Merenkulun kyberturvallisuus ja kyberhyökkäysten vaikutus kansainväliseen kauppaan

LAB-ammattikorkeakoulu
Tradenomi (AMK), Liiketalous, kansainvälinen kauppa
Jesse Jaakkola
Lari Juonala

Tiivistelmä

Tekijä(t)	Julkaisun laji	Valmistumisaika
Jaakkola, Jesse Juonala, Lari	Opinnäytetyö, AMK	2022
	Sivumäärä 42	

Työn nimi

Merenkulun kyberturvallisuus ja kyberhyökkäysten vaikutus kansainväliseen kauppaan

Tutkinto

Tradenomi (AMK)

Tiivistelmä

Opinnäytetyön tarkoituksena oli tarkastella merenkulun kyberturvallisuutta ja selvittää merenkulkuun kohdistuvien kyberhyökkäysten vaikutuksia kansainväliseen kauppaan. Työn teoriaosuudessa käsiteltiin konttiliikenteen merkitystä globaalissa kaupankäynnissä, merilogistiikkaan kohdistuvia kyberhyökkäyksiä sekä kyberturvallisuutta yleisellä tasolla. Teoreettinen osuus pohjautui erilaisiin tutkimuksiin, artikkeleihin, yritysten tietokantoihin ja painettuihin kirjoihin. Työssä pyrittiin hyödyntämään mahdollisimman tuoreita lähteitä. Tutkimusmenetelmäksi valittiin empiirinen tutkimus, jossa haastateltiin kahta merenkulkualan asiantuntijaa. Haastattelut toteutettiin puolistrukturoituina haastatteluina. Haastatteluiden tarkoituksena oli saada käsitys siitä, minkälaisia kyberhyökkäyksiä suomalaiset varustamot ovat kohdanneet ja minkälaisia vaikutuksia niillä on ollut yritysten toimintaan. Haastattelusta saatua aineistoa analysoitiin tutkimuksen johtopäätöksissä. Tutkimuksen perusteella todettiin, että jatkuvasti kehittyvä automaatio kasvattaa riskiä joutua kyberhyökkäyksen kohteeksi ja että kyberhyökkäýsten odotetaan kehittyvän ja lisääntyvän tulevaisuudessa. Hyökkäysten vaikutus kansainväliseen kaupankäyntiin on vakava, ja tunnetut esimerkkitapaukset maailmalta vahvistavat tätä käsitystä.

Asiasanat

merenkulku, merilogistiikka, kyberhyökkäys, kansainvälinen kauppa, kyberturvallisuus, automaatio

Abstract

Author(s)	Type of Publication	Published
Jaakkola, Jesse Juonala, Lari	Bachelor's thesis	2022
	Number of Pages 42	

Title of Publication

Maritime cyber security and effects of cyber attacks on international trade

Name of Degree

Bachelor of Business Administration

Abstract

The purpose of the thesis was to find out facts about the effects of cyberattacks on international maritime trade. Theoretical part focused on the importance of container traffic to global trade, maritime cyberattacks and cyber security in general. Theoretical part was based on research, articles, business databases and printed books. Information of the thesis was based on recent sources. Empirical research was chosen as a research method. The subject was researched by conducting two interviews, which were semi-structured. The purpose of the interviews was to find out what kind of cyberattacks Finnish shipping companies have faced and what kind of effects they have had in their business operations. The material obtained from the interviews was analyzed in the conclusion part of the thesis. Automation was found to bring new and advanced cyber security threats. Cyberattacks are expected to develop and increase in the future. The impact of these attacks on international trade is serious, and examples of different cases around the world confirm this perception.

Keywords

seafaring, marine logistics, cyberattacks, international trade, cyber security, automation

Sisällys

1 Johdanto

1.1 Opinnäytetyön tausta

Globaali merikonttiliikenne on kansainvälisen kaupankäynnin perusedellytys. Tänä päivänä lähes 90 % kauppatavarasta kulkee meriteitse, ja volyymin odotetaan kolminkertaistuvan vuoteen 2050 mennessä (OECD). Vuosittain konttikuljetuksia tehdään noin 300 miljoonaa kertaa, ja kontteja on käytössä globaalisti lähes 20 miljoonaa kappaletta (Logistiikan Maailma). Voidaan puhua tärkeästä logistisesta kuljetusmuodosta, joka koskettaa niin suuryrityksiä kuin tavallisia kuluttajiakin. Mitkä olisivat vaikutukset arkiseen elämäämme, jos merillä, satamissa tai kanavissa sattuisi onnettomuuksia johtuen hakkeroinnin aiheuttamasta järjestelmäkaappauksesta?

Opinnäytetyössä käsitellään tärkeää ja alati kehittyvää ongelmaa, joka liittyy vahvasti maailman merikontti- ja laivaliikenteeseen sekä sitä kautta kansainvälisen kaupankäynnin sujuvuuteen. Merikonttiliikenteessä ja logistiikassa aina ollut omat ongelmansa ja riskinsä, ja tänä päivänä kyberhyökkäykset ovat kasvava ja yhä todennäköisempi uhkakuva. Mahdollisessa esimerkkiskenaariossa rahtialuksen navigointi- ja varoitusjärjestelmää voitaisiin häiritä, mikä saattaisi aiheuttaa karilleajon ja esimerkiksi öljyvuoto-onnettomuuden.

Merirosvous on kautta historian ollut maailman merillä seilaavien laivojen ongelma, mutta kovaa vauhtia kehittyvä teknologia ja digitalisaatio tuovat paljon uudenlaisia uhkakuvia mukanaan. Mahdolliset hyökkäykset uhkaavat logistista toimitusketjua erilaisilla alusten tietojärjestelmiin kohdistuvilla kaappausyrityksillä. Voidaankin puhua digiajan merirosvouksesta, jossa rikolliset toimivat laivaliikennettä vastaan ilman fyysistä voimaa (Gröndahl 2021). Jatkuvasti kehittyvä automaatio on auttanut kehittämään rahtialusten ohjaus- ja varoitusjärjestelmiä. Järjestelmiä pystytään ohjaamaan etänä, ja ne auttavat rahtialuksia välttämään vaarallisia matalikoita ja reittejä, joihin niiden ei kuulu ajautua. Automaatiossa piileekin edellä mainittuja ongelmakohtia, koska järjestelmät ovat vahvasti kytköksissä ulkopuolisiin tietoteknisiin ympäristöihin. (Kovanen 2021.)

Opinnäytetyön aihe on ajankohtainen, sillä kyberhyökkäykset ovat kasvava uhkakuva kansainväliselle meriliikenteelle. Koronavirusepidemian aikana kyberhyökkäysten on arvioitu jopa nelinkertaistuneen (Tuomaala 2021). Tämän vuoksi päätimme lähteä tutkimaan aihetta lisää. Aiheesta löytyy jo paljon fakta- ja tutkimustietoa. Suomessa aihetta ovat tutkineet muun muassa Liikenne- ja viestintäviraston alainen Kyberturvallisuuskeskus sekä Huoltovarmuuskeskus.

Huoltovarmuuskeskuksen julkaisema ohjeistus perustuu Vesikuljetuspoolin ja Suomen Varustamot ry:n tilaamaan selvitykseen, ja siinä käsitellään alusten kyberturvallisuuden osa-alueita. Selvitys kattaa käytännöllisiä ohjeita vesiliikennetoimijoille, ja siinä ohjeistetaan muun muassa tunnistamaan alusten kriittisten toimintojen riskejä sekä segmentoimaan kriittisiä järjestelmiä eri verkkoihin. (Huoltovarmuusorganisaatio 2021.)

Kansainvälinen merenkulkujärjestö IMO (International Maritime Organization) on koonnut verkkosivuilleen ohjeistuksia ja raportteja aiheesta. Järjestö on julkaissut virallisen ohjeistuksen (Guidelines on Maritime Cyber Risk Management), jossa annetaan korkean tason suosituksia alusten kyberturvallisuuden hallintaan ja turvalliseen merenkulkuun. (International Maritime Organization.)

Aiheesta kiinnostunut lukija saa opinnäytetyön luettuaan käsityksen siitä, mitkä ovat keskeisimpiä konkreettisia konttiliikenteeseen kohdistuvia kyberturvallisuuden uhkia, ja miksi juuri merikonttiliikenteeseen kohdistuvat kyberhyökkäykset voivat olla niin merkittäviä kansainvälisen kaupan sujuvuuden kannalta. Opinnäytetyö voi myös tarjota alalla toimiville suomalaisille yrityksille tietoa siitä, minkälaisiin uhkiin yritysten kannattaisi varautua ja minkälaisia riskejä heidän kannattaisi toiminnassaan huomioida.

1.2 Opinnäytetyön tavoite ja rajaukset

Opinnäytetyön tavoitteena on selvittää, minkälaisia kyberturvallisuusuhkia kansainväliseen meriliikenteeseen tällä hetkellä kohdistuu ja minkälaisia vaikutuksia mahdollisilla kyberhyökkäyksillä on meriliikenteeseen ja kansainvälisen kaupan sujuvuuteen.

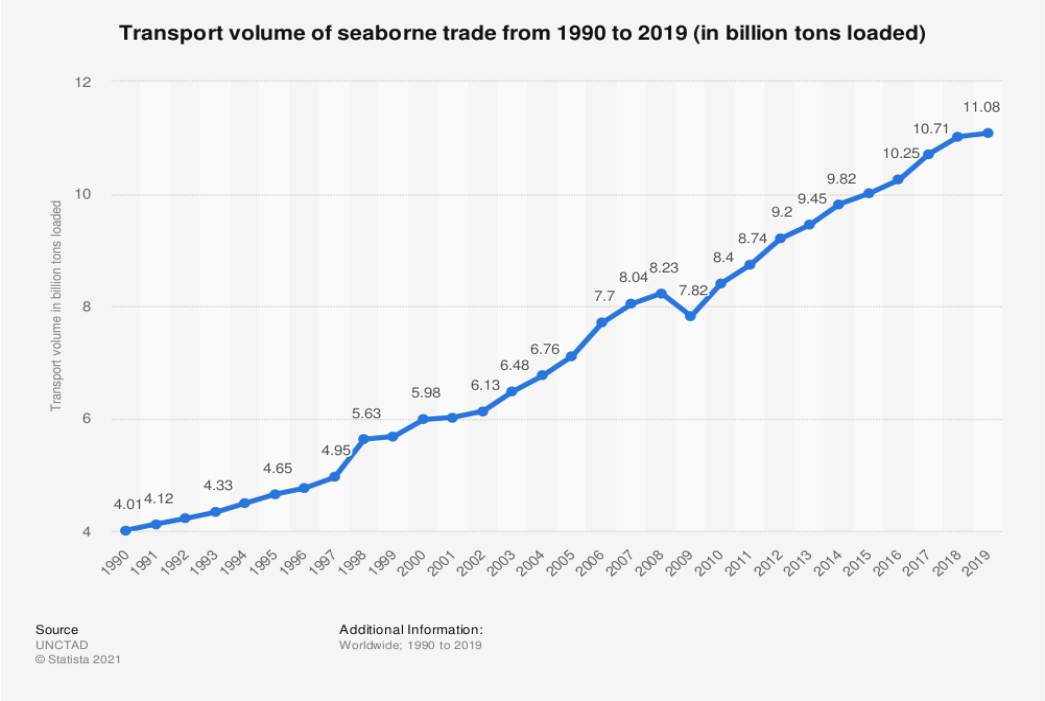
Uhkakuvien tarkastelu on rajattu kyberturvallisuuteen aiheen ajankohtaisuuden vuoksi: verkkourkinta ja tietojenkalastelu muodostavat tällä hetkellä suurimman merenkulun turvallisuuteen kohdistuvan uhan (Tuomala 2020). Työn teoriaosuus on rajattu meriliikenteen tarkasteluun osana logistista toimitusketjua. Valtaosa maailman kauppatavarasta kulkee meriteitse, joten kokonaisvaikuttavuuden kannalta on loogista tarkastella aihetta meriliikenteen näkökulmasta.

Tutkimusosuus on rajattu koskemaan suomalaista varustamoyhtiötä Finnlines Oyj:ta sekä Suomen Varustamot ry:tä, joka toimii suomalaisten varustamoyhtiöiden jäsenyhdistyksenä. Tutkimus suoritetaan kahden haastattelun muodossa. Tutkimuksella pyritään selvittämään, onko Finnlines kohdannut kyberhyökkäyksiä ja miten nämä ovat mahdollisesti vaikuttaneet yrityksen toimintaan. Suomen Varustamot ry:n osalta pyritään selvittämään, ovatko muut suomalaiset varustamoyhtiöt kohdanneet kyberhyökkäyksiä, ja millaisia vaikutuksia näillä

on mahdollisesti ollut yhtiöiden liiketoimintaan ja kansainväliseen kauppaan. Haastatteluiden ja teoriatiedon avulla pyrimme vastaamaan tutkimuskysymyksiin. Tutkimuskysymykset ovat seuraavat: minkälaisia kyberturvallisuusuhkia varustamoyhtiöt kohtaavat ja miten merenkulun kyberhyökkäykset voivat vaikuttaa kansainvälisen kaupan sujuvuuteen.

1.3 Opinnäytetyön teoreettinen lähtökohta

Opinnäytetyön teoriaosuuden on tarkoitus toimia pohjana tutkimukselle. Jotta kyberhyökkäysten mahdollisia vaikutuksia maailmankaupalle on helpompi ymmärtää, on tärkeää käsitellä merikonttiliikennettä yleisellä tasolla ja sen merkitystä kansainvälisessä kaupassa. Kuten kuviosta 1 näkee, merikonttiliikenteen kuljetusvolyymi on kasvanut lähes tasaisesti vuodesta 1990 lähtien. Vuonna 1990 meriteitse kuljetettiin noin 4 miljardin tonnin edestä rahtia. Vuosien 1990 ja 2019 välillä määrä on ollut laskusuunnassa vain kerran, vuosien 2008 ja 2009 välillä, kun maailmantalous koki Yhdysvalloista alkunsa saaneen finanssikriisin seuraukset. Kriisin aiheuttaman notkahduksen jälkeen merikonttiliikenteen volyymi on ollut jälleen nousussa, ja oli vuonna 2019 noin 11 miljardia tonnia.



Kuvio 1. Maailmanlaajuisen merikonttiliikenteen volyymin kasvu 1990–2019 (UNCTAD, Statista 2021 mukaan)

Meriteitse kulkevan tavaran määrä on niin suuri, että mahdolliset viivästykset ja ongelmat kuljetusten aikana näkyvät vääjäämättä ihmisten arkisessa elämässä. Maaliskuussa 2021 taiwanilaisen Evergreen-varustamon 400-metrinen konttilaiva Ever Given tukki Suezin kanavan lähes viikoksi, aiheuttaen valtavia taloudellisia tappioita ja viivästyksiä usealle merkittävälle toimialalle, kuten elektroniikka-, auto- ja IT-teollisuudelle (Osto&Logistiikka 2021). Ever Given -konttilaivaan liittyvät tapahtumat johtuivat pääasiassa poikkeuksellisen kovasta tuulesta ja hiekkamyrskystä, jotka aiheuttivat laivan karilleajon (BBC 2021). Kyseinen tapahtumaketju oli ilmasto-olosuhteista johtuva onnettomuus, mutta tapahtuma on mahdollinen myös ulkopuolisen toimijan aiheuttamana ilman fyysistä kontaktia itse alukseen. Mahdollisen kyberhyökkäyksen sattuessa vaikutukset logistiseen toimitusketjuun ja ihmisten arkielämään voivat olla suuria.

Opinnäytetyön toisessa teorialuvussa käsitellään rahtialusten kyberturvallisuutta ja kyberhyökkäyksiä laajemmin, jolloin lukija ymmärtää paremmin kyberturvallisuuden merkityksen alusten kokonaisturvallisuuden kannalta. Tässä luvussa avataan myös kyberturvallisuusalan käsitteistöä, sillä aihealue on laaja ja sen ymmärtäminen vaatii asiaan perehtymistä.

1.4 Tutkimusmenetelmä ja tiedonkeruu

Tutkimusta voidaan lähestyä erilaisilla tavoilla. Induktiivisessa tutkimuksessa pyritään rakentamaan teoriaa ja esittämään sen pohjalta erilaisia malleja ja johtopäätöksiä. Ritala (2013) toteaa, että tässä lähestymistavassa on tärkeää määritellä erilaiset käsitteet muun muassa tutkimuksen laadun ja ymmärrettävyyden kannalta. Induktiivisessa tutkimuksessa hyödynnetään pääasiassa kvalitatiivista aineistoa. Deduktiivinen tutkimus perustuu pääosin kvantitatiiviseen aineistoon, ja siinä keskiössä ovat erilaisten teorioiden ja hypoteesien testaukset. Deduktiivisessa tutkimuksessa hyödynnetään standardoituja välineitä, kun taas induktiivinen tutkimus on joustavampaa.

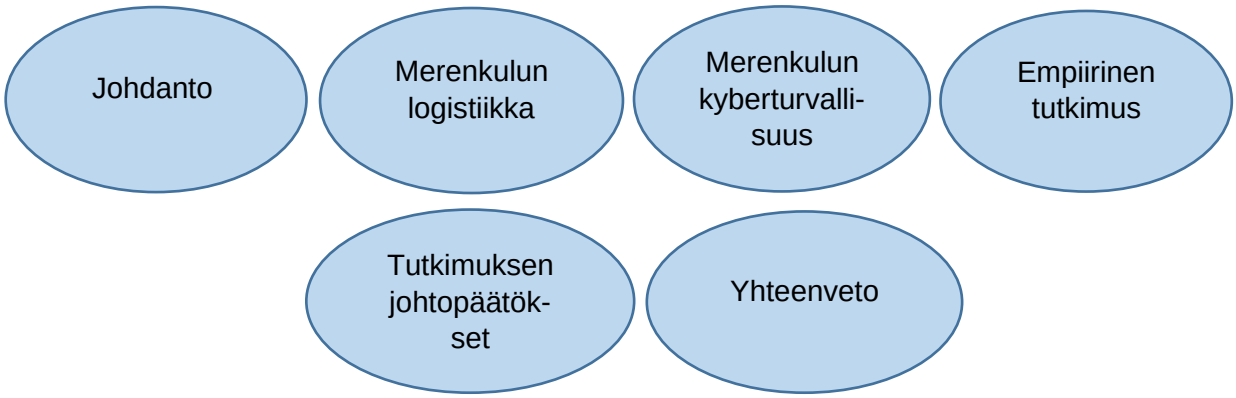
Aineistoa kerätessä voidaan käyttää laadullista tai määrällistä tutkimusmenetelmää. Laadullisessa eli kvalitatiivisessa menetelmässä tutkimus perustuu tulkintoihin, joita aineiston pohjalta tehdään. Aineisto voidaan kerätä esimerkiksi haastattelun tai kyselytutkimuksen muodossa. Tässä tutkimusmenetelmässä aineiston täytyy olla mahdollisimman laadukas ja dataa on kategorisoitava. Määrällisessä eli kvantitatiivisessa tutkimuksessa aineisto on yleensä numeerisessa muodossa, ja sitä on saatava mahdollisimman paljon. Aineiston keruu tapahtuu systemaattisilla ja vakiintuneilla menetelmillä. (Ritala 2013, 20.)

