Opinnäytetyö (AMK)

Tradenomi (AMK), liiketoiminnan logistiikka

2025

Aldijana Hukic & Tom Merikanto

Autonomisten ja miehitettyjen merialusten turvallisuus

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Liiketoiminnan logistiikka

2025 | 59 sivua

Aldijana Hukic & Tom Merikanto

Autonomisten ja miehitettyjen merialusten turvallisuus

Opinnäytetyön tarkoituksena oli analysoida riskejä miehitetyillä ja autonomisilla merialuksilla sekä selvittää ihmisten aiheuttamien uhkien kohdistumista aluksiin ja niiden mahdollista ennaltaehkäisyä. Merenkulun ollessa tärkeää markkinoille, on tärkeää katsastella turvallisuuden tilannetta muuttuneen geopoliittisen sekä globaalin turvallisuuden tilanteessa.

Työ toteutettiin kirjallisuuskatsauksena, jonka myötä perehdyttiin kansainvälisten organisaatioiden ohjeistuksiin, lakeihin sekä määräyksiin. Näiden lisäksi perehdyttiin aiheeseen liittyviin tutkimuksiin ja artikkeleihin. Työssä perehdyttiin autonomisten alusten laitteistoihin sekä verkostoihin kohdistuviin hyökkäyksiin. Miehitettyjen alusten suhteen perehdyttiin laivan fyysiseen pääsyyn.

Tutkimustuloksesi selvisi, että merenkulun turvallisuuden parantamisen eteen on tehty paljon töitä, pysyvää korkeampaa turvallisuustasoa ei ole kuitenkaan saavutettu vaan vallitsevan turvallisuustason ylläpito ja parantaminen vaatii jatkuvaa kansainvälistä työtä. Autonomian ja muun teknologian huomioiminen ja hyödyntäminen on näissä pyrkimyksissä avainasemassa sen kehittyessä jatkuvasti.

Asiasanat:

autonomia, terrorismi, piratismi, merenkulku, riskianalyysi, ennaltaehkäisy

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Business Logistics

2025 | 59

Aldijana Hukic & Tom Merikanto

Security of autonomous and manned ships at sea

The purpose of this thesis was to analyze the risks of manned and unmanned ships and what type of human-based threats they face and how to prevent them. Because of the importance of sea logistics to the markets it is important to investigate the level of security in this changed situation of geopolitics and global security.

This work was done using the literature review method, most of the source material was guides, laws, orders made by international organizations. Source material also includes research and articles from the field. The focus of this thesis on autonomous ships was attacks that happen to the software or networks. The manned ships side was focused on attacks that involve physical access to the ship.

The study found out that there has been a lot of work done to make the seas safer, but there is yet to be any long-lasting changes and upholding or bettering the security requires constant international cooperation. Consideration and making use of constantly evolving autonomy and technology plays a key role in this endeavor.

Keywords:

Autonomy, terrorism, piracy, shipping, risk analysis, prevention

Sisältö

Kuvat

Taulukot

1 Johdanto

Tämän työn tavoitteena on analysoida riskejä miehitetyillä ja autonomisilla merialuksilla. Maailman turvallisuuskuva on muuttunut paljon viime vuosien aikana. Merenkulku on tärkeää globaaleilla markkinoilla, mutta rahtialukset ja muu merellinen toiminta ovat joutuneet hyökkäyksen kohteiksi.

Työ toteutetaan kirjallisuuskatsauksena, jossa selvitetään millaisia ihmisten aiheuttamia uhkia aluksiin kohdistuu sekä miten niitä voidaan mahdollisesti ennaltaehkäistä. Autonomisten alusten suhteen keskitytään laitteistoihin ja verkostoihin kohdistuviin hyökkäyksiin. Miehitettyjen alusten tarkastelussa kiinnitettiin huomiota erityisesti siihen, miten laivaan päästään fyysisesti.

Työssä käytetään aineistona eri kansainvälisten organisaatioiden luomia ohjeistuksia, lakeja ja määräyksiä sekä aiheesta tehtyjä tutkimuksia ja artikkeleita. Aiheen välittömän ajankohtaisuuden vuoksi lähteinä on voitu käyttää luotettavia uutislähteitä kertomaan tuoreista tapahtumista, joista ei vielä ole saatavilla tieteellistä tekstiä.

2 Tutkimusmenetelmät

Työ toteutettiin kirjallisuuskatsauksena, jonka tarkoituksena oli koota yhteen eri lähteiden julkaisemaa tietoa. Työssä käytettiin kvalitatiivista tutkimusmenetelmää, jossa keskityttiin kansainvälisten organisaatioiden ja muiden luotettavien lähteiden analysointiin.

Kirjallisuuskatsaus voidaan jakaa kolmeen alatyyppiin, kuvaileva kirjallisuuskatsaus, systemaattinen kirjallisuuskatsaus sekä meta-analyysi. Kuvaileva kirjallisuuskatsaus on tyypiltään yleiskatsauksellinen, eikä siinä ole tarkkoja metodillisia sääntöjä ja aineistoa haetaan laajasti. Tutkimuskysymys on usein väljempi verrattuna muihin kirjallisuuskatsauksen alatyyppeihin. Systemaattinen kirjallisuuskatsaus keskittyy tiivistämään ennalta määritellystä aihepiiristä löytyvien tutkimusten keskeisimpiä tuloksia. Systemaattisessa kirjallisuuskatsauksessa aineisto on tiiviimmässä ja tieteellisemmässä muodossa kuin kuvailevassa kirjallisuuskatsauksessa. Selkeä raportointi ja tieteellisyys tekee tästä tyypistä hyvän hypoteesien testaamiseen ja lähteiden johdonmukaisuuden arviointiin. Meta-analyysissa pyritään saamaan laajasta määrästä lähteitä numeraalisia ja hyvin tarkkoja analyysin tuloksia. Tässä kirjallisuuskatsauksen tyypissä on tarkasti rajatut metodit ja tavat, miten analyysia suoritetaan. (Salminen 2023, 7–8, 15–16, 20–23.)

Työssä käytetään kuvailevaa kirjallisuuskatsausta tutkimuskysymyksen laajuuden vuoksi. Turvallisuus merellä globaalissa skaalassa rakentuu monesta osasta ja tarkkaa analyysia turvallisuudesta on vaikeaa tehdä eri alueiden poliittisten ja turvallisuustasojen vaihtelun vuoksi.

3 Meriliikenteen merkitys

Meriliikenteellä tarkoitetaan kaikkea meriteitse tapahtuvaa liikennettä. Meriliikenne kattaa noin 90 % maailmankaupan kuljetuksista. Meriteitse kulkee sekä tavara- että matkustajakuljetuksia. Meriliikennettä on käytetty jo vuosisatojen ajan tavaroiden ja ihmisten kuljettamiseen, ja vuosien myötä se on kehittynyt suuresti. Meriliikenteen kehittyminen on seurannut kansainvälisen kaupan kehitystä ja jatkuvasti kasvavan tavaranvaihdon kehittymistä maiden välillä. Meriliikenne on yksi tärkeimmistä kuljetusvälineistä raaka-aineiden kuljettamiseen pitkän matkan päähän. Tämän takia meriliikenne on tilastollisesti katsottuna ympäristöä vähiten vahingoittava kuljetusmuoto, kun huomioidaan sen tuoma arvo. (IMO 2019; Ceva logistics 2024.)

Globalisaation myötä yhä suurempi osa valmistavan teollisuuden yrityksistä ovat siirtäneet tuotantolaitoksiaan ulkomaille, mikä lisää toimivan meriliikenteen ja satamatyön merkitystä. Osa toimivaa meriliikennettä on kuljetusten luotettavuus, sillä huono luotettavuus kuljetuksissa kasvattaa yritysten varastointikuluja turhaan. (Munim & Schramm 2018.)

Suezin kanava ja sen ympäristö muodostavat merkittävän alueen kaupankäynnille. Tätä aluetta ympäröivät maat, kuten Irak ja Jemen, ovat kuitenkin epävakaita ja levottomia, mikä on aiheuttanut väkivaltaisuutta ja rikollisuutta etenkin Punaisellamerellä. Maiden kansainvälisestä yhteistyöstä huolimatta levottomuuksia ja meriliikenteeseen kohdistunutta rikollisuutta ei ole saatu poistettua kokonaan. (Chorev 2023.)

Yhtenä ajankohtaisena esimerkkinä voidaan esittää Iranin tukema Huthi-niminen terrorismiryhmä, joka on hyökännyt kauppa-alusten kimppuun eri keinoin vuoden 2023 marraskuusta lähtien. Näiden hyökkäysten seurauksena alukset ovat alkaneet kiertää Suezin kanavaa Afrikan eteläisen kärjen, Hyväntoivonniemen kautta. Tämä uusi reitti lisää matkaa 4 000 mailia (6 400 km) ja matkan kestoa jopa 10 päivää per suunta. Uusi reitti kuluttaa huomattavasti polttoainetta ja välillisenä vaikutuksena nostaa hintoja. (Chang 2024.)

4 Autonomia

Autonomialla ei ole yksiselitteistä määritelmää, mutta sillä voidaan tarkoittaa muun muassa itselainsäädäntöä, itsehallintoa tai itsemääräämisoikeutta. *Autonomian* käsite tuli ensimmäisen kerran esiin antiikin Kreikassa, jossa se luonnehti itsehallinnollisia kaupunkivaltioita. (Iep 2024.) Merenkulun autonomialla tarkoitetaan alusten ja järjestelmien kykyä itsenäiseen tai puoli-itsenäiseen toimintaa ilman ihmisen suoraa väliintuloa. Kyseinen konsepti kattaa erilaisia teknologioita ja sovelluksia, kuten esimerkiksi robotiikkaa, tekoälyä, navigointijärjestelmiä sekä viestintäteknologioita, joiden avulla aluksen on mahdollista suorittaa tehtäviä itsenäisesti ilman miehistön jatkuvaa valvontaa. (SEAM 2024.)

4.1 Autonomian kehitys

Konsepti autonomisista laivoista tuli esille ensimmäisen kerran 1970-luvulla Rolf Schonknechtin kirjassa ”Ships and shipping of tomorrow”. Kirjassa mainitaan siitä, kuinka kapteenit aikovat tulevaisuudessa hoitaa työnsä maalla sijaitsevassa toimistorakennuksessa ja että aluksia aiotaan ohjata tietokoneiden avulla. (Infomaritime 2018.)

Japanissa toteutettiin vuosina 1983–1988 projekti nimeltään ”Japanese intelligent ship project”, jonka tarkoituksena oli kehittää luotettavia laitoksia ja automaattisia käyttöjärjestelmiä merialalla. Kyseisen automaattisen käyttöjärjestelmän kehittämisellä pyrittiin yhdistämään meri- ja maapuolen osia, kuten avomeren laivaliikennettä, satamaan saapumista, irtautumista, ankkurointia sekä lastinkäsittelyä. Järjestelmän suunniteltiin toimivan ilman miehistön vuorovaikutusta ja saavan tukea maalla sijaitsevasta järjestelmästä, joka on yhteydessä satelliittien kautta. Projektin lopussa vuonna 1988 simuloitiin myös kaikki järjestelmät tietokoneelle. (Infomaritime 2018.)

Korean tutkimuslaitos KRISO (*Korea Research Institute of Ship & Ocean Engineering*) aloitti vuonna 2011 projektin nimeltään ”Autonomous unmanned

surface vessels (USV) for maritime survey and surveillance”, jonka tarkoituksena oli kehittää autonomisia miehittämättömiä aluksia meritutkimuksiin ja valvontaan. Projekti käsittelee myös kansallisia kysymyksiä kehittämällä ja tutkimalla teknologiaa ”ympäristöystävällisen tulevaisuuden meriteknologian, laivojen ja valtameritekniikan, merionnettomuuksien torjunnan ja meriliikennejärjestelmäteknologian sekä vedenalaisen robotin ja merenkulun laiteteknologian” aloilla. (Infomaritime 2018.)

Vuonna 2012 EU lanseerasi projektin nimeltään MUNIN (*Maritime Unmanned Navigation through Intelligence in Networks*), jonka tarkoituksena oli tutkia miehittämättömien alusten teknistä, taloudellista ja oikeudellista toteutettavuutta. MUNIN-projektin tavoitteena oli kehittää ja todentaa konsepti autonomisille aluksille, joita pääasiassa ohjaavat automatisoidut aluksen sisäiset päätöksentekojärjestelmät, mutta joita ohjaavat myös maalla sijaitsevat valvonta-asemilla olevat kauko-operaattorit. (Infomaritime 2018.)

DNV-GL käynnisti vuonna 2013 uuden konseptin miehittämättömästä laivasta nimeltään ReVolt. Konsepti oli tarkoitettu nollapäästöisille lyhyen matkan akkuvirralla toimiville miehittämättömille aluksille. Aluksen kantavuus on 1 800 dwt, joka tarkoittaa aluksen kuollutta painoa, ja kapasiteetti on 100 TEU, joka puolestaan on konttiliikenteen perusmittayksikkö. (Infomaritime 2018.)

Vuonna 2013 myös Norja otti osaa autonomisen miehittämättömän aluksen järjestelmään perustamalla AMOS-konseptin (*Centre for Autonomous Marine Operations and Systems*), jonka tavoitteena oli luoda maailman johtava autonomisten merioperaatioiden ja valvontajärjestelmien keskus (Infomaritime 2018).

Rolls-Royce aloitti vuonna 2015 hankkeen nimeltään AAWA (*Advanced Autonomous Waterborne Applications initiative*), jonka tavoitteena oli analysoida autonomiseen merenkulkuun liittyviä haasteita eri tieteenaloilla. Hanke kehitti sekä autonomisella että etäohjauksella tapahtuvaa toimintaa laivojen navigointiin, koneisiin ja kaikkiin aluksella oleviin käyttöjärjestelmiin.

Rolls-Royce esitteli myös jo vuonna 2017 maailman ensimmäisen kauko-ohjattavan kauppalaivan. (Infomaritime 2018.)

Vuoden 2017 lopuilla Korea testasi ensimmäistä korealaisella teknologialla kehitettyä miehittämätöntä alusta ”Aragon II” -merikokeessa onnistuneesti (Infomaritime 2018).

4.2 Automaation tasot

Automaation tasot voidaan jakaa kolmeen eri ulottuvuuteen, joita ovat kompleksisuus, miehistön taso sekä autonomian taso. Kompleksisuudella tarkoitetaan aluksen toimintaympäristön monimutkaisuutta eli sitä, toimiiko alus suojaisilla tai avoimilla merialuilla, millaiset ovat sää- ja näkyvyysvaikutukset, onko alueella muuta liikennettä ja miten reittien varrella olevat esteet voivat vaikuttaa aluksen reittiin. (Porathe, Hoem, Johnsen & Rødseth 2018, 418.)

Miehistön kannalta aluksella voi olla jatkuvasti miehitetty komentosilta, mutta alus edelleen omaa autonomian automatisoidussa kohteiden havaitsemisessa ja törmäyksen välttämisessä. Aluksiin on mahdollista ennakoida riittävän määrän autonomiaa, jotta miehistö voi nukkua yöllä laivan purjehtiessa avoimilla vesillä hyvällä säällä. (Porathe ym. 2018, 419.)

