisa. WWW-dokumentti. Saatavissa: https://yrityksille.elisa.fi/ideat/varaudu-kyberhyokkaykseen-kyse-ei-ole-jos-vaan-milloin/ [viitattu 13.9.2023].

Määrällinen analyysi. 2021. Koppa. WWW-dokumentti. Saatavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineiston-analyysimenetelmat/maarallinen-analyysi [viitattu 23.4.2024].

Naval Dome: Cyberattacks on OT Systems on the Rise. 2020. The Maritime Executive. WWW-dokumentti. Saatavissa: https://www.maritime-executive.com/article/naval-dome-cyberattacks-on-ot-systems-on-the-rise [viitattu 10.8.2023].

NotPetya: A Columbia University Case Study. 2022. Columbia University. PDF-dokumentti. Saatavissa: https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf [viitattu 29.2.2024].

Ohjeita opinnäytetyön suunnitteluun. XAMK. 2019. WWW-dokumentti. Saatavissa: https://www.xamk.fi/wp-content/uploads/2019/03/Liite-Ohjeita-opinnaytetyon-suunnitteluun.pdf [viitattu 19.1.2024].

Petya Or NotPetya: Why the Latest Ransomware Is Deadlier Than WannaCry. 2017. Forbes WWW-dokumentti. Saatavissa: https://www.forbes.com/sites/thomasbrewster/2017/06/27/petya-notpetya-ransomware-is-more-powerful-than-wannacry/?sh=42fccdbb532e [viitattu 5.3.2024].

Remote Code Execution. 2023. Amit Sheps. WWW-dokumentti. Saatavissa: https://www.aquasec.com/cloud-native-academy/cloud-attacks/remote-code-execution/ [viitattu 21.3.2024].

Riskianalyysi ja riskienhallinta. s.a. Luvat ja valvonta. WWW-dokumentti. Saatavissa: https://luvatjavalvonta.fi/tyokalut/riskianalyysi-ja-riskienhallinta/ [viitattu 25.4.2024].

Riskienhallinta. s.a. Työturvallisuuspakki. WWW-dokumentti. Saatavissa: https://xn--tyturvallisuuspakki-r6b.fi/riskienhallinta/ [viitattu 25.4.2024].

RESOLUTION MSC.428(98) Maritime cyber risk management in safety management systems. 2021 International Maritime Organization. PDF-dokumentti. Saatavissa: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf [viitattu 21.2.2024].

Satelliittipaikannus. s.a. Maanmittauslaitos. WWW-dokumentti. Saatavissa: https://www.maanmittauslaitos.fi/tutkimus/teematietoa/satelliittipaikannus

Security Account Manager (SAM). 2009. Microsoft. WWW-dokumentti. Saatavissa: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc756748(v=ws.10) [viitattu 18.3.2024].

Server Message Block Overview. s.a. Microsoft. WWW-dokumentti. Saatavissa: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831795(v=ws.11) [viitattu 18.3.2024].
Session Hijacking Attack. s.a. OWASP. WWW-dokumentti. Saatavissa: https://owasp.org/www-community/attacks/Session_hijacking_attack [viitattu 21.3.2024].

Svilicic B, Brčić D, Žuškin S & Kalebić D. Raising Awareness on Cyber Security of ECDIS. 2019. PDF-dokumentti. Saatavissa: https://www.transnav.eu/files/Raising_Awareness_on_Cyber_Security_of_ECDIS,894.pdf [viitattu 7.3.2024].

The Great Disconnect. 2022. CyberOwl. PDF-Dokumentti. Saatavissa: https://cyberowl.io/resources/global-maritime-industry-report-the-great-disconnect/ [viitattu 26.2.2024].

The Guidelines on Cyber Security Onboard Ships. 2020. International Chamber of Shipping. PDF-dokumentti. Saatavissa: https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf [viitattu 1.9.2023].

Tuomala, V. 2021. Maritime Cybersecurity. Before the risks turn into attacks. Kaakkois-Suomen Ammattikorkeakoulu. XAMK Research. PDF-dokumentti. Saatavissa: https://urn.fi/URN:ISBN:978-952-344-360-0 [viitattu 1.9.2023].

Tuulaniemi, V. 2020. Katsaus merenkulun kyberuhkiin. Kyberturvallisuuden infopäivä 11.9.2020. PDF-dokumentti. Saatavissa: https://www.traficom.fi/sites/default/files/media/file/2.%20Katsaus%20merenkulun%20kyberuhkiin%2020200911.pdf [viitattu 25.4.2024].

Uusi haavoittuvuus Microsoftin työkalussa mahdollistaa hyökkäykset haitallisten Microsoft Office-dokumenttien avulla. 2022. Liikenne- ja viestintävirasto Traficom. WWW-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/haavoittuvuus_10/2022 [viitattu 28.2.2024].

Vinkkejä informaatiovaikuttamisen tunnistamiseksi – Ole tarkkana ja toimi vastuullisesti. 2020b. Traficom. WWW-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/vinkkeja-informaatiovaikuttamisen-tunnistamiseksi-ole-tarkkana-ja-toimi [viitattu 13.2.2024].

What we do. s.a. International Organization for Standardization. WWW-dokumentti. Saatavissa: https://www.iso.org/what-we-do.html [viitattu 10.9.2023].

Xamk. s.a. Kaakkois-Suomen ammattikorkeakoulu Xamk. WWW-dokumentti. Saatavissa: https://www.xamk.fi/xamk/ [viitattu 18.9.2023].

LIITTEET Liite 1/1

Kyselylomakkeen kysymykset

1. Ymmärrätkö mitä kyberturvallisuus tarkoittaa?

2. Oletko ennen kuullut kyberturvallisuudesta?

3. Tiedätkö mitä haavoittuvuudet ja uhat tarkoittavat kyberturvallisuudessa?

4. Oletko saanut koulutusta tietoturvasta?

5. Jos olet saanut koulutusta tietoturvasta, niin minkä tasoista koulutus on ollut?

6. Minkä verran olet samaa mieltä lauseen kanssa?
   "Minulla on riittävän pitkät ja monimutkaiset salasanat käytössä."

7. Minkä verran olet samaa mieltä lauseen kanssa?
   "Päivitän säännöllisesti sovelluksia ja järjestelmiä, joita käytän."

8. Minkä verran olet samaa mieltä lauseen kanssa?
   "Lukitsen aina tietokoneen tai älylaitteen, kun en käytä sitä."

9. Tiedätkö mitä monivaiheinen tunnistautuminen tarkoittaa?

10. Oletko saanut kalastusviestejä koulun- tai työpaikan sähköpostiin?

11. Tiedätkö minkälaisia kyberhyökkäyksiä merenkulun alalle on tehty?

12. Oletko joutunut kyberhyökkäyksen uhriksi?

13. Oletko huomannut jonkun muun joutuvan kyberhyökkäyksen uhriksi?

14. Minkä verran olet samaa mieltä lauseen kanssa?
    "Uskon, että merenkulun alalla on riittävät toimenpiteet kyberhyökkäyksiä vastaan."

15. Uskotko kyberhyökkäyksien kasvavan merenkulun alalla tulevaisuudessa?

16. Käytätkö tekoälyä hyödyksi koulussa tai töissä?

17. Uskotko tekoälyn käytön kasvavan merenkulun alalla tulevaisuudessa?

18. Mitä alla olevia kyberturvallisuuden haavoittuvuuksia olet huomannut merenkulun alalla? (Esimerkiksi aluksessa tai satamassa)

19. Oletko ennen kuullut riskinhallintasuunnitelmasta?

20. Tiedätkö mitä IT- ja OT-järjestelmät tarkoittavat?

21. Minkä verran olet samaa mieltä lauseen kanssa?
"Merenkulun ala käyttää vanhanaikaisia järjestelmiä tai tekniikoita."

22. Minkä verran olet samaa mieltä lauseen kanssa?
"Merenkulussa on panostettu tarpeeksi kyberturvallisuuteen."

23. Mitkä mielestäsi ovat suurimmat kyberturvallisuuteen liittyvät uhat merenkulussa? (Valitse 3)

24. Minkä verran olet samaa mieltä lauseen kanssa?
"Venäjän hyökkäyssota on vaikuttanut huomattavasti merenkulun kyberturvallisuuteen.

25. Minkä verran olet samaa mieltä lauseen kanssa?
"Olen tarpeeksi tietoinen merenkulun kyberturvallisuudesta."

26. Kuinka tärkeänä pidät kyberturvallisuutta merenkulussa?

27. Onko mielestäsi merenkulun alalla jotain kehitettävää kyberturvallisuuden suhteen?

28. Oletko ollut harjoittelussa tai töissä merellä olevalla aluksessa?

29. Minkä vuoden opiskelija olet?

Liite 2/1

GPS-häirinnän uutisartikkelit

1.1.2024

Datasivusto: Suomen alueella runsaasti gps-järjestelmän häiriöitä - Kotimaa | HS.fi

2.1.2024

Suomessa on tehty kymmeniä ilmoituksia viikonlopulta GPS-häiriöistä – Finnairin lentäjä kertoo, miten silloin toimii | Kotimaa | Yle

Gps-järjestelmässä uudenvuodenaattona häiriöitä Suomessa - Digitoday - Ilta-Sanomat (is.fi)

3.1.2024

Suomessa havaittujen gps-häiriöiden syyksi epäillään venäläisiä järjestelmiä – Mutta mitä vaaraa häiriöistä aiheutuu? | Tekniikka&Talous (tekniikkatalous.fi)

5.1.2024

Sotilasprofessori kertoo, miten Venäjän GPS-häirintä toimii: Yksi yllätysvaikutus | Verkkouutiset

Näin satelliittipaikannuksen häirintä näkyy tavalliselle GPS-käyttäjälle | Demokraatti.fi

Gps-häirintä voi sotkea urheilukellon, mutta tärkeät järjestelmät eivät lepää satelliittien avaruussignaalien varassa - Digitoday - Ilta-Sanomat

Itämeren häiritsijä saattoi löytyä (iltalehti.fi)

8.1.2024

GPS-häirintään käytettävät pikkulaitteet ovat kasvava ongelma – professori tutkii, miten niiltä voidaan suojautua | Tiede | Yle

SvD: Joulun aikaan nähty gps-häirintä Itämerellä liittyi Venäjän harjoituksiin Kaliningradissa - Ulkomaat | HS.fi

Ruotsalaisasiantuntija: Venäjä oli joulukuisen gps-häirinnän takana - Ulkomaat - Ilta-Sanomat

13.1.2024

GPS-häiriöt jatkuvat Ruotsissa – Sotilastiedustelupalvelu: Kyse hybridivaikuttamisesta (iltalehti.fi)

22.1.2024

Onko Itämerta vaivaavien GPS-häiriöiden takana venäläinen satelliittien häirintälaite? | Verkkouutiset

26.1.2024

Pekka Toverin mielestä Venäjän GPS-häirintään pitäisi vastata - "Olemme liian kilttejä" | Verkkouutiset