Tämä opinnäytetyö suoritetaan kvalitatiivisella tutkimusmenetelmällä. Tutkimuksen teoria-osuutta varten kerätään tietoa kirjallisista lähteistä, kuten tutkimuksista, uutisista ja artikkeleista. Teoria toimii pohjana empiiriselle tutkimukselle, joka toteutetaan haastatteluiden muodossa. Haastattelujen pohjalta saamme aineistoa analysoitavaksi. Aineiston pohjalta voimme tehdä erilaisia johtopäätöksiä ja tulkintoja. Valitsimme laadullisen tutkimusmenetelmän, koska analysoitavan datan määrä on suhteellisen pieni ja aineisto pohjautuu haastatteluihin sekä olemassa olevaan tietoon, kuten artikkeleihin, tutkimuksiin ja uutisiin.

1.5 Opinnäytetyön rakenne

Opinnäytetyö alkaa johdannolla, kuvion 2 mukaisesti. Johdannon perusteella lukija saa käsityksen opinnäytetyön rakenteesta, taustoista, tutkimusmenetelmästä ja teoreettisista lähtökohdista. Johdannossa käsitellään myös opinnäytetyön tavoitteita ja rajauksia. Toinen pääluku kattaa merikonttiliikenteen tarkastelun osana logistista toimitusketjua. Tässä pääluvussa käsitellään merikontin merkitystä globaalissa kaupankäynnissä sekä merenkulun valvontaa ja turvallisuusmääräyksiä, jotka liittyvät olennaisesti alusten kyberturvallisuuteen. Kolmannessa pääluvussa käydään läpi alusten kyberturvallisuutta yleisellä tasolla sekä erilaisia uhkakuvia ja niiden mahdollisia seurauksia. Tähän lukuun tulee osaksi myös havainnollistavia kuvioita.

Neljäs pääluku on empiirinen tutkimus. Luvun alussa käsitellään haastattelua tutkimusmenetelmänä. Itse tutkimus koostuu kahdesta haastattelusta, joiden on tarkoitus antaa tietoa lukijalle siitä, miten kyberhyökkäykset käytännössä vaikuttavat laivayhtiöiden toimintaan ja miten eri uhkakuviin voidaan varautua. Haastattelututkimuksen jälkeen käsitellään tutkimuksen johtopäätöksiä. Tässä luvussa vastataan tutkimuskysymyksiin, analysoidaan reliabiliteettia ja validiteettia sekä esitetään mahdollisia jatkotutkimusehdotuksia. Työn loppuun tulevat yhteenveto ja lähdeluettelo.



Kuvio 2. Opinnäytetyön rakenne

2 Merenkulun logistiikka

2.1 Merikontin historia

Modernin kontin kehitti yhdysvaltalainen Malcolm McLean, ja ensimmäinen konttialus lähti matkaan vuonna 1956. Vuonna 1966 tehtiin ensimmäinen merikonttikuljetus Atlantin valtamerellä, jolloin Yhdysvaltojen itärannikolta matkaan lähtenyt alus kuljetti lastin Eurooppaan. Tämä tarkoitti osaltaan kaukoliikenteen kaupankäynnin ajanjakson alkua. Konttilaivojen maailmanlaajuiset kuljetusverkostot alensivat merirahdin hintoja, ja yhä useampaa tavaraa kuljetettiin meriteitse. Tämä mahdollisti myös uudenlaisia strategioita kansainvälisillä markkinoilla toimiville yrityksille. (Rodrigue & Notteboom.)

Vuoden 1966 loppupuolella kehitettiin ja tuontiin käyttöön uusi konttityyppi ja sen mitat standardisoitiin. Rodrigue ja Notteboom toteavat, että tämän ansiosta satamissa pystyttiin jatkossa säästämään aikaa, jolloin logistiikka muuttui nopeaksi ja kustannustehokkaaksi. Satamista käsin pystyttiin jatkamaan kontin matkaa maalogistiikan keinoin, jolloin kontti pystyttiin siirtämään nopeasti esimerkiksi proomulle, trailerille tai tavarajunan kyytiin.

Ensimmäinen standardimitoitetuilla konteilla lastattu alus oli vuonna 1968 Japaniin rekisteröity konttilaiva, joka kulki Japanin ja Yhdysvaltojen länsirannikon välillä. Alus pystyi kuljettamaan yhteensä 752 standardikokoista konttia. (Menon 2021.) Näistä konteista käytetään nykyisin nimitystä TEU-kontti (twenty foot equivalent unit). Kontin sisätilavuus on 32 kuutiometriä ja kokonaistilavuus 38 kuutiometriä. Kontit ovat standardikokoisia, joten niiden päällekkäin lastaaminen ja liittäminen toisiinsa on helpompaa. Kuvassa 1 on esimerkki standardimitoitetusta kontista.

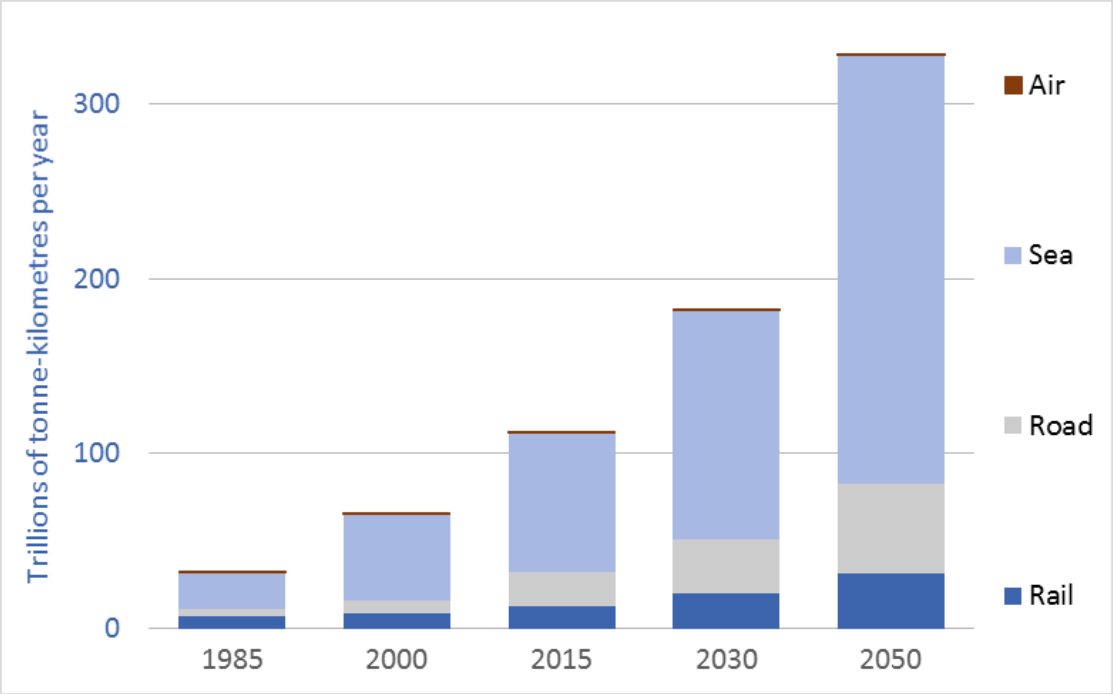
Kuva 1. Standardimitoitettu TEU-kontti (Blue-Growth 2021)

2.2 Globalisaatio ja meriliikenteen kasvu

Merikontti on ollut yksi tärkeimmistä vastauksista maailman logistisiin kysymyksiin ja ongelmiin. Se on ollut globalisaation ja kansainvälisen kaupan kasvun avaintekijä 1970-luvulta lähtien. Globalisaation seurauksena maailmankauppa on kasvanut kovaa vauhtia 1950-luvulta lähtien, ja vuonna 2007 ylitti ensimmäisen kerran 50 % maailman bruttokansantuotteesta. (Rodrigue & Notteboom).

Yksi merkittävä syy meriliikenteen kasvulle on niin sanottu skaalaetu (economies of scale). Meri on mahdollistanut eritäin suurten kuljetusjärjestelmien käytön logistiikan alustana. Alus vaatii merkittävän alkuinvestoinnin, mutta matalan riskin operointi yhdistettynä arvokkaaseen lastiin kumoaa alkuinvestoinnin nopeasti. Kuljetusten yksikköhinta saadaan vietyä alas, ja kuluttaja joutuu maksamaan tuotteen hinnassa ainoastaan muutamia prosentteja kuljetuskustannuksia. Merenkulkua odottaa niin sanottu neljäs vallankumous. Maailman talousfoorumi WEF ennustaa käynnissä olevan neljännen vallankumouksen koostuvan kasvavan älykkään automaation tuomista parannuksista tehokkuuteen. Tästä syystä merirahti tulee jatkossakin olemaan merkittävä globalisaation edistäjä. (Leppänen ym. 2020.)

Globaalin tavaramäärän kasvaessa myös merirahdin määrä on kasvanut voimakkaasti vuodesta 1985 lähtien, kuvion 3 mukaisesti. Kuviossa yksi tonnikilometri kuvastaa tuhatta kilogrammaa kuljetettua tavaraa yhtä kilometriä kohden. Vuonna 2015 kuljetettavan tavaran määrä oli ylittänyt jo 100 biljoonaa tonnikilometriä. Meriteitse kuljettavan tavaran määrä suhteessa lento-, maa- ja raidekuljetuksiin on pysynyt korkealla, ja ennusteen mukaan osuus kasvaa entisestään vuoteen 2050 mennessä. Merirahdin osuus pysyy tulevaisuudessa korkealla erityisesti halvempien kuljetuskustannusten ansiosta.



Kuvio 3. Merirahdin osuus globaaleista kuljetusmuodoista (Qualman 2017)

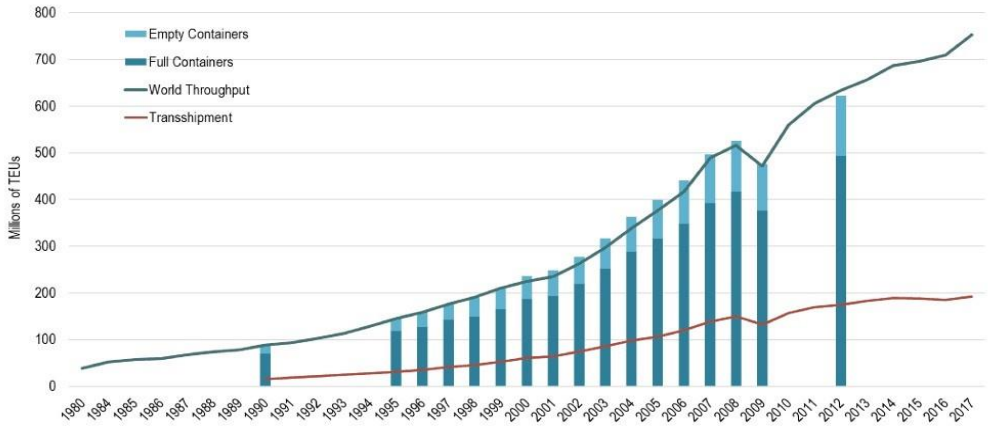
Globalisaation nopeaa kehitystä ei olisi tapahtunut ilman halpoja kuljetuskustannuksia, jotka merikontti on mahdollistanut. Maailman BKT:n kasvaessa merikuljetukset ovat kasvaneet entistä nopeammin. Tuotteita ei valmisteta yhdellä kertaa yhdessä maassa, vaan raaka-aineet kulkevat pääasiassa maasta toiseen useampaan kertaan. Välituotteita kuljetetaan lisäjalostusta varten, ja usean kuljetuskerran jälkeen lopputuotteet päätyvät kulutettaviksi. (Tapaninen 2019, 13)

Maailman meriliikenteessä suuret teollisuusmaat toimivat pääasiassa lastin lähettäjinä tai vastaanottajina. Valtaosa meriliikenteestä kulkee Pohjois-Atlantilla ja pohjoisella Tyynellä valtamerellä sekä Suezin ja Panaman kanavien kautta. Länsimaissa kulutettavat hyödykkeet ja kulutustavarat on yhä useammin valmistettu Kiinassa tai muualla Kaukoidässä. Nämä tavarat kuljetetaan konteissa kuluttajille, minkä johdosta myös konttiliikenne kasvaa jatkuvasti, kun hyödykkeitä tuotetaan yhä enemmän ja yhä kauempana länsimaisista kuluttajista. Tapaninen (2019, 14) uskoo, että konttien käyttö kasvaa yhä enemmän tulevaisuudessa, koska Kaukoidästä länteen ei ole saatavilla muita yhtä kustannustehokasta kuljetusvaihtoehtoja. Maailmankauppa ei ole tasapainossa, sillä lasteja kuljetetaan enemmän esimerkiksi aasialaisilta raaka-ainekeskittymiltä läntiselle puolelle maapalloa kuin päinvastoin. Rahtialusten palatessa Euroopasta Kaukoitään on todennäköistä, että konteissa on paljon tyhjää tilaa.

Euroopan unioni ja Suomi ovat riippuvaisia kansainvälisestä kaupasta. EU:n yhteinen kauppapolitiikka yhdessä EU:n neuvottelemien kauppasopimusten kanssa on tehnyt Euroopan unionista yhden maailman tärkeimmistä kaupankäyjistä, Yhdysvaltojen ja Kiinan jälkeen. EU:n vienti kattaa yli 15 % maailmanlaajuisesta viennistä. Eurooppalaisille kuluttajille globalisaatio näyttäytyy laajempana tuotteiden ja palveluiden valikoimana sekä lisääntyneen kilpailun johdosta alentuneina hyödykkeiden hintoina. (Euroopan parlamentti 2019.)

2.3 Merikontin merkitys ja hyödyt

Kuviosta 4 voidaan tarkastella merikonttien tuotannon globaalia kasvua. Yhä kiihtyvä globalisaatio ja robotiikka lisäävät tuotannon tehokkuutta ja sen seurauksena kontteja tuotetaan yhä enemmän. Merkittävä osa kulutustavarasta tuotetaan Aasian suurissa teollisuusmaissa, joten myös konttien tarve on näissä maissa suurta. Konttikuljetus on tehokkain tapa kuljettaa tavaraa Aasiasta maailmanmarkkinoille, joten konttien kysyntä ja käyttötarve on alati kasvava. Multasen (2021) artikkelissa käsitellään merikonttien riittämättömyyttä ja sitä, kuinka kysyntä ylittää nykypäivinä merikonttien tarjonnan. Huomiota herättävää merikonttikuljetuksessa on myös se, että se mahdollistaa syrjäisempien maiden kaupankäynnin ja näin ollen tuotteita saadaan maailmanmarkkinoille näiltä alueilta tehokkaammin. (Reinikkala 2007.)



Kuvio 4. Konttien tuotanto maailmanlaajuisesti 1980–2017 (The geography of transport systems 2021)

Kontilla on todettu olevan useita hyötyjä tavaran kuljetuksessa, mikä on johtanut konttien tuotannon suureen kasvuun vuosien varrella. Monissa konteissa tarvittavat tiedot on merkitty kontin ulkopuolelle, mikä helpottaa tavaran tunnistamissa satamissa ja nopeuttaa lastaamisprosessia. Kontti tarjoaa myös hyvän suojan hyödykkeille, sillä ne on tehty kestäviksi ja sinetöity asianmukaisilla tavoilla. Tavaroiden laatu säilyy hyvänä koko kuljetuksen ajan. Tämä on tärkeää, sillä sääolosuhteet voivat kuljetusten aikana muuttua. Kontissa voidaan

kuljettaa hyvin monenlaisia hyödykkeitä, kuten elintarvikkeita, kulutustavaraa tai myös vaarallisiksi luokiteltavia aineita ja nesteitä. (Adams 2020.)

Rodriguen ja Notteboomin mukaan kontti tarjoaa maailmanlaajuiselle logistiikalle standardin, jonka ympärillä fyysiset jakelujärjestelmät voivat toimia tehokkaasti. Konttien merenkulku on tullut myös olennaiseksi osaksi maailmanlaajuisten toimitusketjujen muokkaamista. Se on mahdollistanut monikansallisten yritysten hankintastrategioita sekä kehittänyt maailmanlaajuisia tuotantoverkkoja. Uudet toimitusketjun käytännöt ovat lisänneet osaltaan konttikuljetuksen vaatimuksia liikenteen tiheyden, aikataulun luotettavuuden, palvelujen maailmanlaajuisen kattavuuden, tehokkuuden ja ympäristönsuojelun tasoilla.

Kontti voi kestää käytöstä riippuen 10 vuodesta 25 vuoteen. Kun kontin käytöstä luovutaan, sitä voidaan käyttää esimerkiksi tavaroiden varastoimiseen. Jakelijat voivat hyödyntää konteja väliaikaisina varastotiloina silloin, kun varastotila uhkaa loppua. Kontin elinkaaren loputtua se päätyy normaalisti kierrätykseen. (Menon 2021.)

Koronapandemian aikana ilmennyt konttipula ja sen aiheuttamat viivästykset tavaroiden kuljetuksessa ovat koskettaneet koko maailmankauppaa. Tämä on johtanut siihen, että konttien hinnat ovat jopa kahdeksankertaistuneet. Uusia merikontteja valmistetaan vuonna 2021 noin 5,4 miljoonaa kappaletta, mutta korkean kysynnän johdosta tämä ei riitä. Suuren tavaramäärän vuoksi kontteja tarvittaisiin erityisesti Aasian suurissa satamissa. Kontin merkittävimpiin etuihin ovat aina lukeutuneet alhaiset rahtikustannukset, ja konttipulasta johtuvat rahtihintojen nousut tulevat näkymään kuluttajilla ympäri maailmaa. (Aamulehti 2021.)

Myös Multasen (2021) artikkelissa käsitellään globaalia konttipulaa. Se on koskettanut erityisesti maita, joiden konttitarve vaihtelee. Suuret vientimaat voivat varmistaa konttien saatavuuden vuosisopimuksilla. Suurimmat ongelmat konttien saannissa heijastuvat varustamoyhtiöihin, ja ongelman korjaamiseksi konttien kiertoa on pyritty nopeuttamaan. Ongelmia ovat aiheuttaneet koronapandemia, suurten satamien ruuhkautuminen sekä Iso-Britannian irtautuminen EU:sta. Konttipulan seurauksena myös rahtien hinnat ovat nousseet moninkertaisesti.

Ever Given -konttialuksen jumittuminen Suezin kanavalla todisti, kuinka riippuvainen globaali toimitusketju on konttikuljetuksista. Arvioidaan, että noin 30 % globaalista merikonttiliikenteen volyymista kulkee Suezin kanavan kautta (Nagurney 2021). Mikäli Suezin kanavalla tai muulla tärkeällä merireitillä tapahtuisi jatkossa tukoksia, vaikuttaisi se lukemattomiin kuluttajiin ja yrityksiin ja aiheuttaisi suuria taloudellisia tappioita ja pahimmassa tapauksessa maailmankaupan seisahtumisen tietyn reitin osalta. Huomioimalla alusten

kyberturvallisuuden, varustamoyhtiöt voivat vähentää riskiä tällaiselle toimitusketjujen katkeamiselle.