Autonomian tasolla tarkoitetaan sitä, miten alukset hoitavat toimintojaan itse automatisoinnin myötä. Autonomian alimmalla tasolla aluksen operointi on miehistön hallinnassa, ja järjestelmät tarjoavat päätöksentekotukea tai hyvin vähäistä automaattiohjausta, kuten autopilottia. Toisella tasolla aluksen toimintaa ja navigointia hoitaa automaatio ja miehistö puuttuu sen toimintaan tarvittaessa. Kolmannella tasolla alus on osittain autonominen ja se voi suorittaa tiettyjä tehtäviä itsenäisesti, esimerkiksi kulkea avomerellä hyvällä säällä. Tätä voidaan hyödyntää ajoittaiseen miehittämättömään komentosiltaan. Neljännellä tasolla alus on täysin autonominen ja se hoitaa kaikkia tehtäviä itsenäisesti kokonaan ilman miehistön väliintuloa. (Porathe ym. 2018, 419–420.) Kyseisiä tasoja voidaan tarkastella Traficomin laatiman taulukon avulla, jossa on kuvattu automaationtasoja aluksen matkan eri vaiheissa.

Traficom on luonut Porathen autonomian tasojen määritelmän perustella taulukon, jossa on kuvattu, kuinka kyseiset automaation eri tasot toimivat aluksen matkan eri vaiheissa sekä poikkeustilanteessa. Taulukon avulla voidaan havainnollistaa, millaisissa vaiheissa, tilanteissa sekä päätöksenteossa on mahdollista hyödyntää autonomiaa ja millaisissa puolestaan tarvitaan edelleen miehistöä. (Traficom 2019, 6.)

Taso	Satama-manöveeraus	Rannikko- ja saaristonavi-gointi	Avomeri-navigointi	Poikkeus-tilanteet
1	Operointi ja päätöksenteko tapahtuu aluksen miehistön toimesta	Operointi ja päätöksenteko tapahtuu aluksen miehistön toimesta	Operointi ja päätöksenteko tapahtuu aluksen miehistön toimesta	Operointi ja päätöksenteko tapahtuu aluksen miehistön toimesta + esim. MIRG
2	Operointi ja päätöksenteko tapahtuu aluksen miehistön toimesta	Operointi ja päätöksenteko tapahtuu aluksen miehistön toimesta	Operointi ja päätöksenteko tapahtuu etäohjauksena maista	Operointi ja päätöksenteko tapahtuu aluksen miehistön toimesta + esim. MIRG
3	Operointi ja päätöksenteko tapahtuu etäohjauksena maista	Operointi ja päätöksenteko tapahtuu etäohjauksena maista	Alus operoi autonomisesti	Operointi ja päätöksenteko tapahtuu etäohjauksena maista
4	Alus operoi autonomisesti	Alus operoi autonomisesti	Alus operoi autonomisesti	Alus operoi autonomisesti

Taulukko 1. Automaatiotasot aluksen matkan eri vaiheissa ja poikkeustilanteissa (Traficom 2019).

4.3 Automaation riskejä

Automaatio voi johdattaa turvallisempaan ympäristöön, sillä sen on mahdollista korjata ja käsitellä inhimillisiä puutteita, kuten väsymystä, tarkkaavaisuutta, informaation ylikuormitusta sekä onnettomuuksien mahdollisuutta. Uuden teknologian myötä kehittyy myös uudentyyppisiä onnettomuuksia. Tutkimuksien tulokset (Wróbel, Montewka & Kujala 2017) osoittivat, että navigointiriskit, kuten törmäys ja karille ajo, voivat vähentyä ja muut kuin navigointiriskit puolestaan lisääntyvät autonomisilla aluksilla. Kyseisiä riskejä ovat muun muassa tulipalo, räjähdys sekä tulvat. (Mingyu, Tae-Hwan, Byongug & Han-Seon 2020, 21–22.)

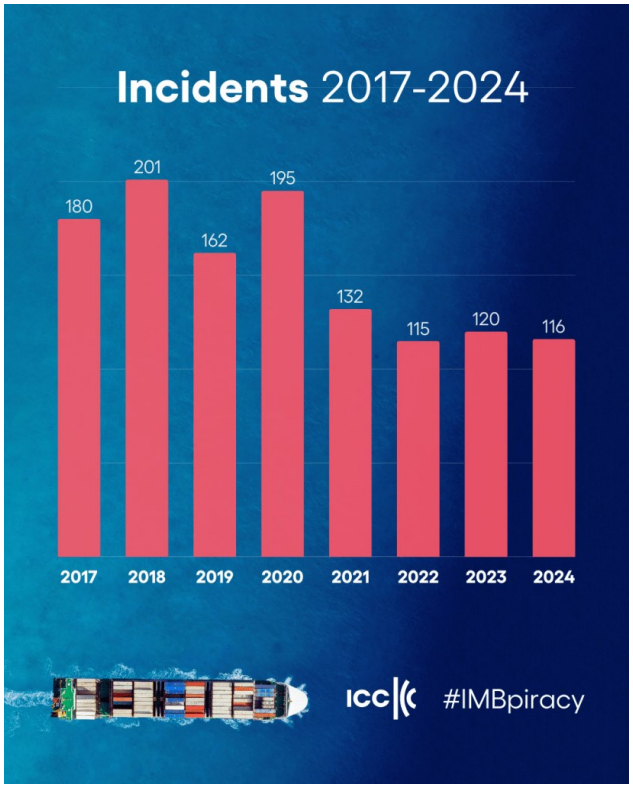
Koska autonomiset alukset ovat riippuvaisia ohjelmistoista ja liitettävyydestä, on kyberturvallisuuden riski noussut esiin niiden kauko-ohjauksessa ja hallinnassa. Kun alukset ovat riippuvaisia tietoteknisistä järjestelmistä sekä aluksella että maalla, tulevat kyberhyökkäykset kohdistumaan todennäköisemmin niihin kuin perinteisiin aluksiin. Kyberterroristien on mahdollista hakkeroida tietoyhteys päästääkseen etäohjaukseen ja aluksen hallintaan. (Mingyu ym. 2020, 22.)

Yritykset ovat ottaneet käyttöön kehittyneitä uusia teknologioita parantaakseen liiketoiminnan suorituskykyä, alentaakseen kustannuksia sekä tehostaakseen turvallisuutta. Teknologioiden kehittämiseen ja hyödyntämiseen kuluu vähemmän aikaan kuin sääntelyviranomaisten kykyyn kehittää uusia käytäntöjä ja standardeja. Tämä voi aiheuttaa haavoittuvuuksia ja teknologioiden kehityksen hidastumista tai jopa estymistä. Meriliikenteessä vastuu on tavallisesti liitetty ihmisiin tai organisaatioihin, kuten varustamoihin. Vastuuta on vaikea kohdistaa algoritmiin väärinkäytöksen suhteen, sillä sitä ei pidetä moraalisena tai laillisena toimijana. Kyseistä haastetta käsitellään eri autonomisten yritysten ympärillä ja sen myötä turvallisuudesta käytävässä keskustelussa testataan yleisempiä moraalisia pulmatilanteita. (Mingyu ym. 2020, 23.)

Autonomisten alusten kehittämis- ja käyttöönottoprosessissa odotetaan nousevan esille monia eettisiä kysymyksiä. Aiemmin viestintä aluksen toiminnasta on ollut ihmisen vastuulla, kun tulevaisuudessa sen odotetaan monipuolistuvan ihmisen ja koneen sekä koneiden väliseen viestintään. Tämän myötä on tarpeen tarkastella erilaisia skenaarioita, joissa viestintä koneiden kanssa epäonnistuu tai katkeaa. Sellaisen teknologian, jonka on mahdollista vastata kaikkiin mahdollisiin skenaarioihin, on haastava kehittää. Tämän myötä oikeudellisen vastuun rajaaminen on toinen huoleen aihe. Erityisesti kohtuullisten kriteerien ja vastuun laajuuden määrittäminen laivanvarustajan ja valmistajan välillä on ongelmallista, mukaan lukien asianmukainen turvarakenne vakuutusturvaa varten. (Mingyu ym. 2020, 23.)

5 Uhkien määritelmät

Meriliikenteen suuren globaalin kaupan roolin vuoksi kuljetusten ja satamien toiminnan turvaaminen on elintärkeää. Merellinen uhka ei ole uusi, vaan esimerkkejä terroristisista teoista aluksia kohtaan löytyy vuosikymmenen takaa. Terrorismi ei ole ainoa uhka, joka aluksiin ja satamiin kohdistuu, vaan myös piratismi ja järjestäytynyt rikollisuus, kuten salakuljetus ja salamatkustus, ovat asioita, joihin varustamoiden täytyy varautua. IMB on kerännyt tietoa raportoiduista piratismi hyökkäyksistä vuosilta 2017–2020.



Kuva 1. Piratismi hyökkäysten määrä vuositasoilla (International Chamber of Commerce 2025).

Kuvassa kuvataan sitä, miten hyökkäykset ovat laskeneet 2020-luvun alussa verrattuna 2010-luvun loppuun. Tämä on seurausta kollektiivisista toimista piratismia vastaan. Vaikka tapahtumien määrä on laskenut, niiden aggressiivisuus ja vaara miehistölle ovat nousseet. Yhä useammissa

hyökkäyksissä otetaan panttivankeja tai kidnapataan miehistön jäseniä. (International Chamber of Commerce 2025.)

5.1 Terrorismi

Kansainvälisesti terrorismilla ei ole yhteistä sovittua määritelmää ja jokaisella maalla on omat lakinsa sen määrittelemiseksi. Laaja kuvaus terrorismista kuitenkin on seuraava: Väkivallan tai väkivallan uhan käyttö omien tavoitteiden saavuttamiseksi tai pelon aiheuttamiseksi. Suurin ero terrorismin ja piratismin välillä on motiivit; terroristeillä tekojen takana toimivat aatteelliset motiivit. (Lucas, Rivera-Paez, Crosbie & Jensen 2020; Sisäministeriö 2024b.)

5.1.1 Terrorismin vaikutukset

Terrorismilla on laaja-alaisia vaikutuksia yrityksiin ja yhteiskuntaan. Yrityksillä tappiot koostuvat lähinnä menetetystä tavarasta ja hyökkäyksien epäsuorista vaikutuksista, kuten myöhästymisestä. Terroristiset hyökkäykset ovat luonteeltaan hyvin julkisia. Tämän vuoksi myös yritykset, jotka eivät ole hyökkäyksen kohteena tai kärsi epäsuorista vaikutuksista, alkavat panostamaan turvallisuuteen mahdollisten hyökkäysten varalta. Nämä investoinnit ovat aina pois muista investoinneista, jotka parantaisivat yrityksen tuottavuutta. Yritykset voivat myös joutua nostamaan hintoja asiakkailleen. Pelkkä terrorismin pelko vaikeuttaa markkinoiden tilannetta, sillä globaalit sijoitukset vähenevät. Pelko muuttaa myös ihmisten kulutustottumuksia, mikä saattaa vaikeuttaa joidenkin yritysten toimeentuloa. Tämä mittava terrorismista aiheutuva kulurakenne pakottaa kärsivät yritykset nostamaan hintojaan, mikä johtaa hintojen nousuun globaalisti, sillä yritykset eivät halua pienentää voittomarginaalejaan. (Tauringana, Tingbani, Okafor & Sha’ven 2020, 5639.)

Kaikki yritykset eivät kuitenkaan kärsi tällaisista tragedisista tapahtumista, vaan epävarmuus herättää yritykset kehittämään toimintaansa, jotta se selviää paremmin tulevista haasteista. Turvallisuusalan yritykset voivat hyötyä ihmisten

turvattomuuden tunteesta. Esimerkiksi syyskuun 11. päivän terrori-iskujen jälkeen turvallisuusalan ja teknologia yritysten tilanne ja kysyntä paranivat huomattavasti. (Tauringana ym. 2020, 5639.)

5.1.2 Terrorismin tapoja

Terroristiset ryhmät käyttävät monenlaisia tapoja aiheuttaakseen vahinkoa kohteilleen. Yleisempiä tapoja ovat aseelliset kaappaukset, panttivankien ottaminen ja erilaiset räjähteillä tehdyt hyökkäykset. (Schneider 2022, 110–111.) Esimerkkejä räjähteiden käytöstä ovat erilaiset lennokit, jotka kuljettavat räjähteet kohteeseen. Tällaisia lennokkeja on niin ilmassa kulkevia kuin myös veneitä, joita ohjataan kauko-ohjauksella. Nykypäivänä suurin uhka on vuoden 2023 lopulla nousseen Huthi-järjestön tekemät ohjusiskut ballistisilla ja risteilyohjuksilla. Nämä ohjukset luovat erityisen haasteen alusten kululle Punaisenmeren kautta, sillä vaikka kauppa-alukset pystyvät käyttämään erilaisia metodeja torjuakseen aluksen valtaukseen pyrkiviä hyökkäyksiä, niiltä uupuu laitteistoa ohjusten torjumiseen. Eri maiden laivastojen aluetta rauhoittamaan lähetetyt taistelualukset toki pystyvät suojaamaan itseään ja kauppa-aluksia kalustollaan, mutta niilläkin on vain rajattu määrä torjuntaohjuksia. (Haugstvedt 2021.) Verrattuna piratismiin terroristeilla on yhä enemmän nykyaikaista teknologiaa käytettävissä sekä suurempaa ja parempaa kalustoa. Tästä hyvänä esimerkkinä on Huthien tekemä hyökkäys rahtialukseen vuoden 2023 marraskuussa, jossa käytettiin armeijatason helikopteria alustavassa hyökkäyksessä. (The Maritime Executive 2024.)

5.2 Piratismi

Piratismi on ollut merta seilaavien alusten kiusana jo satoja vuosia. Se on kuitenkin lisääntynyt ja kehittynyt toimintatavoiltaan, minkä vuoksi on pyritty luomaan kansainvälistä koodistoa ja toimintatapoja sen määrittelemiseksi ja ennaltaehkäisemiseksi. Tästä ei ole kuitenkaan päästy vain yhteen määritykseen, vaan määritelmä riippuu kunkin maan omista laeista. Yhtenä

määritelmänä pidetään yksityishenkilön tai -henkilöiden tekemiä hyökkäyksiä aluksella toiseen alukseen, joiden motivaationa on omat henkilökohtaiset tavoitteet. Tämän määritelmän suurin kiistanaihe on, että se rajaa ulkopuolelleen valtioiden sponsoroimat hyökkäykset, joissa valtiolla on omat motivaationsa. (Ahmad 2020, 1.)

5.2.1 Piratismin vaikutukset

Piratismin korkea uhka lisää varustamoiden kustannuksia aina työntekijöiden palkkavaatimuksista nousseihin vakuutusmaksuihin. Näiden kustannusten vähentäminen on vaikeaa, sillä mikäli halutaan kiertää vaarallisin alue eli Suezin kanavan ja Somalian rannikko, matkan kesto pitenee huomattavasti, mikä lisää polttoainekuluja ja työntekijöiden työtunteja. Laivan matkan kaikki kustannukset jaetaan konttien hintoihin, joten kaikki nousseet kustannukset vaikuttavat suorasti muiden yritysten maksamiin rahdin hintoihin. (Sandkamp, Stamer & Yang 2022.)

5.2.2 Piratismin tavat

Piratismin määritelmään sisältyvien hyökkäysten tavoitteet jaetaan tyypillisesti kahteen tapaan, aluksen valtaus ja lunnaiden vaatiminen panttivankien vapauttamiseksi tai aluksen tilapäinen valtaus ja materiaalin ryöstö laivasta. Joillain alueilla, missä piratismia esiintyy, on kohdattu myös tapauksia, joissa vain yksi aluksen miehistön jäsen kidnapataan ja hänen vapauttaan vastaan vaaditaan lunnaita. (Frane, Miskovic & Pavic 2023.)

Länsi-Afrikan alueella raportoitiin vuosina 2019–2020 172 hyökkäystä, joista 89 (51,7 %) oli tavoitteiltaan onnistuneita. Tämä alue on miehistölle vaarallisin muihin alueisiin verrattuna, joissa piratismia esiintyy, sillä tällä alueella hyökkäykset ovat aggressiivisempia ja motivoituneempia. Myöskään yksityisistä yrityksistä palkatut aseelliset vartijat eivät ehkäisseet hyökkäyksiä ja loukkaantumisia ja kuolemia tapahtuu enemmän kuin muilla alueilla. Yleisimmät

hyökkäysmuodot olivat arvotavaran ryöstö ja yksittäisten miehistön jäsenten kidnappaus. (Frane ym. 2023.)

