Tampereen yliopisto

Emilia Varpio

LAIVOJEN KYBERTURVALLISUUDEN HAAVOITTUVUUDET JA HYÖKKÄYKSEN VAIKUTUKSET

Kandidaatintutkielma
Informaatioteknologian ja viestinnän tiedekunta
Lokakuu 2023

TIIVISTELMÄ

Emilia Varpio: Laivojen kyberturvallisuuden haavoittuvuudet ja hyökkäyksen vaikutukset
Kandidaatintutkielma
Tampereen yliopisto
Tieto- ja sähkötekniikan kandidaattiohjelma
Lokakuu 2023

Laivoihin kohdistuvien kyberhyökkäysten määrä on kasvanut suuresti viime vuosien aikana. Myös automaation ja yhdistettyjen laitteiden merkitys sekä määrä kasvavat laivoilla samalla lisäten hyökkäyspintaa ja haavoittuvuuksia. Tässä kandidaatintutkielmassa selvitetään laivojen eri laiteryhmien haavoittuvuuksia ja niiden mahdollistamia kyberhyökkäyksiä. Työn tavoitteena on selvittää haavoittuvaisimmat järjestelmät ja hyökkäystyypit, joille järjestelmät ovat alttiita. Lisäksi tavoitteena on tutkia mahdollisia laivoihin kohdistuvien kyberhyökkäyksien seurauksia sekä vaikutuksia.

Tutkielma tehtiin kirjallisuuskatsauksena, jonka aineistona käytettiin pääosin tieteellisiä, vertaisarvioituja artikkeleita. Työssä keskitytään laivojen ja niiden järjestelmien kyberturvallisuuteen ja muut merenkulun osa-alueet rajataan tutkielman ulkopuolelle. Lisäksi työssä käsitellään pääasiassa nykypäivän laivoja eikä esimerkiksi kehitteillä olevia autonomisia tai etäohjattavia laivoja. Useat nykylaivojen käyttämät järjestelmät ovat kuitenkin oletettavasti käytössä myös tulevilla autonomisilla ja etäohjattavilla laivoilla, joten myös niiden kyberturvallisuutta käsittelevät tutkimukset ja artikkelit ovat olennaisia tutkielman kannalta.

Kirjallisuuskatsaus osoittaa, että navigaatiolaiteryhmän järjestelmistä löytyy eniten haavoittuvuuksia. Lisäksi näiden haavoittuvuuksien huomataan olevan laajimpia ja vaarallisimpia. Tutkielmassa huomataan, että navigaatiojärjestelmistä erityisen haavoittuvaisia ovat AIS (eng. Automatic Identification System), ECDIS (eng. Electronic Chart Display and Information System) ja GNSS (eng. Global Navigational Satellite System). Myös muista laiteryhmistä löydetään haavoittuvuuksia, jotka altistavat kyberhyökkäyksille. Tutkielmassa huomataan, että yleisimpiä laivojen järjestelmiin kohdistuvia uhkia, erityisesti navigaatiojärjestelmille, ovat signaalien häirintä- ja väärentämishyökkäykset. Toisaalta myös muita kyberhyökkäyksiä voidaan kohdistaa laivoihin. Tutkielma osoittaa myös, että yhden tyyppisen kyberhyökkäyksen vaikutukset, seuraukset ja niiden vakavuus voivat vaihdella hyvin paljon.

Avainsanat: Kyberturvallisuus, haavoittuvuudet, kyberhyökkäykset, laivat, merenkulku

ABSTRACT

Emilia Varpio: Ship's cybersecurity vulnerabilities and effects of an attack
Bachelor's thesis
Tampere University
Bachelor's Programme in Computing and Electrical Engineering
October 2023

The amount of cyberattacks targeting ships has increased drastically over the last years. Also, the importance and amount of automation and connected devices is growing on ships, increasing attack surfaces and vulnerabilities. Ships' systems' vulnerabilities and cyberattacks which they enable are studied in this bachelor's thesis. The objective of this study is to find the most vulnerable systems and attack types that these systems are vulnerable to. In addition, this thesis aims to explore possible consequences of cyberattacks targeted on ship.

The thesis was done as a literature review and mainly utilizes scientific, peer reviewed articles as sources. The thesis focuses on ships and their systems' cybersecurity and leaves out other sectors of the maritime field. Additionally, it mainly focuses on current ships and not, for example, on automated or remote-controlled ships that are in development. However, several systems used by modern ships are presumably to be used in the coming automated and remote-controlled ships, making the articles and studies about their cybersecurity relevant for this thesis.

The literature review shows that navigation systems have the most vulnerabilities. These vulnerabilities are also more extensive and dangerous. In the thesis it is discovered that especially vulnerable out of all the navigation systems are AIS (Automatic Identification System), ECDIS (Electronic Chart Display and Information System) and GNSS (Global Navigational Satellite System). Other systems also have vulnerabilities that subject them to possible cyberattacks. It is discovered that the most common type of threats, especially to navigation systems, are jamming and spoofing. However, other cyberattacks can also be used to target a ship. The thesis also shows that a cyberattack can have a variety of effects and consequences, the severity of which may also vary greatly.

Keywords: Cybersecurity, vulnerabilities, cyberattacks, ships, maritime

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

AIS	Automatic Identification System, automaattinen identifiointi järjestelmä
CAN	Controller Area Network
CPA	Closest Point of Approach, lyhin sivuutusetäisyys
ECDIS	Electronic Chart Display and Information System, elektroninen kartta-, näyttö- ja tietojärjestelmä
GNSS	Global Navigational Satellite System, maailmanlaajuinen satelliittinavigointijärjestelmä
GMDSS	Global Maritime Distress and Safety System, merenkulun maailmanlaajuinen hätä- ja turvallisuusjärjestelmä
GPS	Global Positioning System, maailmanlaajuinen paikallistamisjärjestelmä
LiDAR	Light Detection and Rangin, valotutka
VDR	Voyage Data Recorder, matkadatan tallennin

.

1. JOHDANTO

Nykyajan laivoissa hyödynnetään paljon automaatiota, esineiden internettiä ja muita kyberresursseja. Yhdistettyjen laitteiden lisääntyessä laivoilla, myös hyökkäyspinta kasvaa. Laivoihin, satamiin ja muihin merenkulun osa-alueisiin kohdistuneiden kyberhyökkäysten määrä on ollut kovassa kasvussa. Hyökkäysten lisääntyminen alkoi jo ennen koronaviruspandemiaa, mutta kiihtyi erityisesti sen aikana. Tämän takia kyberturvallisuuden merkitys laivoissa on kasvanut ja kasvaa jatkossakin nopeasti.

Meriteitse kulkee yli 80 % maailmankaupan tavarasta. Monen muun maan tavoin esimerkiksi Suomi on riippuvainen meriliikenteestä muun muassa elintarvikkeiden ja polttoaineiden kuljettamiseksi. Lisäksi etäohjattavien ja autonomisten laivojen kehittäminen on kesken ja Suomessa on jo käytössä autonominen lautta. Myös näiden näkökulmasta laivojen kyberturvallisuus on tärkeä ja ajankohtainen aihe.

Tutkielmassa selvitetään laivojen kyberturvallisuuden haavoittuvuuksia ja potentiaalisia kyberhyökkäyksiä sekä niiden vaikutuksia. Työssä keskitytään nykyajan laivojen kyberturvallisuuteen ja sitä tarkastellaan toiminnalle kriittisimpien laiteryhmien ja muiden osien kannalta. Järjestelmiin liittyviä haavoittuvuuksia tarkastellaan myös niihin kohdistuvien mahdollisten kyberhyökkäysten näkökulmasta ja näihin liittyen tutkitaan potentiaalisia seurauksia ja vaikutuksia sekä välittömästi laivan näkökulmasta, että myös laajemmin esimerkiksi yhteiskunnan näkökulmasta. Näin pyritään muodostamaan kuvaa nykyajan laivoille olennaisista haavoittuvuuksista ja riskeistä kyberturvallisuudessa.