Kuva 2. Ever Given -konttialus tukki Suezin kanavan maaliskuussa 2021 (BBC 2021)

2.4 Merenkulun turvallisuus ja valvonta

2.4.1 Valvonta ja säätely

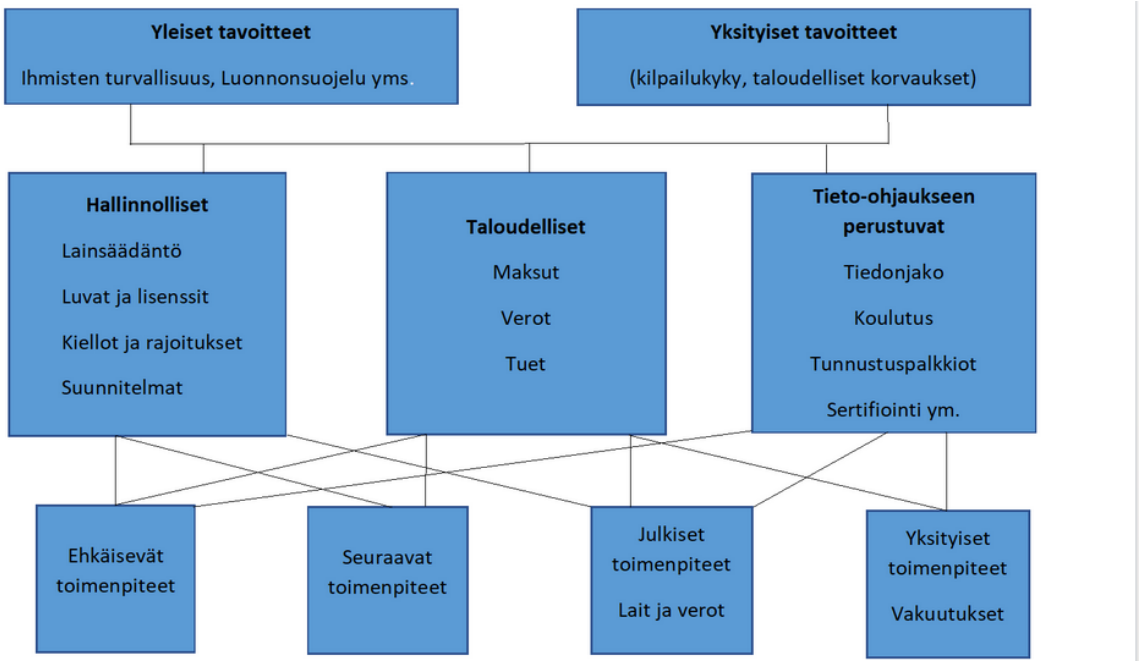
Kansainvälinen merenkulkujärjestö IMO perustettiin vuonna 1948. Se on YK:n alaisuudessa toimiva kansainvälinen merenkulun turvallisuutta valvova järjestö. Käytännön tasolla IMO solmii merenkulkuun osallistuvien maiden kanssa sopimukset, joita sovelletaan kansalliseen lainsäädäntöön. IMO:n ohjauskeinot pitävät sisällään rahtialusten rakenteisiin ja varustukseen, meriturvallisuuteen, meriympäristön suojeluun, alusten kunnon valvontaan, miehistöihin ja merityön harjoittamiseen liittyviä määräyksiä. IMO:n tärkeimpiin sopimuksiin kuuluvat SOLAS-yleissopimus merenkulun turvallisuudesta (Safety of Lives at Sea), MARPOL-sopimus (The International Convention for the Prevention of Pollution from Ships) merenkulun ympäristöasioista sekä STCW-sopimus (International Convention on Standards of Training, Certification and Watchkeeping for Seafarers) merenkulkijoiden koulutuksesta ja miehityksestä. Näiden lisäksi muun muassa EU asettaa omia määräyksiään merenkululle. EU:n alueella merenkulun turvallisuusjärjestelmien ylläpidosta vastaa Meriturvallisuusvirasto (European Maritime Safety Agency, EMSA). (Tapaninen 2019, 120–121)

IMO:n määräykset jaetaan kolmeen luokkaan: saastuttamisen ehkäisyyn liittyvät normit, laivan rakenteita ja tekniikkaa määrittävät tekniset normit sekä toiminnalliset määräykset, kuten määräykset pitää kirjaa jätteistä. Näitä määräyksiä valvotaan kolmella eri tavalla. Rahtialusten rakentamista ja teknistä laatua valvotaan, ja jokaisen käytössä olevan laivan tulee olla jonkin luokituslaitoksen hyväksymä. Luokituslaitosten avulla pystytään valvomaan, että alukset on valmistettu oikeaoppisesti ja niiden kunnosta pidetään huolta. Tarkastuksia toteutetaan 1–5 vuoden aikajaksolla. (Tapaninen 2019, 122)

Kuviossa 5 on esitetty yleisiä tavoitteita kansainväliseen merenkulkuun liittyen. Tärkeimpiä tavoitteita ovat muun muassa merenkulun parissa työskentelevien ihmisten turvallisuus sekä luonnon suojeleminen osana meriliikennettä ja toimivaa kaupankäyntiä. Yksityiset tavoitteet määrittävät varustamoiden taloudelliset odotukset ja tarpeet sekä sen, että yhtiöt pysyvät kilpailukykyisinä. Varustamoiden on noudatettava voimassa olevia lakeja, ja merellä toimimiseen tarvitaan erilaisia lupia ja lisenssejä, kuten esimerkiksi vaarallisten aineiden kuljetukseen vaadittavien kriteerien täyttyminen ja siihen liittyvät dokumentit. Merenkulun ympäristömääräykset ovat yksi suurimmista valvottavista asioista, jossa esimerkiksi rikki- ja kasvihuonekaasupäästöjä pyritään minimoimaan.

Valvontaa kohdistetaan myös huonokuntoisiin aluksiin. Euroopan alueella on voimassa Paris Memorandum of Understanding -sopimus, johon kuuluvat 27 Euroopan unionin valtiota sekä Kanada. Samankaltaisia sopimuksia on maailmalla useita, mutta tarkastukset tehdään samoja periaatteita käyttäen. Merillä toimii vuosittain paljon huonokuntoisia aluksia, jotka eivät täytä yleisiä vaatimustasoja. Näin ollen alukset voivat olla vaaraksi miehistölleen ja ympäristölleen. Paris MoU -sopimus pyrkii estämään huonokuntoisten alusten pääsyn Euroopan satamiin. Esimerkiksi satamavaltiodirektiivi velvoittaa suorittamaan tarkastuksia Suomen satamissa vieraileviin aluksiin, joissa aluksen kunto ja toimintakyky selvitetään. (Logistiikan Maailma.)

Yhtiöiden on huomioitava toiminnassaan kansainväliset ja kansalliset maksut ja verot. Esimerkiksi Suomessa tukea voidaan myöntää kotimaan rekisteriin ja kauppa-alusluetteloon kirjatuille aluksille kilpailukyvyn ylläpitämiseksi tai parantamiseksi (Traficom 2021). Merenkulun koulutusta pyritään jatkuvasti kehittämään merenkulun turvallisuuden takaamiseksi, sillä alaan liittyy useita riskitekijöitä, jotka liittyvät muun muassa suuriin ympäristö- ja henkilövahinkoihin. Kansainvälinen merenkulkujärjestö IMO valvoo ja seuraa osaltaan merenkulkua, mutta ensisijainen vastuu turvallisesta merenkulusta on kuitenkin varustamoyhtiöillä, jotka harjoittavat laivaliiketoimintaa. Turvallinen merenkulku edellyttää vaatimusten, lakien, ohjeistusten ja kansallisen tason sääntöjen noudattamista.



Kuvio 5. Merenkulun valvontamekanismit (Tapaninen 2019, 122)

Lippuvaltiot valvovat itse laivojensa toiminnallista suorituskykyä ja kuntoa. Lippuvaltio on maa, jonka lainsäädännön alle alus on rekisteröity. Esimerkiksi Suomessa valvonta suoritetaan Traficomin eli Liikenne- ja viestintäviraston kautta. Satamaan saapuvien alusten kunnon tarkastus kuuluu sille rantavaltiolle, johon laiva on saapunut. Satamavaltiotarkastukset on tarkoitettu ympäristövahinkojen ja onnettomuuksien ehkäisemiseksi. Myös tämän valvonnan suorittaa Suomessa Liikenne- ja viestintävirasto. Kansallisella tasolla valvonnan tason laatu vaihtelee, ja merillä tavataan ajoittain kunnoltaan kyseenalaisia aluksia, jotka on kuitenkin tarkistettu. (Tapaninen 2019, 122)

2.4.2 Turvallisuusmääräykset

Merenkulkualan turvallisuutta ohjaavat lukuisat erilaiset säädökset ja sopimukset. Kansainvälisellä tasolla tärkeimpiä sopimuksia ovat SOLAS-sopimus, ISM-säännöstö (International Safety Management), ISPS-säännöstö (International Ship and Port Facility Security), Euroopan unionin säännös 725/2004 sekä IMO:n ohjeistus MSC.428(98), joka koskettaa erityisesti kyberturvallisuutta osana alusten muita turvallisuusjärjestelmiä. SOLAS- sopimusta on kehitetty historian aikana aina suurten merionnettomuuksien jälkeen, ja ensimmäisen kerran sopimus tehtiin vuonna 1929 Titanicin uppoamisen seurauksena. SOLAS-sopimusta on uudistettu vuosina 1948, 1960 ja 1974. Muutoksia sopimukseen tekee IMO:n turvallisuuskomitea MSC. Yleissopimuksen alla on useita erilaisia säännöstöjä, jotka ohjaavat alusten turvallisuutta. Sekä ISM että ISPS-säännöstö ovat osa SOLAS-sopimusta. (Suomen Varustamot ry.)

ISPS-säännöstö tuli voimaan vuonna 2004, ja sen tarkoituksena on turvata erityisesti satamien ja alusten turvallisuutta (Suomen Varustamot ry). Alusten osalta ISPS-säännöstö koskee matkustaja-aluksia, lastialuksia sekä liikkuvia porausyksiköitä rannikon edustalla. Varustamoyhtiöiden on huolehdittava alusten turva-arvioinneista, joiden pohjalta alusten turvasuunnitelmat laaditaan. (Traficom 2019.)

Satamien osalta ISPS-säännöstö pyrkii luomaan turvallisuutta muun muassa satamien kulunvalvonnan osalta. Säännöstöllä pyritään siihen, ettei satama-alueille tule ulkopuolisia ja ettei aluksiin päätyisi vaarallisia aineita, kuten räjähteitä tai aseita. Satama-alueella on myös oltava asianmukaiset turvallisuussuunnitelmat ja sataman henkilöstön tulee olla koulutettu erilaisten poikkeustilanteiden varalta. (Marine Insight 2021.)

ISM-säännöstö hyväksyttiin IMO:ssa vuonna 1993, ja Suomessa säännöstöön pohjautuva turvallisuusjohtamisjärjestelmä on ollut pakollinen Roro- ja Ropax- tyypin aluksille vuodesta 1996 lähtien. Muille alustyypeille järjestelmä tuli pakolliseksi vuonna 1998. Turvallisuusjohtamisjärjestelmällä tarkoitetaan dokumentoitua järjestelmää, jonka avulla yhtiö voi toteuttaa sekä turvallisuus- että ympäristönsuojeluohjelmaa tehokkaasti ja tarkoituksenmukaisesti. Säännöstöllä halutaan varmistaa, että aluksia liikennöivät yhtiöt perustavat ja ylläpitävät turvallisuusjohtamisjärjestelmiä maissa ja aluksilla, ja että lippuvaltioiden hallinnot valvovat tätä. (Suomen Varustamot ry.)

IMO:n alainen merenkulun turvallisuuskomitea on hyväksynyt päätöslauselman MSC.428(98), jonka mukaan hallintojen, varustamoyhtiöiden ja luokituslaitosten on huomioitava kyberriskien hallinta yhtenä osana ISM-säännöstön vaatimaa turvallisuusjohtamisjärjestelmää. Kyberriskien hallintajärjestelmä on mahdollista integroida osaksi

turvallisuusjohtamisjärjestelmää, ja kyberturvallisuus on huomioitava kaikissa aluksissa riippumatta aluksen käyttöönottovuodesta tai toiminta-alueesta. (Traficom 2020.)

Tuomalan (2021) artikkelissa mainitaan, että IMO ohjeisti jäsenmaitaan kyberriskien aiheuttamista uhkista ja haavoittuvuuksista kiertokirjeellä jo vuonna 2017. Tällä vahvistettiin kyberriskien hallinnan tarve ja kannustettiin jäsenvaltioita huomioimaan kaikki sidosryhmät osana kyberturvallisuuteen liittyviä varotoimia. Vuoden 2021 alussa tulivat voimaan kyberriskien kansainväliset hallinnoinnin ohjeet. Nämä velvoittavat varustamoyhtiöitä ottamaan merenkulun kyberturvallisuuden mukaan osaksi turvallisuusjohtamisjärjestelmiä.

3 Merenkulun kyberturvallisuus

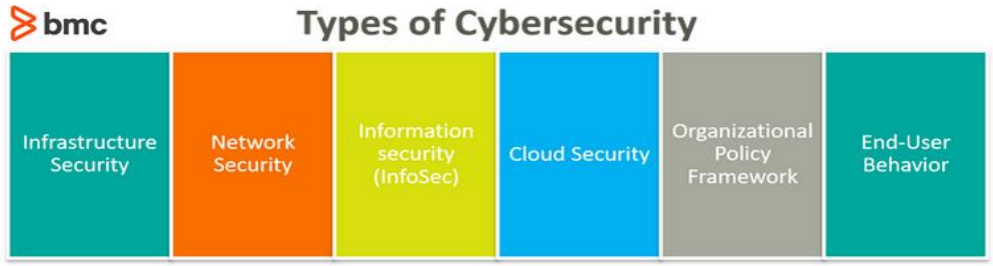
3.1 Kyberturvallisuus yleisesti

Kyberturvallisuuskeskuksen (2020) määritelmän mukaan kyberturvallisuudella tarkoitetaan yhteiskunnan ja organisaatioiden digitalisoitumisen myötä tulleita uudenlaisia turvallisuushaasteita. Käytännössä tämä tarkoittaa laitteiden, tietojärjestelmien, ohjelmistojen ja tietoliikenneyhteyksien suojaamista erilaisilta kyberuhkilta. Kyberuhkat ovat näihin kohdistuvia haitallisia tapahtumia ja kehityskulkuja.

Nykypäivän tietoyhteiskunnassa lähes kaikki yhteiskunnan toiminnot ovat riippuvaisia sähköisistä verkoista ja tiedonsiirrosta verkon kautta. Esimerkiksi viestintä, rahaliikenne, energiahuolto, vesihuolto, rautatiet, maanpuolustus ja myös laivaliikenne ovat kytköksissä verkkoon ja sen myötä alttiita erilaisille kyberhyökkäyksille ja häirinnälle. Kyberhyökkäykset eri aloja kohtaan ovat lisääntyneet erityisesti koronapandemian aikana. (Horelli 2020.)

Kyberhyökkäyksiä kohdistetaan organisaatioihin ja yrityksiin jatkuvasti. Kyberhyökkäyksen tekijä pyrkii hyötymään kohteensa haavoittuvuudesta rahallisesti, esimerkiksi asettamalla kiristysohjelmia ja vaatimalla lunnaita. Kyberhyökkäysten tekijät voivat olla esimerkiksi yksityishenkilöitä, hakkeriryhmiä, rikollisjärjestöjä tai valtiollisia toimijoita. (Neptunet 2020.)

Kuvassa 3 on esitetty kyberturvallisuuden eri muotoja, jotka on jaettu kuuteen osa-alueeseen. Infrastruktuurin turvallisuus tarkoittaa käytäntöjä, joilla suojataan tietokoneiden järjestelmiä, verkkoja ja järjestelmiä, jotka käsittelevät esimerkiksi valtion turvallisuutta, kansantaloutta tai yleistä turvallisuutta maan kansalaisten keskuudessa. Verkkojen turvallisuus pitää sisällään tietokoneiden verkkojen suojaamisen erilaisilta hyökkäyksiltä. Se käsittää sekä langattomat että langalliset yhteydet. Tietoturvalla tarkoitetaan datansuojaamismenetelmiä, kuten esimerkiksi Euroopan unionin GDPR-tietosuoja-asetusta. Tämä turvaa käyttäjän henkilökohtaisen datan, jota ovat muun muassa henkilötiedot, pankkitiedot ja muut vastaavat yksityiset ja arkaluontoiset asiat. Pilvipalveluiden turvallisuudella tarkoitetaan käyttäjien tietojen salaamista pilvessä toimivilla alustoilla. Valtiollisen tason kyberturvallisuuden viitekehys määrittää ohjeistukset ja säännöt yleisellä tasolla. Loppukäyttäjien ohjeistamisella pyritään lisäämään kyberturvallisuuteen liittyvää tietoisuutta eri organisaatioiden välillä. Tällä voidaan tarkoittaa esimerkiksi käyttäjien koulutusta erilaisia tietoturvauhkia vastaan. Jokaista käyttäjää pyritään laajamittaisesti opastamaan tietoturvallisuuden kanssa toimimiseen, jotta pystyttäisiin välttymään kyberhyökkäyksiltä ja erilaisilta tietoturvauhkilta.



Kuva 3. Kyberturvallisuuden muotoja (Raza, 2020.)

3.1.1 Tietojenkalastelu

Tietojenkalastelu on yksi tyypillisimmistä kyberhyökkäysten muodoista. Sen tavoitteena on saada tunkeutujien haltuun esimerkiksi kohteen käyttäjätunnus- ja salasanapareja tai maksukorttitietoja. Tämä voi tapahtua esimerkiksi rikollisten luomalla internetsivustolla, joka on naamioitu muistuttamaan ulkoasultaan palvelun aitoa sisäänkirjautumissivustoa. Näin ollen käyttäjä, joka kirjoittaa tunnuksensa tällaiselle sivustolle, voi tietämättään lähettää tunnuksensa rikollisten nähtäville. Yrityksiin kohdistuvilla tietojenkalasteluilla voidaan vakoilla esimerkiksi yrityssalaisuuksia tai luoda valelaskuja, joilla rikolliset keräävät itselleen tuottoja. (Kyberturvallisuuskeskus 2020.)