5.3 Järjestäytynyt rikollisuus (JR)

Rikoksiksi määritellyt teot vaihtelevat paljon maiden omien lakien mukaan. Järjestäytyneen rikollisuuden määritelmä on kuitenkin maailmanlaajuisesti yhteinen; ryhmä ihmisiä, jotka suorittavat organisoidusti ja järjestelmällisesti rikollista toimintaa. Toiminnan motiivina toimii useasti taloudellisen hyödyn tavoitteleminen. (Sisäministeriö 2024a.)

Tällaiset rikollisryhmittymät ovat hyvin organisoituja ja pystyvät käyttämään hyväkseen maailmalla tapahtuvia kriisejä, kuten taloudellista epävarmuutta ja luonnonkatastrofeja. Maailmanlaajuiset rikollisjärjestöt ovat vaikeita toimijoita estettäväksi, sillä monesti yksi rikosepäily ulottuu moneen maahan ja todistajien tai todisteiden hankkiminen voi olla tämän vuoksi hankalaa. (United Nations 2024.)

5.3.1 Järjestäytyneen rikollisuuden vaikutukset

Kaikista rikollisuuden muodoista, jotka luovat riskejä merikuljetuksille järjestäytyneellä rikollisuudella on suurin vaikutus myös muualle yhteiskuntaan mm. seuraavilla tavoilla (IMO 2023.):

- Ekonomian heikentyminen: JR toiminnan ehkäisy vie resursseja erilaisilta toimijoilta kuten yritykset ja viranomaiset. Se myös ohjaa rahan suuntautumista pimeille markkinoille, joka heikentää ekonomista kasvua, kun laillisiin markkinoihin ei sijoiteta.
- Väkivalta ja sen uhka: JR ryhmät käyttävät useasti väkivaltaa ja sen uhkaa vallan saamiseksi. Tämä voi johtaa turvattomaan ja epävarmaan työympäristöön, joka huonontaa työntekijöiden elämänlaatua.
- Julkinen terveys: Järjestäytyneellä rikollisuudella, etenkin huumekaupalla on suuria vaikutuksia yhteiskunnan terveyteen. Kun salakuljetetut

huumeet päätyvät maahan, niin käyttäjät kuin myös läheiset joutuvat kärsimään.

5.3.2 Erilaisia rikoksia merikuljetuksissa

Rikollisjärjestöt ovat olleet pitkään suuri osa laitonta maahanmuuttoa avustaen ihmisiä, jotka haluavat lähteä maasta. Useimmiten motivaationa lähdölle toimii pelko oman hengen puolesta tai toivo paremmasta elämästä. Koska oma henki voi olla vaarassa, ihmiset usein turvautuvat mihin tahansa tarjolla olevaan keinoon maasta poistumiseksi. Tätä rikollisjärjestöt käyttävät hyväksi laiminlyömällä turvallisuutta. (Papastavridis 2014.)

Salakuljetus, erityisesti huumeiden salakuljetus on suuri ongelma kaupallisille aluksille. Salakuljetus kattaa kaikkien tavaroiden laittoman maahantuonnin, rikollisjärjestöt harjoittavat kuitenkin eniten huumeiden salakuljetusta. (Papastavridis 2014.)

5.4 Kyberuhka

Meriliikenteen kyberriskillä tarkoitetaan sitä mittaa, millä mitataan missä määrin olosuhde tai tapahtuma voi uhata teknologiaomaisuutta, joka voi puolestaan johtaa merenkulkuun liittyviin toiminta-, turvallisuus- tai turvahäiriöihin, jotka johtuvat tietojen tai järjestelmien korruptoitumisesta, katoamisesta tai vaarantumisesta. (IMO 2024a.)

5.4.1 Kyberuhkan vaikutukset

Järjestelmät, jotka mahdollistavat merikuljetusjärjestelmän toiminnan ovat yhä enemmän riippuvaisempia tietokoneista ja verkoista, joka puolestaan tuo mukanaan uusia haavoittuvuuksia ja lisää riskiä. Kyseisen haavoittuvuuden takia kyberjärjestelmien hyväksikäyttö, väärinkäyttö, häiriöt tai yksinkertainen vika voivat aiheuttaa loukkaantumisen tai kuoleman, vahingoittaa

meriympäristöä, häiritä kaupankäyntiä ja heikentää kykyä reagoida muihin hätätilanteisiin. (Maritime-cybersecurity 2024.)

5.4.2 Kyberuhan tapoja

Merkittäviä autonomisia laivoja ympäröivät uhat voidaan luokitella yhdeksään kategoriaan kuten hyökkäykset RF eli radiotaajuus signaalien häiritsemiseksi, sensoreiden huijaamiseen, viestinnän katkaisemiseksi tai muuntamiseksi, OT eli operatiivisiin teknologiajärjestelmiin, IT eli tietoteknisiin järjestelmiin, autonomisiin operaatioihin käytettyä tekoälyä vastaan, toimitusketjujen kautta, fyysisen pääsyn kautta sekä rannikon valvontakeskukseen. (CCDCOE 2022, 3.)

6 Koodisto ja standardit

Merialueet ovat suurilta osin kansainvälisiä, eli mikään valtio ei omista niitä ja täten mikään maa ei voi asettaa näille alueille lakeja omalla päätöksellään. Alueiden luonteen vuoksi on perustettu kansainvälinen organisaatio, joka vastaa lakien laatimisesta ja jossa maat toimivat jäseninä. Myös EU on osana direktiivien ja standardien laatimista.

UN (United Nations) eli Yhdistyneet kansakunnat ovat nimittäneet IMO (International Maritime Organization) nimisen organisaation vastaamaan näiden lakien ja säädösten laatimisesta. Tämän organisaation modernin toiminnan perustana toimii vuonna 1982 käyttöön otettu Yhdistyneiden kansakuntien merioikeussopimus (UNCLOS) niminen asiakirja, jossa määritellään lain hallintoalue maailman merillä. Myös tätä ennen IMO on luonut esimerkiksi turvallisuuteen liittyviä koodistoja. Lait ja säädökset eivät ole rajattuja vain aikaisemmin käsiteltyihin rikoksiin vaan myös esimerkiksi ympäristö rikoksiin. (IMO 2024d.) Tässä työssä keskitytään nimenomaisesti turvallisuuteen ja aiemmin mainittuihin rikoksiin liittyviin säädöksiin.

ISPS-koodisto (International Ship and Port facility Security codes) on osa suurempaa SOLAS (International Convention for the Safety of Life at Sea) kokousta, jossa sovittiin merillä kulkemisen turvallisuudesta. Koodiston päätavoitteita on, luoda yhteiset toimintatavat kansainvälisesti kaikille sidosryhmille, selvittää vastuualueet alusten ja satamien turvallisuudesta sekä varmistaa, että turvallisuuteen panostetaan tarpeeksi ja informaation kulku näissä asioissa on sujuvaa. Koodisto voidaan jakaa pakolliseen ja ei pakolliseen osioon. Pakollisessa osiossa on turvallisuuteen liittyviä vaatimuksia satamille ja varustamoille. Toisessa ei pakollisessa osiossa on ohjeita, miten näihin vaatimuksiin on mahdollista päästä. (IMO 2024c.) Toisen osan ohjeita ei siis ole pakko noudattaa kirjaimellisesti vaan satamat ja varustamot voivat tehdä omia ratkaisujaan, kunhan ensimmäisen osan vaatimukset täyttyvät.

ISPS-koodiston pakollisen A-osan mukaan aluksille ja satamiin on määrättävä turvallisuudesta vastaava henkilö, jonka tehtävä on valvoa, että kaikkia

turvallisuuteen liittyviä määräyksiä noudatetaan. Yritykset määräävät vielä yrityksen oman turvallisuudestavastaavan henkilön, joka huolehtii kaikkien yrityksen alusten tai satamien turvallisuussuunnitelmien noudattamisesta ja päivittämisestä. Aluksessa ja satamassa on oltava turvallisuussuunnitelma, jonka virallisen taho on hyväksynyt. Turvallisuussuunnitelman pohjana käytetään niin sanottua turvallisuuskävelyä, jossa turvattava alue käydään läpi kohta kohdalta ja arvioidaan mahdolliset riskit. (ISPS CODE A 2024, 2–7.)

6.1 Aluksen turvallisuussuunnitelma

Turvallisuussuunnitelma on oltava käännettynä aluksen työskentelykielille ja mikäli mikään näistä ei ole englanti, ranska tai espanja, myös sille kielelle. Suunnitelman ei ole pakollista löytyä fyysisenä kopiona alukselta vaan elektroninen versio riittää. Tällöin tiedosto pitää suojata luvattomalta pääsyltä, editoinnilta ja poistolta ja sen on oltava henkilökunnan saatavissa. Aluksen turvallisuussuunnitelma tulisi pitää sisällään seuraavia asioita: (ISPS CODE A 2024 8–9.)

- Keinot, joilla estetään seuraavien asioiden tuonti alukselle: vaaralliset aineet, laitteet tai aseet, joilla voidaan aiheuttaa vahinkoa henkilölle, alukselle tai satamalle
- Rajatut alueet ja toimet luvattoman pääsyn ehkäisemiseksi sekä kulunvalvonta
- Toimintaohjeet turvallisuusuhkiin, mukaan lukien suunnitelma miten aluksen kriittiset toimet suoritetaan uhan aikana
- Evakuointisuunnitelma
- Laivan turvallisuusvastaavan nimi ja muiden turvallisuuteen liittyvien henkilöiden tiedot, mukaan lukien yrityksen turvallisuusvastaavan ympärivuorokautinen kontaktitieto
- Ohjeet hälytysjärjestelmien käyttöön ja niiden sijainnit aluksella

6.2 Maan riskitaso – MARSEC

ISPS-koodin mukaiset turvallisuustasot kuvaavat miten suuri riski aluksen vierailemassa maassa katsotaan olevan. Maan oman turvallisuustason määrittää sen hallitus ja viestii sen satamaoperaattorille. tämän jälkeen kukin alus yhdessä satamaoperaattorin kanssa sopivat alukselle soveliaan turvallisuustason, kuitenkin niin että sen on oltava sama tai korkeampi kuin valtion asettama taso. Tämä prosessi tehdään ennen satamaan saapumista ja aluksen turvallisuustaso näytetään selvästi sisäänkäynnin yhteydessä. Kukin taso on entistään tiukempi ja tuo mukanaan ennalta määriteltyjä vastuita miehistön jäsenille. (EduMaritime 2022.)

Taso 1

- Normaalit satamatoiminnot käynnissä
- Varmennetaan alukseen kulkevien henkilöllisyys
- Perusturvallisuus pidetään yllä kulunvalvonta, rahdinvalvonta ja minimaalinen liikenne edestakaisin aluksesta
- Normaali sataman ja aluksen lastaus- ja purkutoimintojen valvonta

Taso 2

- Otetaan käyttöön, kun on havaittu turvallisuusriski
- Lisätään valvontakierroksia aluksessa ja satamassa
- Turvallisuustarkastus alukseen kulkeville henkilöille
- Laivassa vieraileville saattajat, jotka kulkevat mukana koko vierailun ajan
- Aluksen osittainen tai täysvaltainen tarkastus
- Luodaan rajatun pääsyn alue aluksen ympärille

Taso 3

- Otetaan käyttöön vastauksena välittömään tai jo tapahtuneeseen uhkaan
- Normaalien satamatoimintojen keskeytyminen
- Alukseen pääsyyn ja poistumiseen oikeus vain rajatulla henkilöstöllä
- Viranomaisyhteistyö

- Aseistetut vartijat mikäli mahdollista
- Aluksessa olevien toimintojen tarkkailu
- Aluksen kokonaisvaltainen tutkinta
- Evakuointi tarvittaessa

6.3 Aluksen kyberturvallisuusvaatimuksia

IMO julkaisi vuonna 2022 riskienhallintaohjeen, jossa annetaan korkean tason suosituksia merenkulun kyberriskien hallinasta merenkulun turvaamiseksi nykyisiltä ja kehittyviltä kyberuhkilta sekä haavoittuvuuksilta. Suositukset sisältävät myös toiminnallisia elementtejä, jotka tukevat tehokasta kyberriskien hallintaa. (IMO 2024a.)

Kyberriskien hallinalla tarkoitetaan näissä ohjeissa prosessia, jossa tunnistetaan, analysoidaan, arvioidaan ja viestitään kyberriski sekä hyväksytään, vältetään, siirretään tai lievennetään sitä hyväksyttävälle tasolle ottaen huomioon sidosryhmille aiheutuvat kustannukset ja hyödyt. Kyberriskin hallinnan tavoitteena on turvallisen merenkulun tukeminen, joka kestää operatiivisesti kyberriskejä. Tämän myötä tehokas hallinta tulisi aloittaa ylimmän johdon tasolla, jonka tulisi sisällyttää kyberriskitietoisuuden kulttuuri organisaation kaikille tasoille ja varmistaa kokonaisvaltainen ja joustava kyberriskien hallintajärjestelmä, joka on jatkuvassa käytössä ja jota arvioidaan jatkuvasti tehokkaiden palautemekanismien avulla. (IMO 2022, 5.)

Ohjeissa mainitut toiminnalliset elementit eivät ole peräkkäisiä, joten niiden kaikkien tulisi olla käytännössä samanaikaisia ja jatkuvia sekä ne tulisi sisällyttää tarkoituksenmukaisesti riskienhallintakehykseen (IMO 2022, 5.):

- tunnistaminen: määritä henkilöstöroolit ja vastuut kyberriskien hallinnassa sekä tunnista järjestelmät, resurssit, tiedot ja kyvyt, jotka häirittynä aiheuttavat riskejä aluksen toiminnalle

- suojaaminen: toteuta riskienhallintaprosessit ja -toimenpiteet sekä varautumissuunnittelu kybertapahtumalta suojautumiseksi ja merenkulun jatkuvuuden varmistamiseksi
- havaitseminen: kehitä ja toteuta toimia, jotka ovat tarpeen kybertapahtuman ajoissa havaitsemiseksi
- vastaaminen: kehitä ja toteuta toimintoja ja suunnitelmia kestävyyden tarjoamiseksi sekä sellaisten järjestelmien palauttamiseksi, jotka ovat välttämättömiä merenkulun toiminnalle tai palveluille, jotka ovat heikentyneet kybertapahtuman vuoksi
- palautuminen: tunnista toimenpiteet, joilla tuetaan ja palautetaan kybertapahtuman kohteeksi joutuneet merenkulun kannalta välttämättömät kyberjärjestelmät

Kansainvälinen luokituslaitosten liitto (IACS) on julkaissut kaksi yhtenäistä vaatimusta (UR) vähentääkseen merenkulun kyberonnettomuuksien esiintymistä ja vaikutuksia: UR E26 – alusten kyberresilienssi ja UR E27 – alusten järjestelmien ja laitteiden resilienssi. UR:t pyrkivät asettamaan vähimmäisvaatimukset uusien alusten ja niihin liitettyjen järjestelmien kyberresilienssikyvyille. (Inmarsat 2024, 5.)