Työssä käy ilmi, että navigointijärjestelmistä löytyy eniten haavoittuvuuksia. Näistä edelleen GNSS (eng. Global Navigational Satellite System), AIS (eng. Automatic Identification System) ja ECDIS (eng. Electronic Chart Display and Information System) ovat haavoittuvaisimmat. Yleisimpiä uhkia ovat signaalien häirintä- ja väärentämishyökkäykset, joita voidaan kohdistaa eri järjestelmiin. Lisäksi huomataan, että jopa yksittäiseen laivaan kohdistuvalla kyberhyökkäyksellä voi olla laajoja vaikutuksia.

Tutkielma tehtiin kirjallisuuskatsauksena. Lähteinä käytettiin pääasiassa tieteellisiä artikkeleita Andor ja Scopus tietokannoista. Tietokantoihin tehtiin hakuja yhdistelemällä hakulauseita sanoista ”cyber security”, ”ship”, ”maritime”, ”vulnerability”, ”malware” ja ”cyberattack”. Tuloksista valittiin lupaavimmat aluksi otsikon ja julkaisuvuoden perusteella ja sitten edelleen tiivistelmän perusteella.

Merenkulun sekä laivojen kyberturvallisuudesta on paljon tutkimuksia sekä artikkeleita. Monien aiheet keskittyvät autonomisiin tai etäohjattaviin laivoihin. Useimmat näissä tutkimuksissa löydetyistä haavoittuvuuksista liittyvät kuitenkin järjestelmiin, jotka ovat käytössä jo nykypäivän laivoissa. Löydökset ovat siis relevantteja myös muille laivoille. Silverajan ja muut (2018) sekä Ashraf ja muut (2023) ovat tutkineet laivoihin kohdistuvia kyberhyökkäyksiä, uhkia ja haavoittuvuuksia. Androjna ja Perkovič (2021) puolestaan tutkivat erään yleisimmän hyökkäyksen AIS signaalin väärentämisen toteutettuja tapauksia ja niiden seurauksia.

Luvussa 2 käsitellään laivojen kyberturvallisuutta ja laivojen eri laiteryhmien sekä järjestelmien kyberturvallisuutta keskittyen erityisesti haavoittuvuuksiin ja luvussa 3 erilaisia mahdollisia kyberhyökkäyksiä, niiden piirteitä, toteuttamista ja välittömiä vaikutuksia. Luvussa 4 tarkastellaan lyhyesti kyberhyökkäysten vaikutuksia laajemmasta näkökulmasta. Luvussa 5 esitetään pohdintaa tutkielmaan ja sen löydöksiin liittyen ja viimeisenä luvussa 6 eli yhteenvedossa kootaan vielä tutkielman tulokset yhteen.

2. KYBERTURVALLISUUS LAIVOISSA

Merenkulun sektorin voimakas digitalisoituminen pandemian aikana johti eksponentiaaliseen kasvuun kyberhyökkäysten määrässä. Moderneilla laivoilla hyödynnetään suurta määrää kyberjärjestelmiä. Niitä ovat esimerkiksi GPS (eng. Global Positioning System), automoidut laitteet, sensorit, sähköiset sertifikaatit ja sähköinen navigointi. (Karim, 2022) Yhdistettyjen laitteiden määrä ja esineiden internetin vaikutus lisääntyy laivoilla jatkuvasti. Tämä kasvattaa hyökkäyspintaa ja mahdollisten kyberturvallisuuden haavoittuvuuksien määrää. Samalla myös radiotaajuuksilla ja satelliiteilla lähetettävän ja vastaanotettavan informaation ja datan määrä kasvaa, mikä edelleen kasvattaa kyberriskejä.

Moderneja laivoja voidaan kuvailla keskitason autonomisiksi laivoiksi, sillä autonomiset järjestelmät ja niiden operoijat tekevät yhteistyötä (Karahalios, 2020). Laivoista, joissa on paljon automaatiota, löytyy myös enemmän hyökkäyspintaa kyberhyökkäyksille, mikä kasvattaa riskien tasoa. Kyberturvallisuusriski kuvaa järjestelmän tai laitteen haavoittuvuuden potentiaalista hyödyntämistä haitan aiheuttamiseksi organisaatiolle, ja sitä voidaan arvioida seuraavien kriteerien avulla: uhan todennäköisyys toteutua, uhalle mahdollisten haavoittuvuuksien laajuus ja potentiaalisten vaikutusten merkittävyys (Kavallieratos ja Katsikas, 2020).

Merenkulkuun ja erityisesti laivoihin sekä muihin merenkulun komponentteihin liittyy erityispiirteitä verrattaessa esimerkiksi maalla kulkeviin ajoneuvoihin. Näitä piirteitä ovat tarve tunnistaa, tietää ja ennustaa muu liikenne hyvin laajalla alueella, odottamattomien huoltotoimenpiteiden haastavuus laivan ollessa merellä, reittien dynaamisuus ja rajoittunut yhteyksien toimivuus rannikko alueiden ulkopuolella (Silverajan ja muut, 2018). Laivan ollessa merellä se on eristyksissä maissa olevista resursseista, mikä voi aiheuttaa lisähaasteita paitsi kyberhyökkäyksen aikana myös muiden odottamattomien toimintahäiriöiden korjaamisessa (Karahalios, 2020). Laivoilla on monien eri laitevalmistajien laitteita ja laitteiden eliniät ovat pitkiä (Silverajan ja muut, 2018). Tämä johtaa erilaisiin standardeihin ja rajapintoihin. Pitkät eliniät puolestaan vaikuttavat laitekannan uusiutuvuuteen ja uusien laitteiden hitaampaan käyttöönottoon.

Navigointijärjestelmät ovat laivojen laiteryhmistä kaikkein haavoittuvaisin (Tusher ja muut, 2022). Navigaatio- ja identifiointijärjestelmien alttius johtuu niiden monimutkaisuudesta ja korkeammasta integraation tasosta (Mileski ja muut, 2018). Propulsiojärjestel-

mät puolestaan ovat vähiten haavoittuvaisia (Tusher ja muut, 2022). Toisaalta propulsiojärjestelmien toiminta on riippuvaista navigointijärjestelmistä ja sijainnista, jolloin navigointijärjestelmien haavoittuvuudet vaikuttavat myös propulsiojärjestelmien toimintaan.

2.1 Viestintäyhteydet

Tietoliikenne ja viestintä kuuluvat tärkeimpiin suojattaviin kybervoimavaroihin laivoilla (Mileski ja muut, 2018). Viestintä yhteyksistä houkuttelevan kohteen kyberhyökkäyksille tekee lisääntyvä kommunikaation määrä niin laivojen ja muiden kohteiden kuin myös laitteiden välillä (Silverajan ja muut, 2018). Automaation tason kasvaessa radiotaajuuksilla ja satelliiteilla lähetettävän datan määrä kasvaa edelleen (Tusher ja muut, 2022), mikä tekee viestintäyhteyksistä yhä kriittisempiä. Samalla luottamuksellisen informaation ja datan pysyminen salassa on tärkeää laivan kyberturvallisuudelle ja turvallisuudelle ylipäänsä (Karahalios, 2020).

Viestintäjärjestelmiin kuuluu paljon laitteita, joista monet ovat yhteydessä internettiin tai telekommunikaatio järjestelemiin. Tämä mahdollistaa etäältä tehtävät yksinkertaiset sekä hienostuneet hyökkäykset. (Ashraf ja muut, 2023) Hyökkääjä voi esimerkiksi päästä wi-fi tietoliikenteeseen käsiksi ja sitä kautta johtaa tietoa älypuhelimista (Karahalios, 2020) tai muista verkkoon kytketyistä laitteista.