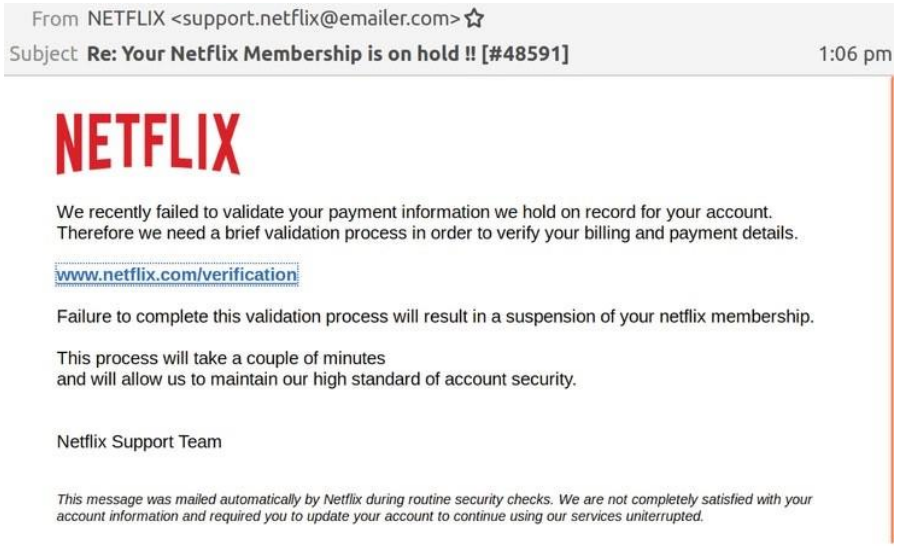
Yksittäisiin henkilöihin kohdistuvat tietojenkalasteluyritykset tapahtuvat yleisimmin joko tekaistulla internetsivustolla tai sähköpostitse linkin kautta. Painamalla linkkiä tietokone voi aloittaa lataamaan haittaohjelmia, jäädyttämään hallintajärjestelmiä tai tiedostoja tai paljastaa henkilön yksityisiä tietoja. Pahimmillaan yksityisten kohteiden varoja käytetään luvatta tai ne varastetaan kokonaan. Uhrin henkilöllisyyden varastaminen on mahdollista hyökkäyksen yhteydessä, ja sitä voidaan käyttää useisiin eri toimiin, joista voi aiheutua uhrille merkittäviä taloudellisia tappioita. (Imperva.)

Tietojenkalasteluyrityksiä kohdistetaan pääasiassa suuryrityksiin ja hallituksiin, joiden taloudelliset tappiot ja menetykset ovat suuruusluokaltaan merkittävimpiä. Advanced Persistent Threat (APT) on eräs hyökkäysmuoto, jossa järjestäytyneet hyökkääjät pyrkivät saamaan jalansijaa kohteena olevaan järjestöön tai yritykseen. Hyökkäys voi olla erityisen haitallinen sen huomaamattomuuden vuoksi. Ajallisesti pitkään kestävän hyökkäyksen aikana pyritään keräämään mahdollisimman laajasti arkaluontoista dataa liittyen organisaation tietojärjestelmiin, jota kautta päästään liikkumaan järjestelmän sisällä huomaamattomasti. Kun hyökkääjät ovat päässeet järjestelmään sisälle, he oppivat tuntemaan järjestelmän ja

sen haavoittuvuudet ja voivat kerätä informaatiota niin paljon kuin haluavat. Hyökkääjät voivat pysyä järjestelmässä yhtäjaksoisesti tai palata siihen myöhemmin, jos kohdeyrityksessä ei olla pystytty havaitsemaan ja sitä kautta torjumaan hyökkäystä. Viruksentorjuntaohjelmat tai palomuuri eivät aina pysty havaitsemaan tämänkaltaisia tunkeutumisia. (Kaspersky.)

Huomaamattomuudella pyritään yleensä pitkään ja laajan hyökkäykseen, jonka aikana pystytään tekemään suurta vahinkoa. Hitaammin toteutettu ja pitkään kestävä hyökkäys voi aiheuttaa suurempia haittoja kohteelle kuin nopea ja lyhytkestoinen hyökkäys. APT-hyökkäyksiä kohdennetaan yhä useammin myös pienempiin yrityksiin, joita voidaan käyttää välietappeina kohti suurempia organisaatioita. Pienemmät organisaatiot ovat usein huonommin suojattuja.

Kuvassa 4 on esimerkki yksityishenkilölle suunnatusta tietojenkalasteluyrityksestä, joka on naamioitu aidon palveluntarjoajan viestin näköiseksi. Viestin mukaan käyttäjätilin maksutietojen vahvistaminen on epäonnistunut, ja käyttäjän olisi vahvistettava tiedot, jotta jäsenyys säilyisi. Linkkien klikkaaminen ja maksutietojen syöttäminen voi kuitenkin johtaa tietojen joutumiseen rikollisten käsiin.


From NETFLIX <support.netflix@emailer.com>
Subject **Re: Your Netflix Membership is on hold !! [#48591]** 1:06 pm

NETFLIX

We recently failed to validate your payment information we hold on record for your account.
Therefore we need a brief validation process in order to verify your billing and payment details.

www.netflix.com/verification

Failure to complete this validation process will result in a suspension of your netflix membership.

This process will take a couple of minutes
and will allow us to maintain our high standard of account security.

Netflix Support Team

This message was mailed automatically by Netflix during routine security checks. We are not completely satisfied with your account information and required you to update your account to continue using our services uniterrupted.

Kuva 4. Tietojenkalastelu (Kotimikro 2020)

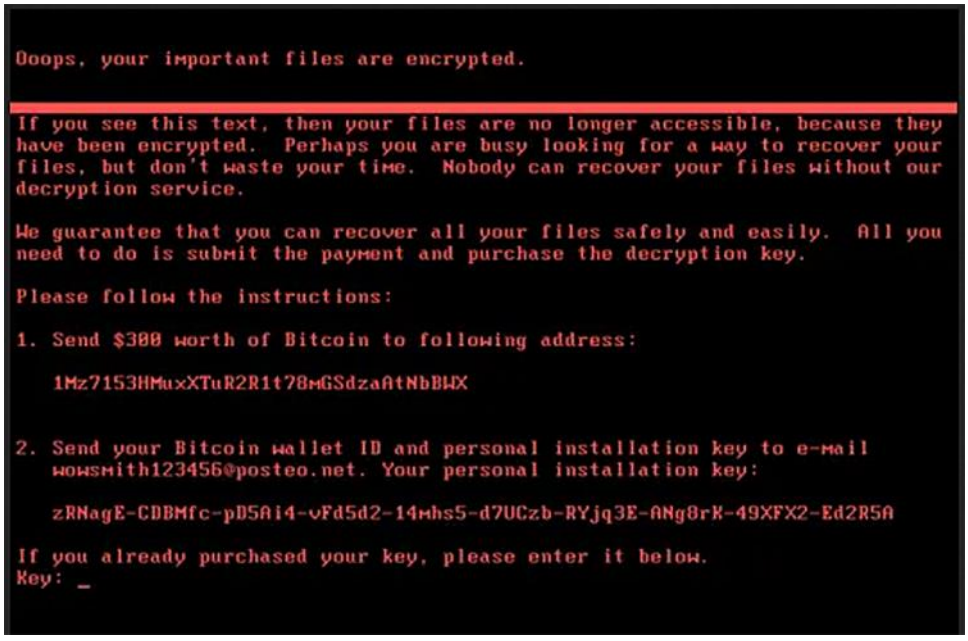
3.1.2 Haittaohjelmat

Haittaohjelmalla tarkoitetaan tietokoneohjelmaa, joka leviää esimerkiksi sähköpostien liitetiedostojen, verkkosivustojen tai haavoittuvien palvelinten kautta. Ohjelmat voivat olla harmittomia, mutta ne voivat myös sisältää esimerkiksi kiristysyrityksiä. Kyberturvallisuuskeskus mainitsee maailmalla yleistyneen tuoreen ilmiön, joka kulkee nimellä Big Game

Hunting, vapaasti suomennettuna suurriistan metsästys. Tällä viitataan rikollisten valitsemiin houkutteleviin tai rahakkaisiin organisaatioihin, joihin tunkeutumiset kohdistetaan. Hyökkääjä tunkeutuu kohteen tietojärjestelmiin ja verkkoihin, ja käynnistää kiristyshaittaohjelman. Ohjelma voi lamauttaa kohteen toiminnan lähes kokonaan. Tämän jälkeen kohteelta vaaditaan lunnaita salauksen purkamiseksi. (Kyberturvallisuuskeskus 2020.)

Haittaohjelman kohteeksi voi joutua esimerkiksi sähköpostin liitetiedoston, haittamainonnan, väärennettyjen asennusten, USB-muistitikkujen, sovellusten, sekä tietojenkalastteluviestien kautta. Yleisimpiä haittaohjelmatyyppejä ovat muun muassa virus, kiristysohjelma, vakoiluohjelma ja mainosohjelma. (McAfee.)

Yksi tunnetuimmista haittaohjelmatyypeistä on Ransomware, jota käsitellään Kyberturvallisuuskeskuksen (2020) ohjeistuksessa. Ohjelma luo kohteelle lunnasvaatimuksia. Lunnasvaatimusviruksella tarkoitetaan haittaohjelmaa, joka sulkee yritykselle tärkeitä palvelimia ja tiedostoja ja siltä osin lamauttaa sen toimintaa. Lunnasvaatimuksen maksettuaan ohjelma myöntää maksajalle sähköisen koodin, jolla pystyy avaaman tiedoston tai palvelimet. Takeita sille, että tiedoston saisi auki, ei kuitenkaan ole. Virusten lähettäjät ovat rikollisia, eikä kiristysyrityksiin tulisi suostua. Kuvassa 5 lunnasvaatimusohjelma on tunkeutunut erään laivayhtiön tiedostoihin ja sulkenut ne. Ohjelma pyytää siirtämään lunnaat bitcoineina hakkereiden salatuille kryptovaluuttatileille, jotta yritykselle tärkeät tiedostot voidaan avata käytettäviksi.



Kuva 5. Laivayhtiössä havaittu lunnasvaatimusohjelma (Tuomala 2021)

F-Secure ohjeistaa, ettei lunnaita tulisi maksaa. Yhtiön tai yksityisen henkilön maksaessa lunnaat ei takeita tiedostojen avaamiselle ole, koska kyseessä on huijausyritys. Mahdolliset salauksenpurkuun vaadittavat työkalut ovat avaintekijänä vaatimusten sivuuttamiseen. Usein kehittyneimmillä yrityksillä on olemassa työkalut kyseiseen ongelmaan, ja kiristyksistä selvitään ilman kalliiden lunnaiden maksua.

Tilastoja tutkittaessa voidaan todeta, että haittaohjelmien määrä kasvaa jatkossakin, ja ne kehittyvät alati tehokkaammiksi ja vaikeammiksi hallita. Maailmalla puhutaankin kyberisaation kilpajuoksusta, jossa valtiot ja yritykset kilpailevat järjestäytynyttä rikollisuutta vastaan uusilla tavoilla suojautua viruksilta ja erilaisilta haittaohjelmilta. Jatkuva teknologian kehittyminen avaa ovia niin valtiollisille toimijoille kuin yksityisillekin rikollisille luoda uusia ja kehittyneitä tapoja kyberhyökkäyksille.

Vuonna 2020 tehdyn tutkimuksen mukaan kyberhyökkäysten tulevaisuus haittaohjelmien osalta näyttää uhkaavalta, ja niiden odotetaan kasvavan ja kehittyvän jatkuvasti huonompaan suuntaan. Heinäkuussa noin 60 % maailman yrityksistä kertoi joutuneensa erilaisten tietomurtojen tai haittaohjelmien kohteeksi. Nykypäivänä ympäri maailmaa tapahtuu noin 30 000 erilaista tietomurtoa, virushyökkäystä ja tietojenkalastusyritystä vuorokaudessa eri alojen toimijoihin. Koronapandemian aikana hyökkäysten määrä on kasvanut. (Horelli 2020.)

3.1.3 Palvelunestohyökkäykset

Palvelunestohyökkäys (DDoS, Distributed Denial of Service) toimii eri tavalla kuin muut kyberhyökkäysten muodot. Palvelunestohyökkäysten tavoitteena ei ole ohittaa tietoturvajärjestelmiä, vaan tehdä verkkosivusta tai servereistä käyttökelvottomia tietyille käyttäjille tai käyttäjäryhmille. Hyökkäykset tulevat usein lyhyinä ryppäinä tai toistuvina hyökkäyksinä. Hyökkäys voi vaikuttaa sivustolla useita päiviä, viikkoja tai jopa kuukausia. Tänä aikana organisaatio yrittää toipua hyökkäyksestä. Palvelunestohyökkäys voi olla tuhoisa mille tahansa verkossa toimivalle organisaatiolle. Hyökkäysten on tarkoitus vaikuttaa yhtiön tuloihin ja luottamukseen asiakkaiden keskuudessa. Ne voivat osaltaan aiheuttaa myös pitkäaikaisen mainehaitan, jos verkkosivustot eivät toimi kunnolla ja jos yhtiön toiminnan luotettavuus on epäselvä. (Imperva.)

Palvelunestohyökkäyksen tarkoituksena on kuormittaa kohteena olevaa verkkoa ylimääräisellä tietoliikenteellä. Kohteena voi olla yrityksen tai organisaation julkinen, asiakkaille tarkoitettu palvelusivusto. Hyökkäyksen seurauksena palvelu voi hidastua huomattavasti ja

aiheuttaa näin asiakkaille merkittävää haittaa. Toiminnan ennalleen palauttaminen voi viedä aikaa. (Kyberturvallisuuskeskus 2020.)

Hyökkääjillä voi olla erilaisia syitä toteuttaa palvelunestohyökkäyksiä. Motiivit vaihtelevat, riippuen hyökkäyksen halutusta vaikutuksesta. Mikkelssonin (2015) mukaan haktivismilla tarkoitetaan tietoverkossa tapahtuvaa aktivismia esimerkiksi hallintoa, suuryrityksiä tai jotakin tapahtumaa vastaan. Nämä verkossa toimivat aktivistit pyrkivät osoittamaan mieltään, jos he kokevat tyytymättömyyttä valtiollisia toimijoita tai talousmaailman vaikuttajia kohtaan. Haktivistit kokevat ajavansa ihmisoikeuksia, sananvapautta ja tiedonsaantivapautta. Toiminnalla pyritään sekoittamaan ja vaikeuttamaan hyökkäyksen kohteen toimintaa ja jakamaan kohteiden arkaluontoisia tietoja.

Palvelunestohyökkäykset voivat olla joko hajautettuja tai kohdennettuja. Hajautetut hyökkäykset voivat perustua bottien käyttöön, jotka lähettävät kohteena olevalle sivustolle suuren tietoliikennetulvan. Kohdennetussa hyökkäyksessä käytetään hyväksi kohteena olevan palvelun haavoittuvuuksia, jolloin toimintaa pystytään tietoliikennetulvan avulla hidastamaan huomattavasti tai lamauttamaan kokonaan. (Poliisi.)

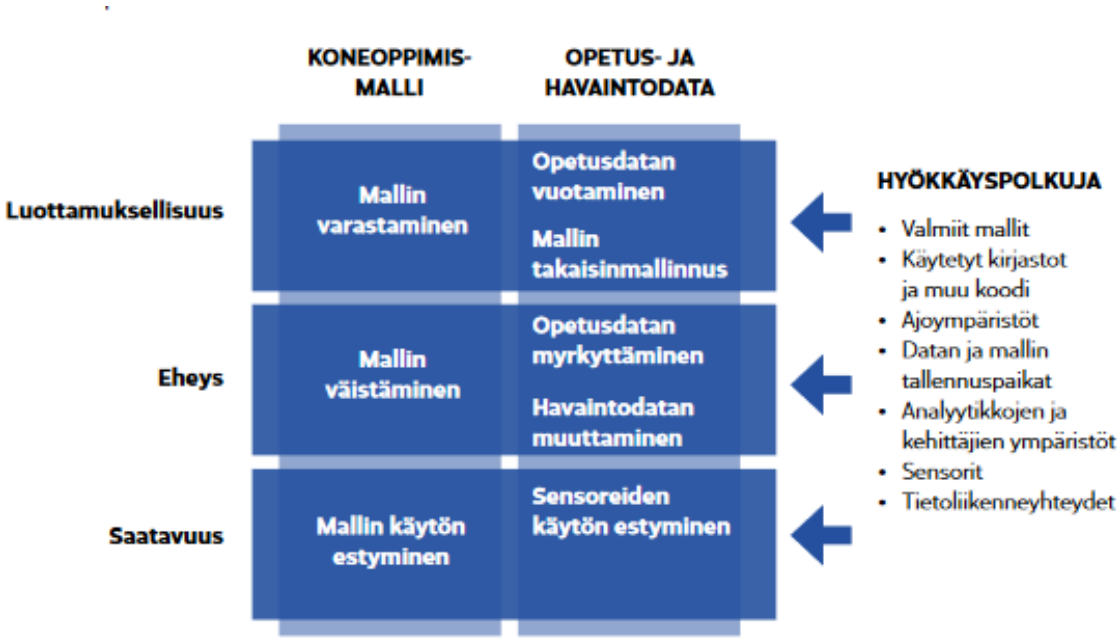
3.2 Robotiikan ja tekoälyn kyberturvallisuus

Tekoäly-termiä käytetään Traficomin (2021) mukaan yleisesti sellaisesta koneen toiminnasta, joka näyttää ihmisen älykkäältä käytökseltä. Vielä tällä hetkellä tekoälyn käyttö rajoittuu kapeisiin sovelluksiin, kuten vaikkapa jonkin ilmiön havaitsemiseen tietomassasta. Vaikka tekoäly suoriutuu ihmistä paremmin joistakin rajatuista tehtävistä, se ei kuitenkaan ole todellista älykkyyttä. Merkittävimpiä eroja tekoälyn ja inhimillisen älykkyyden välillä on kyky siirtää ongelmanratkaisukykyä uuteen viitekehykseen. Yksi tekoälyn toteutusmenetelmien luokka on koneoppiminen. Vielä tällä hetkellä monet tekoälyä hyödyntävät sovelluksen perustuvat neuroverkkopohjaisiin koneoppimismalleihin, mutta kaikkia koneoppimismalleja ei taas luokitella neuroverkoiksi. Monet tekoälyjärjestelmien riskeistä liittyvät siihen, että niiden päätöksenteon perusteiden selittäminen voi olla vaikeaa, ja koneoppimismalleille on helppo luoda vihamielisiä syötteitä.

Merenkulkualalla kansainvälisellä merenkulkujärjestöllä IMO:lla on useita tekoälyyn liittyviä hankkeita, joista merkittävin on autonomisten pinta-alusten kehittäminen. Tekoälyn osalta kiinnitetään erityistä huomiota ihmisen ja koneen yhteistoimintaan ja virhetoimintojen hallintaan. IMO:n ohjeistus merenkäynnin kyberturvallisuudesta ei ota suoraan kantaa tekoälyyn, mutta määrittelee riskienhallintajärjestelmän ja viittaa osaltaan myös automaatioon.

Euroopan meriturvallisuusvirasto on aiemmin julkaissut raportin autonomisten alusten riskeistä ja säätelystä. (Traficom 2021.)