6.3.1 UR E26

UR E26:n ensisijainen tavoite on auttaa merenkulkualan organisaatioita luomaan ja ylläpitämään turvallista laivaympäristöä, joka perustuu tehokkaaseen kyberriskien hallintajärjestelmään. UR E26:n vaatimustenmukaisuuden osoittamiseen vaaditaan dokumentaatiota, joka liittyy aluksen elinkaaren kolmeen vaiheeseen: suunnitteluun ja rakentamiseen, käyttöönottoon sekä käyttöön. Vaatimusten noudattamisen osoittaminen kahdessa ensimmäisessä vaiheessa on järjestelmäintegroijan, joko laivanrakentajan tai nimetyn kolmannen osapuolen vastuulla, kunnes vastuu siirtyy aluksen omistajalle käyttövaiheessa. (Inmarsat 2024, 6.)

Suunnittelu- ja rakennusvaiheessa järjestelmien integroijan on toimitettava luokituslaitokselle kolme asiakirjaa (Inmarsat 2024, 6–7):

- Vyöhykkeet ja järjestelmäkaavio, joka sisältää selkeän kuvauksen turvavyöhykkeistä; yksinkertaistettu kuvaus kustakin tietokonepohjaisesta järjestelmästä, josta käy ilmi turvavyöhyke, jolle se on jaettu, sekä sen fyysinen sijainti; viittaus toimittajien antamiin tietokonepohjaisten järjestelmäkaavioiden hyväksyttyyn versioon; ja kuvaukset verkkoviestinnästä turvavyöhykkeen sisällä olevien järjestelmien välillä, eri turvavyöhykkeiden järjestelmien välillä sekä turvavyöhykkeen järjestelmien ja epäluotettavien verkkojen välillä
- Aluksen omaisuusluettelo, joka kattaa laitteistot, ohjelmistot, E26:n kannalta merkitykselliset tietokonepohjaiset järjestelmät sekä verkot, jotka yhdistävät kyseiset järjestelmät toisiinsa ja muihin tietokonepohjaisiin järjestelmiin aluksilla ja maissa.
- Kyberturvallisuuden suunnittelukuvaus, jossa annetaan tietoa, esitetään yhteenveto tietokonepohjaisiin järjestelmiin upotetuista ja verkkoihin lisätyistä turvatoiminnoista sekä ohjeet niiden turvallisuuskokoonpanoista ja turvallisesta käytöstä.

Käyttöönottovaiheessa järjestelmäintegroijan on toimitettava luokituslaitokselle aluksen kyberresilienssi testausmenettely käyttöönottoajankohtaan mennessä, jolla osoitetaan, että aluksella olevat turvavyöhykkeet täyttävät hyväksytyissä asiakirjoissa asetetut kriteerit. (Inmarsat 2024, 7.)

Käyttövaiheessa, aluksen omistajan on toimitettava aluksen kyberturvallisuus- ja kestävyysohjelma, jossa kuvataan teknisten ja organisatoristen turvatoimien hallitsemisen menettelyt, jotka auttavat aluksen turvallisen ympäristön ylläpitämisenä sellaisena kuin se on vahvistettu aluksen toimitushetkellä sekä myös mahdollisten muutosten hallitsemiseksi aluksen toiminta-aikana. (Inmarsat 2024, 7.)

6.3.2 UR E27

UR E27:n ensisijaisena tavoitteena on tukea merenkulunjärjestöjä niiden kyberresilienssin arvioinnissa ja parantamisessa. UR E27:n vaatimustenmukaisuuden osoittaminen edellyttää viiden asiakirjan toimittamista luokituslaitokselle (Inmarsat 2024, 8.):

- Ensimmäisenä asiakirjana on tietokonepohjaisen järjestelmän omaisuusluettelo, joka sisältää listauksen laitteistokomponenteista, joissa on yksityiskohtaiset tiedot valmistajasta ja mallista sekä lyhyt kuvaus niiden toimivuudesta; fyysiset rajapinnat; järjestelmäohjelmiston nimi/tyyppi, sen versio ja korjaustaso; sekä tuetut viestintäprotokollat.
- Toisena asiakirjana on tietokonepohjaiset järjestelmätopologiakaaviot, jotka muodostavat fyysisen topologiakaavion, joka puolestaan havainnollistaa sekä järjestelmän fyysistä arkkitehtuuria että loogista topologiakaaviota, joka havainnollistaa tietovirtaa järjestelmän osien välillä.
- Kolmantena asiakirjana on kuvaus tietoturvaominaisuuksista, jotka osoittavat kuinka tietokonepohjainen järjestelmä täyttää vaaditut tietoturvaominaisuudet sen laitteisto- ja ohjelmistokomponenteilla.
- Neljäntenä asiakirjana on tietoturvaominaisuuksien testausmenettely, jossa osoitetaan, miten testauksen avulla voidaan osoittaa, että järjestelmä täyttää vaatimukset.
- Viidentenä asiakirjana on tietoturvan määritysohjeet, jotka kuvaavat tietoturvaominaisuuksien suositellut määritysasetukset sekä määritetään oletusarvot.

7 Kyberturvallisuus

Autonomisten laivojen ollessa vielä kehitteillä on myös kyberturvallisuuteen kiinnitettävä erityistä huomiota sen ollessa hyvin ajankohtainen ja tärkeä tekijä turvallisuuden takaamisessa. Kyberturvallisuuteen keskittyy Naton kyberpuolustuksen osaamiskeskus CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence), joka tarjoaa monitieteisen lähestymistavan kyberpuolustuksen keskeisempiin kysymyksiin (CCDCOE 2022, 2).

Kyberhyökkäysten vaikutukset autonomisiin aluksiin ollessa vielä kehitteillä, on turvallisuuteen kiinnitettävä huomiota jo sen kehitysvaiheessa, sillä turvallisuussuunnitteluperiaate käsittää jo aikaisessa vaiheessa mahdollisten uhkien ja vastatoimien huomioimisen. Turvallisuuteen perehtyminen voi estää erilaisten skenaarioiden toteutumisen, sillä esimerkiksi itseohjautuvien alusten turvattomuus voi johtaa erilaisiin ympäristökatastrofeihin, jotka aiheutuvat yhteentörmäyksistä alusten ja satamarakenteiden kanssa, alusten kaappauksesta, varkaudesta tai kiristyksestä. (CCDCOE 2022, 3.)

Uhat ja vastatoimet

Autonominen toiminta ja sen luonne lisää hyökkäyspintaa kyber- ja fyysisiin hyökkäyksiin. Autonomisten alusten haltuunotto voi erityisesti johtaa katastrofiin, sillä vastustajien on mahdollista murtautua aluksiin, muuttaa niiden reittiä ja aloittaa niin sanottu ”itsemurhahyökkäys”. Tämän lisäksi vastustajat voivat toteuttaa yleisiä riskejä aluksilla kuten varastaa lastin, kaapata alus rahallista kiristystä varten tai varastaakseen aluksen teknologioita ja asejärjestelmiä. (CCDCOE 2022, 14.)

Naton kyberpuolustuksen osaamiskeskuksen asiakirjassa luodaan yleiskatsaus autonomisten alusten yleisistä puutteista ja komponenteista sekä niiden turvallisuuteen liittyvästä työstä. Asiakirjassa perehdytään merkittäviin autonomisia laivoja ympäröiviin uhkiin, skenaarioihin sekä sovellettaviin

vastatoimiin. (CCDCOE 2022, 3.) Merkittävät autonomisia laivoja ympäröivät uhat voidaan luokitella yhdeksään kategoriaan:

7.1 Hyökkäykset RF-signaalien häiritsemiseksi

Suurimmalla osalla autonomisista aluksista on viestintäkanava rannikon valvontakeskuksen kanssa. Aluksen ja valvontakeskuksen on mahdollista olla suorassa yhteydessä VHF/UHF-, matkapuhelin- tai Wi-Fi-yhteydellä, kun heidän välinen etäisyys on suhteellisen pieni. Suuremmissa etäisyyksissä yhteyttä on pidettävä satelliittien, poijujen, muiden alusten, lentokoneiden tai sukellusveneiden kautta. Vaikka jokaisella taajuusalueella ja kommunikaatioprotokolalla on omat vahvuutensa ja heikkoutensa, ovat ne siitä huolimatta alttiita palvelunestohyökkäyksille. RF eli radiotaajuus signaalien häirintää voitaisiin käyttää digitalisoiduissa autonomisissa kuljetuksissa niin, että se hämmentäisi alkuperäisen arvion laivan kurssista, elektronisesta sodankäynnistä tai kyberhyökkäyksestä. (CCDCOE 2022, 15.)

Satelliittisignaalien häirintä on melko helppoa lähettimen ollessa satelliitin antennikattavuudessa, koska satelliitin tiedon sisältöä ei suodateta, sillä useimmat viestintäsatelliitit vastaanottavat saapuvan signaalin, vahvistavat sen ja lähettävät sen takaisin maahan eri taajuudella. Näiden lisäksi myös GNSS-signaalit eli maailmalaajuiset satelliittipaikannusjärjestelmät ovat alttiita häirintähyökkäyksille. Kyseisiä GNSS-häirintätapauksia on ollut ympäri maailman kuten esimerkiksi GPS-häirintä itäisellä ja Keski-Välimerellä, Persianlahdella ja useissa Kiinan satamissa. Hyökkäyksen seuraukset voivat olla vakavia varsinkin silloin, jos alus on täysin riippuvainen GNSS:ään sijaintinsa määrittämiseen. (CCDCOE 2022, 15.)

Erilaiset tekniikat kuten kanavahyppely, spektrin hajautus, MIMO-tekniikkaan perustuva lievennys, kanavakoodaus, nopeuden mukauttaminen sekä tehonsäätö voivat olla avuksi RF-häiriöhyökkäyksiä vastaan. Adaptiivisten antennijärjestelmien, algoritmien, jotka havaitsevat tai kieltävät välittömiä hyppyjä paikassa ja ajassa, inertiasuunnistuslaiteyksikön, algoritmien, jotka

suodattavat taajuuskaistojen häiriöitä sekä eLoran eli matalataajuisen radionavigointijärjestelmän vastaanottimien käyttö varajärjestelmänä voivat auttaa häiriöiden nujertamisessa. GNSS-häirintää tai -huijausta vastaan puolustautumisessa voidaan käyttää useita tähdistöjä eli eri maiden ja globaalien järjestöjen satelliittiryhmiä, kuten GPS, QZSS, BEIDOU, GALILEO, GLONASS sekä IRMSS/NAVIC. Useiden tähdistöjen käyttö ei tarjoa kuitenkaan täydellistä suojaa, sillä jos hyökkääjien on mahdollista häiritä tai huijata yhtä tähdistöä, voivat ne tehdä saman myös muille. Tämän takia autonomisilla aluksilla tulisi olla omatoiminen palautuskyky, jos yhteys tai sijainnin havainnointi katkeaa. Palautuskyvyt riippuvat häiriön tyypistä ja olosuhteesta, mutta yhtenä vaihtoehtona voidaan pitää se, että alus jatkaisi purjehtimista gyrokompassin ja kertyneiden matkalokien mukaisesti. Toisena vaihtoehtona olisi se, että alus palaisi ennalta määrättyyn paikkaan samoilla keinoilla, jos häiriö kestäisi kauemmin kuin ennalta määritellyn ajanjakson. Aluksen pysäyttäminen olisi paras vaihtoehto silloin, kun alus on vaara-alueella eikä sen sijaintia voida varmistaa. (CCDCOE 2022, 15.)

7.2 Hyökkäykset sensoreiden harhauttamiseen tai heikentämiseen

Sensoridatan harhauttaminen tai heikentäminen voi tapahtua myös alusten sijaintien ja esteiden tunnistamiseen käytettäville sensoreille kuten GNSS:lle, tutkalle, optisille antureille, ultraääni- ja akustisille antureille. GNSS-huijauksessa radiolähettimestä lähetetään väärennetty signaali vastaanottimen antenniin. Vaikka GNSS-häirintä vaikuttaa merkittävämmältä uhalta, GNSS-huijaus antaa iskuja eri sovelluksille, sillä väärennetyt GNSS-syötteet saavat kuljettajien, alusten kapteenien ja muiden toimijoiden poikkeamaan kurssilta ilman minkäänlaista pakottamista. (CCDCOE 2022, 16.)

Autonomisten alusten ulkopuolella sijaitsevat anturit voivat olla houkuttelevia kohteita hyökkääjille, sillä siinä tilanteessa he eivät tarvitse fyysistä pääsyä aluksen sisälle. Sensorit voivat olla myös suoraan RF-häirinnän uhreja, jos aistitietojen välittämisessä käytetään langattomia signaaleja. Tämän lisäksi

hyökkääjien on mahdollista käynnistää hyökkäys heikentääkseen sensoreita, jotka toimittavat syötteitä autonomisiin toimintoihin. (CCDCOE 2022, 16.)

AIS on yksi merenkulun tilannetietoisuuden ja liikenteen seurannan lähteistä. Aluksen sammutuksen, virheellisen tiedon aluksen nykytilasta, viallisen asennuksen tai konfiguroinnin ollessa mahdollisia, kärsii AIS viestien luotettavuuden ongelmasta. Kyseisten ihmiseen liittyvien riskien lisäksi AIS:n käyttämää VHF-viestintää on mahdollista huijata ja kaapata, mikä aiheuttaa väliintulohyökkäyksen. AIS:iin kohdistuvia huijaushyökkäyksiä on monenlaisia kuten esimerkiksi mahdollisen aluksen kanssa yhteentörmäyksen lavastaminen ja siten aluksen kääntäminen hyökkääjien haluamaan suuntaan, väärien hätämajakoiden luominen sekä väärennettyjen tietojen luominen, jonka avulla houkutellaan kohdealuksia tekemään vääriä liikkeitä. (CCDCOE 2022, 16.)

Tiettyyn sensoriin kohdistuvien hyökkäysten vaikutuksien minimoimiseksi tulisi autonomisessa aluksessa olla riittävästi eri tekniikoihin perustuvia antureita, joilla voidaan vertailla antureiden syötteitä ja tehdä päätöksiä saatavilla olevan tiedon perusteella. Esimerkkinä eri teknologioiden käytöstä on se, että kameroiden sekä LiDAR- ja lasersensoreiden tiedot voivat yhdessä tunnistaa aluksen edessä olevat esteet, jolloin autonomiset alukset voivat saavuttaa sensorien datan osittaisen hajoamisen tai häiriintymisen kestävyyden. Tämän lisäksi eri teknologioiden käyttö vaikeuttaa hyökkääjän onnistua kaiken sensoridatan harhauttamisessa samanaikaisesti. (CCDCOE 2022, 16–17.)

Tiettyyn sensoriin kohdistuvan sabotaasihyökkäyksen ja sen myöhempää epäonnistumista voidaan torjua niin, että sijoitetaan tarpeettomia antureita eri aluspaikkaan. Toisena vastatoimena on antureiden käyttö, jotka eivät ole aluksella, jolloin esimerkiksi satelliittikuvien avulla on mahdollista määrittää aluksen sijainti tai autonomisen aluksen lähistöltä laukaistu drone voi lentää aluksen läheisyydessä ja toimia etäkuvasensorina. Sabotaasihyökkäykset aluksen sisällä oleviin antureihin ovat myös mahdollisia, mutta tällaiset hyökkäykset edellyttävät fyysistä tai loogista pääsyä alusverkkoihin, joten niillä on merkitystä operatiivisten teknologiajärjestelmien turvallisuuden kannalta. (CCDCOE 2022, 17.)

Väärennettyjen AIS-viestien osalta autonomisen aluksen on pystyttävä suodattamaan niitä pois. Väärennettyjen viestien havaitsemiseen on käytettävissä useita tekniikoita kuten laillisten historiallisten viestien paikkansapitävyyden määrittäminen sekä tutka-anturien käyttö täydennyksenä. GNSS-huijaukselle on mahdollista harkita samoja vastatoimia kuin GNSS-häirintää vastaan, mutta GNSS- signaalien salaus on kuitenkin paras ratkaisu huijaushyökkäyksien torjumiseen. (CCDCOE 2022, 17.)