Hyökkäyspintaa viestintäyhteyksiin löytyy laivan sisäisistä verkoista sekä sen yhteydestä maihin. Salaamattomat kommunikaatiokanavat mahdollistavat muun muassa salakuuntelun ja väliintulohyökkäykset. Myös laivan ulkopuolelle ulottuvat osat voivat aiheuttaa haavoittuvuuksia. Esimerkiksi maissa olevaa vaarantunutta kommunikaatiolinkin solmua voidaan käyttää kyberhyökkäyksen tekemiseen laivan järjestelmiin. (Silverajan ja muut, 2018) Kommunikaation häirintää voidaan puolestaan tehdä sähköisillä häirintälaitteilla (Karahalios, 2020).

Laivojen viestintäyhteyksissä käytetään rannikolla tukiasemia ja niiden katealueen ulkopuolella satelliitteja (Ashraf ja muut, 2023). Satelliitit tarjoavat yhteyksiä ja datansiirtomahdollisuuksia rannikkoalueiden ulkopuolella. Niiden mukana tulee kuitenkin myös lisää haavoittuvuuksia ja hyökkääjien on mahdollista salakuunnella, häiritä tai uudelleenreitittää satelliittien tietoliikennettä (Tedeschi ja muut, 2022).

Eräs kriittinen kommunikaatiojärjestelmä laivoilla on GMDSS (eng. Global Maritime Distress and Safety System). GMDSS on hätätilanteiden johtamista ja hallintaa varten. Sillä voidaan lähettää viestejä pelastustoiminta-avun pyytämiseksi ja yleislähetyksellä lähettää viestejä muille laivoille, jotka voisivat auttaa tilanteessa. GMDSS on altis signaalin häirinnälle, väärentämiselle ja haittaohjelmahyökkäyksille. Järjestelmä on tärkeä

pelastusoperaatioille ja jo pieni häiriö sen toiminnassa voi vaarantaa operaation onnistumisen. (Ashraf ja muut, 2023)

Laivojen useista eri viestintäjärjestelmistä löytyy haavoittuvuuksia, joita hyökkääjät voivat hyödyntää viestinnän häirinnässä, salakuuntelussa tai väärentämisessä. Lisäksi myös muista laiteryhmistä löytyy järjestelmiä, jotka tarvitsevat tietoliikennettä toimintaansa. Koska nämä järjestelmät hyödyntävät samoja teknologioita ja yhteyksiä, haavoittuvuudet ulottuvat myös niiden toimintaan.

2.2 Navigaatiojärjestelmät

Laivan turvallinen navigointi on nykypäivänä riippuvaista kyberfyysisistä järjestelmistä ja niiden oikeasta toiminnasta (Svilicic ja muut, 2020). Eräitä hyvin keskeisiä navigointijärjestelmiä ovat ECDIS, AIS ja GNSS. Navigointijärjestelmistä löytyy enemmän ja vakavampia haavoittuvuuksia kuin laivojen muista laiteryhmistä (Tusher ja muut, 2022). Niiden alttius kyberhyökkäyksille johtuu korkeasta integraation tasosta ja järjestelmien monimutkaisuudesta (Mileski ja muut, 2018). Merenkulussa yleisin kohde kyberhyökkäyksille ovatkin navigaatiojärjestelmät (Ashraf ja muut, 2023). Niihin liittyvää hyökkäyspintaa löytyy esimerkiksi AISista, ECDISistä, GNSS:stä, tutkasta ja sijaintiin liittyvistä sensoreista (Silverajan ja muut, 2018). Yleisimpiä hyökkäyksiä ovat signaalin häirintä tai väärentäminen (Tusher ja muut, 2022).

AIS välittää navigointiin liittyviä tietoja, kuten laivan tyyppi, sijainti, kurssi, nopeus ja status tarjotakseen turvallista navigointia ja keinoja törmäysten välttämiseksi (Ashraf ja muut, 2023). AIS-lähettimiä ja vastaanottimia on muun muassa laivoilla ja satamissa ja niitä voidaan myös asentaa muihin paikkoihin, kuten majakoihin (Kontopoulou, 2021). AISin haavoittuvuuksia ovat AIS nettisivujen turvattomuus ja radio lähetyksen turvattomuus (Mileski ja muut, 2018), salaamaton formaatti (Karahalios, 2020) sekä riittämättömät protokollat tietojen oikeellisuuden varmistamiseksi ja salaamiseksi (Ashraf ja muut, 2023). AISiin voi kohdistua signaalin häirintää, väärentämistä (Ashraf ja muut, 2023; Karahalios, 2020; Mileski ja muut, 2020; Silverajan ja muut, 2018) ja kaappaamista (Karahalios, 2020; Ashraf ja muut, 2023). Myös palvelunestohyökkäykset, väärennetyt CPA (engl. Closest Point of Approach, lyhin sivuutusetäisyys) hälytykset ja datatulva korkeammalla taajuudella lähettämällä ovat mahdollisia (Ashraf ja muut, 2023). AISin vaatimattomat salaukset, autentikoinnit ja verifioinnit (Silverajan ja muut, 2018) mahdollistavat monipuolisia tavoitteitta hyökkääjille.

ECDIS esittää laivan reitin miehistölle komentosillan käyttöjärjestelmällä (Ashraf ja muut, 2023). Se käyttää muun muassa GPS, AIS, tutka ja kompassi tietoja (Svilicic ja muut,

2020). ECDISin on huomattu olevan helppo kohde hyökkääjille (Ashraf ja muut, 2023). ECDIS päivitetään joko internettiin yhdistämällä tai USB:llä (Ashraf ja muut, 2023; Karahalios, 2020). Molempiin näistä liittyy riskejä. USB:llä voidaan siirtää haitallisia ohjelmia tai koodia. Pääasiallinen lähde haitallisen koodin suorittamiselle ECDIS-järjestelmässä on alkeellinen käyttöjärjestelmä tai käyttöjärjestelmä, joka ei salli päivityksiä (Ashraf ja muut, 2023). Internettiin yhdistämisessä on kuitenkin enemmän riskejä, esimerkiksi mahdollisuus väliintulohyökkäykselle tai datan menettämiselle (Karahalios, 2020).

GNSS tarjoaa navigointi tietoja ohjatun GPS-navigoinnin muodossa (Ashraf ja muut, 2023). Nykypäivänä navigaatio on hyvin riippuvaista GPS-signaaleista (Karahalios, 2020). Signaalin häirintä ja väärentäminen ovat GNSS:n kannalta olennaisimmat kyberhyökkäyksen muodot (Ashraf ja muut, 2023). Useat järjestelmät, mukaan lukien aiemmin esitellyt AIS ja ECDIS, hyödyntävät GPS tietoja. Esimerkiksi AISin GPS-signaalin häirintä onnistuu halvoilla internetistä saatavilla häirintälaitteilla (Karahalios, 2020).

Näiden laitteiden ja järjestelmien väleiltä löytyy myös paljon riippuvaisuuksia sekä yhteyksiä. Esimerkiksi ECDIS käyttää muun muassa GPS, AIS ja tutka dataa hyödykseen (Svilicic ja muut, 2020). AISilla puolestaan voi olla jopa seitsemän avainasemassa olevaa, siitä riippuvaista järjestelmää (Mileski ja muut, 2018). Tämän takia yhteen järjestelmään kohdistuva kyberhyökkäys voi vaarantaa myös muiden järjestelmien oikean toiminnan.

Tusher ja muut (2022) pitävät GNSS:ää ja ECDISiä haavoittuvaisimpina navigaatiojärjestelmistä. Ashraf ja muut (2023) kuitenkin asettavat AISin kaikkein haavoittuvaisimmaksi sen tekemän kommunikaation takia, ja GNSS:n toiseksi haavoittuvaisimmaksi. Vähiten haavoittuvainen navigaatiojärjestelmä puolestaan on tutka (Tusher ja muut, 2022).