Suuri osa tietoturvallisuusriskeistä ja niiden hallintamuodoista on tekoälyjärjestelmissä samoja kuin perinteisissäkin järjestelmissä. Koneoppimisjärjestelmissä datan tulkinta, koneoppimismallien tiedot, ennalta opetettujen mallien käyttäminen ja opetusprosessit ovat perinteisistä järjestelmistä poikkeavia osa-alueita, ja tarvitsevat erityistä huomiota. Näiden osa-alueiden turvallisuusriskejä voidaan kuitenkin jäsentää perinteiseen luottamuksellisuuteen ja eheyteen perustuvan tietoturvan kautta, kuvion 6 mukaisesti. Keskeisimpiä riskejä teknisestä näkökulmasta ovat muun muassa koneoppimismallin sabotointi väärällä datalla, mallin anastaminen, mallin kiertäminen väärillä syötteillä sekä sensorin ja päätöksenteon välisen kommunikoinnin epäonnistuminen. (Traficom 2021.)



Kuvio 6. Koneoppimisjärjestelmän riskejä (Traficom 2021)

Etenkin teollisuudessa lisääntynyt robotiikan ja tekoälyn käyttö lisäävät huomattavasti niiden haavoittuvuutta kyberturvallisuuden osalta. Tällä hetkellä maailmanlaajuisesta näkökulmasta katsoen teollisuudessa käytetään yhä enemmän robotteja, ja niiden käytön on arveltu kasvavan tulevaisuudessa 20 % vuosivauhtia. Elokuussa 2020 tehty tutkimus Rogue Automation – Vulnerable and Malicious Code in Industrial Programming kahden alan tutkijan toimesta (Federico Maggi ja Marcello Pogliani) kertoo, että robottien käyttöjärjestelmissä piilee vielä heikkouksia, jotka avaavat ovia edistyneille tietokonerikollisille (Horelli 2020). Käytännössä hakkerit pystyvät vakoilemaan eri yhtiöiden tuotannollisia salaisuuksia tai jopa aiheuttamaan tuotantoon vakavaa tuhoa esimerkiksi koodaamalla robotin

käskyt erilaisiksi, jolloin robotti aloittaa erilaisia työstövaiheita vääriin aikoihin. Hakkerit pystyvät pahimmillaan aiheuttamaan pitkiä seisahduksia suurten yhtiöiden tuotantoon. Tämä voi kestää useita päiviä. Tällaisella hyökkäyksellä pystytään mahdollistamaan suuret taloudelliset menetykset yhtiölle, johon kyberhyökkäys on haluttu kohdistaa. (Niemelä 2020.)

Automatisoidun tuotannon sisällä oleviin järjestelmiin on vaikea tehdä muutoksia. Kun tuotannon käytäntöihin tehdään muutoksia, niitä tulee tehdä varovasti ja pala kerrallaan erilaisilla varajärjestelmillä tai niiden kopioita testaten. Tuotannon sisäisen verkkoliikenteen tulee olla tarkkaan suunniteltu, ja sen sisällä pitää sallia vain välttämätön ja tarvittava dataliikenne. Tuotantoa rakentaessa tulisi alustavasti käyttää niin sanottuja pehmitettyjä rajoitusmuotoja, jossa epäilyttävän ja tuntemattoman verkkoliikenteen vaikutus tuotantoon pyritään ottamaan huomioon tutkimalla ja ilmoittamalla tarvittaessa asiasta eteenpäin. (Niemelä 2020.)

3.3 Rahtilaivojen automaatio

Tietotekniikan kehittymisen myötä myös meriliikenne on kehittynyt viimeisen vuosituhannen alun jälkeen nopealla tahdilla. Jatkuvasti madaltuvien satelliittikustannusten ja uusille taajuuksille pohjautuvien tiedonsiirtojärjestelmien avulla datan siirto aluksesta maihin on entistä halvempaa. Myös erilaisten laitteistojen ja koneiden toimintaa seuraavien sensorien hinta on laskenut jatkuvasti. Tämä on luonut uusia mahdollisuuksia meriliikenteen ja automaation yhdistämiselle. Miehistön on entistä helpompi toimia komentosillalla kehittyneen automaation ansiosta ja hyödyntää esimerkiksi automatisoituja navigointi- ja etäohjausjärjestelmiä. Nämä lisäävät oikein käytettyinä alusten tehokkuutta ja turvallisuutta. (Tapaninen 2019, 127)

Älykkäillä väylillä kehittyneemmät rahtialukset pystyvät saamaan navigointitiedot sähköisessä muodossa ja voivat navigoida automaattisesti. Samalla vanhemmat alukset hyödyntävät perinteisiä karttoja ja väylämerkkejä. Älyväylillä mahdollistetaan etäluotsaus, joka tarkoittaa osaltaan sitä, että luotsien ei tarvitse osallistua laivan ohjaamiseen aluksesta käsin, vaan ohjaus voidaan toteuttaa maista. Etäluotsaus vaatii tulevaisuudessa kuitenkin paljon kehittämistä ja erilaisia testausmenetelmiä. Turvallisuus on tärkeässä osassa kehitystyössä ja testauksessa erityisesti miehittämättömissä aluksissa. (Tapaninen 2019, 127)

Meriliikenne pitää sisällään suuren määrän erilaista tiedonvaihtoa, joka tehostaa toimintoja mutta vie aikaa laivan ohjaamiselta. Tapaninen (2019, 139) toteaa, että ongelmaan on

haettu ratkaisuja älykkään liikenteen keinoilla. Älykäs liikennejärjestelmä pitää sisällään palveluketjun osat tietojen keruusta, käsittelystä ja jakelusta matkan suunnitteluun ja matkan aikaisiin tietopalveluihin. Näiden järjestelmien keskeisiä vaatimuksia ovat ajantasaisuus, luotettavuus ja helppokäyttöisyys. Merikuljetuksia ei kuitenkaan ole integroitu maakuljetusten logistisiin ketjuihin tarpeeksi hyvin, mikä heikentää logististen ketjujen tehokkuutta.

Laivan rungon ja järjestelmien osalta perinteisesti kertatarkastuksina tehdyt huolto ja seuranta ovat siirtyneet jatkuvaan digitaaliseen seurantaan. Laivojen reaaliaikainen seuranta antaa uudenlaisia mahdollisuuksia nopeisiin reitityksen muutoksiin. Esimerkiksi päivittyviä säätietoja sekä tietoja lastin myöhästymisestä tai muista ongelmista voidaan hyödyntää laivan reitin suunnittelussa. Nykypäivänä myös muiden kuin merenkulkualan tutkijat ja yrittäjät ovat muuttaneet merenkulkualan perinteistä tutkimus- ja kehitystoimintaa. Merenkulun innovaatiot voivat saada vaikutteita muilta teollisuuden aloilta, kuten autoteollisuudesta tai lentoliikenteestä. (Tapaninen 2019, 139)

Miehittämättömät alukset voivat toimia joko etäohjatusti tai täysin automaattisesti. Etäohjatulla aluksella tarkoitetaan sitä, että aluksella ei ole miehistöä vaan operoinnin kannalta merkittävät tiedot sen järjestelmistä siirretään tietojärjestelmien kautta ohjauskeskuksessa olevan miehistön saataville. Tällöin miehistö operoi alusta ohjauskeskuksesta käsin. Automaattinen alus operoi täysin itsenäisesti. Se valvoo aluksen operoinnin kannalta olennaisia tietoja ja operoi alusta itsenäisesti. Täysin automaattista alusta on kuitenkin vaikea rakentaa nykyisellä tietojärjestelmien tiedonsiirto- ja laskentakapasiteetilla. Tästä johtuen tarvitaan autonomisia aluksia, jotka ovat etäohjatun ja automaattisen aluksen välimuotoja. Autonominen alus suorittaa osan tehtävistä itsenäisesti, mutta osa operaatioista olisi edelleen suoritettava miehistön toimesta. (Leppänen ym. 2020.)

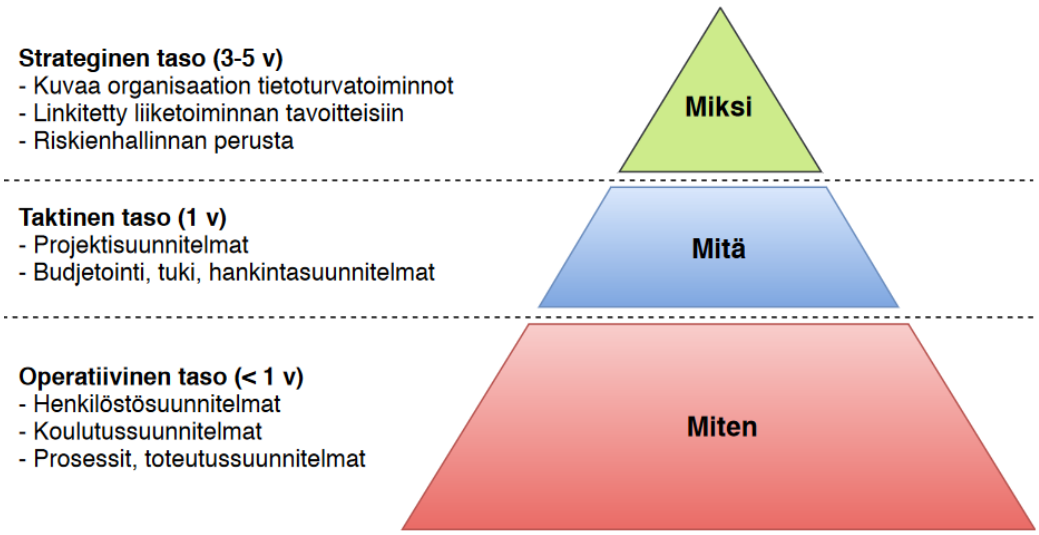
3.3.1 Rahtilaivojen kyberturvallisuus

Merenkulun jatkuvat digitalisaation myötä etenkin uudemmat rahtilaivat hyödyntävät automatiikkaa ja erilaisia digitaalisesti integroituja järjestelmiä. Nämä järjestelmät ovat internetin kautta yhteydessä muun muassa organisaatioihin ja operaattoreihin maalla. Järjestelmien toimintavarmuus perustuu informaatioteknologiaan (IT) sekä operatiiviseen teknologiaan (OT). Jotta toimintavarmuus pystytään säilyttämään, on varustamoiden kehitettävä riskienhallintaa, joka ottaa huomioon näiden järjestelmien kyberturvallisuuden. Kyberturvallisuuden huomioiminen perustuu osaltaan myös Merenkulun turvallisuuskomitean hyväksymään päätöslauselmaan, jonka mukaan myös varustamojen on huomioitava toiminnassaan

kyberriskien hallinta osana ISM-säännöstön tavoitteita ja valmiuksia. Riskienhallinta on riippumatonta aluksen järjestelmien käyttöönottovuodesta. (Traficom 2020.)

Digitalisaatio on mahdollistanut aluksissa IT- ja OT-järjestelmien integroinnin. OT-järjestelmiä käytetään muun muassa moottoreiden järjestelmien hallinnointiin, navigointiin sekä lastinkäsittelyyn (Tuulaniemi 2020). Aiemmin tyypillisesti eristetyt OT-järjestelmät ovat yhä useammin integroituina tietoverkkoon liitettyjen IT-järjestelmien kanssa, mikä kasvattaa mahdollisen kyberhyökkäyksen kokonaisvaltaisia vaikutuksia. Pahimmassa tapauksessa laivan navigointijärjestelmä voidaan kaapata.

OT-järjestelmiin tunkeutuminen voi olla erityisen haitallista niiden kriittisten toimintojen vuoksi. Ne voivat olla aikakriittisiä ja niiltä vaaditaan reaaliaikaista suorituskyvyn varmuutta, mistä johtuen esimerkiksi päivityksistä ja korjauksista johtuvia huolto- ja käyttökatkoja vältetään. (Tuulaniemi 2020.)

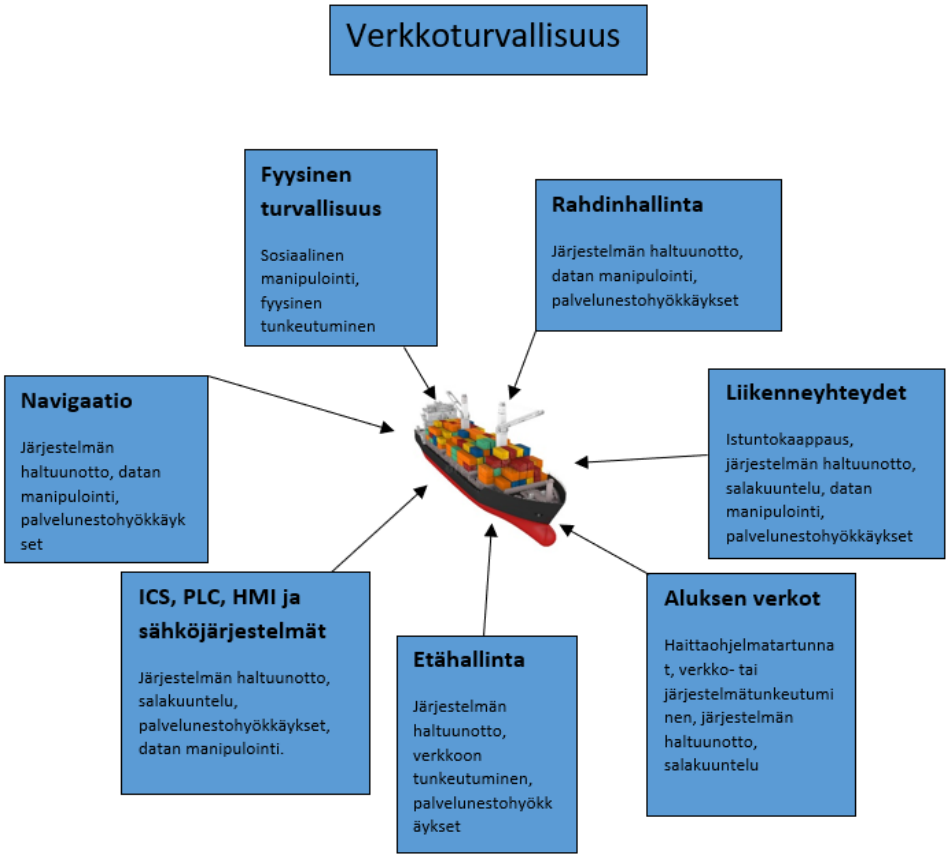


Kuvio 7. Tietoturvallisuuden hallinnan 3 tasoa (Leppänen ym. 2020)

Rahtilaivoihin kohdistuvat kyberhyökkäykset voivat kohdistua itse alukseen tai esimerkiksi miehistöön, matkustajiin, lastiin, varustamoon tai omistajiin. Kuviossa 7 tarkastellaan tietoturvan toteutukseen ja hallintaan liittyviä tasoja. Operatiivinen taso määrittää itse toteutuksen, joihin kuuluvat muun muassa laivan henkilöstösuunnitelmat, koulutussuunnitelmat ja toteutussuunnitelmat. Taktisella tasolla määritetään aluksen projektisuunnitelmat, budjetti sekä hankintasuunnitelmat. Pidemmällä aikavälillä kuvataan organisaation strategiset toiminnot. Tavoitteet on linkitetty liiketoiminnan tavoitteisiin ja kuvaavat koko organisaation tietoturvatoimintoja. Strategisen tason päätökset luovat perustan riskienhallinnalle

kokonaisuudessaan. Jotta uhkia voidaan torjua, on uhkat pyrittävä kartoittamaan ja ennakoimaan sekä estämään uhkien ja haavoittuvuuksien hyväksikäyttö. Mikäli suojaustoimet pettävät, hyökkäysten vaikutukset pyritään minimoimaan. (Leppänen ym. 2020.)

Kuviossa 8 käydään läpi erilaisia laivojen verkkoturvallisuuden osa-alueita ja niihin kohdistuvia kyberturvallisuusriskejä. Fyysisen turvallisuuden osalta laivan miehistöön saattaa kohdistua käyttäjien manipulointia, jolla tarkoitetaan rikollisten tapoja hankkia itselleen esimerkiksi käyttäjien salasanoja tai pankkitunnuksia (Webroot). Mahdollista on myös niin sanottu tailgating, jolla tarkoitetaan rikollisen tunkeutumista laivan rajoitetulle alueelle kulkuoikeudet omaavan käyttäjän perässä (Carnegie Mellon University 2020).



Kuvio 8. Rahtilaivojen verkkoturvallisuus (Huoltovarmuusorganisaatio 2021)

Rahdinhallinnan osalta mahdollisia skenaarioita ovat järjestelmän haltuunotto, datan manipulointi ja erilaiset palvelunestohyökkäykset. Hallintajärjestelmään voidaan kohdistaa verkkohyökkäys, jossa hyökkääjä pyrkii kaatamaan järjestelmän kohdistamalla sinne ylimääräistä dataliikennettä. Tämän seurauksena järjestelmän toiminta voi hidastua merkittävästi tai jopa lakata kokonaan. Näitä palvelunestohyökkäyksiä voidaan kohdistaa myös laivan etähallinta- navigaatio- tai sähköjärjestelmiin. Navigaatiojärjestelmään tehty hyökkäys voi

olla erityisen haitallinen. Pahimmassa tapauksessa navigaatiojärjestelmä voidaan kaapata, ja laiva voidaan ohjata pois reitiltä, mikä voi pahimmillaan aiheuttaa esimerkiksi karilleajon tai öljyvuodon. Verkon kautta toimiviin järjestelmiin voidaan kohdistaa myös istuntokaappauksia tai salakuuntelua, joilla rikollisten on mahdollista saada haltuunsa laivan turvallisuuden kannalta olennaisia tietoja. Rahtilaivojen ohjausjärjestelmiin tunkeutumisella yritetään tavoitella kuljetettavan rahdin myöhästymistä ajattamalla alus väärälle kurssille tai tukkimalla tärkeitä laivareittejä. Tarkoituksena on aiheuttaa halutulle yhtiölle taloudellisia menetyksiä tai haittaa sen imagolle. Näin ollen hyökkääjät pystyvät tavalla tai toisella hyötymään useimmiten rahallisesti yhtiön menetyksistä.

Huoltovarmuusorganisaation (2021) kyberturvallisuuden ohjeistuksessa mainitaan, että alusten kriittisten toimintojen huomioiminen osana kyberturvallisuutta on yksi keskeisimmistä ennaltaehkäisevistä toimenpiteistä. Varustamoyhtiön on tunnistettava toimintoihin liittyvät riskit, jotta uhkaavissa tilanteissa osattaisiin toimia oikealla tavalla. Riskien tunnistamisen jälkeen niitä on arvioitava ja dokumentoitava. Suomen Huoltovarmuuskeskuksen julkaisemassa ohjeistuksessa käydään läpi keskeisimpiä ennaltaehkäiseviä toimenpiteitä kyberturvallisuuden ylläpitämiseksi. Ohjeistuksessa suositellaan luomaan aluksille riskienhallintasuunnitelmat, jotka pohjautuvat vakiintuneisiin ISM- ja ISPS-säännöstöjen mukaisiin menetelmiin.