7.3 Hyökkäykset viestinnän katkaisemiseksi tai muuntamiseksi

Siirtotietojen luvattomalla paljastamisella tai manipuloinnilla aluksen ja rannikon valvontakeskuksen/muiden välityspisteiden välillä voi olla huomattava vaikutus. Esimerkkejä siirtotiedoista ovat C2-ohjeet rannikon valvontakeskukselta, kuittaukset alukselta saaduista ohjeista, erilaiset aluksen tilaa koskevat tiedot, kuvat ja videot sekä muut aluksen ottamat havainto- ja tiedustelutiedot. RF-signaalien sieppaus on mahdollista, jos hyökkääjät ovat oikeassa paikassa vastaanottaakseen signaaleja ja kuunnellakseen oikeaa taajuutta. (CCDCOE 2022, 17.)

RF-signaalien sieppauksen kustannukset ovat laskeneet dramaattisesti SDR:n eli ohjelmistoradion järjestelmän myötä. On olemassa erilaisia edullisia sieppauslaitteita, jotka on suunniteltu eri taajuuskaistoille, mukaan lukien satelliittisignaalit. Tämän myötä välitettyjen tietojen salakuuntelu, toistaminen ja manipulointi tai pahimmassa tapauksessa koko C2- ja tietoyhteyksien haltuunotto voisivat olla mahdollisia, jos tiedonvälitystä ei ole riittävästi suojattu. Autonomisen aluksen C2-ohjeiden manipulointi voi johtaa aluksen suunnan ja lopullisen määränpään muuttamiseen ja aseistettujen sotilaslaivoissa puolestaan ohjus voitaisiin laukaista väärään kohteeseen. Sama asia koskee myös virheellistä tiedustelua väärien tietojen välittämisen takia, jos autonominen valvontasukellusvene lähettää muutettua tietoa takaisin tukikohtaansa. (CCDCOE 2022, 17.)

Tiedonsiirron turvallisuuden vaarantumisen estämiseksi käytössä olisi oltava vahvoja salausmekanismeja, jotka takaavat muun muassa todennuksen, luottamuksellisuuden, eheyden ja kiistämättömyyden. Kaikki kommunikoivien osapuolten väliset esiasennetut yhteiset salaisuudet tulee syöttää turvallisesti hallintaprosessin aikana ja hallintaan käytettyä laitetta tulee ylläpitää turvallisesti, jotta sitä ei käytetä luvatta. Näiden lisäksi tarkoituksenmukaiset fyysiset kerrosturvamekanismit olisi otettava käyttöön. Hyökkääjien signaalisieppauskyvyn vähentämiseksi voidaan käyttää samaa tai samankaltaista tekniikkaa kuin häirinnän estossa. Turvamekanismien lisäksi useiden viestintäkanavien käyttö eri tekniikoilla voisi parantaa kestävyyttä luvatonta manipulointia vastaan. Ylimääräisyyden päätarkoituksena on vaihtoehtoisen keinon tarjoaminen, kun yksi teknologia vaurioituu, mutta sen avulla voidaan myös varmistaa, ettei mikään kanavista vaarannu, kun vertaillaan eri kanavista vastaanotettua tietoa. (CCDCOE 2022, 17.)

7.4 Hyökkäykset operatiivisiin teknologiajärjestelmiin

Hyökkäysten tunkeutuessa autonomisten alusten OT eli operatiivisiin teknologiajärjestelmiin, aiheuttavat ne toimintahäiriöitä ja palvelunestoa. OT-järjestelmissä jo vuosia käytetyt perinteiset teollisuusprotokollat ovat alttiita kyberhyökkäyksille, koska turvallisuutta ei ole otettu riittävästi huomioon niitä suunniteltaessa. Esimerkkinä tästä on se, että kaikista tärkeimmistä kenttäväylä protokollista kuten Modbus, DNP3, Profinet ja EtherCat, puuttuu todennus ja salaus, joten hyökkääjien on mahdollista häiritä verkon toimintaa tai manipuloida IO-viestejä aiheuttaen ohjausprosessissa häiriön, jos he pääsevät OT-verkkoon. Vaikka autonomisissa aluksissa käytettäisiin protokollia, joihin on lisätty turvallisuusominaisuuksia kuten suojattu Modbus ja suojattu DNP tai jopa uuden sukupolven suojattu protokolla, voivat turvallisuusongelmat jatkua edelleen. Tämä johtuu siitä, että sensoreilla ja toimilaitteilla voi tästä huolimatta olla rajoitettu laskennallinen teho ja muisti, mikä estää turvatoimintojen toteuttamisen tai käytössä voi olla edelleen vanhat protokollat. (CCDCOE 2022, 18.)

OT-järjestelmään tunkeutumista on mahdollista tehdä joko epäsuorasti laivaverkoston kautta tai suoraan fyysisen pääsyn kautta OT-komponentteihin. Hyökkäysvektorit voivat sisältää: C2-ohjeiden manipuloinnin mahdollistaakseen langattomat päivitykset haittakoodien asentamista varten; tunkeutumista ylläpitoon käytettävään etätukipisteeseen; tunkeutumista ulkoiseen IT-komponenttiin ja sitten sivusuunnassa siirtymistä OT-verkkoon hyödyntämällä konfigurointivirheitä verkon erottelussa; sekä fyysisen pääsyn ylläpitoporttiin kuten USB, RJ45, UART ja JTAG tai jopa pääsy OT-järjestelmien käyttämiin fyysisiin johtoihin. (CCDCOE 2022, 18.)

Jotta OT-järjestelmiä voidaan suojata kyberhyökkäyksiltä, tulisi tietoturvan karkaisukäytäntöjen kuten vahvojen salasanojen käyttö, käyttämättömien palveluiden ja porttien poistaminen käytöstä sekä kaikkien komponenttien pitäminen ajan tasalla olla käytössä, niin kuin niiden pitäisi olla missä tahansa IT-järjestelmässä. Näiden lisäksi tulisi myös muita OT-järjestelmiin liittyviä turvatoimenpiteitä tunnistaa ja toteuttaa. Erilaisia OT-järjestelmille ominaisia turvatoimia ovat muun muassa OT-verkon erottaminen pienemmiksi loogisiksi erillisalueiksi (virtuaaliset lähiverkot), OT-verkon erottaminen IT-verkosta, yksipuolisen verkkolaitteen (mieluiten laitteistopohjaisen datadiodin) käyttö tiedonkulun mahdollistamiseksi vain yhdellä tavalla sekä fyysisten suojatoimenpiteiden soveltaminen kaikkiin huoltosatamiin. (CCDCOE 2022, 18–19.)

Kyberturvallisuusvirastot ympäri maailmaa ovat julkaisseet monia tietoturvaohjeita OT-järjestelmille mukaan lukien Yhdysvaltain DHS:n suosittelemat käytännöt ICS:lle eli teolliselle valvontajärjestelmälle sekä EU:n ENISAn ICS:n suojaamista koskevat suositukset. Tietoturvaohjeet muodostavat IEC 62443:n kanssa joukon kansainvälisiä standardeja ICS-turvallisuudelle sekä tarjoavat arvokasta tietoa OT-järjestelmien kyberuhkien sietokyvyn rakentamiseen. Tulevaisuudessa OT-järjestelmien turvallisuusteknologiat ovat paljon kypsempiä. Mahdollisuuden tullen turvallisia teollisuusprotokollia ja tietoturvatietoisuusominaisuuksia, jotka voivat ymmärtää protokollat täysin sekä voivat valvoa ja suojata OT-järjestelmiä, tulisi käyttää aktiivisesti. Myös

laiteohjelmiston ja ohjauslogiikan päivitysprosessit tulisi suojata luvattomilta päivityksiltä. (CCDCOE 2022, 18–19.)

7.5 Hyökkäykset tietoteknisiin järjestelmiin

Autonomisissa aluksissa voi olla myös IT eli tietoteknisiä järjestelmiä, joilla tarkoitetaan tässä yhteydessä järjestelmiä ja komponentteja, jotka eivät liity suoraan aluksen ohjaamiseen ja jotka sisältävät verkkokomponentteja, joita käytetään kommunikointiin ulkopuolisten tahojen kuten rannikon valvontakeskuksen ja välityspisteiden kanssa. Tyypillisiä esimerkkejä IT-järjestelmistä verkkokomponenttien lisäksi ovat miehistön käyttämät hallinto- ja tukitietokoneet. Miehittämättömillä aluksilla voi olla myös joitain IT-järjestelmiä kuten esimerkiksi tiedostopalvelin, joka voi tallentaa kuvia, videoita, ääniä ja muun tyyppistä tietoa, joka kerätään osana valvonta- ja seurantatehtävää. Toisena esimerkkinä on datahistorioitsija, joka kerää ja tallentaa aluksen tilasta aikasarjatietoja. Datahistorioitsija voidaan sijoittaa OT-verkon ulkopuolelle, jotta insinööreillä on etäkäyttömahdollisuus vianmääritystä varten. IT-järjestelmillä voi olla olemassa erilaisia verkkokonfiguraatioita, toteuttamalla demilitarisoidut alueet palomuureja ja yksipuolisia verkkolaitteita käyttäen. (CCDCOE 2022, 19.)

IT-järjestelmiin kohdistuvat hyökkäykset voivat johtaa järjestelmien häiriintymiseen sekä järjestelmissä olevien tietojen paljastumiseen, poistamiseen tai muuttamiseen. Hyökkäysten vaikutus IT-järjestelmiin voitaisiin kuvitella olevan marginaalinen olettaen, että OT-ydinjärjestelmä on riittävästi suojattu verkon erottelulla ja muilla turvatoimilla. Verkon erottelussa voi olla kuitenkin konfiguraatiovirheitä ja joissakin IT-järjestelmissä voi olla tärkeitä tietoja liiketoiminnasta tai sotilaallisesta näkökulmasta sovelluksesta riippuen, sen takia IT-järjestelmien turvallisuutta ei pidä unohtaa. Tämän takia IT-järjestelmien suojaamiseksi hyökkäyksiltä tulee ottaa käyttöön tietoturvan vahvistamiskäytännöt kuten OT-järjestelmissä. Yleensä IT-järjestelmissä on enemmän laskentatehoa ja muistia kuin OT-järjestelmissä sekä enemmän tilaa käyttää tietoturvaratkaisuja kuten tietoturvatieto- ja tapahtumahallintajärjestelmää (SIEM) tai tunkeilijan havaitsemisjärjestelmää

(IPS). Verkon kaikkien resurssien valvomiseksi ja suojaamiseksi tulisi tietoturvaratkaisujen käyttöönottoa harkita. Kun tietty järjestelmä vaarantuu, tulisi verkon segmentointia ja erottelua soveltaa VLAN-verkkojen, palomuurien ja ohjelmallisesti määritettyjen verkkojen avulla sivuttaisliikkeen minimoimiseksi. (CCDCOE 2022, 19.)

7.6 Hyökkäykset autonomisiin toimintoihin käytettävää tekoälyä vastaan

Autonomisten alusten käyttämät tekoälyteknologiat ovat myös alttiita kyberhyökkäyksille. Monet nykyiset tekoälyjärjestelmät käyttävät ML:ää eli koneoppimista, joka poimii tietoa oppimalla monia esimerkkejä tietoaineistosta, joten jos hyökkääjä korruptoi tai myrkyttää tietoaineiston voi ML vaarantua, koska se on riippuvainen siitä. Tämän takia hyökkääjien pyrkimyksenä on hyökätä tekoälyä vastaan aiheuttaakseen virhearvioita tai toimintahäiriöitä autonomisissa toiminnoissa. Autonomisissa aluksissa avainasemassa on tekoälyn turvallisuus ja erityisesti eheys, kun viestintä rannikon valvontakeskuksen kanssa ei ole mahdollista ja ohjailu on tekoälyn varassa. (CCDCOE 2022, 19–20.)

Koska huoli erilaisten tosimaailman sovellusten tekoälyhyökkäyksistä kasvaa, aloitti MITRE yhtiö vuonna 2020 tekoälyjärjestelmien vastakkaisen uhkamaiseman (ATLAS) -projektin, jonka avulla tutkijoiden on mahdollista navigoida ML-järjestelmien uhkien maisemaa. ATLAS-projekti tarjoaa yleiskatsauksen ML:ään liittyvistä turvallisuushäiriöistä sekä hyökkääjien taktiikoista ja tekniikoista, joita sovelletaan kuhunkin tapaukseen. Tyypillisiä ATLASin tunnistamia hyökkäyksiä ovat mallin kiertäminen ML-mallin muokkaamiseksi haitallisilla syötteillä, jotka aiheuttavat hyökkääjän toivotun vaikutuksen mallissa, mallin myrkytys kouluttamalla sitä myrkytetyillä tiedoilla sekä tietoaineistojen tietomyrkytys. Myös muun tyyppiset hyökkäykset, jotka kohdistuvat yhdistämisen ja laskennan syöttöarvoihin, ovat mahdollisia. Esimerkkinä on se että, jos tiedonsiirtoliitäntää ei suojata riittävästi, viestintäyökkääjät voivat muuttaa anturin arvoja ennen kuin tekoäly käyttää niitä. Myös ennalta määritettyjä matka-asetuksia kuten määränpäätä, reittiä,

vaihtoehtoisia reittejä ja rajoitettuja alueita voidaan muuttaa, jos todennus puuttuu, kun arvoja syötetään tai muutetaan. (CCDCOE 2022, 20.)

On tärkeää turvata kaikki rajapinnat kuten viestintä rannikon valvontakeskuksen kanssa ja tekoälytoimintoihin käytetyt laskentaresurssit tekoälyhyökkäyksiä vastaan suojautumiseksi. Kaikki tunkeutuminen näihin resursseihin voi johtaa toimintahäiriöihin tai tekoälyn toiminnan häiriöihin. Kun ML-mallia rakennetaan myyjän tai aluksen omistajan laboratoriossa ennen kuin se sijoitetaan autonomiseen alukseen, tulisi asianmukaisten turvatoimien olla käytössä myös silloin. Kehittämis- ja oppimisympäristöihin tulisi soveltaa turvallisia kehityskäytäntöjä kuten irrotettavaa laiteohjausta, kehitysverkon erottelua internetistä sekä riittävää konfiguraation hallintaa. Hyökkääjä voi päästä käsiksi ML-malliin ja tietoaineistoihin myös toimitusketjuhyökkäyksillä vaarantamalla oppimiseen käytettäviä laitteistoja, ohjelmistoja ja tietoja kuten grafiikkasuorittimet (GPU), koulutusaineistot, ML-ohjelmistopinot sekä itse malli. Kun ennalta määrättyjä ML-malleja, koulutusaineistoja ja avoimen lähdekoodin arkistoon ladattuja ML-ohjelmistopinoja käytetään, tulisi niiden eheyttä ja aitoutta tutkia perusteellisesti ennen niiden käyttämistä oppimiseen. (CCDCOE 2022, 20.)

7.7 Hyökkäykset toimitusketjujen aikana

Toimitusketjuhyökkäyksiä on tunnistettu tietoturva ammattilaisten ja päättäjien keskuudessa jo vuosien ajan, sillä niitä voi tapahtua missä tahansa sovelluksessa koko IT- ja OT-laitteisto- ja ohjelmistokomponenttien elinkaaren aikana, milloin ja missä tahansa. Autonomisten alusten on mahdollista joutua toimitusketjuhyökkäyksien uhriksi, kun ne ovat avomerellä ja kaukana rannikon valvontakeskuksesta, jolloin turvallisuushäiriöitä ei pystytä hoitamaan nopeasti. Tämä voi johtaa pahimmassa tapauksessa aluksen vaurioitumiseen, jonka seurauksena alus uppoaa tai kaapataan. Hyökkäykset eivät tapahdu ainoastaan tunkeutumalla toimittajan ohjelmointiympäristöön tai päivityspalvelimeen vaan myös manipuloimalla kolmannen osapuolen moduuleja ja kehityksessä käytettyjen avoimen lähdekoodin kirjastoja. Esimerkkejä kyseisestä

hyökkäyksestä ovat Python-pakettihakemistoon sekä avoimen lähdekoodin Python-arkistoon ladatut haitalliset kirjastot. (CCDCOE 2022, 20.)

Kaikkien autonomisissa aluksissa käytettävien laitteisto- ja ohjelmistokomponenttien toimitusketjua tulee suojata sen elinkaaren ajan tahallisilta ja vahingossa tapahtuvilta muutoksilta, sillä toimittajan tai palveluntarjoajan fyysisen ja kyberturvallisuuden puute voi johtaa OT- tai IT-järjestelmien rikkoutumiseen. Aluksen omistajan on suotuisaa vaatia tavarantoimittajia, myyjiä ja palveluntarjoajia täyttämään tietyn turvallisuustason, jolloin hän voi pyytää heitä hankkimaan kolmannen osapuolen suojaussertifikaatti, ISO 27001 tai asettaa lisävaatimuksia turvallisuuden lisäämiseksi. Tähän ei kuitenkaan riitä, että toimittajia pyydetään toteuttamaan turvallisuutta yleisellä tasolla saavuttaakseen kaikkien komponenttien turvallisuuden, sillä aina on olemassa riski, että hyökkääjät tunkeutuvat valmistajien kehitysympäristöihin muokatakseen tuotteita. Myyjien on myös mahdollista tuottaa virheiden tai tietoturvataitojen ja -tietoisuuden puutteen vuoksi epävarmoja tuotteita, joten apuna voidaan käyttää kolmannen osapuolen tietoturvasertifiointijärjestelmiä kuten yhteisiä kriteereitä, Euroopan kyberturvallisuussertifiointia ja IEC 62443-sertifiointia. (CCDCOE 2022, 20–21.)

Vaikka kyseiset järjestelmät eivät takaa haittakoodien ja tietoturvavirheiden täydellistä havaitsemista, tutkivat ne toimittajien kehittämiseen ja toimitukseen liittyviä tietoturvakäytäntöjä ja tarkistavat tuotteen turvallisuustoiminnot. Aluksen omistajan on suotuisaa myös tarkistaa ennen asennusta tai käyttöönottoa tuotteiden tiivistearvot ja fyysiset suojasinetit varmistaakseen, että tuotteet ovat aitoja ja että niitä ei muuteta toimituksen aikana. Tämän lisäksi ohjelmistoluettelon, ohjelmistokomponenttien ja -riippuvuuksien luettelon sekä kyseisiä komponentteja ja niiden hierarkkisia suhteita koskevien tietojen ylläpitäminen autonomisissa aluksissa käytettävien ohjelmistojen osalta voivat auttaa myyjiä ja omistajia tunnistamaan toimitusketjun riskit ja selviytymään niistä. (CCDCOE 2022, 21.)

7.8 Hyökkäykset fyysisen pääsyn kautta

Itseohjautuvien alusten alttius fyysisille hyökkäyksille kasvaa, kun se liikennöi avomerellä, sillä silloin kuka tahansa voi päästä alukselle luvatta. Tällaisia luvattomia pääsyjä voivat tehdä esimerkiksi merirosvot, rikolliset tai vastustajat, jotka voivat nousta alukseen ja vahingoittaa järjestelmää kuten muuttaa reittiä tai määränpäätä ja pysäyttää moottorin kaappausta varten. Itseohjautuvien alusten kaappaus voi johtua itse aluksen ja sen kuljettaman lastin taloudellisesta arvosta sekä teknisestä arvosta teollisen vakoilun näkökulmasta. Vastustajien on mahdollista saada tietoa sotilasoperaatioista ja autonomisissa laivaston aluksissa sovellettavista teknologioista käänteistekniikan avulla. Huolena on myös se, että jos merirosvot tai terroristit kaappaavat aseistettuja sotilasaluksia, saavat he käsiinsä aseita ja käyttävät niitä terrorismiin. Merirosvot voisivat myös ohjata aluksen toiseen paikkaan ja ottaa itse aluksen niin sanotusti panttivangiksi ja uhata räjäyttää tai upottaa sen aiheuttaen massiivisen ympäristön saastumisen. (CCDCOE 2022, 21.)

Vaikka tähän ongelmaan ei ole selkeää vastausta, on kaikin keinoin pyrittävä nostamaan tällaisten hyökkäysten kustannuksia (CCDCOE 2022, 21.):

- Virta- ja tietoliikennekaapeleita ei saa olla aluksen ulkopuolella ja sisäänkäynnin oven tulisi olla tiukasti lukittu.
- Aluksen sisällä verkkoportit tai muut järjestelmän komponenttien huoltoportit tulee sulkea eikä kaapeleita saa paljastaa asettamalla ne lattian alle tai seinän sisälle.
- Hälytysjärjestelmät, jotka lähettävät turvahälytyksiä rannikon valvontakeskukseen tunnistettaessa tunkeutumista ja kaapelivika-antureita, jotka havaitsevat kaapeleiden katkaisun, tulisi asentaa.
- Väärinkäytöksen kestäviä mekanismeja, jotka poistavat tärkeitä liike- ja sotilastietoja tunkeutumisen jälkeen, voidaan myös harkita sellaisten kriittisten tietojen osalta, joita ei pitäisi paljastaa muille osapuolille.

On olemassa myös fyysisiä suojatoimenpiteitä, jotka tekevät aluksista kestävämpiä fyysisiä hyökkäyksiä vastaan. Alusta ei voi kuitenkaan suojata

mikään avomerellä, joten aluksen arvoa, fyysisen hyökkäyksen todennäköisyyttä ja vastatoimen kustannuksia tulee tarkastella yhdessä kustannustehokkaimman ratkaisun löytämiseksi. (CCDCOE 2022, 21.)

7.9 Hyökkäykset rannikon valvontakeskukseen

Riittämätön erottelu C2-verkon ja rannikon valvontakeskuksen toimistoverkon välillä tai irrotettavan viestimen epäasianmukainen valvonta C2-verkossa voi aiheuttaa kompromisseja, jotka voivat aiheuttaa luvattomien komentojen välittämisen autonomisille aluksille tai häiriöitä viestintäyhteyksissä rannikon valvontakeskuksen ja alusten välillä. Kuten autonomisten alusten OT- ja IT-järjestelmät, tulisi myös rannikon valvontakeskuksen C2- ja toimistoverkkojen suojaamiseen soveltaa parhaita turvallisuuskäytäntöjä kuten SIEM-valmiuden käyttöönotto. Rannikon valvontakeskuksessa tulisi myös toteuttaa rakennuksen ja valvomon fyysistä ympärys- ja kulunvalvontaa. (CCDCOE 2022, 21–22.)

8 Torjunta ja ennaltaehkäisy

Merellä tapahtuva rikollisuus eroaa huomattavasti normaalista maalla tapahtuvasta rikollisuudesta. Rikollisten on helpompi valmistella hyökkäyksiä huomaamatta ja hyökkäysten ennaltaehkäisy on vaikeampaa. Tällaisen ympäristön vuoksi alukset eivät voi luottaa eri maiden laivastojen tai merivartiostojen apuun hyökkäyksen torjunnassa, sillä avun saapuessa alus on jo todennäköisesti vallattu. (Marine Insight 2019b.)

IMO on suuresti myös mukana operatiivisessa toiminnassa aluksiin kohdistuvien hyökkäyksien ehkäisemiseksi. Yhdessä eri varustamoiden kanssa IMO on luonut ohjeet, jossa kerrotaan parhaat yleiset tavat hyökkäysten torjumiseksi ja ennaltaehkäisemiseksi ja paljon muita keinoja, jotka ovat osaltaan vähentäneet hyökkäysten määrää. IMO tarjoaa myös neuvontaa ja avustusta jäsenvaltioille, jotka haluavat parantaa omaa kykyään puuttua alueillaan tapahtuviin hyökkäyksiin. Tällä hetkellä IMO on mukana operaatiossa punaisella merellä, jonka tarkoituksena on lisätä vakautta punaista merta ympäröivissä valtioissa ja taata tavaran vapaa kulku tulevaisuudessa. (IMO 2024b.)

Aluksien on aluksi tehtävä omakohtainen riskiarvio, jonka perusteella päätetään millaisia torjuntakeinoja käytetään. On myös hyvä muistaa, että hyökkäykset voivat tapahtua myös aluksen ollessa ankkurissa, eikä vain sen ollessa liikkeessä, joten tämä tuo uuden huomioitavan näkökulman riskianalyysiin. (Tseng ym. 2021, 6.) Läpikäytävät torjunta ja ennalta ehkäisykeinot on jaettu kolmeen eri tasoon liittyen hyökkäyksen eri vaiheisiin.

Tutkimalla hyökkääjien toimintatapoja voidaan luoda parempia suojauskeinoja niitä vastaan. Toimintatapoja analysoitaessa tulee katsoa missä hyökkäykset ovat tapahtuneet (satamissa, rannikoilla vai kauempana merellä), miten hyökkäykset toteutetaan, esimerkiksi piraatti hyökkäykset suoritetaan usein heikommin aseistautuneina pienillä ja nopeilla aluksilla sekä mikä on ollut hyökkäysten tavoite (lastin varastaminen, kidnappaus vai koko aluksen anastaminen). Tällainen analyysi lisättynä miehistön korkeaan tilannetajuun

seilatessa korkean riskin alueilla laskee huomattavasti hyökkääjien kykyä. (Critical maritime routes 2023.) Suojauskeinoja suunnitellessa ei saa sortua keskittymään vain yhteen uhkaan, esimerkiksi vain piratismiin, sillä myös terrorismi ja muu rikollisuus aiheuttaa uhan alukselle ja niiden toimintatavat ovat hyvin erilaisia.

8.1 Ensimmäinen taso

Tämä taso koskee vaihetta, jolloin hyökkäys on vasta alkamassa ja hyökkääjät eivät vielä ole päässeet alukseen.
Tarpeeksi hyvin miehitetty vahtivuoro on ensimmäinen askel hyökkäyksien torjuntaan, sillä mikäli hyökkäys huomataan ajoissa alus voi liikkeillään tehdä alukseen noususta vaikeampaa ja miehistö keretään hälyttämään torjuntatoimiin. On tärkeää, että vahtivuorossa on tarpeeksi henkilöstöä, heillä on tarvittavat varusteet kuten kiikarit ja radiopuhelimet ja että he ovat tietoisia sen hetkisestä riskitasosta. Myös ihmisen kokoisten nukkejen asettelu aluksen laidoille on tehokas tapa luoda illuusio hyvinkin suuresta vahtivuorosta. Lennokit ovat hyvä tapa pidentää tarkkailukykyä ihmissilmiä pidemmälle. Piikkilanka on erittäin tehokas väline alukseen nousun estämiseksi. piikkilanka toimii parhaiten, kun se on asennettu aukottomasti ja kiinnitetty roikkumaan aluksen laidan ylitse. Piikkilankaa valittaessa on hyvä huomioida sen laatu, esimerkiksi paksumpaa lankaa on vaikeampi katkaista työkaluilla. Vesi- ja vaahtotykkejä voidaan käyttää vaikeuttamaan aluksen vierellä pysymistä ja alukseen nousemista. Etenkin vaahto on tehokas sillä se vaikeuttaa näkemistä ja tekee pinnoista liukkaampia. Kunnollinen valaistus aluksella on tärkeää, kuitenkaan yöaikaan ulkoisten valojen käyttö tulisi pitää minimissä ja vahtivuoroissa käyttää erilaisia pimeänäkölaitteita tai lämpökiikareita. Hyökkäyksen sattuessa laidan yli kohdennetut kirkkaat valot haittaavat hyökkääjien näkökykyä. Erityyppisiä lankoja ja verkkoja voidaan vetää aluksen sivulla, kun hyökkäystä yrittävän veneen moottori osuu niihin, kyseinen materiaali kietoutuu potkurin ympärille ja pysäyttää moottorin. (UKMTO 2025, 26–36.)

Yksityiset erikseen palkatut turvallisuustoimijat voivat olla iso etu alukselle, sillä heidän tarjoama kokemus auttaa miehistöä toimimaan paremmin hyökkäyksen tapahtuessa, ja he voivat toimia myös yhteyshenkilöinä aluksen, eri laivastojen sekä merivartiostojen välillä. Yksityisiä turvallisuustoimijoita kovempi turvakeino on aseistetut yksityiset turvallisuustoimijat. Tällaisen henkilöstön palkkaus on kuitenkin harvinaista monien lakiongelmien takia, huomioon on otettava muun muassa kaikkien maiden lait, joiden vesialueiden läpi alus kulkee ja sen maan lait, jonka lipun alle alus on rekisteröity. Tällaisen henkilöstön hankkimista harkittaessa on otettava huomioon lakien lisäksi sen hetkinen riski hyökkäykselle, kuljetettava tavara ja pyrittävä hakemaan muita ratkaisuja. Riskin ollessa erityisen suuri esimerkiksi tavaran luonteen takia on mahdollista, että jokin maa määrää alukselle aluksen suojaus osaston (VPD – Vessel Protection Detachment) tämä koostuu kyseisen maan koulutetusta ja aseistetusta armeijan/puolustusvoimien henkilöstöstä ja aiheuttaa samanlaisia oikeudellisia ongelmia kuin yksityisesti hankittu aseellinen henkilöstö. Näiden keinojen lisäksi on laitteita, joita käytetään harvemmin. Nämä laitteet ovat ei-kuolettavia, mutta aiheuttavat mahdollisesti suurtakin kipua (Marine Insight 2024; UKMTO 2025, 26–36.):

- Pitkän kantaman äänitykki – Long Range Acoustic Device (LRAD) lähettää korkeataajuista ääniaaltoa, jota ihmisen korvat eivät kestä ja tämä tuottaa kipua.
- Keskitetyt valo aseet – Tämä termi tarkoittaa joko alukseen kiinnitettyjä tai käsin kannettavia laitteita, jotka lähettävät keskitetyn valokeilan, joka väliaikaisesti sokaisee kohteen.
- Elektromagneettinen säteily – Tällä laitteella hyökkääjiin kohdistetaan elektromagneettista säteilyä. Säteily läpäisee ihon ja saa aikaan kovan poltteen tunteen, kuitenkaan aiheuttamatta pysyvää vahinkoa kohteisiin.
- Vesiletku verho – Vesiletkuja jätetään vapaasti roikkumaan laivan kyljelle. Kun näiden letkujen läpi ohjataan vettä kovalla paineella ne alkavat heilumaan holtittomasti ja osuvat kovaa laivaan yrittäviin hyökkääjiin.

8.2 Toinen taso

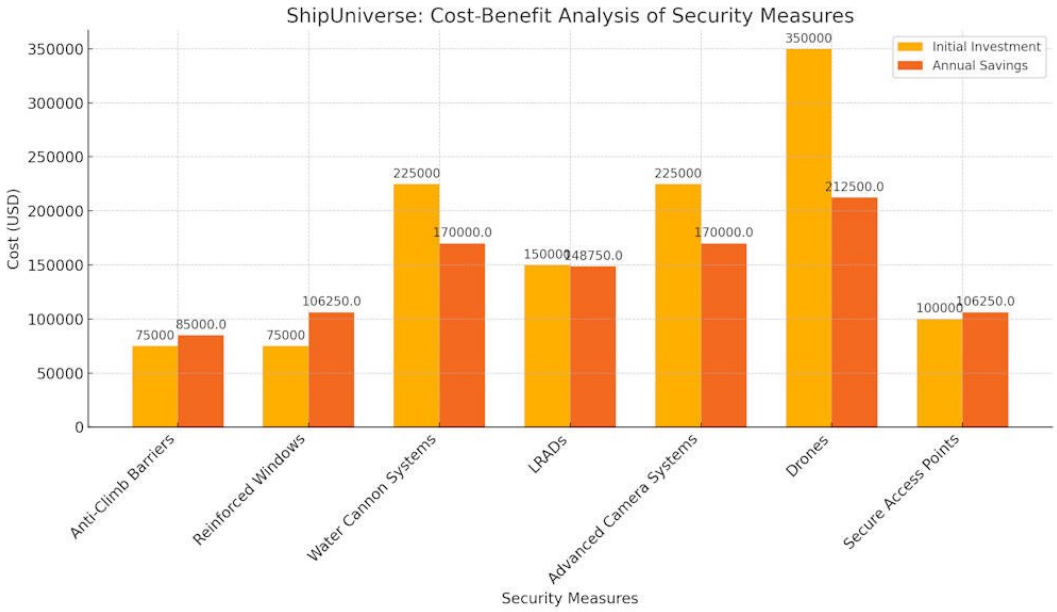
Toinen taso kattaa kaikki muut paitsi laivan elintärkeät osat. Toisen tason torjuntakeinot ovat sellaisia, jotka vaikuttavat siinä vaiheessa, kun hyökkääjät ovat jo päässeet nousemaan laivaan.
Vaikka valvontakamerat eivät ole fyysisiä esteitä, jotka vaikeuttavat kulkua laivassa, voivat ne auttaa havaitsemaan mihin osiin hyökkääjillä on jo pääsy ja näin auttaa miehistöä toimimaan paremmin. Valvomo tulee asettaa turvalliseen sijaintiin aluksen sisällä, esimerkiksi komentosillalle. Aluksen kannella kohdistettuja valoja voidaan käyttää tässäkin vaiheessa hyökkääjien toiminnan vaikeuttamiseen. Hyökkääjien yleisin keino laivan sisärakenteisiin pääsemiseksi on ikkunat ja ovet, tämän vuoksi kaikkiin ulkoisiin ikkunoihin ja mahdollisiin ovissa oleviin ikkunoihin on hyvä asettaa kalterit pääsyn estämiseksi. Ovien ja luukkujen tulee olla vesitiiviitä ja lukituksen lisäksi on mahdollista käyttää erilaisia väliaikaisia barrikadeja, jotka voidaan asentaa ja poistaa kulkiessa riskialueiden läpi. (Marine Insight 2019a: Shipuniverse 2024; UKMTO 2025, 26–36.)

8.3 Kolmas taso

Kolmas taso kattaa aluksen tärkeimmät ydinalueet eli konehuoneen, miehistön elintilat ja komentosillan, tämä taso on myös viimeinen puolustus aluksen hallinnan menettämisen estämiseksi. Kolmas taso käyttää paljon samoja lukitusmetodeja kuin aikaisempi toinen taso, mutta sen tarkoitus on suojata aluksen kontrollin kannalta tärkeät alueet.
Miehistön turvaksi suunnitellaan kokoontumispiste jonne miehistö, jota ei tarvita komentosillalla voi hakeutua hyökkäyksen tapahtuessa. Kyseinen kokoontumispiste voi olla esimerkiksi miehistön elintilat tai konehuoneisto. Kokoontumispiste pitää suunnitella niin, että sinne pääsy hyökkääjiltä on estetty ja se vaatii suurta vaivaa. Kokoontumispisteessä tulee myös olla ruokaa, vettä ja jokin kommunikointikyky, esimerkiksi satelliittipuhelin. Komentosilta on usein hyökkääjien ensimmäinen kohde, jotta he saisivat kyvyn hallita aluksen liikkeitä.

Aseellisissa hyökkäyksissä komentosiltaan kohdistuu tulitusta jo ennen laivaan pääsyä tarkoituksena saada laivaa hidastamaan vauhtiaan tai pysähtymään kokonaan. Tämän aseellisen uhan vuoksi komentosillan ikkunoiden tulisi kestää useimpien käsiaseiden tuli, myös hiekkasäkkejä voidaan käyttää suojauksena. Niin kuin muun miehistön kokoontumispisteen myös komentosillan sisäänkäynti täytyy suojata hyvin, sillä se on viimeinen keino säilyttää aluksen hallinta. Hyökkääjät saattavat käyttää käsiaseiden lisäksi erilaisia räjähteitä, yleisimpänä RPG eli käsin pidettävä panssarintorjuntasinko. Räjähteitä vastaan voidaan käyttää verkkoaitaa, jotta räjähdyksen suurin voima ei kohdistu itse komentosillan rakenteisiin ja teräksestä valmistettuja kilpiä räjähteistä aiheutuvien sirpaleiden torjuntaan. toimivat kommunikointijärjestelmät ovat todella tärkeitä, sillä yleensä viranomaiset haluavat tietää koko miehistön sijainnin ennen kuin he aloittavat pelastusoperaation. (UKMTO 2025, 26–36.)

Turvallisuutta parantavat investoinnit eivät ole halpoja ja kertakustannukset voivat olla erittäin suuret. Ne ovat silti kannattavia jo miehistön turvallisuuden ja tätä kautta saavutettavan pienemmän vaihtoasteen vuoksi. Miehistön mielenrauha ei kuitenkaan ole ainoa syy parantaa aluksen turvallisuutta, sillä ne tuovat myös taloudellisia säästöjä. (Shipuniverse 2024.)



Taulukko 2. Suojausmenetelmien alkuinvestoinnit ja vuosittainen säästö (Shipuniverse 2024).

Taulukko näyttää eri turvallisuutta nostavien toimintojen investointi hinnan ja siitä seuraavat vuosittaiset säästöt. Säästöt muodostuvat halvemmista vakuutusmaksuista vakuutusyhtiön tekemän riskiarvion myötä. Nämä maksut voivat pienentyä jopa 10–20 %, joka tarkoittaa satojen tuhansien vuosittaisia säästöjä. Myös onnistuneiden hyökkäysten määrä laskee, joka vähentää hyökkäyksistä tapahtuvien toimintapysähdyksien määriä ja myös tapauksia, jossa joudutaan maksamaan lunnaita kaappaajille. (Shipuniverse 2024.)

9 Teknologia

Autonomisten tasojen lisäksi on hyvä tarkastella aluksissa hyödynnettäviä teknologioita. Tässä työssä käydään läpi MUNIN- projektin kehittämiä teknologioita. MUNIN- tutkimusprojektina oli kehittää konsepti miehittämättömän kauppa-aluksen toiminalle, jossa arvioitiin aluksen teknistä, taloudellista ja oikeudellista toteutettavuutta (Fraunhofer CML 2025). MUNIN kehittämän konseptin mukaan autonomisen aluksen teknologiat voidaan jakaa seitsemään kategoriaan (Fraunhofer CML 2025).

9.1 Kehittynyt sensorimoduuli

Aluksilla sensorit ja sensorin datojen käsittely korvaavat miehistön tarvetta tarkkailla ympäristöä laivalla. Sensorimoduulin vastuulla on kohteiden havainnointi ja luokittelu sekä ympäristön havainnointia. Sensori käyttää infrapuna- ja visuaalisten spektrikameroista sekä tutkasta saatavaa dataa kohteiden havaitsemiseen. Kohteen havaitsemisen yhteydessä sensori määrittää, ovatko ne vaaraksi aluksella tai onko niitä tutkittava tarkemmin. Järjestelmä myös kerää ja arvioi navigaatio-, meteorologisten ja turvallisuusantureiden dataa, jonka pohjalta se rakentaa paikallisen kartan kohteista ja mahdollisista vaaroista. Sensorin tietoja käyttää pääasiassa syvänmeren navigointijärjestelmä, mutta se on esitetty myös rannikon ohjauskeskuksen integroidulla tilannenäytöllä. (Fraunhofer CML 2025.)

RADAR ja LiDAR

Kyseisiä aluksilla käytettäviä sensoreita ovat muun muassa RADAR ja LiDAR. RADAR (Radio detection and ranging) mittaa etäisyyksiä radiotaajuuksia hyödyntämällä ja LiDAR (Light detection and ranging) puolestaan visuaalisia- tai infrapunavaloja. Etäisyyslaitteessa on lähetin, joka lähettää signaaleja ja vastaanotin, joka mittaa kohdepinnoista heijastuvien pulssien aikaviivettä sekä saapumissuuntaa. RADAR- laitteissa käytetään leveän säteen antenneja, minkä

vuoksi kohteen pieniä rakenteellisia yksityiskohtia on vaikea erottaa toisistaan. Nykyaikaiset LiDAR- laitteet perustuvat puolestaan yksinomaan lasereihin, minkä vuoksi niillä on hyvin kapeat ja kollimoidut valonsäteet. Tämän myötä LiDAR voi etäältä rakentaa kohteesta yksityiskohtaisemman mallin. LiDAR:in haittapuolena on se, että ne ovat alttiita erilaisille sääilmiöille kuten esimerkiksi sateelle. Radioaallot puolestaan läpäisevät pilviä, savua ja sumua paremmin kuin visuaaliset aallonpituudet, jonka myötä RADAR- laitteet ovat parempi valinta alusten pitkän kantaman kaukokartoitusjärjestelmäksi. (Thombre ym. 2022, 69.)

9.2 Syvänmeren navigointijärjestelmä

Navigointijärjestelmä otettiin käyttöön, jotta aluksia voidaan käsitellä ilman miehistöä valtameren matkoilla. Navigointijärjestelmällä varmistetaan, että alus noudattaa suunniteltua reittiä nykyisen käyttöalueen antamien sallittujen poikkeamien puitteissa. Kyseiset poikkeamat voivat johtua esimerkiksi vaikeiden sääolosuhteiden kehittymisestä tai monimutkaisten liikennetilanteiden välttämisestä. Poikkeamissa otetaan huomioon aluksen tiedot, tekninen kunto sekä sää- ja liikennetilanne. Navigointijärjestelmän avulla voidaan muun muassa määrittää COLREG-velvoitteet muita aluksia kohtaan ja ohjata autonomista alusta sääntöjen mukaisesti, optimoida meteorologisten ennusteiden perusteella valtameren ylittävät matkasuunnitelmat, operoida alusta turvallisesti välittömissä ja ankarissa sääolosuhteissa IMO:n sääopastuskriteereiden mukaisesti. Syvänmeren navigointijärjestelmä voi toimia täysin itsenäisesti, mutta rannikon ohjauskeskuksella on mahdollisuus olla siihen vuorovaikutuksessa ja siten myös etäohjata alusta. (Fraunhofer CML 2025.)

9.3 Kauko-ohjattava tukijärjestelmä

Kauko-ohjattava tukijärjestelmä kehitettiin rannikon valvontakeskuksen ja syvänmeren navigointijärjestelmän apulaitteeksi. Tukijärjestelmä auttaa aluksia

suorittamaan ohjauksia välttääkseen törmäyksen navigoitaessa rajoitetuilla vesiväylillä ja satamissa. Jotta miehittämättömät ja autonomiset alukset voisivat toimia turvallisesti ja tehokkaasti, tarjoaa tukijärjestelmä alukselle ennakoidun liikeradan. Tukijärjestelmä tarjoaa myös aluksen liike-ennusteita, jotka ovat seurausta tietylle alukselle sen tietyssä ympäristössä annetuista peräsimen tai moottorin komennoista. Liike-ennusteiden myötä tukijärjestelmän on mahdollista tarjota laskelmia ja näyttöjä ennakoiduille alusten liikkeille ohjailukyvyn asettamissa rajoissa. Kyseisiä laskemia ja näyttöjä voidaan tehdä myös rajoitetun tiedonsiirtoyhteyden kapasiteetilla, jota hyödynnetään monimutkaisten ohjausten suorittamiseen tarkistamalla suunnittelun komentosarjan tulokset. Liike-ennusteet ovat tärkeitä sillä ne mahdollistavat tarkan autonomisen sekä etänavigoinnin. (Fraunhofer CML 2025.)

9.4 Moottorin valvonta- ja ohjausjärjestelmä

Moottorin valvonta- ja ohjausjärjestelmä on parannus olemassa oleviin laivojen automaatio- ja ohjausjärjestelmiin. Järjestelmän päätavoitteena on lisätä kehittyneempiä kunnonvalvontatoimintoja. Kunnonvalvonnan lisäksi navigointijärjestelmiin ja rannikon valvontakeskukseen on lisättävä digitaalisia liitäntöjä, jotta konehuoneen ja muiden teknisten järjestelmien autonominen ja miehittämätön toiminta olisi mahdollista. Kriittisten teknisten järjestelmien jatkuva valvonta on hyvin tärkeää, jotta voidaan estää toimintahäiriöt ja rikkoutumiset syvänmeren matkan aikana. Valvonta on tärkeää myös paremman kunnossapidon suunnittelun kannalta. Aluksen yleinen tekninen ja ympäristöllinen suorituskyky riippuu huolellisesta diagnostiikasta. Kyseinen valvonta- ja ohjausdiagnostiikkajärjestelmä kehitettiin vankalla havaitsemiskyvyllä esimerkiksi rikkinäisiä, palaneita ja puuttuvia männänrenkaita tai säteittäistä kulumista varten. Järjestelmän on mahdollista havaita myös sisäsylinterin lämpöylikuormituksen. Teknisten järjestelmien etäinen ja tehokas valvonta sekä ohjaus edellyttää monitasoista päätöstukitietojen yhdistämistä, jonka myötä vähennetään viestinnän

kaistanleveyttä ja mahdollistetaan suorituskykytrendien seuraamista. (Fraunhofer CML 2025.)

9.5 Ylläpidon vuorovaikutusjärjestelmä

Tekninen toiminta on yksi monimutkaisin osa siirryttäessä miehittämättömiin ja autonomisiin aluksiin. Nykypäivän laivojen järjestelmät on suunniteltu ja rakennettu niin, että miehistön saatavuus on otettu huomioon. Ilman miehistöä aluksien järjestelmät on suunniteltava uudelleen tai mahdollisesti otettava uusia prosesseja käyttöön, jotta mahdollisestaan aluksen toimiminen ongelmitta merellä ja että sen yleinen huolto voidaan suorittaa ilman että aluksen huoltokatkon riski kasvaa tarpeettomasti teknisten vikojen vuoksi. Ylläpidonstrategiaan sisältyy alusjärjestelmän uudelleensuunnittelu sekä myös uuden vuorovaikutusjärjestelmän kehittäminen kunnossapidolle. Kyseiset toiminnot sisältävät laajennetun latteiden seurannan sekä ehtojen yhdistämistoiminnot satelliittiviestinnän kaistanleveyden minimoimiseksi. Hanke on analysoinut olemassa olevien alusten teknisiä järjestelmiä ja osoittanut ne järjestelmät, jotka vaativat parempaa valvontaa ja tukea rannikon valvontakeskukselta. (Fraunhofer CML 2025.)

9.6 Energiatehokkuusjärjestelmä

Miehittämättömillä ja autonomisilla aluksilla on monia erilaisia mahdollisuuksia energiatehokkuuden optimointiin. Useat mahdollisuudet soveltuvat myös tavanomaisiin aluksiin ja lisääntynyt instrumentointiaste ja automatisoitu valvonta yksinkertaistavat toteutusta. Miehittämättömillä ja autonomisilla aluksilla omaavat myös erilaiset moottori- ja käyttövoima kokoonpanot verrattuna nykyisiin aluksiin. Yhtenä merkittävänä erona on korkeampi irtisanomisvaatimus. Moottoreiden, käyttövoiman ja ohjausjärjestelmän sekä mahdollisesti dieselsähköjärjestelmän jäljentäminen on välttämätöntä. Majoituksen ja mahdollisen raskaan polttoaineen käsittelyjärjestelmän poisto voi mahdollistaa uudenlaisen energianhallintastrategian. MUNIN analysoi

energiantehokkuusjärjestelmän avulla aluksen tehovaatimuksia ja käyttää tuloksia moottorinohjausjärjestelmän säätelyn perustana, jonka myötä se optimoi energianhallinnan sekä polttoaineen kulutuksen. Järjestelmä pyrkii myös hyödyntämään hukkalämmön talteenottoa sekä muita saatavilla olevia energialähteitä. Järjestelmä laatii samalla säännöllisin väliajoin raportin kulutuksesta, päästöistä ja aluksen suorituskyvystä rannikon operaattorille. (Fraunhofer CML 2025.)

9.7 Rannikon valvontakeskus

Rannikon valvontakeskus toimii yhtämittaisesti miehitettynä valvonta-asemana autonomisten alusten laivaston valvomiseksi ja ohjaukseksi. Alukset liikennöivät yleensä suuriman osan ajastaan ilman rannikon puuttumista tilanteeseen. Sellaisissa tilanteissa, joissa automatisoidut laivajärjestelmät eivät voi käsitellä tilannetta turvallisesti, saavat ne apua rannikolta. Kyseiset turvallisena pidettävät rajat voidaan mukauttaa niin sanotun käyttöalueen sisällä, joka asettaa aluksen navigointirajat. Käyttöalueeseen sisältyy myös muita tekijöitä kuten näkyvyys, aallonkorkeus sekä liikenne. Kyseisen valvontayksikön on oikeudellisesta näkökulmasta visioitu ottamaan edes osan alusten päälliköiden ja insinöörien vastuualueista. Tehtäviä, joita rannikolla toimiville henkilöstöille kuuluu ovat muun muassa VHF- viestintä, VTS- raportointi, energianhallinta, kunnonvalvonta sekä huoltosuunnittelu. Tämän myötä alus toimii pääasiallisesti automaattitilassa ja siirtyy autonomiseen tilaan tehdessään väistöliikkeitä tai rutiininomaisia koneiston säätöjä. Kun rannikon valvontakeskus suorittaa komentoja, siirtyy alusjärjestelmät kauko-ohjaustilaan. Hätätilanteissa puolestaan alus aktivoi vikasietotilan, jos rannikolta tarvittavaa apua ei saada esimerkiksi yhteyden menettämisen vuoksi. MUNIN- konsepti turvautuu valvontakeskukseen monimutkaisten tilanteiden hoitamisessa, sillä aluksessa oleva autonominen ohjain toimii ainoastaan sille määriteltyjen rajoitusten puitteissa. Tämä edistää tasapainoa teknologisen monimutkaisuuden ja taloudellisen rationaalisuuden välillä, joka tekee siitä toteuttamiskelpoisen konseptin. (Fraunhofer CML 2025.)

10 Johtopäätökset

Kirjallisuuskatsaus tutkimusmenetelmänä toimi hyvin, sillä se mahdollisti erilaisten lähteiden käytön ja tarjosi laaja-alaisen näkökulman turvallisuuteen ja ennaltaehkäisyyn vaikuttaviin asioihin. Lähteiden luotettavuus on vahva, sillä käytössä oli paljon eri kansainvälisten organisaatioiden ja valtiollisten toimijoiden tuottamaa aineistoa.

Merenkulku on merkittävä osa globaalia taloutta ja kaupankäyntiä, eikä sen rooli ole väistymässä. Hyökkäykset aluksia vastaan ovat merkittävä uhka työntekijöiden hyvinvoinnille ja taloudelliselle menestykselle. Siksi on tärkeää, että merenkulun turvallisuuden eteen tehtyä kansainvälistä yhteistyötä jatketaan ja mukautetaan teknologian muuttaessa toimintaympäristöä.

Autonomiaa ja tekoälyä käytetään jo laajasti, mutta se on vielä alkeellista sen mahdollisuuksiin nähden, sillä täysin autonomisia aluksia ei juurikaan ole vaan ne kykenevät vain osittaiseen autonomiaan ja toistaiseksi autonomiaan ei voida luottaa tarpeeksi eli sitä ei voida jättää ilman valvontaa. Teknologia on mahdollistanut kauko-ohjauksen maalta käsin, joka mahdollistaa paremman tuottavuuden ja miehistön turvallisuuden.

Viime vuosien aikana esimerkiksi Itämerellä on tapahtunut useita tapauksia, joissa laiva on raahannut ankkuria ja rikkonut valtioille tärkeitä sähkö- ja tietoliikennekaapeleita. Ottamatta kantaa syyllisiin tai tahallisuuteen tutkintojen ollessa käynnissä herättää tämä huolen siitä millä tavoin hyökkääjät voivat käyttää kaappaamiaan aluksia hyväksi. Mahdollinen riski laivan käyttämisestä infrastruktuurin vahingoittamistarkoitukseen nostaa esille aluksen suojauksen ja kansainvälisen yhteistyön merkittävyyttä valtausyrityksien torjunnassa. Erityisesti rannikkovaltioilla tulisi olla kyvykkyys pysäyttää ja tunkeutua jo vallattuihin laivoihin maan oman ja kansainvälisen lain näin salliessa.

Mahdollinen jatkotutkimuksen kohde on rannikkomaiden kyvykkyys ja valtuudet ennaltaehkäistä sekä torjua turvallisuusuhkia alue ja kansainvälisillä vesillä. Tutkimuksessa voisi tarkastella syvemmin millaisia resursseja valtioilla tulisi olla

turvallisuuden parantamiseksi ja miten valtioiden omia sekä kansainvälisiä lakeja ja sopimuksia tulisi muuttaa, jotta näiden resurssien käyttö olisi tehokkaampaa.

Lähteet

Ahmad, M. 2020. Maritime piracy operations: Some legal issues. Viitattu 30.10.2024. https://www.tandfonline.com/doi/epdf/10.1080/25725084.2020.1788200?needAccess=true

CCDCOE 2022. Cybersecurity considerations in autonomous ships. Viitattu 9.11.2024. https://ccdcoe.org/uploads/2022/09/Cybersecurity_Considerations_in_Autonomous_Ships.pdf

Ceva logistics 2024. Maritime transport. Viitattu 9.11.2024. https://www.cevalogistics.com/en/glossary/maritime-transport

Chang, A.; Robles, P.& Bradsher, K. 2024. How Houthi attacks in the Red sea have upended global shipping. Viitattu 5.10.2024. https://go.gale.com/ps/i.do?id=GALE%7CA781187179&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=03624331&p=AONE&sw=w&userGroupName=anon%7E83efb940&aty=open-web-entry

Chorev, S. 2023. The Suez Canal: Forthcoming strategic and geopolitical challenges. Viitattu 4.11.2024. https://link.springer.com/chapter/10.1007/978-3-031-15670-0_1#author-information

Critical maritime routes 2023. Preventing piracy: Best practices for maritime security. Viitattu 24.12.2024. https://criticalmaritimeroutes.eu/preventing-piracy-best-practices-for-maritime-security.html

Edumaritime 2022. Ship security (MARSEC levels) – ISPS code requirements. Viitattu 23.11.2024. https://www.edumaritime.net/isps-code/ship-security

Frane, M.; Miskovic, J.; Pavic, I. 2023. Analysis of current threats to ships from 2019 to 2022 in selected regions. Viitattu 21.11.2024. https://www.proquest.com/docview/2806184270/9BC02341A90A46AEPQ/7?accountid=14446&sourcetype=Scholarly%20Journals

Fraunhofer CML 2025. MUNIN – research in maritime autonomous systems project results and technology potentials. Viitattu 18.1.2025. https://www.cml.fraunhofer.de/en/research-projects/munin.html

Haugstvedt, H. 2021. Red sea drones: How to counter Houthi maritime tactics. Viitattu 28.11.2024. https://warontherocks.com/2021/09/red-sea-drones-how-to-counter-houthi-maritime-tactics/

Iep 2024. Autonomy: normative. Viitattu 15.11.2024. https://iep.utm.edu/normative-autonomy/

IMO 2019. Marine environment. Viitattu 25.12.2024. https://www.imo.org/en/OurWork/Environment/Pages/Default.aspx

IMO 2022. Guidelines on maritime cyber risk management. Viitattu 15.1.2025. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf

IMO 2023. Consideration of the reports and recommendations of the maritime safety committee – Combating security threats by organized crime in the maritime industry. Viitattu 5.11.2024. https://sustainableworldports.org/wp-content/uploads/IMO-33-11-1-Combating-security-threats-by-organized-crime.pdf

IMO 2024a. Maritime cyber risk. Viitattu 25.12.2024. https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

IMO 2024b. Red Sea project. Viitattu 25.11.2024. https://www.imo.org/en/OurWork/Security/Pages/RedSeaProject.aspx

IMO 2024c. SOLAS XI-2 and the ISPS Code. Viitattu 27.11.2024. https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

IMO 2024d. United Nations Convention on the Law of the Sea. Viitattu 28.11. 2024. https://www.imo.org/en/OurWork/Legal/Pages/UnitedNationsConventionOnTheLawOfTheSea.aspx

Infomaritime 2018. Timeline – development of autonomous ships (1970s-2018). Viitattu 10.11.2024. http://infomaritime.eu/index.php/2018/06/08/timeline-development-of-autonomous-ships/

Inmarsat 2024. IACS unified requirements E26 and E27 Cyber security beyond compliance. Viitattu 8.1.2025. https://www.inmarsat.com/content/dam/inmarsat/corporate/documents/maritime/insights/MBU_IACS_UR_E26_E27_whitepaper_June_2024.pdf.downloadasset.pdf

International Chamber of Commerce 2025. Maritime piracy dropped in 2024 but crew safety remains at risk. Viitattu 22.1.2025. https://iccwbo.org/news-publications/news/maritime-piracy-dropped-in-2024-but-crew-safety-remains-at-risk/

ISPS code A 2024. Viitattu 17.12.2024. https://www.classnk.or.jp/hp/pdf/activities/statutory/isps/code/ISPS_CodeA.pdf

Lucas, E.; Rivera-Paez, S.; Crosbie, T. & Jensen, F. 2020. Maritime security: Counter-terrorism lessons from maritime piracy and narcotics interdiction. Viitattu 22.10.2024. https://www.proquest.com/docview/2447469582/bookReader?accountid=14446&sourcetype=Books

Marine Insight 2019a. 10 Things to consider before your ship enters piracy prone area. Viitattu 17.12.2024. https://www.marineinsight.com/marine-piracy-marine/entering-piracy-zone/

Marine Insight 2019b. What can shippers do against pirate attacks at sea? Viitattu 19.12.2024. https://www.marineinsight.com/marine-piracy-marine/can-shippers-pirate-attacks-sea/

Marine Insight 2024. 18 Anti-piracy weapons for ships to fight pirates. Viitattu 28.12.2024. https://www.marineinsight.com/marine-piracy-marine/18-anti-piracy-weapons-for-ships-to-fight-pirates/

Maritime-cybersecurity 2024. Cybersecurity for the maritime industry. Viitattu 25.12.2024. https://www.maritime-cybersecurity.com/

Mingyu, K.; Tae-Hwan, J.; Byongug, J. & Han-Seon, P. 2020. Autonomous shipping and its impact on regulations, technologies, and industries. Viitattu 28.11.2024. https://www.tandfonline.com/doi/epdf/10.1080/25725084.2020.1779427?needAccess=true

Munim, Z. & Schramm, H. 2018. The impacts of port infrastructure and logistics performance on economic growth: the mediating role of seaborne trade. Viitattu 12.10.2024. https://link.springer.com/article/10.1186/s41072-018-0027-0#Abs1

Papastavridis, E. 2014. Crimes at sea: A law of the sea perspective. Viitattu 22.10.2024. https://www.semanticscholar.org/paper/Crimes-at-Sea%3A-A-Law-of-the-Sea-Perspective-Papastavridis/c8705cbaf6bcc2685a337d685c254fd6343414b6

Porathe, T.; Hoem, Å.; Johnsen S. & Rødseth, Ø. 2018. At least as safe as manned shipping? Autonomous shipping, safety and “human error.” Viitattu 15.12.2024. https://www.researchgate.net/publication/328042940_At_least_as_safe_as_manned_shipping_Autonomous_shipping_safety_and_human_error

Salminen, A. 2023. Mikä kirjallisuuskatsaus? Viitattu 22.4.2025. https://osuva.uwasa.fi/bitstream/handle/10024/15470/978-952-395-081-8%20%28PDF%29.pdf?sequence=2&isAllowed=y

Sandkamp, A.; Stamer, V. & Yang, S. 2021. Where has the rum gone? The impact of maritime piracy on trade and transport. Viitattu 12.12.2024. https://link.springer.com/article/10.1007/s10290-021-00442-1#Abs1

Schneider, P. 2023. Maritime terrorism and piracy: The development of maritime security and its governance. Viitattu 10.11.2024 https://ediss.sub.uni-hamburg.de/bitstream/ediss/10506/1/HabilitationPatriciaSchneider2023.pdf

SEAM 2024. Embracing maritime autonomy. Viitattu 5.1.2025. https://www.seam.no/insights/embracing-maritime-autonomy

Shipuniverse 2024. Innovative ship modifications to combat piracy. Viitattu 3.2.2024. https://www.shipuniverse.com/innovative-ship-modifications-to-combat-piracy/

Sisäministeriö 2024a. Järjestäytynyt rikollisuus vaikuttaa laajasti yhteiskuntaan. Viitattu 22.10.2024. https://intermin.fi/poliisiasiat/jarjestaytynyt-rikollisuus

Sisäministeriö 2024b. Terrorismin torjunta perustuu laajaan yhteistyöhön. Viitattu 16.10.2024. https://intermin.fi/poliisiasiat/terrorismin-torjunta

Tauringana, V.; Tingbani, I.; Okafor, G. & Sha'ven, W. 2020. Terrorism and global business performance. Viitattu 7.11.2024. https://onlinelibrary.wiley.com/doi/epdf/10.1002/ijfe.2085

The Marine Executive 2024. Galaxy leader's crewmembers mark one year in Houthi captivity. Viitattu 1.12.2024. https://maritime-executive.com/article/galaxy-leader-s-crewmembers-mark-one-year-in-houthi-captivity

Thombre, S. 2022. Sensors and AI techniques for situational awareness in autonomous ships: a review. Viitattu 5.1.2025. https://ieeexplore.ieee.org/document/9207841?denied=

Traficom 2019. Meriliikenteen automaation kehitys. Viitattu 15.12.2024. https://www.traficom.fi/sites/default/files/media/publication/Meriliikenteen_automaation_kehitys_Traficom_julkaisuja_122_2019.pdf

Tseng, P.; Her, Z. & Pilcher, N. 2021. Piracy defense strategies for shipping companies and ships: A mixed empirical approach. Viitattu 3.1.2025. https://www.napier.ac.uk/~/media/worktribe/output-2774695/piracy-defense-strategies-for-shipping-companies-and-ships-a-mixed-empirical-approach.pdf

UKMTO 2025. BMP maritime security. Viitattu 22.3.2025. https://cd.royalnavy.mod.uk/-/media/ukmto/bmp/bmp-ms_hi-res_s.pdf?rev=2c338d856b0b4c169364b96766b12b27&hash=8A19D49513D46613C44C7B51FC16F8D1

United Nations 2024. Organized crime. Viitattu 12.11.2024. https://www.unodc.org/unodc/en/organized-crime/intro.html

Wróbel, K.; Montewka, J. & Kujala, P. 2017. Towards the assessment of potential impact of unmanned vessels on maritime transportation safety. Viitattu 28.11.2024. https://www.sciencedirect.com/science/article/pii/S095183201630337?via%3Dihub