2.3 Propulsiojärjestelmät

Propulsiojärjestelmät ovat laivan vähiten haavoittuvaisia järjestelmiä (Tusher ja muut, 2022). Niiden toiminta on kyberturvallisuuden kannalta paremmin suojattua kuin esimerkiksi navigointijärjestelmien. Toisaalta propulsiojärjestelmät tarvitsevat monia muita järjestelmiä oikean toiminnan tueksi ja siten niiden toimintaa voidaan kyberhyökkäyksillä vaikuttaa epäsuorasti. Hyökkäyspintaa löytyy esimerkiksi sensoreista ja muista laiteryhmistä (Silverajan ja muut, 2018). Pääkoneen sensoreiden data sekä navigaatio- ja sijaintidata ovat propulsiojärjestelmien kannalta olennaisia. Automoidut propulsiojärjestelmät tarvitsevat myös informaatio- ja kommunikaatioteknologioita toimiakseen (Tusher ja

muut, 2022). Erityisesti saaristoisilla alueilla, kuten Suomen rannikolla, tai muilla kapeilla väylillä propulsion oikea toiminta on tärkeää karilleajojen välttämiseksi.

2.4 Miehistö

Laivoilla olevat ihmiset voivat tahallaan tai tahattomasti aiheuttaa riskejä ja lisätä haavoittuvuuksia kyberhyökkäyksille. Osaamaton tai huolimaton miehistön jäsen voi esimerkiksi mahdollistaa haittaohjelmahyökkäyksen (Svilicic, 2019). Ashraf ja muut (2023) mainitsevat merenkulun työntekijöiden huolimattomuuden yhtenä pääsyistä kyberhyökkäyksille. Esimerkiksi haitallista koodia sisältävän USB-tikun liittäminen USB-porttiin riittää aiheuttamaan ongelmia (Karahalios, 2020). USB:llä tehty haittaohjelman siirto on tapahtunut aasialaisessa satamassa olleelle tankkerille, jonka miehistön jäsen oli tuonut tulostettavia papereita mukanaan USB-tikulla. Kun karttoja päivitettiin tulostamisen jälkeen USB:llä haittaohjelma pääsi vaikuttamaan ECDIS-järjestelmään. (Roberts, 2019)

Lisäksi on kyberhyökkäyksiä, jotka hyödyntävät ihmisten tietämättömyyttä niiden toteutuksessa. Tällaisia ovat esimerkiksi kalastelu- ja ”watering hole” -hyökkäykset, joita molempia voidaan käyttää merenkulkuun ja laivoihin kohdistuvissa hyökkäyksissä (Ashraf ja muut, 2023).

Fyysiset turvatoimet ovat tärkeässä roolissa pitämässä kuulumattomat henkilöt poissa laitteiston läheltä. Myös heikot tai tilanteeseen sopimattomat käytännöt ja menettelyt sekä puutteellinen miehistön ja muun henkilökunnan koulutus voivat pahentaa järjestelmien haavoittuvuuksia tai lisätä niitä. (Svilicic ja muut, 2019)

2.5 Laivojen ulkopuoliset järjestelmät

Merenkulun sektorin digitalisoitumista on tapahtunut myös laivojen ulkopuolella. Käytössä on esimerkiksi sähköisiä sertifikaatteja ja rahdin jäljitystä (Karim, 2022). Koska myös muissa merenkulun osa-alueissa käytetään tietokoneita ja tietokonejärjestelmiä, ovat laivat vain osa merenkulun kyberturvallisuutta (Karim, 2022). Toisaalta koska maissa on laivoihin liittyviä järjestelmiä ja niiden osia, ovat laivalla olevat järjestelmät vain osa laivan omaa kyberturvallisuutta. Haavoittuvaisten komponenttien määrä esimerkiksi satamissa on suurempi kuin laivoilla (Ben Farah ja muut, 2022).

Laivaan voi tulla uusia haavoittuvuuksia kolmannen osapuolen laitteiston tai ohjelmistojen mukana. Esimerkiksi ohjelmistoissa olevat virheet, takaovet tai niiden heikko testaus voivat aiheuttaa haavoittuvuuksia ja riskejä. (Ashraf ja muut, 2023) Myös hyökkäys yrityksen verkkoon voi sallia pääsyn laivan järjestelmiin (Karahalios, 2020). Lähes kaikki teollisiin ohjausjärjestelmiin tehdyt kyberhyökkäykset on toteutettu ensin vaarantamalla

yrityksen verkko ja hyödyntämällä sitä hyökkäyksessä järjestelmää vastaan (Kavallieratos ja muut, 2019). Tämä korostaa muiden osa-alueiden kyberturvallisuuden tärkeyttä ja yhteyksien merkitystä yksittäisen laivan kyberturvallisuudessa.

3. KYBERHYÖKKÄYKSET

Kyberhyökkäyksiä tehdään monien eri ryhmien toimesta ja niille löytyy paljon syitä sekä motiiveja. Potentiaalisia hyökkääjiä laivoihin ovat aktivistit, kilpailijat, rikolliset ja terroristit (Tusher ja muut, 2022). Myös valtioilla on motiiveja kyberhyökkäysten tekemiseen. Kyberhyökkäysten luonteen takia tekijää voi olla vaikea löytää. Hyökkäyksen tyyppi valitaan tarkoitukseen sopivaksi. Tavoitteena saattaa olla esimerkiksi datan varastaminen tai muokkaaminen markkinoiden manipuloimiseksi, laivan vahingoittaminen, salakuljettaminen, rahdin varastaminen tai laivan varastaminen (Tusher ja muut, 2022). Kyberhyökkäystä voidaan käyttää myös apuvälineenä fyysisen hyökkäyksen tekemiseen esimerkiksi merirosvojen toimesta (Karahalios, 2020). Mahdollisia päämääriä ovat lisäksi kiristäminen, vakoilu, huijaaminen ja petos (Silverajan ja muut, 2018), mediahuomion saaminen, organisaation resurssien tuhoaminen, luottamuksellisen datan myyminen, laivan ohjaileminen toiseen sijaintiin (Ashraf ja muut, 2023) sekä laivan tai muiden resurssien sabotoiminen (Ashraf ja muut, 2023; Tusher ja muut, 2022).

Merenkulku ja kyberrikollisuus ovat molemmat kansainvälistä, valtioiden rajat ylittävää toimintaa. Merenkulun kyberrikollisuuslainsäädäntö on erityisen vaikeaa verrattuna yleiseen lainsäädäntöön, koska laivan lipun ja sataman sekä rannikko- ja muiden valtioiden sekä valtioiden toimivallan ulkopuolella olevien alueiden välillä on monimutkaista vuorovaikutusta ja kilpailua (Karim, 2022). Tämä johtaa tietyillä alueilla epäselvyyksiin niillä vaikuttavista laeista, muista säännöistä ja määräysvallasta. Kyberhyökkäyksiä tehdään tällaisella harmaalla alueella tutkinnan ja rankaisemisen vaikeuttamiseksi (Mileski ja muut, 2018).

Olennaisimpia hyökkäyspintoja löytyy paikannus- ja navigointijärjestelmistä, sensoreista, laiteohjelmistosta, VDR:stä (eng. Voyage Data Recorder), laivan sisäisistä verkoista ja laivan yhteydestä maihin. Sensoreita käytetään esimerkiksi hälytysjärjestelmissä, kriittisen infrastruktuurin kuten propulsion, pääkoneen ja rungon eheyden valvonnassa, liikkeen kuten nopeuden, aallokon ja tuulen havaitsemisessa ja audiovisuaalisissa laitteissa kuten kameroissa ja mikrofoneissa sekä syvyyksien havainnoinnissa ultraäänilaitteilla. Erilaiset hyökkäykset sopivat eri järjestelmiin kohdistettaviksi eli eri hyökkäyspinnoille tosin näistä löytyy myös päällekkäisyyksiä. (Silverajan ja muut, 2018)

3.1 Signaalin häirintä ja väärentäminen

Signaalin häirintä on tahallista signaaliin vaikuttamista sen tekemiseksi käyttökelvottomaksi. Se aiheutetaan lähetyksillä, joiden tarkoituksena on tehdä oikea signaali kokonaan tai osittain käsittämättömäksi. Häirinnän tavoitteena on estää signaalin saaminen vastaanottimessa (Silverajan ja muut, 2018). Signaalin väärentäminen puolestaan tarkoittaa väärennetyn signaalin lähettämistä (Mileksi ja muut, 2018): laivan laitteille pyritään uskottelemaan, että väärennetty signaali on oikea (Silverajan ja muut, 2018). Signaalin häirintä ja väärentäminen ovat navigointijärjestelmille yleisiä uhkia (Tusher ja muut, 2022). Vaikuttamalla navigointijärjestelmiin voidaan mahdollisesti ohjailla laivaa haluttuun sijaintiin (Ashraf ja muut, 2023) esimerkiksi fyysistä hyökkäystä varten. Häirintä voi navigointijärjestelmien lisäksi kohdistua esimerkiksi viestintäyhteyksiin, tutkaan (Karahalios, 2020), sensoreihin tai kameroihin (Silverajan ja muut, 2018).

GPS-signaalin väärentämisen tavoitteena on saada laivan sijaintijärjestelmät käyttämään väärennettyä signaalia ja sen perusteella muuttamaan kurssia. Signaalin väärentäminen tehdään asentamalla laivalle GPS-lähetin, joka lähettää väärää signaalia, ja hiljalleen nostamalla sen lähetystehoa. Lähetystehon nostaminen tehdään niin, että vastaanottimet eivät huomaa epätavallisia signaalin muutoksia. Vastaanotin alkaa vaiheittain käyttää väärennettyjä GPS-koordinaatteja. Maa- ja ilmakulkuneuvoihin on tehty tällaisia hyökkäyksiä, joiden tavoitteina ovat olleet kaappaus, kontrolli ja varkaus. (Silverajan ja muut, 2018) Merellä vastaava jahtiin kohdistettu hyökkäys on toteutettu Texasin yliopiston toimesta vuonna 2013 (Ben Farah ja muut, 2022). GPS-signaalin häirintä tehdään samalla tavalla kuin väärentäminen. Tavoitteena on kuitenkin estää GPS-signaalin saaminen. (Silverajan ja muut, 2018) Signaalin väärentäminen on tässä tapauksessa vaikeampaa, sillä se vaatii satelliittisignaalin jäljittelyä, mikä puolestaan vaatii suurempaa tehoa ja monimutkaisempia laitteita (Ashraf ja muut, 2023).

AISin manipulointi on usein signaalin väärentämistä (Mileski ja muut, 2018). Tämä voidaan toteuttaa ilman fyysistä läsnäoloa kohteessa. AISin vaatimat salaus, autentikointi ja verifiointi ovat vaatimattomia, ja on todistettu, että AISiin kohdistuvalla väärentämishyökkäyksellä voidaan väärentää tietoja suositulle tiedontarjoajalle. (Silverajan ja muut, 2018) AISin GPS-signaalia puolestaan voidaan häiritä halvoilla häirintälaitteilla. Myös AIS-formaatin suojaamattomuus voi altistaa väärentämis- ja häirintähyökkäyksille. (Karahalios, 2020) Näillä keinoilla voidaan esimerkiksi manipuloida laivan sijainti tai tunnus näkymään vääränä tai jopa saada laiva katoamaan muista AIS-vastaanottimista kokonaan (Mileski ja muut, 2018). Laivan AIS-signaali voidaan myös kaapata tai sekoittaa. Tällaiset tilanteet vaikuttavat paitsi tiedon oikeellisuuteen ja siten muiden alueella olevien

toimintaan, samoin kaikkiin niihin laivojen järjestelmiin, jotka hyödyntävät kyseistä dataa. (Mileski ja muut, 2018)

3.2 Haittaohjelmat

Eräs laivoista yleisesti löytyvä haavoittuvuus on haitallisen koodin viemisen helppous kriittisiin järjestelmiin (Silverajan ja muut, 2018). Haitallinen koodi eli haittaohjelma voi olla esimerkiksi virus, kiristyshaittaohjelma tai vakoiluohjelma (Ashraf ja muut, 2023). Haittaohjelma voidaan tuoda järjestelmään esimerkiksi miehistön jäsenen toimesta (Silverajan ja muut, 2018).

Vakoiluohjelmilla voidaan seurata käyttäjien toimintaa tai varastaa luottamuksellista tai arkaluontoista informaatiota kiristämistä tai julkaisemista varten. Kiristyshaittaohjelmilla estetään pääsy resursseihin, joiden palauttamisesta pyydetään lunnaita. (Ashraf ja muut, 2023)

Esimerkiksi ECDISin päivitys on mahdollista USB-tikulla (Karahalios, 2020), jolla onnistuu myös haittaohjelmien siirtäminen. Roberts (2019) esittelemä haittaohjelma hyökkäys aasialaisessa satamassa kohdistui ECDISiin ja siinä hyödynnettiin USB:tä. On todennäköistä, että haittaohjelma tilanteessa ECDISin navigaatiokartat jäätyvät (Karahalios, 2020). Tämän voi nähdä myös etuna, sillä se saattaa helpottaa toimintavirheen ja siten hyökkäyksen huomaamista.

Haittaohjelmahyökkäysten tekijät ovat yleensä varkaita tai hakkereita. Erityisesti kiristyshaittaohjelmiin liittyvät motiivit ovat usein rahalliset. Vakoiluhaittaohjelmilla puolestaan pyritään varastamaan luottamuksellista informaatiota ja dataa. Tätäkin voidaan käyttää kiristämiseen. Haittaohjelmien seurauksiin kuuluvat yleensä järjestelmävauriot ja informaation menetys. (Silverajan ja muut, 2018)

3.3 Palvelunesto

Palvelunestohyökkäyksessä järjestelmään kohdistetaan niin paljon liikennettä, että sen käyttäminen tulee mahdottomaksi. Hyökkäys hyödyntää kohteen resurssien rajallisuutta.

Kommunikaatioverkossa olevaa vaarannettua solmua voidaan käyttää palvelunestohyökkäyksen tekemiseen laivaan. Vaarantuneen solmun ei tarvitse olla laivassa, vaan myös maissa olevaa solmua voidaan hyödyntää tähän tarkoitukseen. Toisaalta sama pätee myös toisinpäin ja hyökkäys maissa olevaan järjestelmään voidaan tehdä laivassa olevan vaarantuneen solmun avulla. Erityisesti laivan ollessa laajakaistayhteyden ulkopuolella vaarantunutta solmua voidaan käyttää palvelunestohyökkäyksen tekemiseen kommunikaatiojärjestelmiin. (Silverajan ja muut, 2018) Palvelunestohyökkäykset voivat

kohdistua esimerkiksi yhteyksien käytettävissä olevaan kaistanleveyteen. Laajakaistayhteyksissä on laajempi kaistanleveys ja suuremmat datan siirtonopeudet kuin satelliittiyhteyksissä. Tämän takia satelliittiyhteyksiin voi olla helpompi kohdistaa palvelunesto hyökkäyksiä.

3.4 Manipulointi ja muokkaaminen

Manipulointi tai muokkaaminen voi kohdistua tietoliikenneyhteyksiin, laitteistoon tai informaatioon. Nämä voidaan tulkita monella tavalla ja laajalla käsityksellä kaikki kyberhyökkäykset voidaan liittää tähän kategoriaan. Tässä kuitenkin käsitellään kyberresurssien manipuloimiseen tai muokkaamiseen tähtääviä keinoja. Näitä hyökkäyksiä voidaan toteuttaa niin etänä kuin paikan päällä.

Audiovisuaaliset järjestelmät ovat alttiita toistohyökkäyksille, jos kameran ja vastaanottimen välinen yhteys on ei ole turvallinen. Toistohyökkäyksessä oikeaa dataa lähetetään useita kertoja uudelleen. Audiovisuaalisten järjestelmien tapauksessa toistohyökkäyksellä kameran suora kuva voitaisiin korvata aikaisemmin tallennetulla pätkällä. Nämä hyökkäykset saattavat aiheuttaa toimintahäiriöitä, virheenkäsittelyä, alkutilaan palauttamista, laskentatehollisesti rajoittuneen järjestelmän ylikuormittumista tai luottamuksellisen datan vuotamista. (Silverajan ja muut, 2018)

Myös CAN-väylään (eng. Controller Area Network) yhteydessä oleva ilkeämielinen solmu voi tehdä paketin sieppauksia yleislähetyksen paketeille ja käyttää niitä toistohyökkäysten tekemiseen. Sen avulla voi myös syöttää muokattuja pahantahtoisia paketteja tai lähettää väärennettyä dataa verkon muille solmuille. (Silverajan ja muut, 2018)

Fyysiset muokkaukset laivan laitteisiin tai informaatioon ovat mahdollisia laivalla olevien toimilaitteiden avulla (Silverajan ja muut, 2018). Näitä toimilaitteita ovat esimerkiksi DVD soittimet, USB-portit tai hälyttimet. Ne voivat mahdollistaa kriittisten laitteiden modifikaation. (Karahalios, 2020) Kyberhyökkäys voi kuluttaa laitteen resursseja kuten kaistanleveys, laskentateho ja akun kesto, ja näin vaikuttaa sen toimintaan heikentävästi (Karahalios, 2020). Esimerkiksi vaikeasti tavoitettavilla esineiden internetin laitteilla akun keston vaatimukset ovat usein kovat. Tällaisiksi voitaisiin luokitella laivalla olevia laitteitta, sillä niiden huoltaminen merellä on vaikeaa. Kyberhyökkäyksen seurauksena myös laitteen akunkesto voi tippua, jolloin akkua joudutaan vaihtamaan tai lataamaan useammin, mikä puolestaan heikentää akkukäyttöisten laitteiden hyötyjä.

Näitä hyökkäyksiä tekevät kilpailijat tai muut teollisenvakoilun harjoittajat, jotka tavoittelevat tiedon varastamista (Silverajan ja muut, 2018). Kilpailun lisäksi tavoitteita voivat

olla tiedon myyminen eteenpäin, kiristäminen tai jonkin asian saattaminen median huomioon (Ashraf ja muut, 2023). Toisaalta voidaan myös haluta poistaa raskauttavaa informaatiota laivan toiminnasta ja tehdä huijaus tai petos (Silverajan ja muut, 2018).

3.5 Viestinnän salakuuntelu ja häirintä

Salaamattomiin yhteyksiin voidaan tehdä salakuuntelu- ja väliintulohyökkäyksiä (Silverajan ja muut, 2018). Salakuunteluhyökkäyksessä hyökkääjä kuuntelee osapuolten välistä keskustelua näiden tietämättä ja voi siten saada tietoonsa luottamuksellista informaatiota. Informaatio voi olla esimerkiksi salasanoja, henkilökohtaisia keskusteluja tai yrityksen luottamuksellista tietoa. Salakuunteluhyökkäyksiä voivat tehdä esimerkiksi kilpailijat liikesalaisuuksien selvittämiseksi. Hyökkäykselle on myös muita motiiveja, esimerkiksi kiristäminen tai tiedon myyminen. Väliintulohyökkäys on salakuuntelun muoto. Siinä kahden viestijän välissä on hyökkääjä, joka esiintyy molemmille osapuolille toisena viestijänä. Laivalla esimerkiksi ECDISin yhdistäminen internettiin voi altistaa väliintulohyökkäykselle (Karahalios, 2020).

4. KYBERHYÖKKÄYSTEN VAIKUTUKSET

Merenkulkuun ja laivoihin liittyy monia yrityksiä, yhteiskuntien osa-alueita ja ihmisiä. Tämän takia laivaan kohdistuvalla kyberhyökkäyksellä voi olla laajoja vaikutuksia jopa globaalilla tasolla. Tämä edelleen johtaa siihen, että kyberhyökkäyksillä on korkea potentiaali häiriön ja vahingon aiheuttamiseen.

4.1 Yritykset

Laivoihin ja niiden toimintaan liittyy monia yrityksiä laitevalmistajista omistajiin. Näille kuuluu erilaisia rooleja sekä vastuita. Kyberhyökkäysten kohteena oleviin yrityksiin kohdistuu ennen kaikkea taloudellisia vaikutuksia ja mainehaittaa (De Albaquerque ja muut, 2022). Tämä on lähestulkoon riippumatonta hyökkäyksen tyypistä. Laivoihin kohdistuviin kyberhyökkäyksiin liittyy mahdollisesti myös muita seurauksia, kuten kuljetusten epäonnistuminen tai ihmishenkien vaarantuminen.

Useiden eri navigaatiojärjestelmiin kohdistuvien kyberhyökkäyksien seurauksena laiva saattaa päätyä kulkemaan väärän suuntaan tai sijaintiin. Tästä voi aiheutua viivästyksiä ja vaaratilanteita, kuten karilleajoja tai törmäyksiä. Laivalle aiheutuneet vahingot voivat puolestaan johtaa edelleen suurempiin vaikeuksiin, jos esimerkiksi runko rikkoutuu ja vesi pääsee tulvimaan sisään.

Vakoiluohjelma-, salakuuntelu tai väliintulohyökkäyksen kohteeksi joutuessaan laiva ja sen omistava yritys voivat menettää kriittistä tai arvokasta tietoa kilpailijoille tai rikollisille. Esimerkiksi merirosvoille hyödyllistä tietoa voisi olla miehistön jäsenten ja vartijoiden määrä laivalla ja tietojen vuotaminen altistaa laivan hyökkäyksille. Jos hyökkääjät puolestaan tuhoavat dataa hyökkäyksen aikana, voi sen rekonstruktio olla kallis ja hidas prosessi (De Albaquerque ja muut, 2022).

Kyberhyökkäyksen kohteeksi joutuneelle laivalle saattaa tulla rahallisia tappioita. Tappioita voi syntyä kuljetusten viivästymisestä tai estymisestä, rahdin menettämisestä, laitteiston tai muun laivan vahingoista ja niiden korjauskuluista sekä poikkeamiin vastaamisen kuluista. (Androjna & Perkovič, 2021)

Kyberhyökkäyksiin liittyy usein yrityksiin kohdistuva mainehaitta. Esimerkiksi tietomurron ja siitä aiheutuneen huonon julkisuuden kohteeksi joutunut Vastaamo haettiin konkurssiin 2021 (Yle, 2021). Kyberhyökkäyksestä aiheutuva mainehaitta vaikuttaa olevan eri-

tyisen vaarallista yrityksen toiminnalle, jos luottamus on tärkeässä roolissa sen liiketoiminnassa. Toisaalta kyberhyökkäyksien tutkinnassa saattaa tulla ilmi myös väärinkäytöksiä yrityksen puolelta, jotka aiheuttavat sidosryhmien luottamuksen menettämisen.

4.2 Yhteiskunta

Koska meriteitse kuljetetaan yli 80 % maailman kaupan tavarasta (Karim, 2022), monet yritykset ja valtiot sekä muut toimijat ovat riippuvaisia sujuvasta meriliikenteestä. Pidemmät katkokset tai häiriöt voivat aiheuttaa ongelmia niin yrityksille kuin yksityishenkilöillekin. Lisäksi väärin toimiva laitteisto voi aiheuttaa vaaratilanteita, joiden vahingot ulottuvat laivan ulkopuolelle.

Suurin osa maailmankaupan tavarasta kuljetetaan meriteitse. Tähän tavaraan sisältyy yhteiskunnan toiminnalle ja ihmisten turvallisuudelle kriittisiä asioita, kuten elintarvikkeet, polttoaineet ja lääkkeet. Suuremmat häiriöt meriliikenteessä voivat aiheuttaa tuonnin ja viennin häiriintymistä. Ääritapauksissa jopa alueiden huoltovarmuus voi heikentyä, jos tärkeiden tarvikkeiden ja materiaalien kuljetukset estyvät. Toisaalta suurimpaan osaan paikoista on myös vaihtoehtoisia tapoja kuljettaa näitä asioita, esimerkiksi lentokoneet tai maantiet. Nämä tavat ovat kuitenkin kalliimpia ja niiden käyttöönottamiseen kuluu hieman aikaa. Lisäksi ne otetaan käyttöön luultavasti vasta sen jälkeen, kun toimitus on jo myöhästynyt tai estynyt.

Maailmassa on muutamia väyliä, joiden toiminta on olennainen osa sujuvaa valtioiden ja mannerten välistä meriliikennettä. Suomen ja muiden Itämeren rannikko valtioiden kannalta Tanskan salmet ovat tärkeät, sillä niiden kautta laivat pääsevät kulkemaan Itämerelle ja pois. Toinen esimerkki on vuonna 2021 kuudeksi päiväksi tukkeutunut Suezin kanava, joka on tärkeä reitti Euroopan ja Aasian välillä. Vaikka Ever Givenin pohjaan juuttuminen johtuikin sää olosuhteista, voisi vastaava tilanne syntyä esimerkiksi laivan navigaatiojärjestelmiin kohdistuvasta kyberhyökkäyksestä. Ever Givenin tapauksessa epäiltiinkin aluksi navigointiin kohdistunutta kyberhyökkäystä (Thomas, 2022). Kanavan tukkeutuminen aiheutti kaupankäynnissä arviolta 7 miljardin Yhdysvaltain dollari tappiot vuorokaudessa (Fan ja muut, 2022). Jos Suezin kanava on tukkeutunut joutuvat laivat kiertämään Afrikan päästäkseen Euroopasta Aasiaan ja päinvastoin. Tästä tulee huomattavasti lisää matkaa, ja kuluu sekä enemmän aikaa, että polttoainetta. Lisäksi Afrikan rannikolla liikkuu merirosvoja. Reitti voi siis olla vaarallinen niin kalustolle, rahdille, kuin ihmisillekin.

Hyökkäämällä navigointijärjestelmiin laiva voidaan ohjailla ulkopuolisen toimijan haluamaan sijaintiin. Laiva voi päätyä esimerkiksi vihamielisen valtion aluevesille, jolloin sille,

sen rahdille ja miehistölle aiheutuu vaaraa. Näin tapahtui isobritannialaiselle öljytankkerille kesällä 2019. Tankkerin AISin GPS-signaalin kohdistui väärentämishyökkäys, jonka avulla laiva ohjattiin Iranin vesille. (Androjna & Perkovič, 2021)

Meriliikennettä voidaan häiritä myös laajemmassa mittakaavassa AIS-signaalin väärentämisen avulla. Androjna & Perkovič (2021) esittelevät joulukuussa 2019 tapahtuneen signaalin väärentämishyökkäyksen, jossa Elba-saaren lähellä väärennettiin AIS-viestejä melkein 4000 valelaivalta. Laivoja näytti olevan alueella jopa 45/km^2 tiheydellä. Hyökkäyksen seurauksena alueen meriliikenteen valvonta vaikeutui ja oikeat laivat näyttivät olevan törmäyskurssilla useiden valelaivojen kanssa. Tämä puolestaan aiheutti paljon törmäyshälytyksiä. Tässä tapauksessa vahingoilta vältyttiin, mutta Androjna & Perkovič (2021) huomauttavat, että seuraukset olisivat voineet olla huomattavasti pahemmat vilkkaasti liikennöidyllä väylällä huonon näkyvyyden aikana.

Tavaran tai ihmisten laiton liikkuminen on mahdollista tietojen muokkauksella. Rahtitietoihin kohdistuva muokkaaminen ja manipuloiminen sallivat tavaran rikollisen salakuljettamisen. Matkustajalistan muokkaaminen puolestaan mahdollistaa ihmisten laittoman matkustamisen. (Androjna & Perkovič, 2021)

4.3 Ympäristö

Merenkulun onnettomuuksiin liittyy riski ympäristön vahingoista. Pienet merialueet, joilla veden vaihtuvuus on hidasta, ovat erityisen herkkiä vieraille aineille. Esimerkiksi Itämeri on pieni, herkkä alue, jonka vesi vaihtuu pääosin Tanskan salmien kautta. Jo pienet määrät polttoainetta, öljyä tai kemikaaleja voivat aiheuttaa ongelmia Itämeren ja sen rantojen ekosysteemeille. Pienten ekosysteemien selviytyminen ja toipuminen on sekä hidasta että vaikeaa. Vuodot voivat vaikuttaa kasvillisuuteen, eläimiin ja ihmisiin.

Kyberhyökkäyksillä voidaan myös piilottaa laittomia toimia. Esimerkiksi heinäkuussa 2020 eräs kalastuslaivasto käytti signaalin väärentämistä kätkeäkseen oikean sijaintinsa Galápagossaarten lähettyvillä, missä kalastaminen on kiellettyä (Androjna & Perkovič, 2021).

Luonnon lisäksi myös rakennettuun ympäristöön voi kohdistua haittoja ja jopa vaaroja törmäyksen seurauksena. Väärään sijaintiin päätynyt laiva voi törmätä esimerkiksi siltaan, satamarakennelmiin tai muihin rakenteisiin. (Thomas, 2022) Näistä aiheutuu vaaraa ihmishengille sekä rannikkojen infrastruktuurille, jotka eivät kestä laivan törmäämistä niihin.

5. POHDINTA

Tutkielman perusteella haavoittuvaisimpia järjestelmiä ovat navigointijärjestelmät AIS, ECDIS ja GNSS. Haavoittuvuuksia löytyy myös muista laiteryhmistä. Lisäksi laivan kyberturvallisuuteen vaikuttavia osia löytyy myös siihen läheisesti liittyvistä järjestelmistä, kuten yritysten verkoista. Yleisimpiä laivoihin kohdistuvia kyberhyökkäyksiä ovat navigaatiojärjestelmiin kohdistuvat signaalien häiritseminen ja väärentäminen. Lisäksi työssä huomattiin, että kyberhyökkäyksillä voi olla hyvin vaihtelevia ja laajoja seurauksia sekä vaikutuksia.

Useat järjestelmät kaipaavat päivittämistä kyberturvallisuuden parantamiseksi. Tunnistettuihin haavoittuvuuksiin sekä riskeihin tulisi reagoida ja niiden hallintaan, vähentämiseen sekä lieventämiseen kehittää uusia ratkaisuja. Nämä ratkaisut olisivat erityisen hyödyllisiä, jos ne onnistuisivat koskemaan laajempaa joukkoa kuin vain yksittäistä laivaa tai laivoja omistavaa yritystä.

Vaikka tutkielmassa käsitelläänkin useita laiteryhmiä ja niistä löytyviä haavoittuvuuksia, jää sen ulkopuolelle joitain laiteryhmiä sekä suurelta osin laivan ulkopuoliset osat. Laivoilta löytyy yhteyksiä moniin kohteisiin, kuten satamiin, yritysten verkkoihin ja satelliitteihin. Täten myös nämä ulkopuoliset osat ja niiden kyberturvallisuus vaikuttavat laivan omaan kyberturvallisuuteen. Lisäksi näiden osien ja laivan välisen yhteyden turvallisuus on vaikuttava tekijä. Nämä kaipaisivat laajempaa tutkimista kokonaisvaltaisemman kuvan saamiseksi laivojen haavoittuvuuksien sekä mahdollisten hyökkäysten laajuudesta. Lisäksi suojautumiskeinojen käsittelystä olisi hyötyä eri haavoittuvuuksien vakaavuuden kuvaamisessa.

Tulevaisuudessa tietotekniikan sekä automaation merkitys tulee kasvamaan merenkulussa autonomisten ja etäohjattavien laivojen sekä kehittyvien prosessien ja järjestelmien myötä. Kyberturvallisuus tulisi ottaa huomioon jo laivojen kehitys- ja suunnitteluvaiheessa. Kyberturvallisuutta laivoissa pitää tarkastella usealta kannalta, sillä eri näkökulmat tarjoavat eriäviä huomioita ja painopisteitä kyberturvallisuuden suunnittelulle. Muun muassa haavoittuvuuksien, riskien, hyökkäysten ja vaikutusten tutkiminen on olennaista. Toisaalta kaikkea ei pysty ennustamaan ennen kuin prosessi on pidemmällä.

Tähän liittyen myös standardien, säännösten ja lakien kehittäminen sekä tarkentaminen voisi parantaa prosessia. Tästä olisi apua myös nykypäivän laivoille, joissa kyberturvallisuuden merkitys lisääntyy. Prosessi on jo aloitettu ja esimerkiksi luokituslaitos DNV on ottanut käyttöön ”kyberturvallinen” -luokkamerkinnän. Tähän kuitenkin liittyy myös paljon

haasteita. Näitä ovat esimerkiksi sekä merenkulun, että kyberrikollisuuden kansainvälinen luonne, valtioiden rajat ja kansainväliset merialueet sekä vaihteleva ymmärrys ja suhtautuminen kyberturvallisuuden tärkeyteen eri alueilla.

6. YHTEENVETO

Kyberturvallisuus on nykyään tärkeässä roolissa turvallisessa merenkulussa. Se on kehittynyt viime vuosina, mutta tutkimus paljastaa edelleen puutteita. Lisäksi kyberturvallisuus ei ikinä voi olla ”valmista”. Tämä johtuu jatkuvasta kehityksestä ja uudesta teknologiasta. Kehityksen myötä myös hyökkäykset kehittyvät ja siten muodostuu jatkuva kilpailu puolustuksen ja hyökkäysten välille.

Erityisesti navigaatiojärjestelmistä löytyy paljon haavoittuvuuksia, joita voidaan hyödyntää kyberhyökkäyksen tekemisessä. GNSS, AIS ja ECDIS ovat haavoittuvaisimpien järjestelmien joukossa. Myös muista laiteryhmistä ja osista löytyy haavoittuvuuksia, esimerkiksi viestintäyhteyksistä ja laivan ulkopuolisista järjestelmistä, kuten yritysten verkoista. Vähiten haavoittuvuuksia puolestaan on propulsiojärjestelmissä. Haavoittuvuuksien vakavuuteen voidaan vaikuttaa, muun muassa järjestelmän yhdistäminen internettiin ja vähäinen miehistön koulutus vaikeuttavat ja lisäävät haavoittuvuuksia.

Yleisimpiä laivoihin kohdistuvien kyberhyökkäysten tyyppejä ovat signaalien häirintä sekä väärentäminen. Näitä hyökkäyksiä kohdistuu erityisesti navigaatiojärjestelmiin. Myös muita hyökkäyksiä, kuten haittaohjelma-, salakuuntelu-, väliintulo-, manipulointi- ja muokkaushyökkäyksiä tehdään laivojen järjestelmiin. Eri kyberhyökkäykset sopivat erilaisiin tarkoituksiin. Niitä hyödyntävät monenlaiset hyökkääjät, joiden motiivit sekä tavoitteet vaihtelevat. Kyberhyökkäysten seuraukset voivat kohdistua niin yksilöön, yritykseen, yhteiskuntaan kuin ympäristöönkin.

LÄHTEET

Androjna, A., & Perkovič, M. (2021). Impact of spoofing of navigation systems on maritime situational awareness. Transactions on Maritime Science, 10(2), 361–373. https://doi.org/10.7225/toms.v10.n02.w08

Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., & Nosheen, S. (2023). A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry. IEEE Transactions on Intelligent Transportation Systems, 1–14. https://doi.org/10.1109/TITS.2022.3164678

Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. Information (Basel), 13(1), 22–. https://doi.org/10.3390/info13010022

De Albuquerque, C. E. P., Machado, R. C. S., De Sa, A. O., & De Toledo, C. R. B. (2022). Bibliometric Analysis on Cyber-Attacks in Naval Sensors and Systems. 2022 IEEE International Workshop on Metrology for the Sea; Learning to Measure Sea Health Parameters, MetroSea, 474–478. https://doi.org/10.1109/MetroSea55331.2022.9950939

Fan, S., Yang, Z., Wang, J., & Marsland, J. (2022). Shipping accident analysis in restricted waters: Lesson from the Suez Canal blockage in 2021. Ocean Engineering, 266, 113119–. https://doi.org/10.1016/j.oceaneng.2022.113119

Karahalios, H. (2020). Appraisal of a Ship's Cybersecurity efficiency: the case of piracy. Journal of Transportation Security, 13(3-4), 179–201. https://doi.org/10.1007/s12198-020-00223-1

Karim, M. S. (2022). Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat? Marine Policy, 143, 105138–. https://doi.org/10.1016/j.marpol.2022.105138

Kavallieratos, G., & Katsikas, S. (2020). Managing Cyber Security Risks of the Cyber-Enabled Ship. Journal of Marine Science and Engineering, 8(10), 768–. https://doi.org/10.3390/jmse8100768

Kavallieratos, G., Katsikas, S., & Gkioulos, V. (2019). Cyber-Attacks Against the Autonomous Ship. In Computer Security ESORICS 2018 International Workshops, Cyber-ICPS 2018 and SECPRE 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers. Springer Verlag. http://hdl.handle.net/11250/2624943

Kontopoulou, S. (2021). Everything You Wanted to Ask About AIS. MarineTraffic Blog. https://www.marinetraffic.com/blog/ais-faq/

Mileski, J., Clott, C., & Galvao, C. B. (2018). Cyberattacks on ships: a wicked problem approach. Maritime Business Review, 3(4), 414–430. https://doi.org/10.1108/MABR-08-2018-0026

Roberts, F. S. (2019). From Football to Oil Rigs: Risk Assessment for Combined Cyber and Physical Attacks. Journal of Benefit-Cost Analysis, 10(2), 251–273. https://doi.org/10.1017/bca.2019.15

Silverajan, B., Ocak, M., & Nagel, B. (2018). Cybersecurity Attacks and Defences for Unmanned Smart Ships. 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 15–20. https://doi.org/10.1109/Cybermatics_2018.2018.00037

Svilicic, B., Kristić, M., Žuškin, S., & Brčić, D. (2020). Paperless ship navigation: cyber security weaknesses. Journal of Transportation Security, 13(3-4), 203–214. https://doi.org/10.1007/s12198-020-00222-2

Svilicic, B., Rudan, I., Jugović, A., & Zec. D. (2019). A Study on Cyber Security Threats in a Shipboard Integrated Navigational System. Journal of Marine Science and Engineering, 7(10), 364–. https://doi.org/10.3390/jmse7100364

Tedeschi, P., Sciancalepore, S., & Di Pietro, R. (2022). Satellite-based communications security: A survey of threats, solutions, and research challenges. Computer Networks (Amsterdam, Netherlands : 1999), 216, 109246–. https://doi.org/10.1016/j.comnet.2022.109246

Thomas, M., L. (2022) Maritime Hacking Using Land-Based Skills. The Institute of Electrical and Electronics Engineers, Inc. (IEEE) Conference Proceedings, 700. https://doi.org/10.23919/CyCon55549.2022.9811049

Tusher, H. M., Munim, Z. H., Notteboom, T. E., Kim, T.-E., & Nazir, S. (2022). Cyber security risk assessment in autonomous shipping. Maritime Economics & Logistics, 24(2), 208–227. https://doi.org/10.1057/s41278-022-00214-0

Yle. (2021). Psykoterapiakeskus Vastaamo asetettiin konkurssiin. https://yle.fi/a/3-11790537 (Haettu 15.8.2023)