Verkkojen segmentointi on käytännön tasolla yksi merkittävimmistä suojaavista toimenpiteistä, jolla pyritään hidastamaan ja rajoittamaan mahdollisten kyberhyökkääjien etenemistä alusten verkoissa. Huoltovarmuusorganisaatio suosittelee varustamoja luomaan omat verkot kriittisten järjestelmien eri ryhmille, kuten esimerkiksi viestinnälle, koneistolle, hallinnolle ja miehistölle. Tähän kuuluvat myös palomuurien päivitykset. Haittaohjelmien välttämiseksi suositellaan asentamaan torjuntaohjelmistot kaikkiin kriittisiin järjestelmiin, ja tarkastamaan esimerkiksi USB-muistitikut ennen niiden kytkemistä laitteisiin. (Huoltovarmuusorganisaatio 2021.)

Tunnistus on menetelmä, jolla käyttäjä tunnistetaan ja eritellään muista käyttäjistä. Käyttäjätunnus on yksi esimerkki yksilöivästä tunnistautumisesta. Tunnistettava kohde voi olla käyttäjä, laite tai organisaatio. Tunnistautuva käyttäjä esittää identiteetistään väitteen, joka varmistetaan todentamalla. Todennus varmistaa tunnistuksen eli käyttäjän esittämän väitteen identiteetistään. Perinteisin esimerkki todennuksesta on salasanan kirjoittaminen kirjauduttaessa johonkin järjestelmään. Todennus voi olla myös jotain konkreettista, mikä käyttäjällä on hallussaan. Esimerkkejä tästä ovat erilaiset sähköiset avainkortit tai käyttäjän yksilöiminen fyysisellä ominaisuudella, kuten sormenjäljellä tai kasvojentunnistuksella.

Kiistämättömyydellä tarkoitetaan sitä, että käyttäjä ei voi onnistuneesti kiistää suorittamaansa toimintoa. Esimerkiksi etäohjattavalle alukselle annettavia komentoja on seurattava väärinkäytösten ehkäisemiseksi. Käyttäjien toimintoja voidaan tallentaa erillisille palvelimille, jolloin voidaan tarkistaa käyttäjien tekemät toimenpiteet tiettyinä ajankohtina. (Leppänen ym. 2020.)

3.3.2 Kyberhyökkäyksiä rahtilaivoihin

Tuomalan (2021) artikkelissa todetaan, että kyberhyökkäyksiä toteutettiin ympäri maailmaa vuonna 2020 paljon ja niitä kohdistettiin moniin eri toimialoihin kuten julkishallintoihin, puolustus-, sosiaaliturva-, terveys-, rahoitus- ja vakuutussektoreihin sekä myös merillä rahtialuksiin. Maaliskuussa vuonna 2020 toteutettiin laaja tietomurto Norwegian Cruise Linen matkatoimistokumppanin tietokannan portaaliin. Tietokannan asiakirjat levisivät kattavasti Dark Webiin, josta ne löydettiin myöhemmin anonyymisti. Hyökkäys pohjautui tietojenkalasteluun, jossa hyökkääjä pyrki kalastelemaan yrityksen asiakkaiden henkilökohtaisia tietoja.

Maailman suurimpiin konttivarustamoihin kuuluva Mediterranean Shipping Co (MSC) joutui kyberhyökkäyksen kohteeksi huhtikuussa 2020. Hyökkäys aiheutti laajamittaisen häiriön yhtiön palvelinkeskukseen. Hyökkäyksen vuoksi pääkonttori Genevessä jouduttiin sulkemaan viiden päivän ajaksi, aiheuttaen suuria taloudellisia menetyksiä. Norjalaiseen risteilyalan yritykseen Hurtigruteniin keskitettiin joulukuussa 2020 mittava ransomware-hyökkäys, jolla vaadittiin kohteelta lunnaita. Se sulki ja lamaannutti käytännössä suuria määriä yritykselle tärkeitä ja keskeisiä järjestelmiä, jolloin yhtiön toimintaa pystyttiin horjuttamaan. (Tuomala 2021.)

Koronapandemian aikana kyberhyökkäysyritykset laivavarustamoihin ovat olleet kasvussa. Ylen (2021) julkaisemassa uutisartikkelissa mainitaan, että maailman johtavat varustamoyhtiöt sveitsiläisen MSC:n lisäksi (tanskalainen Moeller-Maersk, ranskalainen CMA-CGM ja kiinalainen COSCO) ovat kaikki joutuneet verkkohyökkäysten ja kiristysyritysten kohteeksi vajaan kahden vuoden sisällä. Tuomaalan (2021) mukaan tunnetuin näistä lienee Maerskiin kohdistunut virus vuonna 2017, joka tiettävästi oli lähtöisin Venäjältä. Tämä Not-Petya-niminen virus haittasi jopa 76 eri satamaterminaalin toimintaa, ja aiheutti arviolta 350 miljoonan euron tappiot. Virus saattoi tarttua Maerskiin vahingossa, sillä tiettävästi viruksen pääasiallinen kohde oli Ukraina, jonka pankki- ja hallintojärjestelmää Venäjä pyrki häiritsemään.

4 Empiirinen tutkimus

4.1 Haastattelu tutkimusmenetelmänä

Haastattelu on aineistonkeruumenetelmä, joka soveltuu monenlaiseen käyttötarkoitukseen. Haastatteluja voidaan jaotella sen mukaan, kuinka muodollisia ne ovat. Haastattelu voidaan tutkimustarkoituksessa ymmärtää systemaattisena tiedonkeruun muotona. Haastattelulla on jokin etukäteen määritelty tavoite, ja sen avulla pyritään keräämään haastateltavalta luotettavia ja päteviä tietoja. (Kajaanin ammattikorkeakoulu.)

Haastattelussa tutkija osallistuu haastateltavan ohella vuorovaikutteisesti aineiston tuottamiseen. Haastattelulla on useita erilaisia toteutustapoja, ja myös tutkijan rooli vaihtelee haastattelun tyypistä riippuen. Haastattelu voidaan toteuttaa strukturoidusti, puolistrukturoidusti, avoimen haastattelun menetelmällä tai syvähaastatteluna. (Jyväskylän yliopisto 2020.)

Strukturoitua haastattelua voidaan käyttää tilanteissa, joissa haastateltavia on useita ja he edustavat yhtenäistä ryhmää. Tässä haastattelumuodossa haastattelijalla on ennalta jäsennelty haastattelu, jonka kysymykset ovat kaikille haastateltaville samassa järjestyksessä. Strukturoidussa haastattelussa kerätty tieto on keskenään vertailukelpoista ja se on mahdollista kerätä nopeasti. Kajaanin ammattikorkeakoulun haastatteluohjeistuksessa mainitaan, että puolistrukturoitu haastattelu eli teemahaastattelu perustuu haastattelijan ennalta määrittämiin teemoihin. Vaikka kysymykset on laadittu etukäteen, niitä ei välttämättä esitetä ennalta määritetyssä järjestyksessä. Teemahaastattelussa haastattelijalta vaaditaan enemmän perehtymistä haastateltavaan ja sillä voidaan käsitellä myös arkoja aiheita, joista haastateltava ei ole tottunut puhumaan. Avoin haastattelu on vapaamuotoinen keskustelutilannetta muistuttava haastattelumuoto. Haastattelun kulku etenee pitkälti haastateltavan vastausten mukaan eikä noudata tiettyä kaavaa. Syvähaastattelu on avoimen haastattelun muoto, jossa paneudutaan syvemmälle keskusteltavan asian ytimeen. Tämä haastattelumuoto sopii tilanteisiin, joissa halutaan selvittää haastateltavan asenteita tai suhtautumista tiettyyn asiaan.

4.2 Haastattelu: Finnlines Oyj

Tämän työn ensimmäinen haastattelu toteutettiin puolistrukturoituna haastatteluna, sillä kysymykset oli luotu etukäteen mutta niiden esittäminen tapahtui vapaamuotoisesti ja kysymysten muoto muuttui haastattelun aikana. Haastattelu toteutettiin Microsoftin Teams-työkalulla.

Haastattelun tavoitteena oli selvittää, mitä kyberturvallisuusuhkia suomalainen laivavarustamoyhtiö Finnlines Oyj on kohdannut, miten yhtiö niihin varautunut, kuinka ongelmia on pystytty käsittelemään ja miten mahdolliset hyökkäykset ovat vaikuttaneet yhtiön harjoittamaan liiketoimintaan. Haastateltavana oli Finnlinesin IT-infrasta vastaava Kimmo Kostia (Head of Group IT, Hardware), joka vastaa 13-henkisen tiiminsä kanssa yhtiön verkoista, palvelimista, datacenterin työasemista, laivan IT:stä sekä tietoturvasta. Toinen puoli IT:stä vastaa osaltaan järjestelmäkehityksestä. Kysymykset olivat alkuperäisessä muodossaan seuraavat:

- Kuka olet ja mikä on toimenkuvasi Finnlines Oyj:lla?
- Miten yhtiössänne on varauduttu mahdollisiin tietoturvauhkiin?
- Minkälaisia kyberhyökkäyksiä Finnlines on kohdannut, ja mitä näistä on mahdollisesti seurannut?
- Onko mahdollisten hyökkäysten alkuperä pystytty selvittämään?
- Miten tietoturvaan liittyvät uhkakuvat ovat kehittyneet vuosien varrella?
- Miten varustamoyhtiöt pysyvät mukana alan kehityksessä?
- Millaisena näet kyberturvallisuuden tulevaisuuden yhtiössänne?

Haastattelun alussa oli tarkoitus kerätä perustietoa Finnlines Oyj:stä sekä haastateltavasta. Finnlinesin tarjoamat rahtipalvelut painottuvat Suomen ja sen tärkeimpien kauppakumppaneiden, kuten Saksan ja Venäjän välille. Finnlinesilla on toimipisteitä Suomen lisäksi muun muassa Belgiassa, Tanskassa, Saksassa, Venäjällä ja Iso-Britanniassa. Yhtiö tarjoaa säännöllistä rahti- ja matkustajaliikennettä Suomen ja Saksan välillä, sekä ro-ro- aluksilla tapahtuvaa liikennettä muun muassa Suomen ja Puolan, Benelux-maiden sekä Venäjän välillä. (Finnlines Oyj.)

Finnlines kuljettaa pääasiassa trailereita. Toiminnassa käytetään ro-ro aluksia, joissa lastaaminen voidaan suorittaa aluksen perästä, sivusta tai keulasta, jolloin lastaamisessa ei tarvitse käyttää nosturia. Finnlinesin reitit pohjautuvat pääasiassa lyhyille etäisyyksille Itämeren alueella ja painottuvat arvokkaaseen sekä tuoreeseen tavaraan. Näitä ovat muun muassa elintarvikkeet, lääkkeet, kulutustavarat sekä teollisuuden koneet ja pienemmät komponentit. Kostia kertoo, että Finnlinesin kohtaamat kyberhyökkäykset ovat olleet lähinnä pienimuotoista tietojenkalastelua sekä tunnusten ja sähköpostien kaappaamista. Tekijät on saatu nopeasti kiinni, eikä isompaa vahinkoa yhtiölle ole sattunut. Kostia mainitsee,

että tunkeutujilla on usein ollut taitavia teknisiä välineitä, mutta itse toteutus on jäänyt heikoksi.

Yhtiön etuna on Kostian mukaan yhtenäisyys. Finnlines omistaa itse laivansa ja sillä on oma Ship Management -yhtiö. Kostia näkee tämän etuna, sillä monissa muissa varustamoyhtiöissä nämä on usein ulkoistettu. Finnlines on standardisoinut omat verkkonsa ja palvelimensa tarkkaan. Kostian mukaan nykypäivänäkin yhtiö pitää yllä omaa IT-osastoa, eikä sitä juurikaan voi ulkoistaa alan erityispiirteiden vuoksi. Kansainvälinen merenkulkujärjestö IMO on tuonut laivapuolelle uusia vaatimuksia, joihin Finnlines pyrkii vastaamaan mahdollisimman laajasti ja riittävästi. Laivojen ohjaus- ja varoitusjärjestelmät ovat kytköksissä ulkopuolisiin tietoteknisiin ympäristöihin, jolloin kyberhyökkäyksen avulla alus voitaisiin kaapata ja ohjata väärälle reitille. Kostia ei Finnlinesin toiminta- ja navigointimallin näkökulmasta näe kyseistä skenaariota todennäköisenä. Finnlines varautui aikanaan kyseisiin tapahtumasarjoihin jo noin 20 vuotta sitten. Saaristomerellä teknisistä ongelmista johtunut karilleajo aloitti yhtiössä prosessin, jossa yhtiö kehitti menetelmiä, joilla voidaan varautua sekuntipohjalla laivalla olevien tietolähteiden vikaantumiseen.

Käytännössä laivan ohjaamisen merellä hoitavat luotsi ja perämies, jotka kuittaavat toisilleen suoritetut toimenpiteet, joita merellä tapahtuu. Kostia painottaa, että pidemmillä matkaväleillä kuten avomerellä seilaavien rahtilaivojen ongelmana voivat olla väärien tietolähteiden saaminen, jolloin alus voidaan ajattaa syystä tai toisesta päiväkausiksi väärille reiteille. Finnlinesilla tätä ongelmaa ei kuitenkaan ole. Operatiivisiin järjestelmiin nojaavien tietojen mahdollinen varastaminen ja erilaisten häiriöiden aiheuttaminen on Kostian mukaan yleisempää ja sitä tapahtuu enemmän maalla kuin itse aluksilla.

Haastattelun aikana käy ilmi, että yksi keskeisimmistä ennaltaehkäisevistä toimenpiteistä laivojen kyberturvallisuuden osalta on verkon pilkkominen, jota tehdään jatkuvasti sekä maalla että laivoilla. Verkkoja segmentoidaan ja erotellaan, ja tarpeettomat yhteydet pyritään katkomaan. Tämän ansiosta mahdollisilla tunkeutujilla on hankalampaa edetä verkkoympäristössä. Kostia nostaa myös esiin sen, että Finnlines on stabiili organisaatio, jossa henkilökunnan vaihtuvuus on hyvin pientä. Henkilöstön sisällä tunnetaan toisten työntekijöiden kommunikointitavat. Tästä johtuen yhtiön sisällä tapahtuvassa viestinnässä on helppo havaita mahdolliset poikkeamat ja tietojenkalasteluyritykset. Tähän vaikuttavat myös kielelliset tekijät. Koska kyseessä on suomalainen yhtiö, ulkomailta tulevat huijausyritykset on yleensä helppo havaita.

Kostian mukaan kyberhyökkäykset ovat lukumäärältään kasvaneet todella paljon viime vuosina. Myös hyökkäysten laatu on noussut tuntuvasti. Yhtenä haastattelukysymyksenä oli, miten varustamoyhtiöt pysyvät mukana tietoturva-alan kehityksessä ja miten ne pystyvät tulevaisuudessa torjumaan kasvavien kyberhyökkäysten määrän. Kostia uskoo, että etenkin pienemmillä rahtilaivayhtiöillä voi olla suuriakin ongelmia. Finnlinesilla tullaan jatkossakin panostamaan kyberturvallisuuteen, uhkien havainnointiin sekä verkkojen segmentointiin. Myös internetissä toimivat päätelaitteet on suojattava.

4.3 Haastattelu: Suomen Varustamot ry

Tutkimuksen toinen haastattelu toteutettiin ensimmäisen tapaan puolistrukturoituna haastatteluna. Kysymykset oli laadittu etukäteen, ja haastateltava oli vastaanottanut ne sähköpostitse. Haastateltavana oli Suomen Varustamot ry:ssä työskentelevä Sinikka Hartonen, joka toimii yhdistyksessä johtavana asiantuntijana ympäristön ja teknologian osa-alueilla. Kysymysten järjestys ja muoto muuttuivat hieman haastattelun aikana. Kysymykset olivat alkuperäisessä muodossaan seuraavat:

- Kuka olet ja mikä on toimenkuvasi Suomen Varustamot ry:ssä?
- Millaisena näet kyberturvallisuustilanteen merenkulussa tällä hetkellä?
- Miten tietoturvaan liittyvät uhkakuvat ovat mielestäsi muuttuneet vuosien varrella?
- Onko jäsenyrityksiinne kohdistettu kyberhyökkäyksiä?
- Minkälaisia vaikutuksia mahdollisilla kyberhyökkäyksillä on ollut jäsenyritystenne toimintaan?
- Miten varustamoyhtiöt pysyvät mukana kyberturvallisuuden kehityksessä?
- Minkälaisia ohjeistuksia olette antaneet jäsenyrityksillenne kyberturvallisuuteen liittyen?
- Minkälaisia vaikutuksia kyberhyökkäyksillä voi olla meriliikenteeseen ja erityisesti kansainväliseen kauppaan?
- Miten merenkulun kyberturvallisuutta voitaisiin mielestäsi kehittää?

Haastattelun alussa haastateltavalta kysytään hänen omista taustoistaan sekä tämänhetkisestä työnkuvastaan. Tällä hetkellä Suomen Varustamot ry:ssä Hartonen työskentelee merenkulun parissa, keskittyen erityisesti turvallisuuteen, ympäristöasioihin, uudistuvaan teknologiaan ja merenkulun automaation seuraamiseen.

Hartonen nostaa haastattelun alussa esiin aiheen ajankohtaisuuden. Kyberturvallisuus on Suomen Varustamot ry:ssä yksi nousevista puheenaiheista. Varustamoelinkeino ja merenkulkuala ovat heränneet kyberturvallisuuteen ja merkittävimmät kyberhyökkäykset ovat

tulleet myös suuren yleisön tietoisuuteen uutisoinnin kautta. Hartonen nostaa esiin varustamoyhtiö Maerskiin kohdistuneen kyberhyökkäyksen vuodelta 2017, joka aiheutti yhtiölle merkittävät taloudelliset tappiot ja haittasi yhtiön toimintaa lukuisissa eri satamissa. Virus ei ollut kuitenkaan tarkoitettu kohdistettavaksi suoraan Maerskiin, mistä johtuen Hartonen ei pidä tapausta parhaana kyberhyökkäyksen esimerkkinä.

Hartosen mukaan kyberturvallisuuden tarkastelun yhteydessä on hyvä tunnistaa ja erottaa toisistaan itse alukseen kohdistuvat uhkat ja maissa tapahtuvat, varustamoyhtiöön kohdistuvat hyökkäykset. Aluksen haltuun ottamisella voidaan saada aikaiseksi mittavia ympäristötuhoja, henkilövahinkoja sekä suuria taloudellisia menetyksiä. Varustamopuolella mahdollisia haittavaikutuksia ovat niin ikään merkittävät taloudelliset vahingot logistisen toimitusketjun häiriintymisen kautta sekä yhtiöiden mahdolliset mainehaitat. Mainehaittaa voivat aiheuttaa myös aluksiin kohdistuvat hyökkäykset. Hartonen korostaa sitä, että kyberturvallisuus aiheuttaa haasteita sekä maissa että aluksella, mutta erityisen haastavaa on alusten tekeminen kyberturvallisiksi. Maaorganisaatiot osaavat huolehtia kyberturvallisuudesta paremmin, mutta itse alusten kyberturvallisuudessa on vielä kehitettävää.

Tietoturva-asiat nousevat jatkuvasti enemmän esille sekä Suomen Varustamot ry:ssä että yleisellä tasolla. Merenkulun uuden teknologian myötä alukset ovat yhä useammin yhteydessä toisiinsa sekä maaorganisaatioihin. Teknologian kehitys sekä erilaisten sensoreiden ja järjestelmien tulo ovat kohottaneet tietoturvaan liittyviä riskejä. Tämä on johtanut siihen, että toimijat ovat heränneet asian vakavuuteen ja ymmärtäneet, että kyberhyökkäysten seuraukset voivat olla mittavia sekä yrityksille että koko kuljetusketjulle. Kyberturvallisuuden huomioiminen on muuttunut yksittäisen tilanteen tarkastelusta laajemmaksi kokonaisuudeksi, jossa erilaisia uhkia kartoitetaan entistä tarkemmin aina yritysten johtoa myöten.

Hartonen ei halunnut ottaa tarkemmin kantaa Suomen Varustamot ry:n jäsenyrityksiin kohdistuneisiin kyberhyökkäyksiin, joten asiaa tarkasteltiin yleisemmällä tasolla. Esimerkiksi tietojenkalastelua kohdistuu nykypäivänä jatkuvasti niin yrityksiin kuin yksityishenkilöihinkin. Hartonen korostaa, että varsinainen tietopohjan rakentaminen koostuu usein pienemmistä osa-alueista. Hyökkääjät keräävät yllättäviä tietoja, joita ammattilaiset pystyvät yhdistelemään ja sitä kautta luomaan erilaisia profiileja ja väärentämään asioita. Nämä mahdollistavat vakavampien hyökkäysten toteuttamisen.

Haastattelussa kysytään myös varustamoyhtiöiden kyvystä pysyä mukana nopeasti kehittyvässä kyberturvallisuusympäristössä. Hartonen arvioi, että tämä aiheuttaa haasteita suurimmalle osalle alan toimijoista. Varustamoalalla toimii hyvin erikokoisia yrityksiä, aina suuryrityksistä pieniin ja keskisuuriin toimijoihin. Pienempien yritysten osalta etuina voivat olla

helpommin hallittava toimintaympäristö ja vähäisempi alusten määrä. Lisäksi pienemmissä yrityksissä henkilöstö usein tuntee toisensa paremmin. Haasteita voi tuottaa resurssointi ja kyberturvallisuuden huomioiminen kiireellisen arjen keskellä. Isoilla yrityksillä on lähtökohtaisesti enemmän resursseja ja mahdollisuuksia panostaa teknologiaan sekä kyberturvallisuuden seurantaan, mutta haasteita voivat aiheuttaa alusten ja toimijoiden suurempi lukumäärä.

Suomen Varustamot ry on tuottanut yhdessä Huoltovarmuuskeskukseen kuuluvan Vesikuljetuspoolin kanssa kyberturvallisuuden ohjeistukset, jotka on kohdennettu erikseen sekä aluksille että varustamoihin. Ohjeistuksessa annetaan käytännön tason neuvoja alusten ja varustamoiden kyberturvallisuuden parantamiseksi. Lisäksi yhdistys keskustelee jäsentensä kanssa ja tiedottaa näitä erilaisista riskitekijöistä. Lisäksi Hartonen nostaa esiin kansainväliset merenkulkualan toimijat, kuten Suomen Varustamot ry:n kattojärjestön ICS:n (International Chamber of Shipping), joka on laatinut niin ikään kyberturvallisuusohjeita varustamoyhtiöille. Myös IMO edellyttää kyberturvallisuusriskien huomioimista osana alusten turvallisuusjohtamisjärjestelmiä.

Hartonen arvioi haastattelussa kyberhyökkäysten mahdollisia vaikutuksia merenkulkuun ja erityisesti kansainvälisen kaupan sujuvuuteen. Kyberhyökkäyksillä voi olla halvauttava vaikutus koko logistiseen toimitusketjuun. Laivojen tiedot ja dokumentit ovat usein sähköisessä muodossa, ja mikäli järjestelmä kyettäisiin halvauttamaan, voisivat seuraukset olla merkittävät erityisesti nykypäivän verkottuneessa maailmassa. Mikäli lastitiedot katoavat, voi yrityksillä olla merkittäviä vaikeuksia lähteä purkamaan tilannetta.

Haastattelun loppupuolella kysytään merenkulun kyberturvallisuuden kehityskohdista. Hartosen mukaan yksi tapa on asian esille nostaminen ja siitä puhuminen sekä yleisen tietoisuuden lisääminen. Jokaisen tulisi tietää, minkälaisia riskejä kyberturvallisuuteen liittyy. Kyberturvallisuutta aluksilla voidaan lisätä myös fyysisellä tasolla, esimerkiksi huolehtimalla siitä, että aluksille ei pääse ulkopuolisia henkilöitä, etenkin sellaisia, joilla olisi pääsy aluksen järjestelmiin.

Yksi merenkulun turvallisuuden olennaisista tekijöistä on kyberturvallisuuden tekeminen normaaliksi asiaksi, josta täytyy huolehtia kaiken muun ohella. Varustamoiden on tuotava kyberturvallisuusasiat myös yritysten johdon tietoisuuteen, jotta ne voidaan ottaa huomioon henkilöstön koulutuksessa. Keskustelua kyberturvallisuudesta on pyrittävä käymään yhteisellä kielellä, jotta keskustelu voidaan pitää selkeänä ja ymmärrettävänä kaikille osapuolille ja jotta asia saadaan osaksi yhtiöiden ja toimijoiden normaalia arkea.

Asioiden jatkuva esillä pitäminen ja siitä keskusteleminen yleisellä tasolla pitävät Hartosen mukaan ihmiset valveilla kyberturvallisuuden ympärillä liikkuvissa kysymyksissä. Inhimilliset erehdykset ja virheet voivat aiheuttaa mittaviakin tuhoja yritysten tai yksityishenkilöiden tärkeisiin tietoihin. Sen vuoksi Hartonen painottaakin kouluttamisen tärkeyttä aiheeseen liittyen, jotta turhilta ongelmilta vältyttäisiin. Kyberturvallisuus ja sen uhkat kehittyvät kovaa vauhtia ja erilaisissa yrityksissä työskentelevien ihmisten voi olla vaikea pysyä mukana alan kehityksessä, joten yleistä ymmärrystä alaan liittyen on pyrittävä lisäämään. Kyberturvallisuudesta olisi nopeasti saatava yritysmaailmassa yksi normi, johon suhtaudutaan vakavuudella, painottaa Hartonen.

4.4 Tutkimuksen johtopäätökset

Opinnäytetyön tutkimusosuudessa tarkoituksena oli selvittää, minkälaisia kyberhyökkäyksiä merenkulkualaan kohdistuu ja minkälaisia vaikutuksia niillä voi olla kansainvälisen kaupan sujuvuuteen. Tutkimusta varten haastateltiin kahta merenkulkualan asiantuntijaa, jotka edustavat eri organisaatioita. Ensimmäinen haastateltava työskenteli Finnlines Oyj:lla tietoturvaosaston johtotehtävissä. Toinen haastateltavista työskenteli Suomen Varustamot ry:ssä johtavana asiantuntijana ympäristön ja teknologian osa-alueilla. Haastattelut toteutettiin puolistrukturoituina haastatteluina Microsoft Teams -ohjelmalla, ja haastattelut kestivät noin 30 minuuttia. Haastatteluiden avulla pyrittiin keräämään alan ammattilaisten näkemyksiä ja kokemuksia kyberhyökkäysten uhka- ja kehityskuvista merenkulun logistiikkaan liittyen. Tutkimusta varten pyrittiin keräämään muistakin organisaatioista asiantuntijoita haastateltaviksi, mutta määrä jäi lopulta pieneksi, koska useisiin haastattelupyyntöihin ei vastattu. Kahdesta haastattelusta saatu aineisto ei riitä kertomaan kokonaiskuvaa kyberhyökkäysten vaikutuksista kansainväliseen kauppaan, mutta johtopäätöksenä voidaan kuitenkin todeta, että kyberhyökkäysten määrä on jatkuvasti kasvussa ja niillä voi olla mittavia seurauksia logistiseen toimitusketjuun ja kansainvälisen kaupan sujuvuuteen.

Ensimmäisenä kysymyksenä haastateltavilta kysyttiin heidän roolistaan ja työnkuvastaan organisaatiossa. Haastateltavat henkilöt edustivat erilaisia organisaatioita, joten kysymyksiä jouduttiin muokkaamaan haastateltavien rooleihin sopiviksi. Tästä johtuen haastattelut eivät ole täysin vertailukelpoisia keskenään. Ensimmäinen haastateltava edusti varustamoyhtiötä, ja haastateltava vastaa siellä kyberturvallisuudesta käytännön tasolla. Toinen haastateltava edusti varustamoiden etujärjestöä, jossa opastetaan, ohjeistetaan ja tuetaan jäsenvarustamoyhtiöitä. Etujärjestön edustaja ei voinut ottaa kantaa jäsenyrityksiin kohdistuneisiin kyberhyökkäyksiin, joten aihetta käsiteltiin yleisellä tasolla. Muut kysymykset vastasivat pitkälti toisiaan, joten osaa vastauksista voidaan verrata keskenään.

Toinen kysymys liittyi suoraan kyberturvallisuuden uhkakuvien kehitykseen, jota haastateltavat henkilöt avasivat omista näkökulmistaan. Kyberhyökkäysten määrän kasvaessa myös niiden laatu on muuttunut uhkaavammaksi ja kyberhyökkäykset toteutetaan entistä järjestäytyneemmin ja ammattimaisemmin. Haasteltavat olivat yhtä mieltä kyberturvallisuuden kehityksen kulusta, jossa nähtiin varustamoiden osalta haasteena pysyä mukana kyberturvallisuuden kehittyvissä uhkakuvissa. Ensimmäinen haastateltava oli sitä mieltä, että haasteita on erityisesti pienemmillä alan toimijoilla. Toinen haastateltava arvioi, että haasteita on pienten toimijoiden lisäksi mahdollisesti myös suuremmilla toimijoilla.

Haastateltavilta kysyttiin, minkälaisia kyberhyökkäyksiä heidän organisaatioissaan on kohdattu. Pääosin Finnlines Oyj:n organisaatiossa on kohdattu erilaisia tietojenkalasteluyrityksiä, tietojen varastamista ja tietoliikenteen häirintää. Haastattelun perusteella kävi ilmi, että hyökkäykset toteutettiin kehittyneillä välineillä, mutta hyökkäysten laatu jäi kuitenkin osaltaan heikoksi. Alusten ohjausjärjestelmien kokonaisvaltainen kaappaaminen ja ohjaaminen väärille reiteille ei ole Finnlines Oyj:lle todennäköinen skenaario, koska sen toimintamalli on yhtenäinen ja ulkopuolisen on hankala tunkeutua sen järjestelmiin. Toinen haastateltavista ei voinut ottaa kysymykseen kantaa, koska mahdolliset hyökkäykset liittyvät hänen edustamansa organisaation jäseniin, jotka tiedottavat itse mahdollisista hyökkäyksistä niin halutessaan. Tämä johtuu aiheen arkaluontoisuudesta.

Haastattelussa kysyttiin myös sitä, kuinka varustamoyhtiöt pysyvät mukana kyberturvallisuuden kehityksessä. Esille nousi erilaisia teemoja, kuten kouluttaminen ja kyberturvallisuuden yleisen tietoisuuden lisääminen. Kyberturvallisuus tuo tullessaan suuria haasteita etenkin pienemmille yhtiöille, joiden resurssit ovat rajalliset. Hartonen nosti esiin ongelman isojen yhtiöiden suuresta henkilökunnan määrästä, mikä lisää epätietoisuutta ja vaikeuttaa erilaisten tunkeutumisten havaitsemista. Finnlines Oyj:lla Kostia taas näki positiivisena asiana yhtenäisen ja harvoin vaihtuvan henkilöstön. Esimerkiksi hänen yhtiönsä kohdalla henkilöstö tuntee toisensa hyvin, ja väärällä henkilöllisyydellä esiintyminen havaitaan yleensä nopeasti. Kostia kertoi tapauksesta, jossa yhtiön sisäisiä sähköposteja oli tullut ulkopuoliselta henkilöltä. Tapaus pystyttiin havaitsemaan ajoissa, jolloin vahingoilta vältyttiin.

Alusten automatisoituminen tuo mukanaan lisää erilaisia riskejä joutua kyberhyökkäyksen kohteeksi, sillä järjestelmät ovat yhä useammin kytkettyinä verkkoon, toisiin aluksiin ja maassa toimiviin organisaatioihin. Haastateltavat olivat yhtä mieltä siitä, että hyökkäykset tulevat useimmiten ilmi erilaisina tietojenkalasteluyrityksinä, joiden kautta hyökkääjät yrittävät rakentaa laajempaa kyberhyökkäystä. Kyberhyökkäysten merkitystä kansainväliseen

kauppaan voidaan pitää haastatteluiden perusteella jopa halvauttavana. Mahdolliset hyökkäykset voivat asettaa toimitusketjuihin mittavia katkoja, jotka aiheuttavat suuria taloudellisia menetyksiä ja mainehaittoja eri organisaatioille maailmanmarkkinoilla. Tämä johtuu merilogistiikan keskeisestä merkityksestä maailmankaupassa, jolloin se asettuu hyökkääjille merkittäväksi ja hyväksi kohteeksi.

4.5 Tutkimuksen reliabiliteetti ja validiteetti

Tutkimuksessa validiteetilla tarkoitetaan sitä, miten hyvin tutkimuksessa käytetty mittausmenetelmä mittaa sitä tutkittavan ilmiön ominaisuutta, jota on tarkoitus mitata. Validiteetilla voidaan mitata esimerkiksi sitä, kuinka hyvin tutkijan ja haastateltavan ymmärrys kohtaa. Jos keskinäistä ymmärrystä ei ole, tutkimus ei ole validi. (Tilastokeskus.)

Hiltusen (2009) mukaan reliabiliteetti antaa tietoa siitä, kuinka luotettavasti on mitattu haluttua ilmiötä. Reliabiliteettia pystytään arvioimaan toistomittauksilla, ja sen yhteydessä voidaan ilmoittaa mittavirhe. Mitä enemmän samansuuntaisuuksia tuloksista löytyy, sitä luotettavampana tutkimusta voidaan pitää. Jotta saataisiin luotettava tulos, otoksen tulisi olla mahdollisimman kattava ja edustava eli samankaltainen kuin perusjoukko. Reliaabelissa tutkimuksessa haetaan tarkkoja tuloksia, jotka eivät ole sattumanvaraisia.

Tätä tutkimusta voidaan pitää melko luotettavana, mutta reliabiliteettia olisi voinut lisätä toteuttamalla useampia haastatteluja tai luomalla haastatteluiden lisäksi kyselyn useammalle alan toimijalle. Tätä kautta olisi pystytty vertaamaan kattavammin yritysten vastauksia ja luomaan laajempaa kuvaa aiheen todellisesta tilanteesta. Toistettujen haastatteluiden määrä olisi siten lisännyt tutkimuksen reliabiliteettia. Kahden haastattelun perusteella voidaan todeta, että kyberturvallisuus on yhä keskeisemmässä roolissa merenkulussa ja kyberhyökkäysten määrä ja laatu ovat kasvussa. Kyberhyökkäyksillä voi lisäksi olla merkittäviä vaikutuksia logistisen toimitusketjun sujuvuuteen ja kansainväliseen kauppaan. Mikäli haastatteluita olisi ollut enemmän, voidaan pitää todennäköisenä sitä, että vastaukset olisivat olleet pitkälti yhteneväisiä. Teoriaosuuden osalta reliabiliteetti toteutui hyvin, sillä aiheesta on saatavilla runsaasti ajankohtaista ja luotettavaa tutkimustietoa, uutisia ja artikkeleita.

Tutkimuksen validiteettia olisi mahdollisesti lisännyt perinteinen kyselytutkimus haastatteluiden rinnalla. Mikäli kyselytutkimus olisi toteutettu, olisi vastausten vertaaminen keskenään ollut helpompaa. Tässä tilanteessa yrityksille olisi voitu lähettää identtiset kysymykset, jolloin myös reliabiliteetin arviointi olisi ollut helpompaa. Tutkimusta voidaan pitää melko validina, koska kysymykset voitiin kohdentaa suoraan asiantuntijoille soveltuviksi ja niihin saatiin kattavia vastauksia. Haastattelukysymysten avulla saatiin vastattua varsinaisiin

tutkimuskysymyksiin, lukuun ottamatta toista haastattelua, jossa haastateltava ei voinut ottaa kantaa jäsenyrityksiin kohdistuneisiin kyberhyökkäyksiin.

Merenkulun kyberturvallisuus on alalla nouseva trendi, joten jatkotutkimuksille on tarvetta. Jatkotutkimuksia voidaan toteuttaa perustuen asiantuntijoiden kokemuksiin ja tuoreeseen tutkimustietoon. Jatkotutkimus vaatisi laajemman määrän vastauksia alan toimijoilta, jotta niitä voitaisiin analysoida ja vertailla kattavammin. Jatkotutkimuksen kannalta olisi hyvä saada vastauksia eri kokoisilta yrityksiltä ja organisaatioilta, jotta aiheesta saataisiin erilaisia näkemyksiä. Jatkotutkimus voisi tarkastella perusteellisemmin joko itse alusten tai maaorganisaatioiden kyberturvallisuutta, jolloin tutkijalla olisi mahdollisuus perehtyä tarkemmin toiseen osa-alueeseen.

5 Yhteenveto

Työ sai alkunsa kirjoittajien omasta mielenkiinnosta opinnäytetyön aihetta kohtaan. Aiheen valintaan vaikutti myös sen ajankohtaisuus ja merkityksellisyys kansainvälisen kaupan näkökulmasta. Opinnäytetyön tarkoituksena oli tutkia, mikä on merenkulun logistiikan merkitys maailmanmarkkinoihin, minkälaisia kyberturvallisuusuhkia merenkulkuun kohdistuu ja miten ne vaikuttavat kansainvälisen kaupan toimivuuteen ja sujuvuuteen. Työn teoreettinen osuus koostui aineistosta, jota kerättiin erilaisista tilastoista, tutkimuksista, alalla toimivien yritysten ja järjestöjen verkkosivuilta sekä tuoreimmista uutisista ja artikkeleista. Aiheena kyberhyökkäykset ovat alati kehittyvä ja laajeneva ilmiö, joten niistä löytyi runsaasti ajankohtaista tietoa. Tätä tietoa hyödynnettiin erityisesti työn teoriaosuuksissa.

Empiirinen tutkimus koostui tässä työssä kahdesta merenkulkualan ammattilaisen haastattelusta. Haastatteluja varten luotiin lista kysymyksiä, joissa käsiteltiin muun muassa kyberturvallisuuden kehitystä, nykytilannetta ja sen tulevaisuutta. Haastatteluissa pyrittiin selvittämään, minkälaisia kyberhyökkäyksiä haastateltavien edustamissa organisaatioissa on havaittu, kuinka ne ovat vaikuttaneet näiden toimintaan ja millaisena kyberturvallisuuden tilanne nähdään tällä hetkellä. Haastatteluiden lopuksi tarkasteltiin sitä, kuinka kyberhyökkäysten tulevaisuus kehittyy ja miten niiltä voidaan jatkossa suojautua paremmin. Haastatteluista kerättyä aineistoa analysoitiin suhteessa työn teoriaosuuteen. Haastatteluiden perusteella voidaan todeta, että kyberhyökkäykset ovat suuri uhka logistisille toimitusketjuille ympäri maailmaa ja että niiden vaikutukset kaupankäyntiin globaalista näkökulmasta voivat olla halvauttavia. Sama tieto tuli esiin myös työn teoriaosuudessa. Haastateltavat arvioivat hyökkäysten laadun kehittyvän ja määrän lisääntyvän tulevaisuudessa. Tämä johtaa siihen, että varustamoyhtiöillä on haasteita pysyä mukana alati muuttuvassa kyberturvallisuusympäristössä. Samanaikaisesti organisaatiot kuitenkin kehittävät laitteita ja ohjelmistoja sekä kouluttavat henkilöstöään vastaamaan kyberturvallisuuden haasteisiin. On selvää, että hyökkäyksiä ei pystytä tulevaisuudessa poistamaan kokonaan, mutta niitä pystytään rajoittamaan kehittyvillä järjestelmillä, henkilöstön kouluttamisella sekä kyberturvallisuuden yleisen tietoisuuden lisäämisellä.

Haastattelupyyntöihin vastanneiden yritysten määrä jäi toivotusta, joten haastatteluvastauksia saatiin rajallinen määrä. Puutteista huolimatta vastauksia voi kuitenkin yleistää, koska haastateltavat vastasivat kysymyksiin hyvin yhdenmukaisesti. Kun haastatteluvastauksia verrataan erilaisiin teoreettisiin lähteisiin, voidaan todeta näiden vastaavan hyvin pitkälti toisiaan.

Tässä työssä reliabiliteetti toteutui melko hyvin. Teoriaosuus saatiin toteutettua kattavasti, sillä luotettavaa materiaalia oli laajasti saatavilla. Lähteinä käytettiin pääasiassa yritysten, viranomaisten ja organisaatioiden verkkosivuja. Aiheesta oli myös saatavilla kirjapainoksia, joita hyödynnettiin opinnäytetyössä. Työn validiteettia ja reliabiliteettia olisi lisännyt haastatteluiden lisäksi merilogistiikkaa harjoittaville yrityksille suunnattu kyselytutkimus, jolloin vastauksia eri toimijoilta olisi saatu lisää ja vastausten keskinäinen vertailu olisi ollut helpompaa. Voidaan kuitenkin todeta, että suurella todennäköisyydellä vastaukset olisivat olleet melko yhdenmukaisia. Suuri osa organisaatioista ja yksityishenkilöistä kohtaa jatkuvasti kyberhyökkäyksiä, joista tyypillisimpiä ovat tietojenkalasteluyritykset. Maailmalla on myös havaittu useita tapauksia, joissa varustamot ovat kohdanneet erilaisia kyberhyökkäyksiä, jotka ovat haitanneet esimerkiksi satamien toimintaa ja aiheuttaneet yrityksille valtavia taloudellisia tappioita ja liiketoiminnan keskeytymisiä. Myös haastatteluiden perusteella pystytään päättelemään, että kyberhyökkäyksillä voi olla merkittäviä vaikutuksia logistisiin toimitusketjuihin ja kansainvälisen kaupan sujuvuuteen.

Alan toimijoiden tulisi pitää huolta siitä, että kyberturvallisuus huomioidaan jatkossakin yhtenä tärkeänä osana alusten ja maalla toimivien organisaatioiden turvallisuutta, jotta merenkulun logistiikka toimisi tarkoituksenmukaisesti ilman häiriöitä ja keskeytyksiä. Kyberturvallisuudesta tulisi tehdä osa alusten kokonaisturvallisuutta, ja siitä olisi kyettävä keskustelemaan tavalla, jonka kaikki ymmärtävät. Yksi tapa on huolehtia siitä, että kyberturvallisuus otetaan keskeiseksi osaksi alalla toimivan henkilöstön koulutusta, jotta erilaisiin uhkatilanteisiin osataan varautua asianmukaisesti ja että alusten koko miehistöllä olisi käsitys siitä, kuinka kyberturvallisuudesta tulisi huolehtia. Haastatteluiden perusteella on myös syytä erottaa itse aluksen kyberturvallisuus maaorganisaatioiden kyberturvallisuudesta. Alusten kyberturvallisuudessa on erityispiirteitä, jotka tulee ottaa huomioon kyberturvallisuuden suunnittelussa ja toteutuksessa.

Kyberturvallisuus on laaja käsite, eikä sitä voitu tässä työssä käsitellä kovinkaan syvällisesti. Työ on osa tradenomin tutkintoa, joten pääasiallisena tutkimuskohteena oli selvittää kyberhyökkäysten vaikutuksia erityisesti merenkulun logistiikkaan ja kansainväliseen kauppaan. Aihe tarjoaa hyviä mahdollisuuksia jatkotutkimukseen esimerkiksi tekniikan alalla, jolloin kyberturvallisuutta voitaisiin käsitellä huomattavasti laajemmin ja syvällisemmin. Jatkotutkimusta voitaisiin kohdistaa esimerkiksi rahtialusten automatisoitumiseen, alusten tarkempiin tietoteknisiin osa-alueisiin sekä automaation tuomiin ongelmakohtiin ja haasteisiin. Jatkotutkimuksia varten on syytä erottaa toisistaan itse alusten kyberturvallisuus, jossa on haastatteluista saadun tiedon perusteella vielä kehitettävää, etenkin pienemmillä varustamoyhtiöillä. Kyberturvallisuuden hallinta on varustamoyhtiöille keskeinen

ennaltaehkäisevä toimenpide. Kun kyberturvallisuudesta huolehditaan asianmukaisilla tavoilla, voidaan pienentää riskiä liiketoiminnan keskeytymisille ja toimitusketjujen katkeamisille.

6 Lähteet

Aamulehti. 2021. Kontit loppuivat maailmasta. Viitattu 9.11.2021. Saatavissa https://www.aamulehti.fi/paakirjoitukset/art-2000008332782.html

Adams, K. 2020. The Advantages of Container Shipping. Viitattu 19.10.2021. Saatavissa https://businesspartnermagazine.com/the-advantages-of-container-shipping/

BBC. 2021. Ever Given: Ship that blocked Suez Canal sets sail after deal signed. Viitattu 13.12.2021. Saatavissa https://www.bbc.com/news/world-middle-east-57746424

BBC. 2021. Suez Canal: Effort to refloat wedged container ship continues. Viitattu 13.11.2021. Saatavissa https://www.bbc.com/news/world-middle-east-56547383

Blue-Growth. 2021. TEU ISO freight containers. Viitattu 7.11.2021. Saatavissa https://www.blue-growth.org/Climate_Warming_Action_Plans/Cargo_Container_Ships_Zero_Carbon_Emissions_Shipping/Containers_ISO_Standardized_Shipping_International_Intermodal_Cargo_Freight_TEU.htm

Carnegie Mellon University. 2020. The Dangers of Security Tailgating. Viitattu 15.11.2021. Saatavissa https://www.cmu.edu/iso/news/2020/tailgating-dangers.html

Euroopan parlamentti. 2015. Kyberturvallisuus: suurimmat uhat. Viitattu 13.10.2021. Saatavissa https://www.europarl.europa.eu/news/fi/headlines/society/20151207IFG06371/kyberturvallisuus-suurimmat-uhat

Euroopan parlamentti. 2019. Talouden ja globalisaation hyödyt Euroopassa. Viitattu 7.11.2021. Saatavissa https://www.europarl.europa.eu/news/fi/headlines/economy/20190603STO53520/talouden-globalisaation-hyodyt-euroopassa

Finnlines Oyj. Finnlines rahtiliikenne. Viitattu 11.11.2021. Saatavissa https://www.finnlines.com/fi/rahti

F-secure Oyj. Ransomware on haittaohjelmista pahimpia. Viitattu 13.11.2021. Saatavissa https://www.f-secure.com/fi/home/articles/what-is-a-ransomware-attack

Gröndahl, J. 2021. Digiajan merirosvot iskevät ilman fyysistä voimaa. Keskisuomalainen. Viitattu 2.10.2021. Saatavissa https://www.ksml.fi/paikalliset/4278093

Hiltunen, L. 2009. Validiteetti ja reliabiliteetti. Jyväskylän yliopisto. Viitattu 3.12.2021. Saatavissa http://www.mit.jyu.fi/ope/kurssit/Graduryhma/PDFt/validius_ja_reliabiliteetti.pdf

Horelli, M. 2020. Kyberturvallisuudesta tuli loputon kilpajuoksu. Viitattu 8.11.2021. Saatavissa https://www.erillisverkot.fi/kyberturvallisuudesta-tuli-loputon-kilpajuoksu/

Huoltovarmuusorganisaatio. 2021. Merenkulun kyberturvallisuus – alusten parhaat käytännöt. Viitattu 1.10.2021. Saatavissa https://www.huoltovarmuuskeskus.fi/files/a3512a9ae47541a92f002c60c6fa3030dc5327d3/kyberturvallisuus-parhaat-kaytannot-aluksille.pdf

Imperva. Distributed Denial of Service (DDoS). Viitattu 17.11.2021. Saatavissa https://www.imperva.com/learn/ddos/denial-of-service/

Imperva. What is a phishing attack? Viitattu 17.11.2021. Saavissa https://www.imperva.com/learn/application-security/phishing-attack-scam/

International Maritime Organization. Maritime cyber risk. Viitattu 1.10.2021. Saatavissa https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

Jyväskylän yliopisto. 2020. Haastattelut. Viitattu 9.10.2021. Saatavissa https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineistonhankintamenetelmat/haastattelut

Kajaanin ammattikorkeakoulu. Haastattelu. Viitattu 11.11.2021. Saatavissa https://www.kamk.fi/fi/opari/Opinnaytetyopakki/Teoreettinen-materiaali/Tukimateriaali/Aineiston-keruumenetelmat/Haastattelu

Kaspersky. What Is an Advanced Persistent Threat (APT)? Viitattu 17.11.2021. Saatavissa https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

Kotimikro. 2020. Mitä on phishing? Viitattu 12.10.2021. Saatavissa https://kotimikro.fi/tietoturva/mita-on-phishing

Kovanen, T. 2021. Väitös: Laivaliikenteeseen kohdistuu kyberuhkia. Jyväskylän yliopisto. Viitattu 26.9.2021. Saatavissa https://www.sttinfo.fi/tiedote/vaitos-392021-laivaliikenteeseen-kohdistuu-kyberuhkia?publisherId=69817172&releaseId=69916656

Leppänen, V. Rauti, S. Rindell, K. Holvitie, J. 2020. Kyberturvallisuus ja tiedonsiirron turvaaminen autonomisten alusten kehittämisessä ja operoinnissa. Viitattu 20.11.2021. Saatavissa https://www.aboamare.fi/_media_25404_/R&D%20kuvat/%C3%84lyVESI/Tulokset%20201805/Kyberturvallisuus-ja-tiedonsiirron-turvaaminen-autonomisten-alusten-kehittamisessa-ja-operoinnissa.pdf

Logistiikan Maailma. Kontti, logistiikan mullistaja. Viitattu 7.10.2021. Saatavissa https://www.logistiikanmaailma.fi/aineistot/logistiikkaa-lukiolaisille/kontti-logistiikan-mullistaja/

Logistiikan Maailma. Merikuljetus. Viitattu 23.11.2021. Saatavissa https://www.logistiikanmaailma.fi/kuljetus/merikuljetus/

Marine Insight. 2021. The ISPS Code for Ships – An Essential Quick Guide. Viitattu 7.11.2021. Saatavissa https://www.marineinsight.com/maritime-law/the-isps-code-for-ships-a-quick-guide/

McAfee. Mikä on haittaohjelma? Viitattu 7.11.2021. Saatavissa https://www.mcafee.com/fi-fi/antivirus/malware.html

Menon, H. 2021. Advantage and Disadvantages of Containerization. Viitattu 19.10.2021. Saatavissa https://www.marineinsight.com/maritime-law/advantage-and-disadvantages-of-containerization/#Advantages_of_Containerization

Menon, H. 2021. TEU in Shipping – Everything You Wanted to Know. Viitattu 7.11.2021. Saatavissa https://www.marineinsight.com/maritime-law/teu-in-shipping-everything-you-wanted-to-know/

Mikkelsson, V. 2015. Hacktivismi. Viitattu 20.11.2021. Saatavissa https://prezi.com/qgfbj-vlnldl/hacktivismi/

Multanen, E. 2021. Konttipula. Viitattu 15.11.2021. Saatavissa https://www.finnhub.fi/kont-tipula-mutta-miksi-logistiikka-ala-on-otsikoissa-vasta-kun-on-ongelmia/

Nagurney, A. 2021. Today´s global economy runs on standardized shipping containers, as the Ever Given fiasco illustrates. Viitattu 12.11.2021. Saatavissa https://theconversa-tion.com/todays-global-economy-runs-on-standardized-shipping-containers-as-the-ever-given-fiasco-illustrates-158179

Neptunet. 2020. Mitä on kyberhyökkäys ja kyberturvallisuus? Viitattu 7.11.2021. Saata-vissa https://neptunet.net/2020/01/09/mita-on-kyberhyokkays-ja-kyberturvallisuus/

Niemelä, J. 2020. Kehittyvä elintarvike. Viitattu 10.11.2021. Saatavissa https://kehittyva-elintarvike.fi/artikkelit/teemajutut/digitalisaatio-robotiikka/kyberturvallisuuden-pitaa-olla-kiintea-osa-yrityksen-toimintaa/

OECD. Ocean Shipping and Shipbuilding. Viitattu 1.10.2021. Saatavissa https://www.oecd.org/ocean/topics/ocean-shipping/

Osto&Logistiikka. 2021. Suezin kanavan tukoksella mittavat taloudelliset vaikutukset. Vii-tattu 3.10.2021. Saatavissa https://www.ostologistiikka.fi/kategoriat/toimitusketjut/suezin-kanavan-tukoksella-mittavat-taloudelliset-vaikutukset

Poliisi. Palvelunestohyökkäys. Viitattu 7.11.2021. Saatavissa https://poliisi.fi/palvelunesto-hyokkays

Qualman, D. 2017. Fraught freight: trade agreements, globalization, and rising global freight transport. Viitattu 13.11.2021. Saatavissa https://www.darrinqualman.com/global-freight-transport/

Reinikkala, S. 2007. Kontin historia. Viitattu 15.11.2021. Saatavissa https://www.kontti.fi/site/verkkolehti/2007/kontin-historia.html

Ritala, P. 2013. Johdatus tutkimusmetodologiaan. Viitattu 1.10.2021. Saatavissa https://developmentcentre.lut.fi/digi/Moodle_pohjat/Ritala_Johdatus%20tutkimusmetodolo-giaan%202013.pdf

Rodrigue, J-P & Notteboom, T. Chapter 1.1- Maritime Shipping and International Trade. Viitattu 18.10.2021. Saatavissa https://porteconomicsmanagement.org/pemp/con-tents/part1/maritime-shipping-and-international-trade/

Statista. 2021. Transport volume of seaborne trade from 1990 to 2019. Viitattu 1.10.2021. Saatavissa https://www.statista.com/statistics/264117/tonnage-of-worldwide-maritime-trade-since-1990/

Suomen Varustamot ry. Meriturvallisuus. Viitattu 7.11.2021. Saatavissa https://shi-powners.fi/vastuullisuus/turvallisuus/meriturvallisuus/

Tapaninen, U. 2019. Merenkulun logistiikka. Toinen painos. Helsinki: Otatieto.

The Geography of Transport Systems. 2021. World Container Throughput. Viitattu 19.10.2021. Saatavissa https://transportgeography.org/contents/chapter5/intermodal-transportation-containerization/world-container-throughput/

Tilastokeskus. Käsitteet. Validiteetti. Viitattu 3.12.2021. Saatavissa https://www.stat.fi/meta/kas/validiteetti.html#tab1

Traficom. 2019. Aluksen turva-asiat. Viitattu 13.12.2021. Saatavissa https://www.traficom.fi/fi/liikenne/merenkulku/aluksen-turva-asiat

Traficom. 2020. ISM-turvallisuusjohtamisjärjestelmä. Viitattu 7.11.2021. Saatavissa https://www.traficom.fi/fi/liikenne/merenkulku/ism-turvallisuusjohtamisjarjestelma

Traficom. 2021. Kauppamerenkulun tuet. Viitattu 23.11.2021. Saatavissa https://www.traficom.fi/fi/traficom/tietoa-traficomista/kauppamerenkulun-tuet

Traficom. Kyberturvallisuuskeskus. 2020. Kyberturvallisuus ja yrityksen hallituksen vastuu. Viitattu 12.10.2021. Saatavissa https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Traficom. 2020. Merenkulun kyberturvallisuustilaisuus 11.9.2020. Viitattu 13.10.2021. Saatavissa https://www.traficom.fi/fi/ajankohtaista/tilaisuudet/merenkulun-kyberturvallisuustilaisuus-1192020

Traficom. 2021. Tekoälyn soveltamisen kyberturvallisuus ja riskienhallinta. Viitattu 22.11.2021. Saatavissa https://www.traficom.fi/sites/default/files/media/publication/Teko%C3%A4lyn%20soveltamisen%20kyberturvallisuus%20ja%20riskienhallinta.pdf

Tuomaala, E. 2021. Kyberhyökkäyksen uhka kasvaa merillä ja satamissa – kaikkia suurimpia konttivarustamoja on jo yritetty hakkeroida. Viitattu 28.9.2021. Saatavissa https://yle.fi/uutiset/3-11894409

Tuomala, V. 2020. Kyberhyökkäykset merenkulun suurin turvallisuusuhka. Viitattu 22.9.2021. Saatavissa https://read.xamk.fi/2020/logistiikka-ja-merenkulku/kyberhyokkaykset-merenkulun-suurin-turvallisuusuhka/

Tuomala, V. 2021. Merenkulun kyberturvallisuus huomioitava aluksissa ja varustamoissa. Viitattu 13.12.2021. Saatavissa https://read.xamk.fi/2021/logistiikka-ja-merenkulku/merenkulun-kyberturvallisuus-huomioitava-aluksissa-ja-varustamoissa/

Tuulaniemi. 2020. Katsaus merenkulun kyberuhkiin. Viitattu 13.10.2021. Saatavissa https://www.traficom.fi/sites/default/files/media/file/2.%20Katsaus%20merenkulun%20kyberuhkiin%2020200911.pdf

Webroot. What is Social Engineering? Viitattu 15.11.2021. Saatavissa https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering