TALLINNA TEHNIKAÜLIKOOL
EESTI MEREAKADEEMIA

Merenduskeskus

Lauri Roolaid

KÜBERTURBE HARIDUS LAEVAOHVITSERIDE VÄLJAÕPPES NING SOOVITUSED SELLE KORRALDAMISEKS

Magistritöö

Juhendaja: Dan Heering

Tallinn 2018

Olen koostanud töö iseseisvalt.
Töö koostamisel kasutatud kõikidele teiste autorite töödele,
olulistele seisukohtadele ja andmetele on viidatud.
Lauri Roolaid ……
(allkiri, kuupäev)
Üliõpilase kood: 163534VAAM
Üliõpilase e-posti aadress: lauriroolaid@gmail.com

Juhendaja Dan Heering:
Töö vastab lõputööle esitatud nõuetele
……
(allkiri, kuupäev)

Kaitsmiskomisjoni esimees:
Lubatud kaitsmisele
……
(ametikoht, nimi, allkiri, kuupäev)

Annotatsioon

Alates 21. sajandi teisest kümnendist on merendussektoris hakatud küberohtudele suurt tähelepanu pöörama. Sellega tegeletakse mitmel tasandil – seadusandlus, kaubaoma–nikud, kindlustusseltsid, klassifikatsiooniühingud, meremeestele täiendõpet pakkuvad ettevõtted ja muud huvirühmad. Nimetatud probleem on aga avaliku tähelepanuta jäänud meremeeste väljappes mereharidusasutustes. Infotehnoloogia võimekust kasutatakse laevadel nii administratiivseteks tegevusteks kui ka füüsiliste protsesside juhtimise toetamiseks ja pidev võrgusolek on tavaline nähtus. Sellise tehnoloogiaga puutuvad oma igapäevatöös kokku laevajuhid ja -mehaanikud. Laevade ohutu käitamise tagamiseks on just laevaohvitseridele oluline olla teadlik spetsiifilistest küberohtudest merenduses.

Magistritöö eesmärkideks oli selgitada välja küberturbe käsitlemise tase laevaohvitseride väljaõppes ning seejärel teha soovitused selle korraldamiseks. Uuring koosnes neljast etapist: valimi määratlemine ja asutuste kaardistamine, küsitlusuuring, ekspertintervjuud ning tulemuste analüüs ja soovituste koostamine. Valim piiritleti Euroopa mereõppeasutustega, kes pakuvad väljaõpet piiramatu kogumahutavusega laevade vahitüürimeestele ja/või piiramatu peamasinate efektiivse koguvõimsusega mootorlaeva vahimehaanikutele. Kokku leiti 65 kooli 31-st riigist. Valimist leiti piisavat infot 35 kooli kohta, kellest 3 kooli pakkus küberturbe haridust üldisel tasemel ning ainult 2 kooli käsitles seda erialaspetsiifiliselt. Samas koolid üldiselt teadvustasid probleemi ja tunnistasid küberturbe õpetamise olulisust laevaohvitseridele.

Lähtudes uuringu käigus kogutud kvalitatiivsest informatsioonist, leidis autor, et parim lahendus on viia läbi kahepäevane koolitus. Koolituse esimesel päeval käsitletakse merendusega seotud küberturbe teoreetilisi aspekte ning teisel päeval viiakse etteantud stsenaariumite põhjal läbi iseseisev riskide hindamine. Magistritööga pakkus autor mereõppeasutustele, aga ka täiendkursusi korraldavatele ettevõetele ja muudele huvirühmadele, ühe võimaluse erialaspetsiifilise küberturbe hariduse käsitlemiseks laevaohvitseride väljaõppes.

Võtmesõnad: Küberturve, infotehnoloogia, käidutehnoloogia, laeva haavatavused, laevaohvitseride väljaõpe, mereõppeasutused, meresõiduohutus, laevade käitamisohutus.

Sisukord

Sissejuhatus

2017. aastal maksis küberkuritegevus suurematele ettevõtetele, mille arvutivõrgu ühenduste arv on üle 1000, keskmiselt 11,7 mln USD (Ponemon Institute LLC 2017). Arvatakse, et aastaks 2021 läheb küberkuritegevus maailmale maksma 6 triljonit eurot (Cybersecurity Ventures 2017, 3). Transpordisektor, sh merendus, on püsinud aastatel 2015–2017 viie kõige haavatavama majandusharu hulgas ning ka järgmisel aastal ei ole selles suhtes muutusi oodata (*ibid*., 10). Magistritöö kirjutamise ajal viimane kulukaim küberintsident merenduses toimus 2017. aasta juunis, kui lunavaraks (*ransomware*) maskeeritud *NotPetya* pühkuri (*wiper*) rünne läks Taani laevandusettevõttele *A.P. Moller–Maersk Group* maksma kuni 300 mln USD (Mimoso 2017).

Kui küberrünne merendusettevõtte kaldainfosüsteemile võib lõppeda nii finants- kui mainekahjuga, siis rünne laevale paneb lisaks ohtu ka inimesed ja keskkonna. Tänapäeva laevad sõltuvad oma töös suuresti info- ja käidutehnoloogiast (IT - *Information Technology*, OT - *Operational Technology*) ning on seetõttu küberohtudele haavatavad. Magistritöö autor töötab 1989. aastal ehitatud segalastilaeval, kus kogu suhtlus välismaailmaga toimub mobiil- või satelliitside vahendusel, dokumendihalduseks kasutatakse arvuteid ning navigeerimist globaalse satelliitnavigatsioonisüsteemita (GNSS – *Global Navigation Satellite System*) ei kujutaks ettegi. Kaasaegsed laevad on aga juba tõelised küberfüüsilised süsteemid (*cyber-physical system*). 2017. aasta detsembris Shanghais debüteerinud puistlastilaeval *Great Intelligence* on masinõppevõimekus (*machine learning*), mis võimaldab välis- ja sisekeskkonnast ammutatud info põhjal optimeerida teekonda, hinnata laeva füüsilist seisukorda ning tuvastada potentsiaalseid ohuallikaid (CCTV+ 2017).

Rahvusvaheline Mereorganisatsioon (IMO – *International Maritime Organization*) on teema olulisust teadvustanud ning 16.07.2017 võeti mereohutuse komitee (MSC – *The Maritime Safety Committee*) 98. istungjärgul vastu resolutsioon MSC.428(98) – „Merendusega seotud küberriskide haldamine meresõiduohutuse korraldamise süsteemides“ (*Maritime Cyber Risk Management in Safety Management Systems*), millega tehakse küberriskide käsitlemine laeva meresõiduohutuse korraldamise süsteemis (SMS - *Safety Management System*) kohustuslikuks hiljemalt ettevõtte vastavuse

tunnistuse (DOC – *Document of Compliance*) esimeseks iga-aastaseks kontrolliks pärast 2021. aasta 1. jaanuari (Maritime… 2017). Kuna meremehed peavad laeva ohutul käitamisel järgima SMS-is kehtestatud protseduure, siis puudutab see nõue ka neid. Magistritöö kirjutamise ajal ei olda selleks kaugeltki valmis.

2017. aasta augustis ja septembris laevapere liikmete seas läbi viidud küsitlustest selgus, et kuigi meeskonna liikmed mõistavad oma vastutust seoses laeva IT süsteemide turvalisusega, siis 84% neist ei ole saanud kas üldse, või on saanud ainult vähesel määral, küberturbe alast väljaõpet oma tööandjalt (NSSLGlobal 2017). Meremeeste koolitamise vajaduse tõi esile ka Dan Heering oma magistritöös (Küberturvalisuse… 2017, lk 66). Samas selgus küsitlusest Eesti reederite seas, et üheksast ettevõttest on seda teinud ainult kaks, ning 55,6% ei pidanud seda hetkel vajalikuks (*ibid*., 60). Magistritöö autor leiab, et vastutust meremeeste küberturbe alase pädevuse eest ei peaks panema ainult tööandjale, vaid seda peaks käsitlema juba esmase väljaõppe faasis, ehk mereõppeasutustes.

Miinimumnõuded meremeeste väljaõppele on kehtestatud meremeeste väljaõppe, diplomeerimise ja vahiteenistuse aluste rahvusvaheline konventsiooni (STCW - *The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers*) koodeksi A osaga. Magistritöö kirjutamise ajal STCW konventsiooniga meremeestelt küberturbe teadmisi veel ei nõuta. Ka on STCW konventsiooni täiendamine aeganõudev protsess. Näiteks elektronkaartide kuva ja informatsiooni süsteemi (ECDIS - *An Electronic Chart Display and Information System*) kasutamine paberkaartide asemel lubati juba 1995. aastal, kuid pädevusnõuded meremeestele viidi STCW konventsiooni alles 2012. aastal seoses Manila muudatustega (Becker-Heins 2014, 19). Mereõppe-asutused võivad alati STCW konventsiooniga määratust rohkem õpetada ning küberturve peaks olema kindlasti osa meremeeste väljaõppest.

Põhiliselt puutuvad laeva opereerimise seisukohast oluliste IT ja OT süsteemidega kokku masina- ja tekimeeskonna juhtivatel ametikohtadel töötavad meeskonnaliikmed – mehaanikud ja laevajuhid. Magistritöös kasutab autor laevajuhtide ja -mehaanikute koondnimetusena mõistet laevaohvitser. Laevaohvitseridele suunatud küberturbe väljaõpe peaks kindlasti arvesse võtma laevadega seotud ohtusid ning olema erialaspetsiifiline. Andmed selle kohta, kas üldse, kuidas, ja millisel tasemel mereharidusasutused küberturvet laevaohvitseride väljaõppes käsitlevad pole aga

leitavad ja sellpärast on raske teha soovitusi selle korraldamiseks. Seetõttu on tarvis esmalt uurida küberturbe käsitlemise olukorda laevaohvitseride väljaõppes. Seoses sellega püstitab autor hüpoteesi, et mereõppeasutused ei ole tulevaste laevaohvitseride väljaõppes pööranud piisavalt tähelepanu erialaspetsiifilisele küberturbe haridusele võimaldamaks neil laevu ohutumalt käitada.

Magistritööl on kaks eesmärki:

- kinnitada või ümber lükata magistritöös püstitatud hüpotees,
- teha mereõppeasutustele soovitused erialaspetsiifilise küberturbe hariduse korraldamiseks laevaohvitseride väljaõppes.

Nende eesmärkide saavutamiseks on uurimistöö jaotatud nelja etappi:

- valimi määratlemine ja asutuste kaardistamine,
- küsitluse läbiviimine,
- ekspertintervjuude läbiviimine,
- tulemuste analüüsimine ning soovituste esitamine.

Et valimit mitte liiga suureks ajada, piiritleti uuringus osalejad Euroopa mereharidusasutustega, kes pakuvad väljaõpet kas 500 ja suurema kogumahutavusega laeva vahitüürimeestele (OOW 500GT+) ja/või 750 kW ja suurema peamasinate efektiivse koguvõimsusega mootorlaeva vahimehaanikutele (EOOW 750kW+) nagu see on nõutud IMO mudelkursustega 7.03 ja 7.04 (IMO Model Courses). See tähendab, et hariduse andmine koolis ei ole vajalik kapteni ja/või vanemmehaaniku tasemel.

Magistritöö koosneb kolmest osast. Teoreetilises osas käsitletakse teemasid, mida laevaohvitseril on tarvis teada küberturbest, ja mida on oluline õpetada erialaspetsiifilise väljaõppe raames. Teises osas kirjeldatakse uurimistöö metoodikat, st valimi, küsitluse ja ekspertintervjuude koostamise ning läbiviimise põhimõtteid. Kolmandas osas analüüsitakse tulemusi ja leitakse parim viis küberturbe erialaspetsiifiliseks käsitlemiseks laevaohvitseride väljaõppes.

Magistritöös kasutatav IT ja küberturbe alane sõnavara on toodud kasutatud mõistete loetelus lisas 1. Selle koostamisel on peamise allikana kasutatud *Cybernetica* veebipõhist

andmekaitse ja infoturbe leksikoni (AKIT). Töö koostamisel kasutati erinevate merenduse huvirühmade materjale, merendusalaseid regulatsioone, küberturvet merenduses ja teistes sektorites käsitlevaid teadustöid ja muid IT ja OT süsteemidega seotud teadustöid. Selleks, et viia ennast kurssi ka täiendõppena meremeestele pakutavate küberteadlikkuse kursustega, läbis autor *JWC International* poolt koostatud ja Ühendkuningriigi Mere- ja Rannavalveameti (MCA – *Maritime and Coastguard Agency*) poolt tunnustatud merendusalase küberturbe teadlikkuse kursuse, mille tunnistus on toodud lisas 2.

1 Mida peab laevaohvitser küberturbest teadma

Magistritöö üheks eesmärgiks on mereõppeasutustele soovituste andmine küberturbe käsitlemiseks laevaohvitseride väljaõppes. Siinkohal ei pea autor silmas üldist küberhügieeni koolitust, vaid küberturbe käsitlemist spetsiifiliselt meremeeste vajadustest lähtuvalt. Siin võib paralleele tõmmata laevade füüsilise turvalisusega. Alates 1. jaanuarist 2014 peavad meremehed olema läbinud turvaalase koolituse ("Manila Amendments"… 2011), mille korraldamise miinimumnõuded on kehtestatud STCW koodeksi jaotisega A-VI/6. Muuhulgas peavad meremehed olema kursis meresõiduturvalisuse mõistete ja -regulatsioonidega, erinevate osapoolte kohustusega, ohuolukorra plaanide ja ettekannete tegemisega, turvaohtude äratundmisega, vastumeetmete rakendamisega jms (Meremeeste...).

Antud füüsilise turvalisuse pädevusnõuete kohta võib teha kaks järeldust. Esiteks on nende nõuete koostamisel peetud silmas spetsiifilist töökeskkonda laeval. Teiseks, meremeestelt ei nõuta relvade käsitsemist, pommide demineerimist ega piraatide kahjutuks tegemist. Samamoodi ei ole vaja meremeestest koolitada IT spetsialiste või häkkereid ning väga palju on võimalik korda saata omades teadlikkust merenduse ja laevadega seotud spetsiifilistest küberohtudest. Lähtudes sellest teadmises on magistritöö teoreetiline osa jagatud järgmisteks alateemadeks, mille käsitlemist autor laeva–ohvitseride küberturbe koolitusel vajalikuks peab:

- Asjakohased regulatsioonid ja suunised.
- Kes ja miks laeva ründab?
- Mida ja kuidas laeval rünnatakse?
- Kuidas laeva kaitsta?

1.1 Asjakohased regulatsioonid ja suunised

Meresõidu seisukohalt on küberturve oluline nii turvalisuse kui ka ohutuse aspektist lähtuvalt. Küberturve tähendab teabe konfidentsiaalsuse (*confidentiality*), tervikluse (*integrity*) ja käideldavuse (*availability*) säilimist või säilitamist küberruumis (AKIT, *sub* küberturve) ja hõlmab laeva peal meetmeid IT ja OT süsteemide ning andmete kaitsmiseks volitamata juurdepääsu, manipuleerimise ja halvangu (*disruption*) eest (BIMCO jt 2017, 2). Küberohutus omakorda tähendab inimeste või varade kaitstust mingi tervisekahjustust või majanduslikku kahju põhjustava sündmuse või ohule avatuse eest küberruumis (AKIT, *sub* küberohutus) ja katab laeval ohtlike (*safety-critical*) andmete ning IT ja OT käideldavuse ja tervikluse kaoga seotud riskid (BIMCO jt 2017, 2).

Küberohutust vähendava sündmuse põhjused laeval võivad muuhulgas olla küberturbe intsidendid, tarkvara hooldusel tekkivad tõrked ja laeva käitamise seisukohast oluliste andurite andmete kadu või nendega manipuleerimine. Küberturbe intsidendi näitena võib tuua elektronkaardi andmetervikluse rikkumise. (*ibid*.) Koos kaardiuuendustega võib kaasa saada kahjurvara (*malware*), mida arvuti antiviirus programm ja tulemüür ei tuvasta, ning mis elektronkaardid kasutuskõlbmatuks muudab. Selle tulemusena kasvavad riskid inimeludele, varale ja keskkonnale ning väheneb ohutus. Taoliste küberohutusega seotud riskide maandamiseks on laevadelt nõutud kas eraldiseisva ECDIS-e või paberkaartide olemasolu.

Merenduses reguleerivad turvalisust ja ohutust vastavalt rahvusvahelise konventsiooni inimelude ohutusest merel (SOLAS - *International Convention for the Safety of Life at Sea*) peatükid XI-2 ja IX ehk rahvusvaheline laevade ja sadamarajatiste turvalisuse koodeks (ISPS - *The International Ship and Port Facility Code*) ja meresõiduohutuse korraldamise rahvusvaheline koodeks (ISM - *International Safety Management Code*). Need koodeksid on mõningate täpsustustega viidud ka EL seadusandlusse vastavalt Euroopa Parlamendi ja Nõukogu määrustega (EÜ) nr 725/2004 ja (EÜ) nr 336/2006.

ISPS koodeks on loodud eelkõige silmas pidades sadamate ja sadamas viibivate laevade füüsilist turvalisust. Kuid ka füüsiline turvalisus on oluline osa sügavuti kaitsest küberrünnete vastu (UK Chamber of Shipping 2014, 11). Näitena võib tuua Antwerpeni sadama juhtumi, kus kurjategijad murdsid sadamas asuvatesse ettevõtetesse füüsiliselt

sisse, ning selleks, et võimaldada kauba informatsioonile kaugpääs (*remote access*), paigaldasid arvutite külge tugijaamad silla (*bridge*) tekitamiseks (Heering 2017, 35). Koodeks nõuab laevadelt turvalisuse hindamist ning selle alusel turvaplaani väljatöötamist. Turvalisuse hindamise käigus peab muuhulgas kindlaks tegema kaitse seisukohast olulised pardatoimingud ja neid ähvardavad ohud. Koodeksi B osa suuniste kohaselt peab turvalisuse hindamise käigus arvesse võtma ka raadio- ja kaugsidesüsteeme ning arvutisüsteeme ja -võrke. Kuna tänapäeva laevade olulised pardatoimingud sõltuvad IT-st ja OT-st, siis sellest lähtuvalt soovitatakse reederi turvaülematel määratleda laeva turvaplaanis arvutisüsteeme sisaldavad ruumid piirangualadena (UK Chamber of Shipping 2014, 14) ning panna paika laeva ja kalda vahelise võrguühenduse kontrolli ja seire protseduurid (BIMCO jt 2017, 2).

ISM koodeksi eesmärk on meresõiduohutuse tagamine, inimvigastuste ja inimelude kaotuse tõkestamine ning keskkonna ja vara kahjustamise vältimine. Nende eesmärkide saavutamiseks peavad nii reederi laev kui kaldastruktuurid toimima vastavuses reederi loodud SMS-ile. Magistritöö kirjutamise ajal ISM koodeksis küberturvet ei käsitletud, kuid kui laeva ohutu ekspluatatsiooni seisukohalt olulised süsteemid nagu navigatsioon, side või käiturid sõltuvad arvutitest, siis peab SMS sisaldama protseduure selliste seadmete küberohutuse tagamiseks.

Eelnevalt mainitud koodeksite ja küberturbe vaheline seos on ebamäärane ning suuresti tõlgendamise küsimus. Nagu autor magistritöö sissejuhatuses mainib, on IMO teema olulisust juba teadvustanud 16.07.2017 vastu võetud resolutsiooniga MSC.428(98) – „Merendusega seotud küberriskide haldamine meresõiduohutuse korraldamise süsteemides“ (Maritime… 2017). Selle resolutsiooniga seoses andis IMO välja ka ringkirja MSC-FAL.1/Circ.3 – „Suunised küberriskide haldamiseks merenduses“. Suunistes toodud soovitused täiendavad teisi IMO poolt loodud ohutuse ja turvalisuse juhtimise praktikaid ning need võib viia juba olemasolevatesse riskihaldamise süsteemidesse. (Guidelines… 2017)

Küberriskide haldamisega seotud protseduuride loomine ja SMS-i viimine on ettevõtja ülesanne. Ettevõtja abistamiseks on loodud küberruumi ohtusid arvesse võtvad rakenduslikud nõuded, mis hõlmavad tõhusaks küberriskide haldamiseks vajalikke tegevusi ja soovitud tulemusi arvestades kõiki merendusega seotud toiminguid ja

infovahetust mõjutavaid kriitilisi süsteeme. Vastavalt nendele nõuetele peab ettevõtja (*ibid*.):

- määratlema laeva- ja kaldapersonali kohustused, pädevuse, vastutuse ja vastastikused suhted ning tuvastama kõik süsteemid, varad, andmed ja võimekused, mille halvamine kujutab ohtu laeva käitamisele;
- rakendama kaitseks kübersündmuste eest riskide ohjamise korra ja meetmed ja töötama välja hädaolukordadeks valmistumise kava;
- välja töötama ja rakendama kübersündmuste õigeaegseks tuvastamiseks tarvilikud tegevused;
- välja töötama ja rakendama tegevused ja plaanid küberintsidendi tõttu kahjustunud laeva käitamise ja teenuste pakkumise seisukohalt oluliste süsteemide paindlikkuse tagamiseks ning selliste süsteemide taastamiseks;
- määratlema laeva ekspluatatsiooni seisukohalt oluliste kübersüsteemide varundamise ja taastamise meetmed.

Rakenduslikele nõuetele lisaks on ISM koodeksis soovitatud SMS-i koostamisel arvesse võtta mitmesuguste huvirühmade koostatud koodekseid, juhiseid ja standardeid. Magistritöö kirjutamise ajal oli selliseid dokumente ilmunud juba väga palju, millest mõned on ära toonud ka IMO merendusega seotud küberriskide haldamise suunistes (MSC-FAL.1/Circ.3):

- Balti ja Rahvusvahelise Merendusnõukogu (BIMCO – *The Baltic and International Maritime Council*) jt poolt koostatud suunised küberturbe käsitlemiseks laeval (*The Guidelines on Cyber Security Onboard Ships*).
- Standard ISO/IEC 27001 – Infotehnoloogia, turbemeetodid, infoturbe halduse süsteemid, nõuded.
- USA Riikliku Standardite ja Tehnoloogia Instituudi (NIST - National Institute of Standards and Technology) kriitilise infrastruktuuri küberturbe parendamise raamistik.

Laevaohvitseridele on oluline nende meetmetega kursis olla ning neid vastavalt SMS-is sätestatule rakendada. Arvestama peab sellega, et kuigi magistritöö kirjutamise ajal ei ole

küberturbe käsitlemine SMS-is veel kohustuslik, on paljud laevaomanikud seda juba teinud. Magistritöö autori töökohaks oleva laeva SMS-is on muuhulgas öeldud, et IT ohutuse eesmärk on kaitsta ettevõtte andme- ja võrgusüsteeme katkestuste, soovimatu muutmise, kopeerimise ja lugemise eest ning kõikidel arvutitel peab olema paigaldatud viirusetõrjeprogramm.

Mõned laevandussektori huvirühmad on kvaliteedi ja ohutusstandardite parandamise oma kätte võtnud. Näiteks teostavad Naftaettevõtete Rahvusvahelise Merefoorumi (OCIMF - *Oil Companies International Marine Forum*) liikmed tankeritele kontrolle veendumaks nende heaperemehelikus käitamises ja hoolduses. Reederi ja meeskonna abistamiseks on loodud tankerite haldamise ja enesehindamise programm (TMSA – *Tanker Management and Self Assessment*) (OCIMF). Programmi eesmärk on julgustada reedereid programmis määratud tulemuslikkuse võtmenäitajate alusel hindama laeva SMS-i ning puudujääkide korral seda täiendama (*ibid*.). Programmi kolmas täiendus, mis on OCIMF liikmetele alates 1. jaanuarist 2018 kohustuslik, sisaldab muuhulgas peatükki 13 – „Meresõidu turvalisus“ (*Maritime Security*), millega nõutakse laevadelt küberturbeplaani olemasolu (Textor 2017). Plaan peab sisaldama ohtude tuvastamise, vähendamise ning nendele reageerimise meetmeid. Olulisel kohal on küberturbega seotud õppuste ja infotundide läbiviimine meeskonnale ning protseduurid patrullide ja otsingute teostamiseks. Uue peatükiga soovitakse edendada ka küberturbe teadlikkust ning meeskondi julgustatakse lukustama valveta tööjaamu, kaitsma paroole ning kasutama sotsiaalmeediat ja mälupulkasid vastutustundlikult. Kuigi TMSA on oma olemuselt vabatahtlik, võivad reederitel tekkida mittevastavuste korral probleemid kauba leidmisega. (*ibid*.)

Autor mainib siinkohal veel kahte 2018. aasta mais jõustuvat seadust – Euroopa Liidu isikuandmete kaitse üldmäärus (GDPR – *General Data Protection Law*) ja võrgu- ja infoturbe direktiiv (NIS-directive – *The Directive on security of network and information systems*). Need kaks õigusakti mõjutavad peaaegu kõiki meremajandusega seotud sektoreid (Hellenic Shipping News 2017). Mittevastavus tähendab ettevõtetele suuri rahatrahve ja mainekahju. Laevandusettevõtted, kellele need õigusaktid kehtivad, peaksid esmalt tuvastama olulise vara ja taristu ning ettevõtte poolt hallatavad isikuandmed, teiseks tuvastama tegevused, kus neid andmeid, vara ja taristut kasutatakse ning kolmandaks viima läbi küberturbe riskide hindamise. Sellise riskide hindamise

protseduuri tulemused aitavad ettevõtteid küberturbe plaanide, poliitikate ja protseduuride loomisel ning isikuandmete kaitse ja haldamise võimekuse demonstreerimisel. (*ibid.*)

Küberturve muutub nii maailmas kui ka merenduses üha olulisemaks ning vastavaid eeskirju, õigusakte, standardeid ja suuniseid tuleb pidevalt juurde. Magistritöö eesmärk ei ole siinkohal kogu merendusega seotud küberturbe seadusandlust ja suuniseid läbi võtta. Küll peab reeder oma laevade ohutul ja turvalisel käitamisel kõiki neid arvestama ning looma meeskonnale võimalused ja eeldused nende täitmiseks. Laevaohvitseridelt nõutakse seega piisavaid küberturbealaseid teadmisi uute nõudmistega toimetulekuks ja meresõiduohutuse tagamiseks. Mittevastavuste korral võivad tagajärjed reederile olla mitmesugused – põrumised inspektsioonidel, probleemid lasti leidmisel, veolepingute kaotamine, kindlustusjuhtumid jms.

1.2 Kes ja miks laeva ründab?

Laevad kasutavad oma töös IT ja OT süsteeme, käitlevad kommertsinformatsiooni ja isikuandmeid ning veavad hinnalisi ja potentsiaalselt keskkonnaohtlike laste, olles seetõttu ahvatlev sihtmärk erineva profiiliga tegutsejatele küberruumis (UK Chamber of Shipping 2014, 2). Oht sõltub laeva tüübist, sõidupiirkonnast, veetavatest kaupadest, töö laadist ja mitmest muust tegurist ning seetõttu tuleb küberriske hinnata laevaspetsiifiliselt. Senine madal huvi läbi küberruumi laevu rünnata on seotud olnud keerukusega neile ligi pääseda. Seoses sateliitside tehnoloogia arenguga on see aga muutumas ning magistritöö kirjutamise ajal saab laevadel ka keset ookeani internetiühendust kasutada. See omakorda on nad küberkurjategijatele potentsiaalseks sihtmärgiks muutnud.

Laevad on küberrünnetele haavatavad olnud lühikest aega ja seetõttu on raske määrata just laevandusele omaseid ründajate profiile. Samas on juba loodud laevadega seotud küberintsidentide teavitussüsteem ning 2018. aasta mai seisuga on raporteeritud ka üks intsident. Nimelt oli laev kahjurvaraga nakatunud naivgatsioonisüsteemi tõttu sunnitud ankrusse jääma (Safety4Sea… 2018). Esialgu peab aga potentsiaalsete ründajate, nende võimekuse ja motivatsioonide koostamisel toetuma muude tööstusharude ja füüsilise maailma kogemusele. Ka seab tehnoloogia kiire areng ajalooliste andmete kasulikkusele teatud piirangud ning võimaluste täienemisel ja uute haavatavuste tekkimisel ründajate

profiilid kindlasti muutuvad (Marsh & McLennan Companies 2017, 72). Magistritöö kirjutamise ajal võib laevadele suurimaks ohuks olevad tegutsejad küberruumis kategoriseerida järgmiselt:

- töötajad,
- pühapäevahäkkerid,
- häktivistid,
- küberkriminaalid,
- terroristlikud ühendused,
- riigid ja riigi poolt rahastatud grupid.

Nende tegutsejate eesmärgid rünnakute korraldamisel on muuhulgas järgmised (Boyes jt 2017, 18):

- hävitada laev, last, sadam või muud rajatised;
- Mõjutada laeva kiirust ning manööverdus- ja navigeerimisvõimet;
- tõkestada juurdepääs informatsioonile ja laeva süsteemidele väljapressimise eesmärgil või laeva ja meeskonna röövimiseks;
- põhjustada viivitus laeva või laeva süsteemide töös eesmärgiga häirida ärilisi protsesse ja tuua laevaomanikele kaela trahvid või muud karistused;
- heidutada äritegevust teatud piirkondades, sadamates või turgudel;
- tuvastada inimesi, laevu, lasti ning neid jälitada varguse või lastiga manipuleerimise eesmärgil;
- häirida tähelepanu näiteks mingi anduri oleku muutmisega eesmärgiga samal ajal muid andmeid või informatsiooni ekstraktida (*data extraction*).

Eelnev nimekiri eesmärkidest ei ole ammendav ning seetõttu käsitleb magistritöö autor järgmistes alapeatükkides potentsiaalseid ründajaid ning nende motivatsioone ja võimekust lähemalt (*ibid.*).

1.2.1 Töötajad

Siia gruppi kuuluvad nii laeva meeskonnaliikmed kui ka kolmanda osapoole töötajad – hooldustehnikud, sadama töötajad, inspektorid jms. Oht nende poolt jaguneb omakorda tahtlikuks ja tahtmatuks, millest enam levinud on tahtmatu tegevuse tõttu toimunud

intsidendid. Tihtipeale on põhjusteks puudujäägid töötajate teadlikkuses ja väljaõppes ning laeva töökorralduse reeglites ja protseduurides. Sellised levinud eksimused laeval on näiteks tundmatu mälupulga sisestamine arvutisse, sotsiaalmeedias asukoha jagamine, e-kirjas olevale kahjursisuga lingile vajutamine jms. (JWC International) Näiteks on töötajad kahjurvaraga nakatunud muusikat ja pornograafiat alla laadides blokeerinud liikur-merepuurtorni (MODU – *Mobile Offshore Drilling* Unit) dünaamilise positsioneerimise süsteemi. Tagajärjeks oli platvormi positsioonilt triivimine, mistõttu tuli kaev ajutiselt sulgeda. Ilmnes, et liikur-platvormi navigatsioonisüsteem ei olnud kuidagi eraldatud töötajate isiklikuks tarbeks mõeldud võrgust. (Swanbeck 2015)

Laeva sadamas olles käivad pardal tihtipeale mitmesugused hooldustehnikud, kes diagnostika ja hoolduse läbiviimiseks ühendavad oma seadmed, mälupulga või sülearvuti laeva süsteemidega. Ka koostatakse paljude konteinerlaevade lastiplaan kaldal ning tuuakse mälupulgaga laeva arvutisse kooskõlastamiseks. Kõikide selliste situatsioonide jaoks peavad olema protseduurid laeva süsteemide kaitseks. Näiteks kolmandate osapoolte pardale toodud mälupulkade kasutamise luba ainult selleks ettenähtud ning teistest laeva võrkudest eraldatud arvutis ja kohustus eelnevalt viia läbi viirusekontroll. Üha kasvav võimalus on kaugdiagnostika läbiviimine satelliitside vahendusel. Näiteks autori laeval kasutatakse IT probleemide korral kaugtoe tarkvara *TeamViewer*, mille kaudu võimaldatakse kaldaspetsialistidel ligipääs laeva arvutile. Samasugune võimalus kaugdiagnostika läbiviimiseks on juba ka laeva masinatel ja muudel OT süsteemidel. Laeva meeskond peab olema teadlik, et sarnaselt volitatud isikutele, on võimalik laeva võrku pääseda ka kurjategijatel.

Meeskonnaliikmed võivad laevasüsteeme rünnata ka tahtlikult. Selle põhjuseks võivad olla konfliktid tööandja või kaastöötajatega, aga ka rahaline kasu. Omad inimesed ei vaja rünnaku korraldamiseks suuri oskusi ja ressursse, sest nad omavad siseinfot ning piiramatut ligipääsu laeva süsteemidele (Jain jt 2014, 78). Eesmärkide saavutamiseks võivad nad varastada konfidentsiaalset infot ja ärisaladusi, põhjustada häiringuid seadmete töös jms (*ibid*.). Rahulolematud meeskonnaliikmed on näiteks lavastanud piraadirünnaku omale laevale (Tam ja Jones 2018, 14). See juhtum ei olnud küll küberrünne, kuid aitab näitlikustada potentsiaalset ohtu omade töötajate poolt.

1.2.2 Harrastushäkkerid

„Harrastus“ tähendab eelkõige seda, et nende isikute eesmärk ei ole rahaline kasu (Pipkin 2002, 8). Nad murravad arvutivõrkudesse väljakutsete ja põnevuse pärast ning selleks, et oma oskustega kogukonnas kiidelda (Jain jt 2014, 78). Sellesse gruppi kuuluvad väga erinevate oskustega inimesed alates teiste väljatöötatud ja kergesti leitavat kahjurvara kasutavatest skriptinagadest (AKIT, *sub* skriptinaga) kuni põhjalike teadmiste ja oskustega nn klassikaliste häkkeriteni (Pipkin 2002, 8). Kuna laeva süsteemid on alles hiljuti avanenud ohtudele küberruumis ning nende küberturbesse pole väga palju panustatud, on nad potentsiaalseteks ründeobjektideks igasugusel tasemel harrastus–häkkeritele (Jones jt 2016, 8). Kahjurvara arendamise vahendid ja eksploidipakid (*exploit kit*) on väga kergesti hangitavad ning võimaldavad ka kogenematul ründajal tõsist kahju tekitada (*ibid.*).

Eric Forner ja Brian Meixell demonstreerisid 2013. a küberturbe konverentsil *Black Hat* naftaplatvormi simulatsiooni peal, et häkkides programmeeritavasse kontrollerisse (PLC – *Programmable Logic Controller*), on võimalik kaugjuhtimise teel pumpasid sisse ja välja lülitades purustada torujuhe (Smith 2013). Naftaplatvormidel ja ka laevadel kasutatakse füüsiliste protsesside kontrollimise hõlbustamiseks masina kasutajaliideseid (HMI – *Human-Machine Interface*), mis on üldiselt *Windows*’i baasil tööjaamad. Eric Forner’i ja Brian Meixell’i sõnul on enamik Windows’i baasil tööjaamu iganenud ning kontrollerid niivõrd ebaturvalised, et nende häkkimisega saaks hakkama iga skriptinaga (*ibid.*).

Skriptinagade teadlikkus ja oskused on puudulikud ja nad ei oska oma jälgi peita, mistõttu on võimudel neid lihtne tuvastada (Tam ja Jones 2018, 3). Seetõttu peab autor ohtu skriptinagade poolt madalaks. Suurema tõenäosusega võivad nad probleeme tekitada laevandusettevõtete äriprotsessidele veebilehtede rikkumisega (*defacement*) või teenuse–tõkestusrünnete (DoS – *Denial of Service*) korraldamisega. Tõenäolisemalt võivad laevu rünnata põhjalike teadmiste ja oskustega häkkerid. Nad on võimelised arendama ja täiustama häkkimistööriistu ning oskavad süsteemi logisid kustutade ja muutes peita oma tegevuse jälgi (Boyes jt 2017, 35). Harrastushäkkeritel puudub küll otsene motivatsioon kahju tekitamiseks, kuid nende tegevuse tagajärjed võivad siiski laevale ohtlikuks saada.

1.2.3 Häktivistid

Häktivistid ründavad või saboteerivad poliitiliste, sotsiaalsete või keskkonnakaitsega seotud eesmärkidel (UK Chamber of Shipping 2014, 3). Nad võivad püüda DoS rünnete abil häirida süsteemide tööd või leida publitseerimiseks kompromiteerivat informatsiooni (Boyes jt 2017, 35). Maailmas kõige tuntum häktivistide kollektiiv *Anonymous* on korraldanud mitmesuguste riiklike asutuste, eraettevõtete ja indiviidide vastu suurt avalikku tähelepanu pälvinud DoS ründeid ja veebilehtede rikkumisi ning põhjustanud seetõttu ebamugavusi, finantskahju ja emotsionaalseid pingeid (Kenney 2015, 141-143)

Üldiselt ei ole merendussektor häktivistidele prioriteetne sihtmärk, kuid negatiivsesse meediafookusesse sattumisel võib olukord muutuda (Centre for Cyber Security 2017, 4). Ründeobjektideks võivad olla laevad ja ettevõtted, keda aktivistid on traditsiooniliselt kimbutanud ka füüsilises maailmas (UK Chamber of Shipping 2014, 3). Näidetena sellistest gruppidest võib tuua keskkonnakaitseorganisatsioonid *Greenpeace* ja *Sea Sheperd Conservation Society*, kes on häirinud vastavalt nafta- ja kalapüügisektoris tegutsevaid laevu ja ettevõtteid.

1.2.4 Küberkriminaalid

Kriminaalide eesmärgiks on peamiselt rahaline kasu, aga ka tööstus- ja kommertsspionaaž (BIMCO jt 2017, 6). Kui arvestada, et 2017. aasta seisuga transporditi meritsi mahult üle 80% ja väärtuselt üle 70% maailma kaupadest (UNCTAD 2017) ning seda, et lasti on transpordi käigus lihtsam varastada kui kellegi omandusest (Marsh & McLennan Companies 2017, 32), võib küberkuritegevuse ohtu merendusele pidada suureks. Seda toetab ka asjaolu, et 2017. aastal korraldatud küberrünnetest 77,4% oli seotud küberkuritegevusega ning 14,5% küberspionaažiga (Passeri 2018).

Küberkriminaalide poolt kasutatavad ründemeetodid võib jagada üldisteks ja sektoripõhisteks. Üldised meetodid on näiteks lunavararünded ja pettused ning sektoripõhised smuugeldamine ja vargused. Smuugeldamine ja lastivargused on merendussektoris küll teada-tuntud murekohad, kuid küberruum on loonud kurjategijatele nende korraldamiseks uued võimalused. (Centre for Cyber Security 2017, 3)

Kuna kahjurvara ja muude küberrünnete jaoks kasutatavate vahendite arendaja ja operaatorid kauplevad oma toodete ja oskustega mustal turul, võivad kurjategijate tööriistad ja meetodid väga kõrgel tasemel olla (Boyes jt 2017, 35). 2012. aasta andmete põhjal kaubeldi Venemaal tegutseval mustal turul järgmiste hindadega (Cyberkeel 2014, 19-20):

- Kahjurrakenduse (*malicious application*) installeerimine 1000 arvutile – 100 kuni 500 USD.
- Veebiserveri häkkimine – alates 250 USD.
- Troojan pangakontode varguseks – 1300 USD.
- Troojan kliendi brauseris veebilehtede andmete asendamiseks – 850 USD.
- Hajus ummistusrünne (DDoS – *distributed denial-of-service attack*) üheks päevaks – 30 kuni 70 USD.

Küberkriminaalid on vahendusründe (*man-in-the-middle attack*) abil teeselnud laevade punkerdamisega tegelevat ettevõtet ning lasknud laevafirmal kütuse eest raha oma kontole kanda (*ibid.*, 5). Ka ilmnes 2013. aastal, et kurjategijad manipuleerisid Antwerpeni sadama terminali süsteemides andmetega ning suutsid vahele jäämata kaks aastat salakaubaga konteinerid oma autojuhtidele väljastada (*ibid*., 8).

Küberkriminaalideks võib lugeda ka piraadid, kui nad kasutavad laevade kaaperdamiseks kübervõimekust. Aastatel 2005–2012 maksid 179-st kaaperdatud laevast 152 laeva Somaalia piraatidele lunarahana 300 kuni 400 mln USD, mis näitab selgelt selle äri tulusust (*ibid*., 16). Kuigi see pole iseenesest küberrünne, on piraadid kasutanud automaatse identifitseerimise süsteemi (AIS – *Automatic identification system*) andmeid ohvrite tuvastamiseks, nende eksitamiseks ja enda asukoha peitmiseks (Tam ja Jones 2018, 8). Füüsilise kaaperdamise asemel on küberpiraatidel võimalik laeva või laevandusettevõtte arvutite ja andmebaaside andmed krüpteerida ning nende andmete taastamise eest lunaraha nõuda (Cyberkeel 2014, 15). Potentsiaalselt ohtlike tagajär–gedega võib olla laeva OT süsteemide krüpteerimine ning näiteks laev koos reisijatega keset ookeani triivima jätta (Jones jt 2016, 6). Sarnane juhtum toimus 2017. aasta veebruaris, kui häkkerid suutsid väidetavalt kümneks tunniks võtta täieliku kontrolli konteinerlaeva navigatsioonisüsteemi üle (Blake 2017).

1.2.5 Terroristlikud ühendused

Terroristide eesmärgiks on hirmu tekitamine ja võimalikult suure meediakaja saavutamine (Centre for Cyber Security 2017, 5). Rünnaku alla võivad sattuda laevad, mis omavad sümboolset tähendust, mille hävitamisega tekib oluline kahju kas majandusele või keskkonnale, millega tekitatakse inimohvreid, või mida saab kasutada kui relva (Nelson 2012, 18). Sellisteks laevadeks on sõja-, nafta- ja gaasisektori laevad, puurtornid või reisi- ja kruiisilaevad (*ibid.*). Terroristid võivad sarnaselt piraatidele häkkida laeva ohutuse seisukohalt kriitilisi süsteeme, kuid lunaraha saamise asemel on nende eesmärgiks füüsiliste purustuste ja inimohvrite tekitamine. Kuna aga purustavate küberrünnete läbiviimine laevade vastu on küllaltki keeruline ja terroristidel üldiselt selline võimekus puudub, siis tõenäolisemalt püüavad nad kübervõimekust kasutada relvade ja muude vahendite salakaubaveoks (Centre for Cyber Security 2017, 5).

Terroristlike ühenduste rünnet laevadele ei saa aga täielikult välistada. Sarnaselt kriminaalidele võivad nad väga kergesti hankida kõikvõimalikke küberrünnete korraldamise vahendeid ja teenuseid mustalt turult. Näiteks on *Al Qaeda* arvutitest leitud materjale superviisorsüsteemide (SCADA – *Supervisory Control and Data Acquisition*) häkkimiseks, mistõttu Ameerika Kaitseluureagentuur peab küberohtu terroristide poolt kriitiliseks (Hart 2004, 7). SCADA on liik tehnojuhtimissüsteeme (ICS – *Industrial Control System*), mida antud magistritöös nimetatakse üldnimega OT ja mida ka laevadel füüsiliste protsesside juhtimiseks ja monitoorimiseks laialdaselt kasutatakse.

1.2.6 Riigid ja riikide poolt rahastatud grupid

Küberruum aitab riikidel oma majanduslikke, poliitilisi ja sõjalisi huvisid ellu viia ulatuslikumalt ja odavamalt ning seda võimalust kasutatakse üha enam ära (Centre for Cyber Security 2017, 4). Riikide käsutuses olevad ressursid ja erioskused võimaldavad neil läbi viia kõrgel tasemel sihikindlaid ja kohanduvaid kestusründeid (AKIT, *sub* kinnisründeoht). Nende poolne oht laevandusele on eelkõige läbi küberspionaaži ja purustavate küberrünnete (Centre for Cyber Security 2017, 4).

Riikide korraldatud purustavate küberrünnete oht laevadele ja sadamatele on madal, kuid võib ilmneda konfliktiolukorras. Kaubalaevad varustavad riike sõjatehnika, toidu ja muude varudega ning nende hävitamine on oluline sõjastrateegia. Riikide poolset

spionaaži ohtu loetakse suureks. Tööstusspionaaž äritegevuse ning olulise tähtsusega tehnoloogiate ja varade kohta tundliku informatsiooni omandamiseks on tavaliselt suunatud merendusettevõtete kaldaosakondade vastu. Poliitilist huvi pakuvad riikidele mereteed, laevad ja sadamad, mis teenindavad geopoliitilisest seisukohast olulise tähtsusega ja pingelisi piirkondi. Riiklikult rahastatud organisatsioonid on rünnanud teiste riikide relvajõududele teenuseid pakkuvaid logistika- ja transpordiettevõtteid ning muid merendus- ja laevaehitusektoris tegutsevaid ettevõtteid. (*ibid*.)

Tavalisi kaubalaevu puudutav oht riikide poolt tuleneb eelkõige nende võimekusest segada (*jamming*) ja võltsida (*spoofing*) GNSS signaale. Üks paremini dokumenteeritud riigi poolt korraldatud signaalide segamine viidi läbi Põhja-Korea poolt Korea Vabariigi vastu (Centre for Cyber Security 2017, 4). Põhja-Korea kasutas kolmel korral võimsaid veoautodele paigaldatud segamisseadmeid, mis näiteks 2012. aastal häirisid üle 1000 lennuki ja 250 laeva tegevust (*ibid.*). Teine juhtum toimus 2017. aasta 22. juunil, kui Mustal Merel Novorossiiski lähedal jäi ulatusliku GPS signaalide võltsimise mõjupiirkonda üle 20 laeva (Goward 2017). Isegi kui laevad ei ole otsene sihtmärk, peavad meremehed sellise võimalusega arvestama.

1.3 Mida ja kuidas laeval rünnatakse?

IT-d ja OT-d on oma erinevate eesmärkide tõttu ajalooliselt käsitletud isoleeritud süsteemidena (Harp jt, 3). IT-d kasutatakse laeva administratiivse poole korraldamiseks ning OT-d kõikvõimalike füüsiliste protsesside seireks ja juhtimiseks. Tehnoloogia arenguga on avanenud võimalus ühendada IT võimekus OT süsteemidega ning optimeerida laeva ekspluatatsiooniks olulisi füüsilisi protsesse (Mihanović jt 2016, 38). Selleks, et mõista laeva haavatavust küberrünnetele, käsitleb autor järgmistes alapeatükkides esmalt IT ja OT erinevusi ning seejärel laeva käitamise seisukohalt muid olulisi süsteeme ja nendega seotud küberohte.

1.3.1 Infotehnoloogia ja käidutehnoloogia

IT hõlmab riistvara- tarkvara-, side- ja muid vahendeid, mida kasutatakse andmete sisestuseks, talletuseks, töötluseks, edastuseks ja väljastuseks (AKIT, *sub* infotehnoloogia). Süsteemid asuvad puhastes ja heade keskkonnatingimustega ruumides

ning tehniline tugi on üldiselt vahetusläheduses. Tehnoloogia arengut on kannustanud kiirema ja usaldusväärsema andmetöötluse ning kasutajamugavuse vajadus, mistõttu on suurt rõhku pandud riist- ja tarkvarakomponentide ühilduvusele (*compatibility*) ja vahetatavusele (*interchangeability*) ning süsteemi rikketaluvusele (*fault tolerance*). (*ibid.*, 6-7) Jõudluse ning teabe konfidentsiaalsuse ja tervikluse tagamisel on teatav hilistus (*delay*), puhvri ületäitumine (*buffer overflow*) ning piiratud käideldavus lubatav ning süsteemi taaskäivitamist loetakse aktsepteeritavaks (Stouffer jt 2015, 2.14).

IT on inimeste jaoks muutunud osaks igapäevaelust ning arvutikasutamise oskus töökohal on iseenesest mõistetav. Laeva peal kasutatakse IT-d administratiivseteks tegevusteks nagu e-post, lastiga seotud dokumentatsioon, planeeritud hooldussüsteem, varude ja proviandi tellimine jms. Meeskond suudab enamasti lihtsamad IT-ga seotud probleemid iseseisvalt lahendada. Keerukamate probleemide korral võib internetiühenduse olemasolul kasutada kaugtoe tarkvara *TeamViewer* või tellida sadamas pardale vastav spetsialist.

OT-d seevastu kasutatakse laeva käitamiseks oluliste füüsiliste protsesside juhtimiseks ja seireks. Süsteemidel on piiratud funktsionaalsus ja tihtipeale on need kavandatud täitma ainult ühte ülesannet. Komponendid võivad asuda üksteisest kaugel, peavad taluma raskeid keskkonnatingimusi ning olema võimelised püsima tehnilise toeta pikka aega töökorras. (Harp jt, 6) Seetõttu oodatakse käidutehnoloogial põhinevatelt seadmetelt töökindlust, käideldavust ja protsesside juhtimist reaalajas hilistuse ja hälveteta, kusjuures jõudluse tõstmine ning küberturvalisus koos konfidentsiaalsusega on teisejärgulised. (Stouffer jt 2015, 2.16)

Nende nõuete tagamiseks hoitakse seadmed õhkeraldatuna (*air gap*) ja kasutatakse juba sissetöötatud ja vigade paranduse läbinud omandtark ja -riistvara ning -sideprotokolle (*proprietary software, -hardware and -communication protocols*) (Drias jt 2015). Kui IT eluiga on lühike ning komponendid peab suurenenud jõudluse ja turvalisuse nõuetega toime tulemiseks iga 2–5 aasta tagant välja vahetama, siis OT süsteemid jäävad vähemalt generatsiooni tehnoloogia arengust maha. Juba sissetöötatud ja ennast tõestanud tehnoloogia kasutamise eesmärgiks on stabiilsuse tagamine ning 10–20 aasta vanused seadmed on tavaline nähtus. (Harp jt, 6-7)

Tänu uutele võimalustele tehnoloogias on IT-d ja OT-d hakatud üha enam integreerima. Peamine ajend nende kahe tehnoloogia liitmiseks on otsuste toetamiseks ning äriprotsesside optimeerimiseks vajalike kvaliteetsete andmete toimetamine füüsilisi protsesse juhtivatelt seadmetelt ettevõtte tasandile (Inductive Automation 2016, 4). Selliseid arenguid tööstuses ja kaasnevat tehnoloogilist innovatsiooni on nimetatud erinevates allikates mitmeti. Segaduste vältimiseks kasutan ma edaspidi 2012. aasta lõpus ettevõtte *General Electric* poolt kasutusele võetud mõistet tööstusinternet, millega tähistatakse tööstussüsteemide põimimist kõrgtasemel andmetöötluse, analüütika, odavate andurite ja kiire internetiga (Evans jt 2012).

Merenduses toimub selliste innovaatiliste tehnoloogiate rakendamine teatava hilinemisega. Selle põhjusteks on üheltpoolt laevaehituse kallidus ning ajamahukus (Jones jt 2016, 10) ning teisalt satelliitside tehnoloogia keerukus ja hind. Ajal, mil maismaal kasutati juba stabiilset, kiiret ja piiramatut internetiühendust, sai keset ookeani oleval laeval parimal juhul tekstipõhiseid e-kirju saata. Kuid ka selles vallas on areng olnud kiire ja näiteks 2018. aasta veebruari lõpus üritati kruiisilaeval *Regal Princess* VSAT-side (VSAT - *very small aperture terminal*) tehnoloogiat kasutades saavutada internetiühenduse kiiruseks 1,5 Gbit/s, mis oleks võimaldanud korraga kuni 1500 reisijal voogedastusena vaadata telesaateid või filme (Russell 2018). Eesmärk saavutati ning lõplikuks tippkiiruseks kujunes 2,6 Gbit/s (*ibid.*). Ka magistritöö autori laeval on internetiühendus pidevalt saadaval. Kalda lähedal kasutame 4G mobiilsidevõrku ning kaldast eemal võimaldab VSAT muuhulgas vaadata lühemaid videosid, surfata internetis ning paigata (*patch*) tarkvara.

Tööstusinterneti märksõnadeks merenduses on kiirus, kokkuhoid ja teenuse kvaliteet ning parimaid võimalusi selleks pakuvad teekonna optimeerimine, tehnohooldus ja kaupade seire (Tracy 2016). Laeva reisiplaani ja positsiooni on võimalik reaalajas edastada kontorisse, teistele laevadele, liikluskorraldusteenindusele ja muudele asjaosalistele (*ibid.*). Kaubaseiresüsteemid võimaldavad jälgida kiiresti rikneva kauba seisukorda ja edastada reaalajas infot kauba asukoha, seisundi ja eeldatava saabumisaja kohta alates tootmishoonest kuni kaubasaajateni (*ibid.*). Mitmesuguste tehniliste süsteemide olukorda seiravad andurid edastavad reaalajas tohutul hulgal andmeid, mille analüüs võimaldab laeva meeskonnal, kontoril ja tootjal avastada koheselt kõrvalekalded normaalsusest ja

planeerida remonti vastavalt vajadusele, mitte aga vastavalt hooldusplaanile (Wärtsilä 2015).

Laevaomanike ja muude huvirühmade motivatsioon IT ja OT integreerimiseks on selgelt mõistetav. Peab aga arvestama, et nende kahe ajalooliselt lahus arenenud tehnoloogia ühendamine loob lisaks võimalustele ka uusi ohte. OT, mis töötab vananenud omandsüsteemidel ja -protokollidel, ning mille ainuke küberturbe meede oli seadmetele ja võrkudele füüsilise juurdepääsu piiramine, on nüüd avatud välismaailmale ja IT-ga kaasaskäivatele ohtudele. Järgnevates alapeatükkides kirjeldan põhilisi küberohte laevasüsteemidele. Kuigi olenevalt laevast ning selle otstarbest võib neid süsteeme olla palju, siis järgnev nimekiri kehtib praktiliselt kõikide laevade kohta ning on antud magistritöö kontekstis piisav:

- Inimesed,
- navigatsioonisüsteemid,
- Masinaruumi süsteemid.

1.3.2 Inimesed

Sellesse kategooriasse kuuluvad laeva meeskond, kolmandad osapooled ning reisijad. Üheltpoolt peetakse inimest süsteemi turvalisuse seisukohast nõrgimaks lüliks (Boyes jt 2017, 51) ning uuringud on näidanud, et umbes 75%–96% õnnetusjuhtumitest merel on põhjustatud vähemalt osaliselt inimese poolt (Tam ja Jones 2018, 13), kuid teisalt võib teadlik meeskond tuvastada kõrvalekalded süsteemi töös, avastada varakult küberründed ja reageerida probleemidele adekvaatselt. Olgu kuidas on, kuid seni kuni autonoomsed laevad meremehe ametit üleliigseks pole muutnud, tuleb inimfaktoriga arvestada.

Paljud ründajad eelistavad raskesti ligipääsetavatesse ja turvatud süsteemidesse häkkimise asemel logida sinna kasutaja enda nime ja parooliga (JWC International). Peamiselt kasutatakse inimeste ründamisel küberruumis manipuleerimisvõtteid (*social engineering*), mis hõlmavad veenvat teesklust, valesid, altkäemaksu, ähvardusi jms peamiselt konfidentsiaalse või tundliku teabe saamiseks (AKIT, *sub* social engineering). Manipuleerimisega soovitakse panna töötajad avama kahjurvaraga nakatunud manuseid, vajutama linkidele, millele nad ei tohiks vajutada, avaldama telefoni teel salajast informatsiooni ning ühendama volitamata riistvara laeva arvutisüsteemidega (Cyberkeel

2014, 23–24). 2015. aastal läbiviidud uuringus selgus, et enim laevale kaasatoodud seadmed on mobiiltelefonid, sülearvutid ja kõvakettad. *Android*'i baasil mobiiltelefon on 90% tõenäosusega kasutaja teadmata nakatunud kahjurvaraga ja *iOS* puhul on see vastavalt 80%. On olnud juhus, kus meeskonnaliige kasutas ECDIS-e tööjaama oma mobiiltelefoni laadimiseks, nakatas süsteemi kahjurvaraga ning kustutas kõik elektronkaardid. (Adamson 2016) Internetiühendus laeval annab küll meeskonnale võimaluse sotsiaalmeedia ja e-kirjade vahendusel lähedastega kontaktis püsida, kuid muudab nad haavatavaks isiklikele rünnetele ja väljapressimistele (UK Chamber of Shipping 2014, 6).

Manipuleerimisvõtted küberruumis võib jaotada massidele suunatud rünneteks ja konkreetsetele isikutele mõeldud ehk sihtrünneteks (*targeted attack*). Massidele suunatud ründed, näiteks rämpskirjad ja õngitsusründed (*phishing*), on väga lihtsad ja odavad ning panustavad sellele, et ju keegi ikka õnge läheb. Sihtründed on suunatud kindlatele kriteeriumitele vastavatele gruppidele või ettevõtte juhtkonnale, need nõuavad aega ja planeerimist ning on seetõttu keerukamad korraldada. Sellised ründed on näiteks harpuunimine (*spearphishing*) ja vaalapüük (*whaling*). (EUROPOL 2014, 44)

Tavaliselt saadab ründaja potentsiaalsele ohvrile e-kirjaga kahjurvara sisaldava lingi või manuses oleva nakatunud faili, mille ohver pahaaimamatult avab. Kahjurvarasid võib jagada nende eesmärgi järgi ning olulisemad neist on nuhkvara, lunavara, zombi (*bot*), juurkratt *(rootkit*), uss (*worm*), viirus ja troojan. Nende eesmärgid on tähtsate andmete lugemine, kustutamine või lukustamine, salaja pealtkuulamine, paroolide varastamine, elu- ja tegevustähtsate süsteemide töö halvamine, süsteemi tagaukse avamine jms (JWC International).

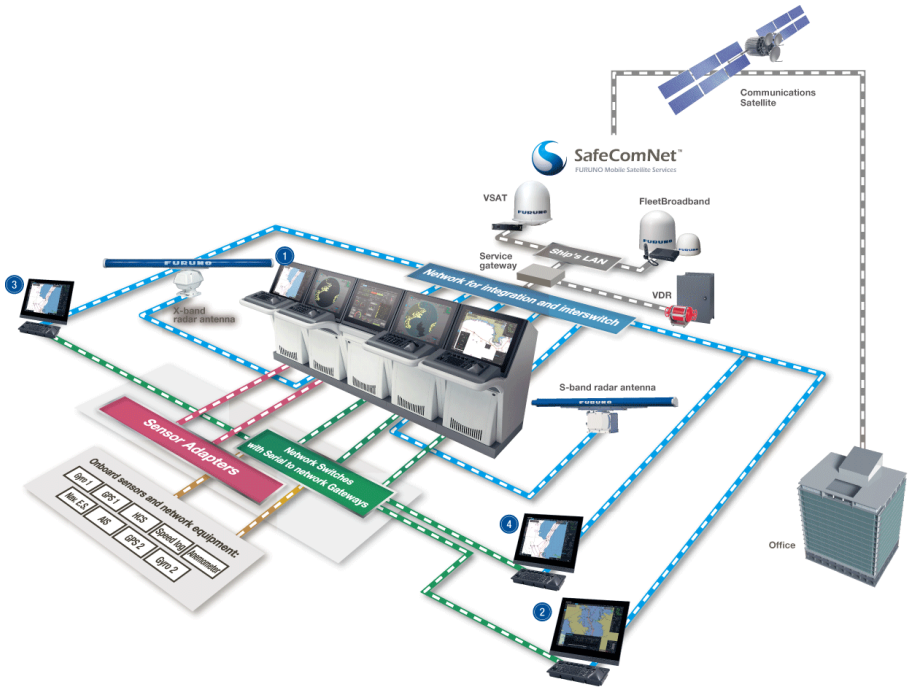
Õngitsuskirjad saadetakse laiali suurele hulgale isikutele ning nad näivat tulevat usaldusväärsest allikast nagu pangad, krediitkaardiettevõtted või populaarsed veebilehed. Adressaatidelt soovitakse konfidentsiaalset infot nagu paroolid, kasutajanimed ja krediitkaardiandmed, või seda, et nad külastaksid teatud veebilehte või avaksid manuse. Harpuunimise puhul saadetakse kiri laiali mingi organisatsiooni siseselt vähestele inimestele. Sellised kirjad võivad olla väga personaalsed ja rõhuda emotsioonidele. Vaalapüügiks nimetatakse küberründeid suurte kalade (*big phish*) ehk organisatsiooni tippjuhtkonna vastu. Ründajad näevad väga palju vaeva, et kaevandada isikute ja

ettevõttete kohta informatsiooni. Teeseldes ettevõtte e-posti või esinedes ettevõtte juhi, advokaadi või tarnija nime all, lastakse endale teha rahalisi ülekandeid. (JWC International)

Inimestega manipuleerimise näitena merendusest võib tuua 2016. aastal Lääne-Aafrika rannikul pikemat aega ankrus olnud laeva meeskonnaliikme väljapressimisjuhtumi. Antud isik võttis ennast pahaaimamatult veebikaamera ees riidest lahti ja tegeles seksuaalsete toimingutega. Kurjategijad salvestasid selle ning nõudsid video mitteavalikustamise eest raha. (JWC International)

1.3.3 Navigatsioonisüsteemid

Tänapäeva laevade sillasüsteemid koosnevad omavahel integreeritud komponentidest, mis võimaldavad tuua info mitmetelt anduritelt ja seadmetelt otse silla keskjuhtimispulti, juhtida ja jälgida masinaid, elektri- ja lastisüsteeme ning monitoorida laeva asukohta, liikumist ja teekonda reaalajas arvutiekraanilt (SKEMA 2009). Need süsteemid omakorda on sateliit- või mobiilside vahendusel ühenduses reederi, tehnohoolduse ja muu välise maailmaga (vt Joonis 1). Navigatsioonivahendid on osa sellest integreeritud süsteemist ning laeva käitamise ja ohutuse seisuohalt ühed tähtsamad.



Joonis 1. Integreeritud navigatsioonisild

Allikas: (Furuno)

Üks olulisemaid aspekte navigatsiooni seisukohalt on laeva asukoht, mille määramisel toetutakse suuresti GNSS-le. GNSS on kogum orbiidilt aega ja oma asukohta edastavaid satelliite, mille abil vastuvõtja suudab määrata oma positsiooni maakeral. Selliseid asukohamääramise süsteeme on mitmeid ja enimtuntud neist on USA ülemaailmse asukohamääramise süsteem (GPS – *Global Positioning* System). (Tam ja Jones 2018, 8)

GPS signaali on võrreldud 40 vatise lambi valgusega vaadatuna 17 000 km kauguselt. Niivõrd nõrk signaal on kergesti haavatav segamisele, võltsimisele, majakpettele (*meaconing*) ehk signaali hilistamisele ja taasedastamisele ning kosmoseilmale ja muudele häiringutele nagu satelliitide vastased kineetilised ründed ja kokkupõrked kosmoseprügiga. (Moskoff jt 2015, 7) Erineva suuruse ja võimsusega seadmed signaalide segamiseks ja võltsimiseks on väga kergesti hangitavad. Saadaval on nii väikesed ja odavad käsisegajad kui ka seljakotti paigaldatud 300–400 meetrise toimeulatusega võimsad seadmed hinnaga 10 000–20 000 USD (Cyberkeel 2014, 11). Hea näide võimalustest on 2015. aastal Hiina teadlaste poolt *Defcon*'il esitletud kõigest 300 USD maksnud isevalmistatud GPS signaali võltsimist võimaldav seade (Jones jt 2016, 3).

Signaalide segamist laevadel on testinud Suurbritannia ja Iirimaa tuletornide admini–stratsioon (GLA – *General Lighthouse Authority*). GPS segaja suunati merele ning läbiti see piirkond laevaga *Pole Star*. Segaja mõju alla sattudes lakkasid toimimast laeva DGPS (diferentsiaal-GPS) vastuvõtja, AIS transponder, dünaamilise positsioneerimise süsteem, gürokompassi kalibreerimise süsteem ja digitaalse valikkutsungi süsteem (DSC – *Digital Selective Calling*), käivitusid mitmed alarmid ning ECDIS-e pilt hangus. Sellise situatsiooni tekkimine etteteadmata, öösel ja tiheda laevaliiklusega alal võib lõppeda katastroofiga. (Cyberkeel 2014, 11)

GPS signaalide võltsimine on segamisest keerulisem ja nõuab tehnilisi vahendeid ja teadmisi, mida tavaliselt omavad riigid (Moskoff jt 2015, 11). 2017. aasta 22–24 juunil leidsid paljud Musta mere piirkonnas olevad laevad ennast GPS positsiooni järgi lennuväljalt. Intsidendiga oli seotud üle 20 laeva, kes kõik teatasid anomaaliatest GPS vastuvõtjatega ning laeva asukoha hüplemisest. Avalikult saadaoleva info põhjal arvatakse, et tegu oli riiklikul tasemel GPS signaali võltsimisega. (Jones 2017) Katseliselt on õnnestunud signaali muutmine ka odavate vahenditega. 2013. aastal suutis Texase ülikooli uurimismeeskond edukalt juhtida GPS signaali kontrollimisega 65 meetri pikkust

luksusjahti ilma, et laeva süsteem oleks andnud häireid või meeskond mingisuguseid muutusi tuvastanud (Cyberkeel 2014, 11).

GNSS pakub laevajuhtidele kiiret, täpset ja väga lihtsat moodust navigeerimiseks, asukoha määramiseks ja kiiruse mõõtmiseks (Coffed jt, 399). Laevajuhina teab magistritöö autor väga hästi, et sellel on ka oma varjukülg. Süsteem on pealtnäha usaldusväärne ja töötab tavaliselt probleemideta. Laevajuht muutub mugavaks ja kaotab vilumuse kasutada muid asukoha määramise ja navigatsiooni meetodeid. Koos DGPS vastuvõtjaga ütleb üles rida teisi süsteeme, sealhulgas ka selliseid, mida me GNSS-ga esialgu ei seostagi – gürokompass ja radar. (Grant jt 2011). Radar kasutab GNSS signaali põhi ülal režiimiks ning gürokompass osutinäidu hälbe (*drift error*) stabiliseerimiseks (*ibid.*). Tekkinud segadus võib päädida kas hilinemisel sadamasse tekkinud rahalise kahju ja rikutud mainega, või hullemal juhul laevaõnnetusega.

Üks tähtsamaid GNSS signaali kasutav seade on ECDIS, mis on väga paljudele laevadele vastavalt SOLAS peatükk V regulatsioonile 19.2.10 kohustuslik. Laevale, millel magistritöö autor töötab, need nõuded ei kehti, kuid sellegipoolest kasutatakse navigatsiooniks ainult elektronkaarti. ECDIS-e haavatavus tuleneb tema integreeritusest paljude teiste süsteemidega nagu GNSS, AIS, kajalood, radar jms, nõuetest kaarte iga nädal uuendada ning süsteemi paikamise puudulikkusest (Tam ja Jones 2018, 7).

Magistritöö autori laeval töötab ECDIS *Windows 7* operatsioonisüsteemiga tööjaamas. Alates paigaldamisest 2016. aastal pole süsteemi uuendatud ega turvaauke paigatud. Elektronkaarte uuendatakse iga nädal kasutades mälupulka. Uuendused laetakse administratiivtegevusteks kasutatavas sillaarvutis oleva programmi abil mälupulgale ning seejärel mälupulgaga mõlemasse elektronkaardi süsteemi. On lihtne mõista, et ECDIS pakub küberkurjategijatele mitmeid ründevektoreid.

Rünne ECDIS-ele võib toimuda otse läbi interneti mõnda tööjaamas või arvutivõrgus olevat turvaauku ära kasutades, või kaartide uuendamiseks kasutataval mälupulgal oleva viiruse abil. Katsetega on tuvastatud *Windows 7* operatsioonisüsteemil mitmeid haavatavusi, mida ära kasutades on võimalik ECDIS-e arvutis lugeda, kustutada ja muuta faile ning installeerida kahjurvara. Võimalik on võltsida andmeid, varastada või rikkuda

kaarte ning saada ligipääs kohtvõrgus (LAN - *Local Area Network*) olevatele muudele seadmetele ja teabele. (Dyryavyy 2014, 7)

ECDIS-e väärkasutusest tulenevad õnnetused laevadega pole haruldased. Üks viimaseid juhtumeid oli kaubalaeva *Muros* madalale sõit *Norfolk'i* ranniku lähedal 2016. aasta 3. detsembril (MAIB 2016). Tegemist ei olnud küll otseselt küberründega, kuid näitab selgelt, et laeva asukohta muul viisil ei kontrollitud. Kombineerides ECDIS-e liigse usaldamise selle haavatavusega küberrünnetele, on võimalik laev kaardi andmete, alarmide ja anduritega manipuleerides kas madalale või mõne muu objektiga kokkupõrkesse suunata.

Järgmine haavatav ja paljude seadmetega integreeritud süsteem laeval on AIS, mida kasutatakse põhiliselt abivahendina kokkupõrgete vältimisel, aga ka meremärkide ja muude ohtlike objektide tähistamiseks. AIS võimaldab raadiosagetuste või satelliidi vahendusel edastada laevade vahel navigatsiooniinfot nagu positsioon, laeva nimi, navigatsiooniseisund, kutsung, kurss, pöördekiirus jms. AIS on nii protokolli kui ka rakenduslikul tasandil halvasti kavandatud (Jones jt 2016, 6), paljudel seadmetel puudub sisseehitatud turvalisus, sõnumeid ei krüpteerita ja igasugune info on kergesti manipuleeritav ning eeldatakse olevat tõene (Cyberkeel 2014, 9).

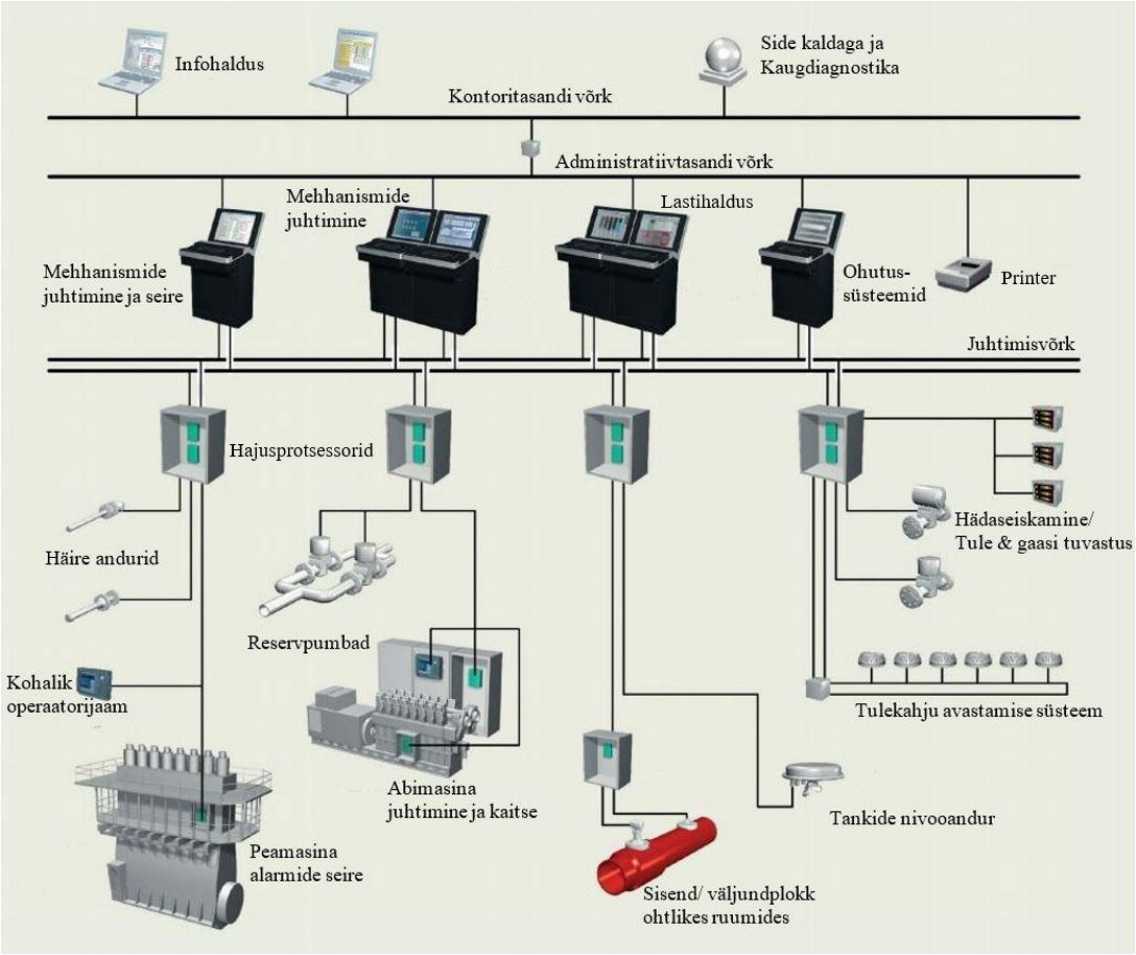
Teadlastel on õnnestunud süsteemi kuritarvitades muuta kõiki laeva andmeid, tekitada üle maailma kummituslaevu ja otsingu- ning pääste helikoptereid, edastada väärat ilmateadet, vallandata kokkupõrkealarme, esineda võimuorganitena, luua mees üle parda avariipoisid ja põhjustada süsteemi ummistust (DoS – *Denial of Service*) (*ibid.*). Piraadid on avalikult internetis saadavat AIS-i teavet kasutanud laevade tuvastamiseks ja jälgimiseks ning AIS-i andmeid võltsides ohvreid segadusse ajanud ja oma asukohta peitnud (Tam ja Jones 2018, 8). AIS-i kasutatakse väga palju meremärkide ja muude objektide nagu tuule- ja kalafarmide tähistamiseks. Lisaks füüsiliste objektide tähistamisele kasutatakse AIS-i virtuaalsete navigatsioonivahendite märkimiseks seal, kuhu pole otstarbekas füüsilist märki panna, või on seda vaja teha kiiresti. Virtuaalse AIS märgi puhul ei ole võimalik selle õigsust kontrollida radarpildilt ning selliste andmete võltsimine võib tekitada küllalt palju segadust ja ohtlikke olukordi.

Lisaks eelnevale on laeva sillas suur hulk muid olulisi süsteeme, mille detailne käsitlus ei ole selle magistritöö raames võimalik. Radar, navtex, elektroonilised publikatsioonid, logi, anemomeeter, reisiinfo salvesti (VDR – *Voyage Data Recorder*), merehäda ja -ohutuse ülemaailmne süsteem (GMDSS - *Global Maritime Distress and Safety System*), laeva turvasignalisatsioonisüsteem (SSAS - *Ship Security Alert System*) – nende kõigega on juhtunud õnnetusi ka küberruumi väliselt, kuid integreeritus ja võrgusolek võimaldab eemalt süsteemide poolt kasutatava olulise infoga manipuleerida või seadmete tööd läbi DoS rünnete häirida. (Tam ja Jones 2018, 8-12)

Eelnevalt kirjeldatud süsteemide ühine nõrgim koht on nende integreeritus ning avatus välismaailmale. Kasutades internetti ühendatud seadmete tuvastamiseks mõeldud otsingumootorit *Shodan*, leidis teadlane Ken Munro laevadele internetti, raadiot, mobiilsidet ja muud kommunikatsiooni võimaldavaid satelliidiantenne üle kogu maailma (Cimpanu 2017). Paljude tootjate mudelid kasutasid sama vaikeparooli „admin/1234“ või omasid kergesti häkitavaid turvaauke (*ibid.*). Terminali sisselogimise lehel olid avalikult nähtaval ka laeva nimi ning võrgus olevad kasutajad. Meeskonnaliikmete nimesid kasutades õnnestus Munrol leida *Facebook*'ist piisavalt infot kalastusründe korraldamiseks. Munro kommenteeris: „Lihtne kalastusrünne, võta sülearvuti üle kontroll, otsi õhkeraldamata laeva võrke ning migreeru teistesse, huvitavamatesse seadmetesse. Või lihtsalt koori (*scrape*) kasutaja pääsumandaat (a*ccess credentials*) ja logi otse satelliidi terminali“. (OSINT 2017) Terminali pääsedes on võimalik kontrollida kogu satelliiti läbivat infot ja muuhulgas laadida ECDIS-esse võltsitud elektronkaarte (Cyberkeel 2014, 13).

1.3.4 Masinaruumi süsteemid

Sellesse kategooriasse kuuluvad masinad ja käiturid ning elektri-, ballasti-, ventilatsiooni- ja muud taolised süsteemid. Need seadmed on juba praegu sellisel automatiseerituse tasemel, et pidevat valvet masinaruumis vaja ei ole. Automatiseeritud ja integreeritud mehhanismidest annab ülevaate joonis 2. Jooniselt näeme, et tehnoloogia arenguga on lisandunud side kaldaga ning kaugdiagnostika võimalus. Diagnostikaprogrammid jälgivad reaalajas seadmete olukorda ning annavad kõrvalekalletest teada meeskonnale ja muudele volitatud isikutele (Mihanović jt 2016, 39). Meeskonnal on probleemide korral võimalus lubada kaugpääs volitatud tehnikule, kes viib läbi diagnostika, võimalusel



Joonis 2. Laeva automaatikasüsteem Kongsberg K-Chief 700

Allikas: (Kongsberg Maritime 2015), autori tõlgitud

parandab rikked ning annab ekspertnõu (*ibid*.). Selline lahendus on kiirem, praktilisem ja palju tõhusam kui saata tehnik raskesti ligipääsetavas sadamas olevale laevale (*ibid*.). Siinkohal peab arvestama võimalusega, et sarnaselt volitatud isikutele võivad laeva süsteemidele ligi pääseda ka volitamata isikud.

Kuigi magistritöö autori laev on peaaegu 30 aastane, on ka seal võimalik erinevaid füüsilisi protsesse seirata ja juhtida sillas ja masinaruumi peajuhtimispuldis olevate operaatorijaamade kaudu. Võimalik on kontrollida ballastvee- tuletõrje-, pilsi-, kütuse- ning jahutusvee süsteemide pumpasid ja klappe ning muuta kõikvõimalike alarmide parameetreid. Arvuti jookseb *Windows 2000 NT* peal ning seda pole alates paigaldamisest paigatud ega uuendatud. See on OT süsteemide puhul tavaline – niikaua kuni töötab, pole vaja torkida. Antud süsteem pole küll ühendatud välisvõrku, kuid mälupulga abil on

võimalik see siiski kahjurvaraga nakatada. Ka *Stuxnet*'i uss, mis suunatud PLC-de, viidi Iraani *Natanz*'i uraani rikastamise tehasesse mälupulgaga (Fruhlinger 2017).

PLC on mitmesuguste tehniliste protsesside juhtimiseks määratud eriotstarbeline mikroarvuti (AKIT, *sub* programmeeritav kontroller), mida kasutatakse ulatuslikult ka laevadel. PLC häkkimise kergust on demonstreerinud professor Helge Janicke, kelle sõnul kasutas ta selleks laialt levinud vaba tarkvara (Watchwood 2017). Kurjategijate ainuke mure on leida laevale sisenemispunkt ning edasi on juba võimalik paari käsklusega võtta kontroll näiteks laeva rooli üle (*ibid.*). Kontrolli taastamiseks piisab mõnikord kui PLC ühendada arvutiga ja seade taaskäivitada, kuid teinekord on vajalik PLC programm uuesti juurutada (*deploy*) (*ibid.*). Autor tõi eelnevalt näite, kuidas häkkerid võtsid kümneks tunniks kontrolli konteinerlaeva navigatsioonisüsteemi üle. Täpseid detaile ei ole teada, kuid juhtumiga kursis oleva allika sõnul proovisid piraadid juhtida laeva sobivasse piirkonda, kus oleks võimalik sellele pardale minna (Hackers… 2017). Laeva meeskond pidi pardale kutsuma IT spetsialistid, kes nägid tunde vaeva, et kontroll laeva üle taastada (*ibid.*). Selliste keerukate arvutisüsteemide mõistmine, nende turbe tagamine ja vajadusel rikete kõrvaldamine nõuab spetsiifilisi teadmisi, mida meremeestelt oodata ei saa. Küll aga peab laevadel SOLAS peatükk II-1 Regulatsioon 31.4 kohaselt olema võimalik kõiki automaatjuhtimissüsteeme käsijuhtimisele võtta ning meremehed peavad olema võimelised seda ka tegema. Meeskonna vastava koolitamise eest vastutab loomulikult ka laevaomanik, kes peab seda tegema koheselt, kui mõni uus seade laevale paigaldatakse.

1.4 Kuidas laeva kaitsta?

Küberriskide viimiseks aktsepteeritavale tasemele peab tähelepanu pöörama kõigile järgnevatele faktoritele (UK Chamber of Shipping 2014, 9):

- inimtegur,
- füüsiline turvalisus,
- arvutisüsteemide kaitse parim praktika,
- kaldatugi.

Füüsilise turvalisusega tegeleb ISPS koodeks ning meremehed saavad oma hariduse käigus sellekohast koolitust piisavalt. Meeles peab pidama, et füüsiline komponent nagu mälupulga sisestamine arvutisse, võib olla küberrünnete üheks osaks. Seetõttu peab meeskond täpselt teadma, millised küberrünnetele haavatavad seadmed neil laevas on ja kus need asuvad. Selliseid seadmeid sisaldavad ruumid peab ISPS koodeksi mõistes määratlema piirangualadena. Selles suhtes on kindlasti oluline ka kaldapoolne tugi. Meeskond peaks kindlasti reederi turvaülemalt ja kaldaesindajalt nõudma igakülgset abi, tehnilist tuge ja küberturbe alaseid koolitusi (UK Chamber of Shipping 2014, 13).

Magistritöö seisukohalt olulisimad faktorid on inimtegur ja arvutisüsteemide parim praktika ning neid käsitletakse siinkohal pikemalt. Inimfaktor tähendab eelkõige küberturbe teadlikkust ja väljaõpet. Teadlikkus heidutab potentsiaalseid ründajaid ning edendab meeskonnas head küberkäitumist ja väljaõpe aitab tuvastada ründeid ning neile vastavalt reageerida (*ibid*., 10).

1.4.1 Teadlikkuse tõstmine

Laevaohvitseride teadlikkuse tõstmiseks nende väljaõppe käigus on autori arvates sobilik vahend Plymouthi ülikooli teadlaste Kimberly Tam'i ja Kevin Jones'i loodud mudelipõhine raamistik merendusega seotud küberriskide hindamiseks (MaCRA – *A Model-Based Framework for Maritime Cyber-Risk Assessment*). Raamistik on mõeldud toetamaks kindlustusseltse, poliitikakujundajaid, laevandusfirmasid ja meeskondi küberintsidentidega seotud riskide hindamisel ja maandamisel (Tam ja Jones 2018, 1). MaCRA kvantifitseerib riskid, mis on seotud potentsiaalsete ründajate, nende motiivide, laeva haavatavuste ja sõidupiirkonnaga ning esitab tulemused visuaalselt. Väljaõppe käigus erinevate stsenaariumite läbimängimine ja iseseisev riskianalüüs võimaldavad laevaohvitseridel küberriske merenduses paremini mõista.

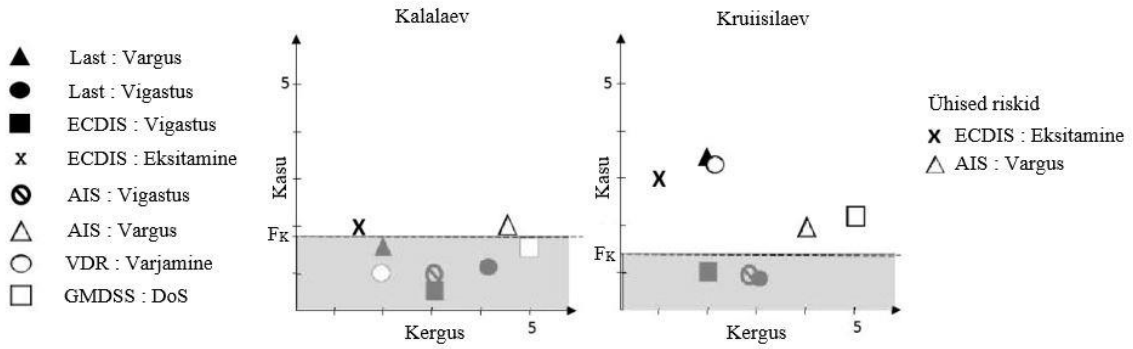
Raamistik baseerub kolmel kriteeriumil (*ibid*., lk 2):

- süsteemi haavatavus ja tagajärg,
- haavatavuse ekspluateerimise kergus,
- kasu ründajale.

Nimekiri süsteemi haavatavustest ja nende ründamise tagajärgedest on tehtud merenduses juba toimunud ning potentsiaalselt võimalike kübersündmuste, aga ka teiste sektorite ja füüsilise maailma kogemuste põhjal. Kriteerium „haavatavus : tagajärg“ on näiteks „GPS signaali võltsimine : laeva teelt eksitamine“. Küberturbe kogemuse vähesuse tõttu merenduses ei ole olnud võimalik kõiki „haavatavus : tagajärg“ kriteeriume määratleda. See on seotud olnud laevade eraldatuse, vähese teadlikkuse ja sündmuste mahavaikimisega, kuid arvestades potentsiaalset kasu ründajatele ning võimaluste paranemist seoses tehnoloogia arenguga, on oodata intsidentide kasvu. MaCRA eeliseks on see, et ta ei ole lõplik ning uue info ilmnemisel on seda võimalik pidevalt täiendada. (*ibid.*, lk 1-3)

Kaks järgmist kriteeriumit olenevad ründaja oskustest ja motivatsioonist. Haavatavuse ekspluateerimise kergus oleneb ründajale saadaolevatest ressurssidest ja ründamise tehnilisest komplekssusest, aga ka laeva kaitsemehhanismidest ning välistest teguritest. Kui laeva meeskond on küberohtudest teadlik, siis ründamise kergus langeb ning kui laev sõidab kitsustes, on teda kergem madalale ajada ja seega ründamise kergus kasvab. Haavatavuse ekspluateerimise kergusele on antud väärtused 1–5, ehk riigist kuni skriptinagani. Kasu ründajale oleneb tema motivatsioonist ning selleks on koostatud ründajate profiilid, mida on käsitletud ka antud magistritöö osas „1.2 Kes ja miks ründab“. Kasu kriteeriumile on antud väärtused 1–5, ehk vähesest kasust kuni suure kasuni. Kõik need kolm kriteeriumit omavad omakorda mitut muutujat nagu ründevektor, kaitsemehhanismid, ressursid jms. MaCRA täielik käsitlemine siinkohal oleks liiga mahukas, mistõttu toob autor mõned näited selle võimalustest. (*ibid.*, 3-6)

Joonisel 3 kujutatud riskide hindamisel võrreldakse küberkriminaali rünnaku riske kala- ja kruiisilaevale. Vasakul on toodud kriteeriumid „haavatavus : tagajärg“. Riskihindamise tulemused on kantud kahemõõtmelisele graafikule, millest üks telg tähistab haavatavuse ekspluateerimise kergust ning teine kasu ründajale. Filter F_K määrab piirkonna, milles olevad haavatavused võib kõrvale jätta nende madala kasulikkuse tõttu ründajale. (*ibid.*, 19)



Joonis 3. Kala- ja kruiisilaeva ühised riskid küberkriminaali rünnakule

Allikas: (Tam & Jones 2018, 18), autori tõlgitud

Küberkriminaali motivatsiooniks on eelkõige rahalise kasu saamine. Seetõttu on teelt eksitamise, varguse ja rünnaku varjamisega seotud riskid graafikul kujutatud suurema kasuga ründajale. Me teame ka, et kruiisilaeva turvalisusele on panustatud kalalaevast rohkem ning rünnak võib põhjustada hoiatuste ja alarmide vallandumise. Samas kalalaev opereerib kalda lähedal ning võimude reaktsioon ründele on kiirem eeldusel, et ei korraldata GMDSS-ile DoS rünnet. Seetõttu on mõlema laeva ründamise kergus peaaegu sama. Graafikult näeme, et ühised riskid laevadele on vargus kasutades AIS-i nõrkusi ning teelt kõrvale suunamine manipuleerides ECDIS-ega. Kruiisilaeva puhul võivad kriminaalid GMDSS-ile DoS ründe korraldamisega takistada suhtlust abistajatega, kasutada ära lasti, s.o inimeste, haavatavust röövimise või varguse eesmärgil ning kustutada ründe varjamiseks ära VDR-i andmed. Joonisele võib lisada ründe kerguse filtri F_{ke}, mis muudab röövimise kruiisilaevale ning ECDIS-ega manipuleerimise mõlemale laevale ründe keerukuse tõttu aktsepteeritavateks riskideks. (*ibid*.)

Eelnev näide oli üks lihtsamaid võimalusi. Realistlikumaks riskide hindamiseks tuleb konkreetse laeva küberriskide kohta koostada kõikehõlmav tabel. Arvestama peab laeva, tema lasti, sõidupiirkonna, kaitsemehhanismide ja muude eripäradega. Igale ründaja profiili kerguse ja tasu kriteeriumitele tuleb konkreetset kriteeriumi „haavatavus : tagajärg“ arvesse võttes määrata numbriline väärtus – näiteks „GMDSS – DoS rünnak“, ründaja – häktivist; kasu – 2; kergus – 1. Tabeli põhjal saab olenevalt riskihindamise eesmärgist koostada erinevat infot esitavaid graafikuid. (*ibid*., 20)

Selle näitlikustamiseks oletame, et on vaja hinnata riske tankeri elektronkaardi süsteemile lähtudes võimalikust terroristlikust rünnakust. Tankeri kohta on teada, et ta läbib kitsusi ning tema ECDIS on uus ja hästi turvatud. Me teame, et terroristide eesmärk on eelkõige laeva vigastamine või laeva kasutamine mõne muu objekti ründamiseks. Kuna tanker läbib kitsusi, on võimalus tankeri madalale suunamisega põhjustada looduskatastroof. Selle korraldamiseks võivad terroristid proovida nakatada laeva ECDIS kahjurvaraga. Arvestades terroristide motivatsiooni ja ECDIS-e turvatust, anname kriteeriumile „ECDIS : füüsiline kahju“ järgmised väärtused: kasu – 4, kergus – 2. Sama loogikat järgides on võimalik kaardistada kõik laeva haavatavused ning lähtudes erinevatest ründaja profiilidest anda ründe kasulikkusele ja kergusele numbrilised väärtused. Kandes haavatavused graafikule ja määrates kasu ja kerguse filtrid, on võimalik leida kriitilised süsteemid, mille turbesse peaks laevaomanik investeerima. (*ibid.* 19–20)

MaCRA võimalused võib kokku võtta järgmiselt (*ibid.*, 21):

- Võimaldab anda kriteeriumile „haavatavus : tagajärg“ numbrilise väärtuse ning kanda see graafikule distantsina koordinaatide alguspunktist. Kõrgema riskiga haavatavus on graafiku algpunktist kaugemal.
- Võimaldab määrata riskivahemikud. Näiteks kasu 3–5 ja kergus 1–2 tekitab riski ümber piirkonna, mille vahemikus võib risk olenevalt ründaja motivatsioonist ja vahenditest asuda. Kriminaalid võivad olla nii väheste ressursside ja oskustega üksiküritajad kui ka professionaalsed grupeeringud.
- Kandes graafikule kerguse ja tasu filtrid saab selle jagada madala-, keskmise-, ja kõrge riskiga piirkondadeks. Kõrge riski piirkonnas asuvad haavatavused peaks likvideerima, keskmise ja madala piirkonna riskidega võib tegeleda vastavalt ressursside olemasolule.

Selliste situatsioonide praktiline läbimängimine aitab paremini mõista ja kinnistada magistritöös eelnevalt käsitletud teemasid – kes võib laeva rünnata, millised on haavatavad süsteemid ning kuidas neid on võimalik ära kasutada.

1.4.2 Arvutisüsteemide kaitse parim praktika

Üldisest teadlikkusest ainuüksi ei piisa ja riske peab oskama ka maandada. Selle eelduseks on täpne teadmine oma laeva küberrünnetele haavatavatest süsteemidest ja

nende asukohast. Keeruline on hakata pärast rünnet laeva tehnilistest raamatutest ja plaanidest otsima, millise seina taga mingi seade asub, selleks, et kahjurvara „füüsiliselt“ eemaldada. (Blake, 2017) Vastava auditi läbiviimine on eelduseks intsidendiplaani koostamisele ja üldisele valmisolekule (*ibid.*). Riskide maandamiseks peavad laevaohvitserid mõistma arvutisüsteemide parimat praktikat, mille võib jaotada isiklikuks küberhügieeniks ja laevasüsteemide hoolduseks ning turbeks (UK Chamber of Shipping 2014, 11).

Isiklik küberhügieen hõlmab eelkõige andmekandjaid, paroole ja e-kirju. Laevadel kasutatakse arvutite vahel andmete jagamiseks väga palju mälupulkasid ja väliseid kõvakettaid. Tööga seotud failide kandmine isiklike- ja tööarvutite vahel, elektronkaartide uuendamine ja ECDIS-esse teekonnaplaanide kandmine, kolmanda isiku poolt konteineriplaani laadimine laeva arvutisse ning paljud muud taolised tegevused on potentsiaalsed küberintsidentide põhjused. Oluliste süsteemide puhul, nagu ECDIS, peab olema määratud üks kindel mälupulk, mida kasutatakse. Igaljuhul peab enne selliseid protseduure mälupulga viirustõrje programmiga üle käima.

Paroolide loomiseks on antud palju soovitusi ja võimalusi. Tugev parool peab olema pikk, erinema kasutajanimest, mitte sisaldama rohkem kui kaks ühesugust märki järjestikku, ei tohi olla sõnaraamatu sõna, sisaldama segamini tähti ja numbreid, ei tohi olla kasutusel mujal ning seda peab mingi aja tagant vahetama (*ibid*., 12). Autori arvates on sellised soovitused problemaatilised. Inimestel on väga palju kontosid ja paroole, mida meelde jätta ning tulemuseks on kas samade paroolide kasutamine või nende kuhugi mujale ülesmärkimine. Võimalus on muidugi kasutada paroolide talletamiseks paroolihaldurit (*password manager*), kuid kui kurjategija programmi sisse pääseb, on talle kasutaja kõikide kontode pääsumandaadid teada. Paljud veebilehed pakuvad kaksikaudentimise (*two-factor authentication*) võimalust, mida peaks alati ka kasutama. Kuna praegu on paroolide kasutamine veel vajalik, toob autor Riigi Infosüsteemide Ameti infoturbeintsidentide käsitlemise osakonna endise juhi Klaid Mägi poolt pakutud mnemoonikal põhineva süsteemi nende loomiseks ja meelespidamiseks. Esmalt valitakse lihtne paroolitüvi, näiteks „karumaja“, ning vajutatakse klaviatuuri peal klahvidest kindlas suunas mööda. Näiteks kirdesse liikudes saame K asemel O, A asemel W jne.

Ühe tüve puhul saab niimoodi koostada mitmeid kergesti meeldejäävaid paroole (Mägi 2017).

Üle 90% õnnestunud küberrünnetest saab alguse lihtsast e-kirjast, milles olevale kahjursisuga lingi või dokumendi inimene avab (Cybersecurity Ventures 2017, 9). Linkide ja failide avamisest täielikult hoidumine ei ole praktiline ning seetõttu ainus võimalus on olla ohust teadlik ning kasutada lisameetmena uuendatud tarkvara ja viirusetõrjet (UK Chamber of Shipping 2014, 12). Igal juhul peaks kahtlusega suhtuma manustesse, mille failidel on programme käitavad laiendid *exe, scr* või *bin*. Kui failil on laiend *.doc.exe*, siis on see peaaegu kindel indikaator soovist inimest petta. Ohtlikud on ka kokkupakitud ja krüpteeritud *zip* ja *rar* failid, sest nendes olevat kahjurvara viirusetõrjeprogramm ei tuvasta. Kahjurvaraga linkide peitmiseks võivad kurjategijad kasutada veebiaadresside lühendamist näiteks *TinyURL* abil. Lühendatud lingid on võimalik originaalkujule tagasi viia selleks mõeldud programmidega nagu *CheckShortURL*. Kui e-kiri tundub kahtlane, tuleks see kas kustutada, või kontrollida selle õigsust, võttes saatjaga telefoni teel ühendust (JWC International).

Praktilised soovitused laevasüsteemide hooldusel ja turbel on järgmised (UK Chamber of Shipping 2014, 16):

- minimeeri pääsuõigused (*access right*),
- eemalda üleliigsed kontod ja minimeeri külaliste konto pääsuõigused,
- uuenda tarkvara,
- varunda (*back up*) andmed,
- deinstalli mittevajalik tarkvara,
- teata süsteemi töö kõrvalekalletest,
- tunne laeva seadmeid ja oska neid kasutada,
- mõista integreeritud seadmetega kaasnevaid lisaohte,
- kaitse võrgud, traadita võrgud ja tulemüürid paroolidega.

Tarkvarauuendusi antakse välja probleemide ja turvaaukude ilmnemisel ning seoses tehnoloogia ja võimaluste arenguga (JWC International). Laeval peab alati kasutama legaalset tarkvara. Piraattarkvaraga võib saada arvutisse ning lisaks ei ole piraattarkvara puhul võimalik tootjapoolsete uuendusi läbi viia. See ei kehti mitte ainult IT tarkvara

kohta. Näiteks laevadel, millel puudub ECDIS-e nõue, on väga tihti kasutusel illegaalselt omandatud ECDIS. Sellistel süsteemidel puudub litsents ning leping kaardiuuenduste saamiseks. Magistritöö autor on töötanud laeval, kus tüürimees planeeris vananenud elektronkaartidel reisi üle liikluseraldusskeemi (TSS – *Traffic Separation Scheme*) tuues sellega laevaomanikule kaasa trahvi. Mõnikord võib OT süsteemide tarkvara uuendamine põhjustada probleeme seadmete töös, mistõttu ei ole selle läbiviimine üldse võimalik. Sellised süsteemid peavad olema muust laeva võrgust õhkeraldatud ning ligipääs nendele võib olla ainult volitatud ja ohtudest teadlikel isikutel. Tihtipeale on internetiühendus merel puudulik ning suuremaid tarkvarauuendusi ei ole võimalik enne sadamasse jõudmist läbi viia. Kriitiline moment laevale on sellisel juhul aeg sadamasse jõudmise ja uuenduste rakendamise vahel. Uuendused tuleks varakult andmekandjal sadamasse organiseerida või need koheselt kai äärde jõudes alla laadida. Mittevajalike programmide hoidmine raiskab asjatult ressurssi ning nende uuendamine ja turvaaukude paikamine unustatakse ära, mistõttu peaks arvutit aegajalt üle vaatama ja sellised programmid deinstallima

Üks olulisimaid tegevusi, mida saab teha ründest taastumise kergendamiseks, on perioodiline andmete varundamine. Laeval peaks olema paika pandud protseduur oluliste andmetest varukoopiate tegemiseks. Protseduurides peab olema määratud, kes vastutab varundamise eest, milliseid andmeid, kui tihti ja millisel viisil varundatakse, millisel andmekandjal ja kus kohas neid säilitatakse ning kuidas toimub taastamine (Toova 2015). Põhjuseid andmete kaotamiseks võib olla mitmeid – arvutisüsteemide tehnilised probleemid, lunavara või pühkuri ründed, pahatahtliku töötaja tegevus vms. Andmete kadumine on üsna sage probleem ja see juhtub tavaliselt halvimal võimalikul momendil. Ka magistritöö autori töökohal on failide kadumine katkise kõvaketta tõttu tekitanud meeskonnale suurt peavalu. Laeval on kõige sobilikumaks varundamise viisiks väliste andmekandjate kasutamine, mida peaks kasutusvälisel ajal hoidma arvutitest eraldi lukustatud kapis.

Laevasüsteemide puhul peab veelkord mainima paroole. Kui laevale paigaldatakse mingi uus seade, siis tihtipeale jäetakse sellele tehaseparool. Eelnevalt tõi autor näite satelliitside terminalidest, millest paljudele oli unustatud vaikeparool „admin/1234. Satelliitside võimaldab pääsu laeva võrku ning on seetõttu küberturbe seisukohalt üks

olulisimaid laeva süsteeme. Satelliitside seadmete pakkuja *Cobham* esindaja ütles järgnevat: „Meie terminalid, nagu on tavaline enamiku sideriistvara puhul, tulevad laevale vaikemandaadiga (*default credentials*). Me soovitame kasutajatel tungivalt seadme paigaldamise ajal parool ära vahetada ning seda ka edaspidi hea tava kohaselt sageli muuta.“ (Hughes 2017).

2 Metoodika

Uurides küberturbe temaatikat merendussektoris selgus, et kuigi teema on väga aktuaalne ja sellega tegelevad nii IMO regulatiivsel tasandil, laeva- ja kaubaomanikud andes välja suuniseid, kindlustusseltsid pakkudes võimalusi laeva ja kauba kindlustamiseks küberohtude eest kui ka tegevmeremeestele kursusi pakkuvad asutused, siis tulevaste laevaohvitseride väljaõpe mereharidusasutustes on tagaplaanile jäänud ning avalikult seda autorile teadaolevalt käsitletud ei ole. Seega on oluline uurida tulevastele laevaohvitseridele pakutavat küberturbe väljaõpet mereharidusasutuste.

Magistritööl on kaks eesmärki:

- Selgitada välja, kas üldse, ja millisel tasemel pakuvad mereõppeasutused laevaohvitseridele erialaspetsiifilist küberturbe haridust ja seoses sellega kas kinnitada või ümber lükata magistritöös püstitatud hüpotees.
- Teha mereõppeasutustele soovitused erialaspetsiifilise küberturbe hariduse korraldamiseks laevaohvitseride väljaõppes.

Nende eesmärkide saavutamiseks on uurimistöö jaotatud nelja etappi:

- valimi määratlemine ja asutuste kaardistamine,
- küsitluse läbiviimine,
- ekspertintervjuude läbiviimine,
- tulemuste analüüsimine ning soovituste esitamine.

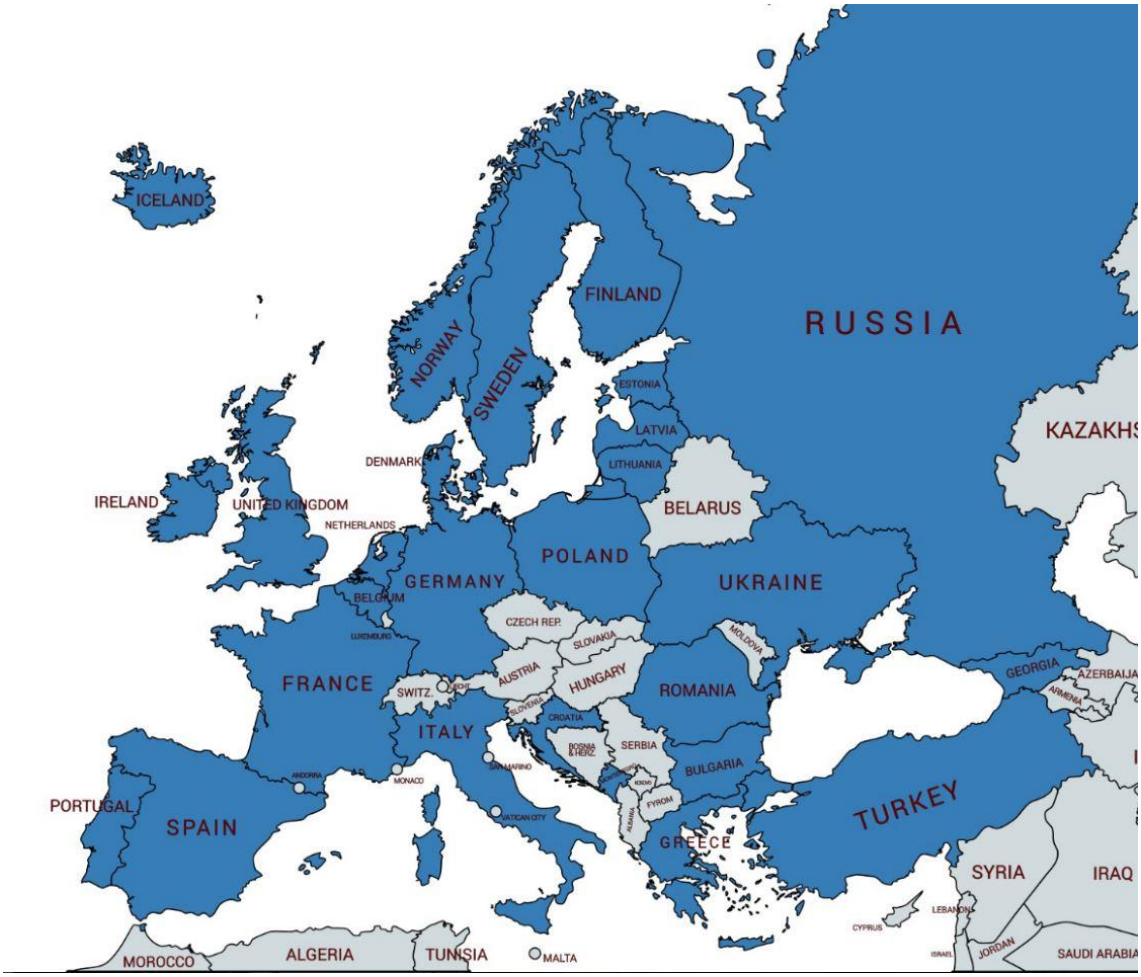
Järgnevates alapeatükkides kirjeldab autor nende etappide läbiviimise protsessi, metoodikat ja piiranguid.

2.1 Valimi määratlemine ja asutuste kaardistamine

Merendust reguleerib rahvusvahelisel tasandil IMO oma konventsioonidega. Meremeeste väljaõppe miinimumnõuded on kehtestatud STCW konventsiooni koodeksi A osaga. Nendest nõuetest peavad oma õppekavade koostamisel lähtuma ka laevaohvitsere koolitavad mereharidusasutused. See, kuidas need miinimumnõuded saavutatakse, on

jäetud suuresti osalisriikide enda otsustada ning on kooliti erinev. Seetõttu on uuringus osalevad mereõppeasutused valitud lähtudes uurija teadmisest antud grupi kohta kindlate kriteeriumite alusel kasutades eesmärgistatud valimi meetodit (Lunenburg jt 2008, 175).

Et valimit mitte liiga suureks ajada, piiritleti uuringus osalejad Euroopa mereharidusasutustega kes pakuvad väljaõpet OOW 500GT+ ja/või 750 kW+ nagu see on nõutud IMO mudelkursustega 7.03 ja 7.04 (IMO Model Courses). See tähendab, et hariduse andmine koolis ei ole vajalik kapteni ja/või vanemmehaaniku tasemel. Euroopa all on siinkohal mõeldud Euroopa maailmajagu, mille hulka on täies mahus arvatud ka Türgi. Valimisse võetud riigid on kujutatud joonisel 4.



Joonis 4. Valimisse võetud riigid (sinisega)

Allikas: Autori koostatud kasutades mapchart.net abi (Mapchart)

Koolide leidmiseks kasutati *Wikipedia* artiklit „*List of maritime colleges*“ ning *Google*'i otsingumootorit proovides erinevaid märksõnu – nt „riigi nimi + *maritime school*“. Leitud koolide koduleheküljegedel tehti kindlaks kas koolid on aktiivsed ning pakuvad haridust vastavalt määratletud kriteeriumitele. Kokku leiti 65 kooli 31-st riigist, mille andmed on toodud tabeli kujul lisas 3. Mingisugust usaldusväärset allikat selle kohta, kui palju määratletud kriteeriumitele vastavaid koole valimisse võetud riikides tegelikult on, ei õnnestunud autoril leida.

Valikusse sattusid riigid, kellel on erinev ajalooline- ja kultuuriline taust, elatustase ning suhted merendusega. Kui arvestada, et 2010. aastal pakkusid EL riigid koos Norra, Türgi, Ukraina ja Venemaaga umbes 37% maailma laevaohvitseridest (Sulpice, Guy 2011, 16) ning seda, et meremeeste haridusele on kehtestatud rahvusvaheliselt miinimumnõuded, võib antud valimi lugeda representatiivseks. See võimaldab üldistada kvantitatiivseid andmeid laevaohvitseridele pakutava merehariduse hetkeolukorra kohta maailmas.

Lisas 3 toodud andmed koolide kohta olid avalikult kättesaadavad nende asutuste koduleheküljegedel. Asutuste kaardistamise eesmärk oli leida koolid, kes juba pakuvad kas üldist või erialaspetsiifilist küberturbe väljaõpet. Selleks otsiti vastava eriala õppekavasid ning õppekavades esinevate õppeainete väljundeid. Tulemused on toodud lisa 3 tabeli veerus „KT koduleheküljel“ ning need on kategoriseeritud erinevate värvikoodidega. Kategooriad on järgnevad:

- Info puudub (must) – õppekava ja/või õppeainete väljundid ei olnud leitavad.
- Väljund puudub (punane) – õppekavas toodud õppeainete all puudusid küberturbega seonduvad väljundid.
- Üldine (kollane) – õppekavas on õppeaine ja/või õppeaine väljund, mis on seotud üldise küberturbe teadlikkusega.
- Spetsiifiline (roheline) - õppekavas on õppeaine ja/või õppeaine väljund, mis on seotud kas erialaspetsiifilise või nii erialaspetsiifilise kui ka üldise küberturbe teadlikkusega.

Õppeainete ja väljundite leidmiseks otsiti kõigepealt IT-ga seonduvaid õppeaineid, millest enim esines nt „Arvuti alused“, „IT alused“, „Arvutiõpetus“, „Infotehnoloogia“, „Infosüsteemid merenduses“ jms. Seejärel otsiti info- või küberturbega seotud õppeained

ja OT-ga seonduvate õppeainete väljundid. OT-ga seotud õppeained on näiteks „Elektroonika“, „Automaatika“, „Elektroonilised laevajuhtimise seadmed“, „Integreeritud silla- ja navigatsioonisüsteemid“, „Masinaruumi simulaatoritreening“, „Silla simulaatoritreening“ jms. Peab mainima, et erinevate koolide laevaohvitseride õppekavad sisaldasid enamjaolt samu õppeaineid ning valdav enamus õppekavasid käsitles mingil tasemel ka arvutiõpetust. Nende õppeainete väljundite all otsiti märksõnu „küberhügieen“, „infoturvalisus“, „küberturve“ jne. Kuigi OT-ga seonduvate õppeainete all esines väljunditena ka „rikete tuvastamine ja kõrvaldamine“ ning „seadmete piirangud“, siis neid arvesse ei võetud. Need väljundid olid olemas aastatel 2010–2015, mil magistritöö autor Tallinna Tehnikaülikooli Eesti Mereakadeemia (TTÜ EMERA) laevajuhtimise erialal õppis, kuid küberturbe ohtusid need endas ei hõlmanud.

Informatsiooni leidmist raskendasid nii selle puudulikkus kui ka keelelised probleemid. Kuigi koolid on loonud võimaluse muuta kodulehekülg inglise keelseks, siis kohalikus keeles on tihtipeale rohkem informatsiooni. Seetõttu kaevandati informatsiooni kohalikus keeles olevatelt kodulehekülgedelt. Tõlkimisel kasutati veebipõhise programmi *Google*'i tõlge abi, millega on võimalik tõlkida nii üksikuid lauseid kui ka terveid veebilehekülgi ja dokumente. Tekstide võrdlemiseks ja vigade avastamiseks tõlgiti tekst nii eesti kui ka inglise keelde, kusjuures kontekst ja mõte oli keelelisest korrektsusest olulisem. Kuigi autor andis andmete õigsuse tagamisel endast parima, siis on võimalik, et vajalikku infot lihtsalt ei leitud, või seda tõlgendati valesti.

Valimi määratlemise ja koolide kaardistamise eesmärk oli esmase info kogumine ning kontaktandmete leidmine. Mingisuguseid üldistavaid järeldusi küberturbe käsitlemise taseme kohta laevaohvitseride hariduses sellest teha ei saa. Seetõttu viidi järgmise etapina läbi küsitlusuuring.

2.2 Küsitluse läbiviimine

Küsitlusuuringu läbiviimiseks koostati küsimustik veebipõhise programmi *Google*'i vormid abil. Küsimustik koostati 11.03.2018 ning oli avatud sama aasta 20. maini. Selle perioodi jooksul saadeti küsimustik kõikide koolide erinevatele e-posti aadressidele koos mitmete meeldetuletustega. Adressaatideks olid osakonnajuhatajad, õppeprogrammi

juhid, aga ka koolide üldine e-post ja muud töötajad märkusega vajadusel kiri edastada pädevale isikule. Inglise keelne kaaskiri ja küsimustik on toodud lisas 4.

Lähtudes magistritöö eesmärkideks jaotati küsitlus kaheks osaks. Esimese osa peamine ülesanne oli välja selgitada kui suur osa mereõppasutustest pakuvad laevaohvitseridele erialaspetsiifilist küberturbe haridust ning selle põhjal magistritöös püstitatud hüpotees kas kinnitada või ümber lükata. Teise osaga soovis magistritöö autor saada kogemuslikku infot õppeasutustelt, kes juba käsitlevad laevaohvitseride väljaõppes küberturvet. Nende koolide kogemused aitavad koostada soovitusi ka teistele mereõppeasutustele.

Küsimustiku esimeses osas on 10 küsimust. Küsimused 1–4 aitavad vastajat tuvastada, kuid anonüümsuse tagamiseks oli nendele küsimustele vastamine vabatahtlik. Küsitakse e-posti, õppeasutuse nime, riiki ning vastaja ametikohta. Need vastused aitavad tulemusi organiseerida, tuvastada ühest asutusest tulnud mitmekordseid vastuseid ning olla kindel vastaja kompetentsuses. 5–7 küsimus annavad ülevaate asutusest. Sooviti teada saada, mis erialasid ja millisel Euroopa kvalifikatsiooniraamistiku (EQF - *European Qualification Framework*) tasemel õpetatakse ning kui palju laevaohvitsere aastas kvalifikatsiooni omandab. Need küsimused aitavad kindlaks teha kas õpetatavad erialad vastavad valimi koostamisel seatud piirangutele ning samas ka õppeasutusi ühtsetel alustel võrrelda – näiteks kas küberturbe käsitlemine oleneb pakutava hariduse tasemest ning kooli suurusest. 8–10 küsimus käsitlevad küberturvet. Uuriti kas kool pakub laevaohvitseridele küberturbe haridust, kuidas vastaja hindab selle vajalikkust ning miks ta just nii arvab. Vastused sellele küsimusele on aluseks magistritöös püstitatud hüpoteesi kinnitamiseks või ümber lükkamiseks ja otsustamiseks, milliste asutustega ekspertintervjuude läbiviimiseks kontakteeruda.

Teine osa sisaldab küsimusi 11–16. Nendele vastamise eelduseks oli see, et asutus viib läbi laevaohvitseridele suunatud küberturbe õpet. Selle osa küsimuste eesmärgiks oli täiendada ekspertintervjuude tulemusi ning saada infot soovituste koostamiseks. Küsiti, millisel viisil ja kuidas vastaja asutuses on küberturbe haridus laevaohvitseride väljaõppe raames korraldatud, kas väljaõppe käigus kasutatakse ka simulaatoritreeningut ja kuidas vastaja hindab oma kooli kogemust küberturbe väljaõppe korraldamisel. Ka sooviti teada saada miks otsustati just sellise õppekorralduse kasuks, millised probleemid tekkisid,

kuidas hindasid õpilased väljaõppe vajalikkust ja kas vastaja hinnangul oleks vaja väljaõpet muuta või seda täiendada.

2.3 Ekspertintervjuude läbiviimine

Mereõppeasutuste kaardistamise ja küsitlusuuringu tulemuste põhjal oli võimalik määrata õppeasutused, kes käsitlevad laevaohvitseride väljaõppes küberturvet. Kõigile neile õppeasutustele saadeti e-kiri sooviga antud teemal viia läbi intervjuu kas e-kirja, *Skype*'i või vahetu suhtluse teel. Intervjuude eesmärgiks oli soov saada täiendavat infot koolide kogemuste ja intervjueeritavate arvamuste kohta. Intervjuu meetodiks valiti poolstruktureeritud intervjuu. Põhiküsimused olid ette valmistatud, kuid vastavalt intervjuu käigus ilmnenud uuele informatsioonile, võisid need muutuda. Intervjuud on tähistatud „intervjuu 1", „intervjuu 2" jne. Küsija ja vastaja tähised on vastavalt „K" ja „V" ning vastaja tekst on kaldkirjas. Erinevate intervjuude küsimused ja vastused on toodud lisas 5.

3 Tulemuste analüüs ning soovitused

Tulemuste analüüs on jaotatud viieks alapeatükiks:

- mereõppeasutuste kaardistamise tulemused,
- küsitluse tulemused,
- ekspertintervjuude analüüs,
- uuringu kokkuvõte,
- soovitused küberturbe väljaõppe läbiviimiseks.

Kõigepealt analüüsitakse uurimismeetodite tulemusi ja seejärel koostatakse nende põhjal soovitused mereõppeasutustele.

3.1 Mereõppeasutuste kaardistamise tulemused

Esmalt otsiti koolide õppekavadest IT-ga seotud õppeaineid ja nende väljundeid. Avalikult kättesaadava info põhjal valimisse võetud 65 mereõppeasutuse seas 7 kooli, kus laevaohvitseride õppekavas infotehnoloogiaga seotud ained puudusid. Autori arvates on arvutioskused eelduseks küberturbe mõistmisel. Tänapäeva õpilased on küll kasvanud arvutitega, kuid oma lõbuks internetis surfamise ja arvutite sihipärasel ja ohutul kasutamisel on vahe sees. Küberturbe käsitlemist üldisel tasemel oli mainitud kahe kooli õppekavades. TTÜ EMERA laevajuhtimise ja -mehaanika õppekavade õppeaine „IT-alused“ õpiväljundites oli kirjas „Mõistab küberturvalisuse ja -eetika põhimõtteid“ ning kooli *Merchant Marine Academy of Syros* õppeaine „infotehnoloogia“ õppematerjalides oli küberturvet käsitlev peatükk.

Edasi otsiti küberturbega seotud õppeaineid ning OT-d käsitlevate õppeainete väljundeid. Eraldi õppeaineid, mis käsitleksid küberturvet ühegi mereõppasutuse õppekavadest ei leitud. Küll aga oli Dubrovniku ülikooli (*University of Dubrovnik*) laevajuhtide ja -mehaanikute õppekavas õppeaine „Infosüsteemid merenduses“ (*Pomorski informatički sustavi*). Õppeaine sisu kohta oli muuhulgas antud järgnev informatsioon – „infosüsteemide avatus ja haavatavus, turvatehnoloogiad süsteemide kaitsmisel, privaatsuspoliitika.“ Sellise käsitluse luges autor erialaspetsiifiliseks.

20 kooli kodulehekülgedel olid leitavad nii õppekava kui ka õppeainete väljundid, kuid nende all puudus informatsioon küberturbe käsitluse kohta väljaõppes. 42 kooli kodulehekülgedel puudusid kas õppekavad või õppekavade olemasolul õppeainete väljundid. Koondinfo kaardistamise tulemuste kohta on toodud tabelis 1.

Tabel 1. Mereõppeasutuste kaardistamise koondinfo

Riikide arv	31	
Koolide arv	65	
Arvutiõpetust pakkuvate koolide arv	51 (7 kohta puudub info)	
Küberturvet käsitlevate koolide arv	Üldine:	2
	Erialaspetsiifiline:	1
	Info puudub:	42
	Väljund puudub:	20

Allikas: (Autori koostatud lisas 3 toodud tabeli andmete alusel)

3.2 Küsitluse tulemused

Vastused saabusid 19 kooli esindajatelt 14-st riigist. Küsimused 1–4 olid mõeldud vastaja tuvastamiseks ning olid vastamiseks vabatahtlikud. Sellegi poolest vastasid neile kõik peale ühe küsitletu, mis välistab mitmekordsed vastused. Vastajateks olid erinevad õppejõud, osakonnajuhatajad ja programmijuhid, aga ka kaks rektorit ning üks endine õpilane.

Järgmise kolme küsimusega saadi ülevaade asutustest. Määratleti, et kõik koolid pakuvad erialasid vastavalt valimis sätestatud kriteeriumitele, st vähemalt OOW 500GT+ ja/või EOOW 750kW+. Üks kool võimaldas laevaohvitseridele väljaõpet ainult EQF tasemel 5, mis antud riigis tähendab kutseharidust. Kõik teised koolid võimaldasid haridust vähemalt EQF tasemel 6, mis Eesti mõistes tähendab rakenduskõrgharidust. Küsitluses osalenud õppeasutustest laevaohvitseri kvalifikatsiooni omandanud õpilaste arv varieerus 20–200.

Kaheksas küsimus oli antud magistritöö hüpoteesi seisukohalt olulise tähtsusega. Uuriti, kas antud õppeasutus pakub laevaohvitseridele küberturbe haridust. Küsimuse tulemused on toodud tabelis 2. Sellele küsimusele vastas jaatavalt ainult kaks õppeasutust ehk 10,5%

vastajatest. Viis kooli planeerivad sellega alustada lähitulevikus ning kaksteist kooli, ehk üle poole vastanutest, ei ole veel mõelnud küberturbe käsitlemisele laevaohvitseride väljaõppes. Üks õppeasutus vastas, et nad proovivad leida külalisõppejõude sellel teemal rääkima. Kuna selle kooli teised vastused andsid mõista, et nad ei ole seda veel teinud, siis loetakse nende vastuseks „Ei“. Antud küsimuse tulemused näitavad, et küberturbe haridus laevaohvitseride väljaõppes ei ole piisav tänapäeva laevade ohutumaks käitamiseks.

Tabel 2. Vastused küsimusele 8

Kas teie õppasutuses pakutakse tulevastele laevaohvitseridele küberturbe väljaõpet?	
Vastus	**Vastanute arv ja osakaal**
Jah	2 (10,5%)
Ei	12 (63,2%)
Ei, kuid planeerime alustada lähitulevikus	5 (26,3%)

Allikas: (Autori koostatud)

Üheksanda küsimusega uuriti, kas õppeasutused peavad üldse vajalikuks küberturvet laevaohvitseride väljaõppes käsitleda. Seda ei pidanud vajalikuks ainult üks õppeasutus. Üksteist, ehk üle poole vastanutest, pidas seda vajalikuks juba praegu, ja seitse vastajat arvas, et selle vajadus võib tekkida millalgi tulevikus. Küsimuse tulemused näitavad, et kuigi vaid vähesed õppeasutused pakuvad magistritöö kirjutamise ajal küberturbe haridust, siis enamik on nõus selle käsitlemise vajalikkusega. Üheksanda küsimuse tulemused on toodud tabelis 3.

Tabel 3. Vastused küsimusele 9

Kas te peate vajalikuks küberturbe väljaõppe pakkumist tulevastele laevaohvitseridele?	
Vastus	**Vastanute arv ja osakaal**
Jah	11 (57,9%)
Ei	1 (5,3%)
Võibolla tulevikus	7 (36,8%)

Allikas: (Autori koostatud)

Eelnevate küsimustega eeldati leida mingisugune seos kas kooli suuruse, pakutava kvalifikatsiooni, riigi elatustaseme või riigi meremajanduse innovatiivsuse ning pakutava küberturbe hariduse taseme vahel. Kuna 19-st küsitluses osalenud koolist võimaldas küberturbe haridust ainult 2 kooli, siis selliseid järeldusi ei olnud võimalik teha. Ühe tähelepanekuna võib välja tuua, et kool, kes ainukesena ei pidanud küberturbe väljaõpet vajalikuks, koolitas laevaohvitsere ainsana kutsehariduse tasemel.

Kümnes küsimus andis vastajatele võimaluse põhjendada oma vastust eelmisele küsimusele. Need koolid, kes pidasid küberturbe väljaõpet vajalikuks, põhjendasid seda järgmiselt:

- kasvav ühenduvus merel nõuab palju rohkem teadmisi küberhügieenist;
- on vajalik, kuid see nõuab lisaaega õppekava läbimiseks, mis praegusel hetkel ei ole võimalik;
- see oleks tõesti vajalik;
- tehnoloogia arenguga on see kasvav oht;
- laevaohvitseridel on vaja paremaid arvutialaseid teadmisi;
- tänapäeval on küberturve väga oluline osa laeva ohutusest;
- küberkuritegevus on kasvamas;
- on väga oluline suhtuda küberturbesse täie tõsidusega.

Koolid, kes arvasid, et küberturbe väljaõppe vajadus tekib tulevikus, põhjendasid oma vastust järgnevalt:

- Praegu ei ole internet laevadel veel sellisel tasemel, kuid tulevikus kindlasti.
- Ma usun, et küberturve on laeva ohutuse seisukohalt oluline. Samas leian ma, et meremeestel on niigi väga palju tööd laeval. Ma arvan, et laevaohvitserid vajavad üldist teadlikkust, turvalisemaid süsteeme ning kalda poolset toetust ja väljaõpet süsteemide kasutamisel.
- Meremeeste õppekava baseerub STCW nõuetel ja küberturve ei ole koodeksiga veel nõutud.

Kool, kes ei pidanud küberturbe väljaõpet vajalikuks, põhjendas seda sellega, et küberrünnetele on haavatavad pigem laevandusettevõtted, mitte aga laevad. Magistritöö

teooria osa põhjal võib selle väite ümber lükata. Laevad on sarnaselt kaldaettevõtetele haavatavad. Pigem on seni olnud neile keerulisem ligi pääseda ja seetõttu on intsidente vähem toimunud. Võib väita, et mereõppeasutused üldiselt teadvustavad probleemi. See võib olla seotud viimasel ajal maailmas toimunud ning laialdast meediakajastust pälvinud suurte küberintsidentidega, aga ka samasugust meediakaja pälvinud ning mais jõustuvate GDPR ja NISD õigusaktidega.

Väitega, et STCW koodeksiga küberturvet et nõua, ja seega ei peaks seda käsitlema, ei saa mitte kuidagi nõustuda. Magistritöö sissejuhatuses oli tähelepanu pööratud asjaolule, et elektronkaarte oli laevadel lubatud kasutada ligi 20 aastat enne pädevusnõuete sisseviimist STCW koodeksisse. Ka võib magistritöö teooria osa põhjal järeldada, et internetiühendus laevadel on juba praegu sellisel tasemel, et muuta laevad küberrünnetele haavatavaks. Nagu eelnevalt mainitud, on ka magistritöö autori laeval internetiühendus koguaeg olemas. Meremeeste suure töökoormusega võib nõustuda. Tehnoloogia areng on muutnud meeskonnad küll väiksemaks, kuid töökoormuse vähenemist ei ole see endaga kaasa toonud. Miks see nii on, jääb antud magistritöö skoobist välja. Väljaõppe korraldamise soovituste koha pealt peab arvestama vastajate tähelepanekutegaa, et laevaohvitserid vajavad paremat arvutialast haridust ja küberturbe käsitlemine väljaõppe käigus on raskendatud ajaliste piirangute tõttu.

Küsimuste plokk 11–16 oli mõeldud vastamiseks nendele õppeasutustele, kes juba pakuvad laevaohvitseridele küberturvbe haridust. Neid õppeasutusi oli ainult kaks. Esimene neist käsitleb küberturvet erialaspetsiifiliselt ning viib seda läbi eraldi õppeainena. Õppeaine koostamisel on nad pidanud nõu küberturbe ekspertidega ning praegust väljaõppe taset peavad nad piisavaks. Õppeaine raames käsitletakse järgnevaid teemasid:

- küberturbe alused (terminoloogia, üldine teadlikkus jms);
- arvutivõrkude ja side alused;
- merendusega seotud rahvuslikud ja rahvusvahelised õigusaktid ning standardid ja suunised;
- laeva info- ja käidutehnoloogia küberturve;

– küberintsidentide vastane kaitse, nende tuvastamine, nendele reageerimine ja nendest taastumine.

Teine kool käsitleb küberturvet muu aine raames. Nemad õpetavad laevaohvitseridele üldist küberturbe teadlikkus ning väljaõppe käigus käsitletakse eelmise õppeasutusega samu teemasid. Juurde lisavad nad, et küberturbe spetsiifiline käsitlus on korraldatud IT-ga mitteseotud õppeainete raames. Ka nemad leiavad, et praegune väljaõpe nende koolis on piisav. Kahjuks ei kasuta kumbki neist koolidest simulaatorit küberintsidentide läbimängimiseks. Lisaks oli üks kool, kes on oma väljaõppe korraldamisega planeerimise faasis. Nemad vastasid, et kavatsevad kõiki eelnevalt mainitud teemasid käsitleda. Kuigi valikuna oli käsitletavate teemade alla lisatud ka „*Ship as a target (who, why and how would attack my ship).*“, siis seda ei olnud ükski kool märkinud. Autori arvates on see erialaspetsiifilise käsitluse puhul üks olulisimaid teemasid.

Viimane küsimus uuris, kas koolid peavad oma praegust küberturbe väljaõppe taset piisavaks. Sellele vastasid positiivselt eelnevalt mainitud kaks kooli, kes küberturvet oma väljaõppes juba käsitlevad. Antud küsimust kommenteerisid ka kaks kooli, kes küberturbe koolitus laevaohvitseridele ei paku. Need kommentaarid oleksid küll rohkem sobinud kümnenda küsimuse vastuseks, kuid tuuakse sellegipoolest siin ära:

– Küberturve on olulisem laevajuhtidele.
– Probleem on selles, et õppekava raames peab käsitlema niigi väga palju uusi teemasid. Keskkond, seadusandlus, energiatõhusus, alternatiivsed kütused jne. Bakalaureuse tasemel on praegu niigi raske kõiki teemasid piisaval tasemel käsitleda. Küberturbe probleemid on väga kiiresti muutuvad. Seetõttu arvan, et ei ole mõttekas õpetada tudengitele selliseid tehnoloogiaid, mis võivad kooli lõpetamisel juba vananenud olla.

Väide, et laevajuhtidele on küberturve kuidagi olulisem, ei pea enam paika. Tänapäeval on nii laeva sild kui ka masin ühendatud laeva võrku ja läbi satelliitside välisohtudele haavatavad. Kindlasti on rakendatud kaitsemehhanisme ja võrgud on üksteisest mingitmoodi eraldatud, kuid see ei muuda neid immuunseteks. Teise väitega on magistritöö autor rohkem nõus. Tehnoloogia kiiret arengut peab arvestama tegelikult kogu haridussüsteem. Oluline on panna rõhku elukestva õppe vajalikkusele ja koolid

saavad siinkohal kujundada õpilaste väärtushinnanguid. Sellest hoolimata ei ole lahendus käega lüüa ja küberturve väljaõppest üldse välja jätta. Eesmärk ei olegi laevaohvitsere koolitada IT ja küberturbe spetsialistideks. Juba koolis antud teema olulisuse rõhutamine annab tulevasele laevajuhile või -mehaanikule arusaamise, et oma töös lihtsate küberhügieeni nõuannete eiramine omab reaalseid tagajärgi füüsilises maailmas.

3.3 Ekspertintervjuude analüüs

Mereõppeasutuste kaardistamise ja küsitluse läbiviimise tulemusena leiti viis õppeasutust, kes pakuvad laevaohvitseridele küberturbe väljaõpet. Kolm neist käsitlevad küberturvet üldise teadlikkuse tasemel ning kaks erialaspetsiifiliselt. Lisaks oli üks kool, kelle küberturbe väljaõpe oli planeerimise faasis. Nendele kuuele koolile saadeti e-kiri sooviga viia läbi intervjuu. Sellega nõustusid kolme kooli esindajad. Info vastajate kohta on toodud tabelis 4. Kuigi põhiküsimused olid ette valmistatud, kujunesid intervjuud erinevateks. Vastajad töötasid erinevates koolides erinevatel ametikohtadel ja nende lähtekohad erinesid. Ka ilmnes intervjuude käigus uusi asjaolusid, mistõttu küsimusi lisandus, jäi ära, või neid muudeti. Intervjuud täies mahus on toodud lisas 5.

Tabel 4. Intervjuude koondinfo

Õppeasutus	**Vastaja amet**	**Intervjuu tähis**
TTÜ EMERA	„IT alused“ lektor	Intervjuu 1
	Laevamehaanika programmijuht	Intervjuu 2
	Laevajuhtimise programmijuht	Intervjuu 3
Läti Mereakadeemia	Kooli esindaja	Intervjuu 4
Ljubljana Ülikooli Merenduse ja transpordi teaduskond	Kooli esindaja	Intervjuu 5

Allikas: (Autori koostatud)

TTÜ EMERA käsitleb küberturvet õppeaine „IT-alused“ raames. Intervjuuga olid nõud „IT alused“ lektor ning laevamehaanika ja laevajuhtimise programmijuhid. Nendega lepiti kokku kohtumine ning intervjuud viidi läbi vahetu suhtluse teel. Intervjuu salvestati nutitelefoni vastava rakendusega, transkribeeriti, ning saadeti e-kirjaga vastajatele

ülevaatamiseks. Intervjueeritavad viisid sisse korrektuurid ning ühtlasi andsid loa kasutada magistritöös oma ametinimetusi nii nagu need on toodud tabelis 4.

Järgnevalt toob magistritöö autor peamised tähelepanekud intervjuudest TTÜ EMERA esindajatega, millega peab laevaohvitseride küberturbe väljaõppes arvestama:

- Teema on uus ja väljaõpe tuleb koostada nullist.
- Emakeelne õppematerjal on puudulik või puudub täielikult.
- Õppekavad on täis ning nõudeid tuleb üha juurde.
- Õppejõud peavad ennast teemaga kurssi viima, kuid koormus on juba praegu suur.
- Üldainete raames küberturvet käsitleda on problemaatiline, sest maht on piiratud.
- Laevajuhid ja -mehaanikud peaksid saama küberturbe haridust samal tasemel.
- Kuigi masina ja silla simulaatorid ei võimalda otseselt küberintsidente läbi mängida, on võimalik simuleerida selliste intsidentide tagajärgi. Näiteks ütleb üles mõni automaatjuhtimissüsteemi lüli või kaob GPS signaal. Selline treening on väga oluline osa väljaõppest.
- Traditsioonilised navigatsioonimeetodid on olenemata tehnoloogia arengust endiselt vajalikud.
- E-kursuste eest ei saa üliõpilased ainepunkte.

Kuigi üldiselt peeti küberturvet oluliseks, tekitas vastakaid arvamusi väljaõppe vajalikkus mehaanikutele. Seda probleemi on eelnevalt antud magistritöös käsitletud ja lähtudes uurimistöös kogutud informatsioonist arvab autor, et laevajuhid ja -mehaanikud peavad küberturbe koolitust saama ühtemoodi. Oluline põhjus, miks küberturvet laevaohvitseride väljaõppes nii vähesel määral käsitletakse, on nõuete puudumine STCW-koodeksis. Me teame aga, et ECDIS-e pädevusnõuete sisseviimine koodeksisse võttis aega peaaegu 20 aastat. Mereõppeasutused peavad arvestama sellega, et lähitulevikus võivad küberturbe teadmised määrata, kelle laevaomanik tööle võtab. Magistritöö teooria osas selgus, et juba praegu võivad laevaomaniku võimalused kaubaveo lepingute saamiseks sõltuda küberturbe protseduuride olemasolust SMS-is.

Läti Mereakadeemia oli magistritöö kirjutamise ajal küberturbe hariduse korraldamisega planeerimise faasis. Kooli esindajaga suheldi e-posti vahendusel. Planeerimise faas

tähendab seda, et nad püüavad koguda informatsiooni ja teadmisi merendussektori vajaduste kohta ning töötavad läbi IMO ja muude huvirühmade suuniseid ja nõuandeid. Läti valitsus ja mereadministratsioon küberturbe käsitlemist laevaohvitseride väljaõppe raames ei nõua ja praegu pole koolil päris selge, kuidas nad sellega edasi lähevad.

Ljubljana Ülikooli Merenduse ja transpordi teaduskonna esindajaga suheldi *Skype'*i vahendusel. Nemad käsitlevad küberturvet nii laevajuhtide kui -mehaanikute väljaõppes üldise teadlikkuse tasemel õppeaine „turvaalane teadlikkus" raames. Selle õppeaine õpetamise kohustuslikud miinimumnõuded on toodud STCW koodeksi tabelis A-VI/6-1. Kuigi tabelis toodud kompetentsinõuded käsitlevad füüsilist turvalisust, on teaduskond leidnud, et ka küberturvet on sobilik selle õppeaine raames käsitleda. Küberturve on üsnagi väike osa sellest õppeainest ja võtab ajaliselt umbes 10-15 minutit. Teaduskonna esindaja leiab, et meremeestele on eelkõige vaja õpetada lihtsat küberhügieeni. Õppeaine raames käsitletakse näiteks e-kirjade, paroolide ja mälupulkadega seotud ohtusid. Vähesel määral mainitakse küberohtusid ka õppeaine „Elektroonilised laevajuhimise seadmed" ja valikaine „Merenduse infosüsteemid" raames. Nendes ainetes mainitakse näiteks laevadel illegaalse tarkvara kasutamisega seotud ohtusid. Kuna maht on väike ja õpetatakse ainult baasteadmisi, siis mingisuguseid probleeme õppe korraldamisega ei ole olnud. Info küberturbe intsidentide ja arengute kohta merenduses saadakse inglise keelsena ja õppejõud vahetavad sellekohaseid teadmisi omavahel. Kui teaduskond soovib õppekavas teha muutusi, on seda vaja põhjendada ülikoolile ja mereadministratsioonile. Kui kõik vastavad ülikooli ja STCW nõuetele, siis muutuste tegemisega õppekavas probleeme ei ole. Teaduskonna esindaja leiab, et praegune küberturbe käsitlemise tase on neile piisav. Laevaohvitserid peavad küll olema teadlikud üldisest küberhügieenist, kuid küberrünnete eest kaitsmine ja neile reageerimine on vastava ala spetsialistide ülesanne.

Ljubljana Ülikooli puhul on positiivne see, et asjaga tegeletakse. Samas ei saa nõustuda, et nende poolt pakutav väljaõpe on piisav. E-kirjade, mälupulkade ja paroolide küberturve peaks olema minimaalne oskus kõigile neile, kes arvutitega kokku puutuvad. Meremeestest ei ole vaja küll koolitada IT spetsialiste, kuid peab aru saama, et häda korral merel võib abi liiga kaugel olla. Seetõttu koolitatakse meremehi ka muudel aladel nagu tuletõrje, meditsiin ja päästevõtted, rohkem, kui kaldal töötajaid. Magistritöö teoreetilises osas käsitletud intsident, kui häkkerid võtsid kontrolli laeva navigatsioonisüsteemi üle,

on tõestus, et laevaohvitseridel on sellekohaseid teadmisi rohkem vaja. Laevaohvitserid peaksid olema võimelised küsima laevaomanikult vastavaid küsimusi, oskama igasuguse situatsiooni korral laeva käsijuhtimisele võtta ja vajadusel täitma kaldapoolse IT toe juhtnööre.

Kahjuks ei õnnestunud autoril saada intervjuud nende kahe kooliga, kes pakuvad laevaohvitseridele erialaspetsiifilist küberturbe haridust. Dubrovniku Ülikooli esindaja oli küll nõus küsimustele vastama, kuid ütles pärast, et temal vastavad teadmised puuduvad. Selle kooli õppeaine „Infosüsteemid merenduses“ väljundite all oli toodud turvatehnoloogiad süsteemide kaitsmisel. Sama õppeaine oli ka Ljubljana Ülikooli laevaohvitseride õppekavas, kuid seal käsitleti küberturvet minimaalsel tasemel. Seetõttu on raske öelda, kas Dubrovniku Ülikool pakub laevaohvitseridele küberturbe haridust piisaval määral.

3.4 Uuringu kokkuvõte

Tabelis 5 on koondatud nii kaardistamise kui ka küsitluse tulemused. Kattuvused on välistatud, sest magistritöö autorile on teada küsitluses osalenud õppeasutused. Valimisse võetud 65-st koolist 30 kooli kohta ei leitud uurimistöö käigus piisavalt informatsiooni küberturbe hariduse läbiviimise kohta järelduste tegemiseks. 19 kooli kohta saadi info küsitluse teel ning 16 kooli kohta leiti piisavalt infot kooli kodulehekülgedelt. Need 35 järelduste tegemisel arvesse minevat kooli moodustavad 53,8% valimist. 35-st koolist ainult kaks ehk 5,7% käsitlevad küberturvet erialaspetsiifiliselt.

Kvantitatiivseid tulemusi toetab magistritöö käigus kogutud kvalitatiivne info. Teema on uus, rahvusvaheliste regulatsioonidega selle käsitlemine väljaõppes nõutud ei ole, õppemahud on suured ning õppematerjal on puudulik. Seda arvesse võttes loeb autor magistritöös püstitatud hüpoteesi kinnitatuks. Mereõppeasutused ei ole tulevaste laevaohvitseride väljaõppes pööranud piisavalt tähelepanu erialaspetsiifilisele küberturbe haridusele võimaldamaks neil laevu ohutult käitada.

Tabel 5. Kaardistamise ja küsitluse tulemuste koondtabel

Riikide arv	31	
Koolide arv valimis	65	
Koolid, kelle kohta infot ei leitud	30 (46,2%)	
Küsitluses osalenud koolide arv	19 (29,2%)	
Koolid, kes lähevad järelduste tegemisel arvesse (kaardistamine + küsitlus)	35 (53,8%)	
Küberturbe käsitlemine koolides (kaardistamine + küsitlus)	**Kokku 35 kooli**	
	Ainult üldine:	3 (8,6%)
	Erialaspetsiifiline:	2 (5,7%)
	Väljund puudub:	13 (37,1%)
	Ei käsitle	17 (48,6%)
Suhtumine küberturbe hariduse vajalikkusesse (küsitlus)	**Kokku 19 kooli**	
	Vajalik	11 (57,9%)
	Ei pea vajalikuks	1 (5,3%)
	Võibolla tulevikus	7 (36,8%)

Allikas: (Autori koostatud)

Positiivseks võib lugeda asjaolu, et enamasti mõisteti küberturbe hariduse vajalikkust. Küsitluses osalenud 19-st koolist 11 pidas selle käsitlemist väljaõppe käigus juba praegu vajalikuks ja 7 kooli leidsid, et seda võiks käsitleda millalgi tulevikus. Ka intervjuudest koolide esindajatega selgus, et küberturbe käsitlemine oleks vajalik. Samas ei ole päris selge, kuidas seda läbi viima peaks. Teema on uus ja nõuded või suunised, kuidas mereõppeasutused seda käsitlema peaksid, puuduvad. Seetõttu koostab magistritöö autor järgmises alapeatükis mereõppeasutustele soovitused küberturbe erialaspetsiifiliseks käsitlemiseks laevaohvitseride väljaõppes.

3.5 Soovitused küberturbe väljaõppe läbiviimiseks

Magistritöö teoreetilises osas selgus, et laevad on juba praegu haavatavad küberrünnetele ning intsidentide arv üha kasvab. Laevaohvitseride koolitamine küberohtudega toimetulemiseks on üks olulisimaid tegevusi meresõiduohutuse tagamisel. Samas selgus magistritöös läbiviidud uuringust, et probleeme küberturbe käsitlemiseks laevaohvi–

tseride väljaõppes on palju ja vaid väga vähesed õppeasutused pakuvad sellist võimalust. Üldiselt koolid siiski teadvustavad probleemi, kuid päris täpselt ei olda kindlad, kuidas peaks edasi minema. Küberturbe korraldamine laevaohvitseride väljaõppes võib esmapilgul tunduda suure ettevõtmisena, kuid oluline on teha esimene samm. Autori arvates on selge, et varem või hiljem tehakse küberturve meremeeste väljaõppes kohustuslikuks. Selles alapeatükis koondab autor kõik magistritöö teoreetilises ja uurimuslikus osas omandatud teadmised ning pakub selle info põhjal mereõppeasutustele parima võimaliku viisi küberturbe käsitlemiseks laevaohvitseride väljaõppes. Lisaks pakub autor välja toetavad tegevused, mida peaks laevaohvitseride väljaõppes arvesse võtma seoses tehnoloogia kiire arenguga.

Eeldused väljaõppe plaani koostamiseks on järgmised:

- ühine koolitus kõigile laevaohvitseridele (laevajuhid ja -mehaanikud);
- koolituse läbiviija peab olema keegi, kes ei ole täiskohaga õppejõud;
- koolitus ei tohiks olla ajamahukas;

Eelnevast loetelust lähtuvalt leiab magistritöö autor, et parim viis küberturbe hariduse pakkumiseks on korraldada laevaohvitseridele kahepäevane erialaspetsiifiline koolitus. See, kuidas koolitus õppekavva integreerida nii, et õpilased selle läbimise eest ka ainepunkte saavad, jääb iga kooli enda otsustada. Mereõppeasutuste õppekorraldused on erinevad ja ühest vastust sellele anda ei saa. Ekspertintervjuude põhjal võib siiski väita, et selliste muudatuste temine ei ole probleem. Järgnevalt kirjeldatud kahepäevane erialaspetsiifiline küberturbekoolitus ei ole mõeldud üksnes kasutamiseks mereõppeasutustes. Sarnase koolituse võivad läbi viia ka ettevõtted, kes pakuvad meremeestele täiendõppekursusi või muud huvirühmad.

3.5.1 Küberturbe koolitus

Autori poolt pakutud koolitus viiakse läbi viimasel kursusel, kui õppurid on läbinud praktika ja omavad juba mingisugust arusaama tööst laeval. Kursuse esimesel päeval käsitletakse teoreetilisi aspekte ja teisel päeval viiakse etteantud stsenaariumite põhjal läbi iseseisev riskide hindamine. Küberturbe teooria päeva aluseks võib võtta antud magistritöö teoreetilise osa. Käsitlema peaks vähemalt järgmisi teemasid:

- Asjakohased regulatsioonid ja suunised – küberturbe ja merendusega seotud konventsioonid ja muud rahvuslikud ja rahvusvahelised õigusaktid ning huvirühmade suunised ja nende mõju laevaohvitseride tööle.
- Kes ja miks laeva ründab? – ründajate profileerimine, nende motivatsioon ja ressursid rünnakute korraldamiseks ning näited elust.
- Mida ja kuidas laeval rünnatakse? – laeva haavatavused: inimesed, IT ja OT süsteemid ning nende eripära lähtudes küberturbest, navigatsioonisüsteemid, masinasüsteemid ning näited elust.
- Kuidas laeva kaitsta? – füüsiline turvalisus, inimtegur ja arvutisüsteemide parim praktika.

Teisel päeval toimub etteantud stsenaariumite põhjal iseseisev riskide hindamine MaCRA raamistiku alusel. Õpilased saavad kasutada eelmisel koolituse päeval omandatud teoreetilisi teadmisi ning määrata laeva, sõidupiirkonda, haavatavaid süsteeme jms arvesse võttes, milliste seadmete küberturbesse peaks laevaomanik investeerima ja laevapere kõrgendatud tähelepanuga suhtuma. Peale riskide hindamist kannavad õpilased tulemustest ette ning toimub üldine arutelu.

3.5.2 Toetavad tegevused

Küberturbe teadlikkust toetavad tegevused, mida mereõppeasutused peaksid laevaohitseride koolitamisel arvesse võtma on järgnevad:

- simulaatoritreening,
- arvutialased teadmised,
- traditsioonilised meresõiduoskused.

Praegu koolides kasutusel olevad silla- ja masinaruumi simulaatorid ei võimalda küll küberintsidente otseselt läbi mängida, kuid lubavad simuleerida erinevate süsteemide rikkeid. Oluline on need rikked siduda küberintsidentidega. Magistritöö teoreetilises osas oli toodud näide GPS signaalide võltsimisest Musta mere piirkonnas. Taoliste stsenaariumite läbi mängimine simulaatoris aitab õpilastel aru saada küberohtude võimalikkusest laevadel ning osata neile adekvaatselt reageerida. Sarnasel põhimõttel

küberintsidentide läbimängimine on võimalik ka masinaruumi simulaatoris. Oluline on rikke põhjus siduda küberintsidendiga.

Enamiku valimisse võetud mereõppeasutuste õppekavades oli olemas arvutiõpetusega seotud õppeaine. Nende õppeainete raames tegeletakse põhiliselt kontoritarkvara õppimisega. TTÜ EMERA õppeaines „IT alused“ on alates 2017. aasta sügistest viidud sisse muudatused ja õppeaine raames käsitletakse muuhulgas arvutite riistva ja võrkusid. See on tervitatav muutus ning ka teised mereõppeasutused peaksid sellest eeskuju võtma. Ka magistritöö autor on oma töö käigus tundnud sellistest teadmistest puudust. Mõistmine, kuidas erinevad laeva seadmed omavahel ning välismaailmaga ühendatud on, aitavad laevaohvitseridel aru saada võimalikest küberohtudest ning rakendada nende kaitsmisel parimat praktikat. Veelgi sügavamaid teadmisi pakub TTÜ EMERA laeva elektromehaaniku õppeaine „Laeva arvutivõrgud ja andmetöötlussüsteemid“. Kõikidel laevadel on olemas sellised süsteemid, kuid väga paljudel ei ole pardal elektrimehaanikut. Vastavate baasteadmiste õpetamist võiks kaaluda ka laevajuhtide ja -mehaanikute õppekavas. Olulised teadmised on muuhulgas:

- tööstuslike arvutivõrkude otstarve ja ehitus;
- interneti ja etherneti protokollid;
- laevajuhtidele: silla integreeritud navigatsioonisüsteemide, dünaamilise positsioneerimise süsteemi ja reisiandmete salvestusseadme otstarve, ehitus ja funktsioonid;
- laevamehaanikutele: programmeeritavate kontrollerite- või arvutipõhiste jõu–seadmete võimsuse juhtimise, kütusekulu optimeerimise ja kütuse säilitamise, ümberpumpamise ja ettevalmistuse süsteemide otstarve, ehitus ja funktsioonid.

Traditsioonilised meresõiduoskused kuuluvad laevajuhtide pädevuse alla. Siia võib lugeda sellised oskused nagu meresõidu astronoomia, laeva asukohamääramine GNSS-i abita nii paber- kui elektronkaardil, radarnavigatsioon jms. Vastavad pädevusnõuded on toodud STCW koodeksis ja mereõppeasutused peavad neid õpetama. Probleem tekib peale kooli lõpetamist laevale tööle minnes. Kui laeval puuduvad paberkaardid ja sõidetakse ainult ECDIS-e järgi, siis laevajuhile jääb üksnes monitoorimise ülesanne. Kuna üldiselt on GNSS ja ECDIS väga usaldusväärsed, siis laevajuht harjub sellega ja ei

oska süsteemi rikkeid oodata. Kui laeva liikumist ja positsiooni muude meetoditega ei määrata, kaob vilumus intsidendi korral piisava kiiruse ja täpsusega laeva liikumist ohutult kontrollida. Kuna praegu mereõppeasutused selliseid meetodeid õpetavad, siis palju rohkem nemad omalt poolt teha ei saa. Õppetöö käigus peab sellistele võimalustele lihtsalt tähelepanu pöörama.

Kokkuvõte

Info- ja käidutehnoloogia integreerimine ning kiire ülemaailmne internetiühendus võimaldavad reederitel laevade teekonna optimeerimise, kaugdiagnostika, kaupade seire jms abil pakkuda kiiremat ja kvaliteetsemat transporditeenust väiksemate kuludega. Teisest küljest muudab sõltuvus tehnoloogiast ja üha kasvav avatus välismaailmale laevad haavatavaks küberrünnetele. Kui arvestada, et meritsi transporditakse mahult üle 80% ja väärtuselt üle 70% maailma kaupadest, siis võib mõista erineva profiiliga küberruumis tegutsejate motivatsiooni laevade ründamiseks. Laevasüsteemide häkkimine on jõudnud laboritest päris maailma ning 2017. aasta veebruaris õnnestus piraatidel kümneks tunniks võtta kontroll laeva navigatsioonisüsteemi üle eesmärgiga juhtida laev pardaleminekuks sobivamasse kohta.

Merendussektor on probleemi mõistnud ning alates 21. sajandi teisest kümnendist on küberturbele hakatud ühe enam tähelepanu pöörama. Sellega tegelevad mitmed huvirühmad – IMO, kaubaomanikud, laevaomanikud, kindlustusseltsid, klassifika–tsiooniühingud ja meremeestele täiendõpet pakkuvad ettevõtted . Millegipärast ei ole aga küberturbe haridusele tähelepanu pööratud meremeeste esmases väljaõppe faasis ehk mereõppeasutustes. Info- ja käidutehnoloogiaga puutuvad laevadel põhiliselt kokku laevaohvitserid ja meresõiduohutuse tagamiseks on nende jaoks oluline erialaspetsiifiline teadlikkus küberohtudest. Seetõttu oli magistritöö üheks väljundiks teha mereõppeasutustele soovitused erialaspetsiifilise küberturbe hariduse korraldamiseks laevaohvitseride väljaõppes. Soovituste koostamise eelduseks oli esmalt välja selgitada kas üldse, kuidas, ja millisel tasemel mereharidusasutused küberturvet laevaohvitseride väljaõppes käsitletavad. Selle küsimuse lahendamiseks püstitas autor hüpoteesi, et mereõppeasutused ei ole tulevaste laevaohvitseride väljaõppes pööranud piisavalt tähelepanu erialaspetsiifilisele küberturbe haridusele võimaldamaks neil laevu ohutumalt käitada.

Magistritöö eesmärkide saavutamiseks viidi läbi neljast etapist koosnev uuring – valimi määratlemine ja asutuste kaardistamine, küsitlusuuring, ekspertintervjuud ja tulemuste analüüs ning soovituste koostamine. Et valimit mitte liiga suureks ajada piirduti Euroopa mereõppeasutustega, kes koolitavad piiramatu kogumahutavusega laevade vahitüürimehi

ja/või piiramatu peamasinate efektiivse koguvõimsusega mootorlaeva vahimehaanikuid. Kokku leiti 65 kooli 31-st riigist. Nende koolide veebilehekülgedelt otsiti laevajuhtide ja -mehaanikute õppekavasid ning küberturbega seonduvaid õppeaineid või nende väljundeid. Lisaks saadeti kõikide koolide esindajatele e-kiri palvega vastata *Google Forms* abil loodud küsitlusele. Küsitlus koosnes kahest osast, millest esimese osa eesmärk oli saada kvantitatiivset infot hüpoteesi kinnitamiseks või ümberlükkamiseks ja teise osa eesmärk oli saada kogemuslikku infot soovituste koostamiseks mereõppeasutustele. Kokku leiti infot 35 kooli kohta, kellest 19 osales ka küsitlusuuringus. Kaardistamise ja küsitlusuuringu kvantitatiivsed tulemused olid järgmised:

- erialaspetsiifilist küberturbe haridust laevaohvitseridele pakkus 35-st koolist ainult 2;
- küberturbe haridust ainult üldisel tasemel pakkus 35-st koolist 3;
- küberturbe haridust pidas vajalikuks 19-st koolist 11;
- küberturbe haridust millalgi tulevikus pidas vajalikuks 19-st koolist 7;
- küberturbe haridust ei pidanud üldse vajalikuks 19-st koolist 1.

Küsitluse tulemustest selgus, et kuigi mereõppeasutused teadvustavad probleemi ning mõistavad küberturbe käsitlemise vajalikkust laevaohvitseride väljaõppes, siis sellist koolitust viivad läbi väga vähesed õppeasutused ja magistritöös püstitatud hüpoteesi võib lugeda kinnitatuks.

Järgnevalt saadeti küberturbe haridust pakkuvate koolide esindajatele e-kiri sooviga viia läbi ekspertintervjuu. Intervjuude eesmärgiks oli saada kogemuslikku infot küberturbe hariduse korraldamise soovituste koostamiseks. Intervjuuga nõustusid viis esindajat kolmest koolist. Nendest koolidest kaks õpetavad üldist küberturbe teadlikkust ning üks kool on küberturbe väljaõppe korraldamisega planeerimise faasis. Kahjuks ei õnnestunud intervjuud saada nende kahe kooliga, kes juba pakuvad laevaohvitseridele erialaspetsiifilist küberturbe haridust.

Küsitlustest ja ekspertintervjuudest saadud kvalitatiivse info põhjal võib järeldada, et kuigi koolide esindajate vahel oli ka eriarvamusi, siis üldiselt nõustuti laevaohvitseridele küberturbe õpetamise vajalikkusega. Peamised takistused erialaspetsiifilise küberturbe

hariduse käsitlemiseks olid õppejõudude suur töömaht, emakeelse materjali puudulikkus ja õppekavade täidetus, aga ka konkreetsete nõuete puudumine STCW koodeksis.

Uuringu tulemustest lähtuvalt leidis magistritöö autor, et parim viis laevaohvitseride väljaõppes küberturvet käsitleda on luua kahepäevane koolitus. Esimesel päeval käsitletakse merendusega seotud küberturbe teoreetilisi lähtepunkte ning teisel päeval toimub etteantud stsenaariumite põhjal iseseisev riskide hindamine. Koolituse materjali koostamisel on soovitav võtta aluseks antud magistritöö teoreetiline osa. Seega peaks koolituse teoreetiline osa koosnema järgnevast:

- Asjakohased regulatsioonid ja suunised.
- Kes ja miks laeva ründab?
- Mida ja kuidas laeval rünnatakse?
- Kuidas laeva kaitsta?

Koolituse praktilise osana mõeldud riskide hindamise koostamise aluseks on Plymouthi ülikooli teadlaste Kimberly Tam'i ja Kevin Jones'i loodud mudelipõhine raamistik merendusega seotud küberriskide hindamiseks. Lisaks põhikoolitusele on magistritöö autor toonud soovitused küberturbe teadlikkuse toetamiseks. Need soovitused on järgnevad:

- simulaatoritreening,
- arvutialased teadmised,
- traditsioonilised meresõiduoskused.

Kokkuvõtteks võib öelda, et kuigi STCW koodeksiga ei ole küberturbe teadlikkus laevaohvitseridelt nõutud, siis meresõiduohutuse tagamiseks on see siiski vajalik. See, et küberturve laevaohvitseride väljaõppes ei ole kohustuslik, annab õppeasutustele võimaluse rahulikult asjaga tegelema hakata ja valmistuda ajaks, mil küberturbe pädevusnõuded STCW koodeksiga kohustuslikuks tehakse. Selge on see, et küberturbe olulisus ajas ainult kasvab. Antud magistritööga on autor pakkunud mereõppeasutustele, aga ka täiendkursusi pakkuvatele ettevõetele ja muudele huvirühmadele, ühe võimaluse erialaspetsiifilise küberturbe hariduse pakkumiseks laevaohvitseridele.

Summary

Information about the dissertation:

- Title: Recommendations for embedding cybersecurity education into ship's officers training;
- Author: Lauri Roolaid;
- Original language: Estonian;
- Volume of thesis' body (theory, methodology and analysis): 51 pages;
- Number of figures: 4;
- Number of tables: 5;
- Number of appendices: 5;
- Number of references: 66;
- Keywords: Cybersecurity, information technology, operational technology, ship's vulnerabilities, ship's officers training, maritime educational institutions, navigational safety, operational safety.

Integration of information- and operational technology and worldwide availability of high speed internet connection enable shipping companies to provide high quality transport service with lower costs through route optimization, remote diagnostics of equipment and real-time cargo monitoring. On the other hand the dependence on technology and ever-increasing connectedness make ships vulnerable to cyber attacks. If we take into account the fact that over 80% of global trade by volume and more than 70% of its value is being carried on board ships, we can understand the motivation behind various actors in cyberspace for attacking ships. Hacking ship's systems is getting out of laboratories into the real world and in february 2017 pirates took control of a vessel's navigation system with the intention to steer it to an area where they could board and take over.

Maritime industry has acknowledged the problem and from the second decade of 21st century onwards increasing attention is being paid to cybersecurity concerns in the sector. This is done by many stakeholders – IMO, cargo owners, ship owners and operators, insurance companies, classification societies and seafarer training providers. That said, somehow there has not been much talk about cybersecurity training in maritime

educational institutions. This is most relevant to ship's officers, who are responsible for operating information- and operation technology on ships. In order to ensure safety of operation and navigation, the officers need to be aware of specific cyber risks related to ships. Therefore one of the objectives of the thesis was to give recommendations to maritime educational institutions for embedding cybersecurity education into ship's officers training. To achieve this objective, the author needed to first find out, if at all, and how specific cybersecurity education is provided to ship's officers in maritime educational institutions. For this, author hypothesized that maritime educational institutions have not given enough attention to specific cybersecurity education in future ship's officers training to ensure their ability to operate ships safely.

To achieve the objectives of the thesis, the author carried out a study in four stages – sampling and mapping the institutions; survey questionnaire; expert interviews; analysis and recommendations. The study sample consisted of European maritime educational institutions, who provide study programmes for unlimited officers of the watch and/or unlimited engineer officers of the watch. Author found 65 institutions from 31 countries. First part of the study was to find out information publicly available on the webpages of these institutions. Author searched for the study programmes, different courses and their learning outcomes related to cybersecurity. Second stage of the study was to send an e-mail to all of the schools with request to complete Google Forms questionnaire. The answer to the questionnaire was received from 19 institutions. Altogether information was found about 35 schools out of 65. The quantitative results of the mapping and questionnare are as follows:

- 2 institutions out of 35 provided specific cybersecurity education for ship's officers;
- 3 institutions out of 35 provided only general cybersecurity awareness education for ship's officers;
- 11 institutions out of 19 thought that it was necessary to teach cybersecurity to ship's officers;
- 7 institutions out of 19 thought that cybersecurity education will be necessary in the future;

– 1 institution out of 19 thought that cybersecurity education is not necessary for ship's officers.

It it clear that although maritime educational institutions acknowledge the problem, only few of the institutions provide cybersecurity training and because of that the hypothesis was confirmed.

For the third stage of the study an e-mail was sent to the institutions who already provide cybersecurity education for ship's officers with request to conduct an interview. Purpose of the interviews was to gather experiential information to provide recommendatons for embedding cybersecurity education into ship's officers training. Request for an interview was accepted by five representatives form three institutions. Two of these institutions provide general cybersecurity awareness training and one institution is in the planning stage. Sadly the author was not able to arrange an interview with those two institutions who already provide specific cybersecurity training for ship's officers.

Although there were disagreements between representatives of the institutions, in general they agreed that it is necessary to provide cybersecurity education for ship's officers. The main obstacles in the way are already excessive workload of the teachers, lack of study material in native language, already filled curricula and no specific requirements in the STCW code.

Based on the information provided by the study, the author recommends a two-day cybersecurity course for ship's officers. On the first day students will receive theoretical knowledge about cybersecurity in shipping and on the second day the students will carry out risk-assessments based on given scenarious. The recommended course material will be based on the theoretical part of this disseratation. The topics to be taught on the first day will be following:

– Relevant regulations and guidelines.
– Who and why would attack a ship?
– What and how can be attacked on a ship?
– How to protect ship from cyber incidents?

Practical part of the course will be based on a model-based framework for maritime cyber-risk assessment created by Kimberly Tam and Kevin Jones from the University of Plymouth. In addition to the cybersecurity course, the author provides suggestions for the support of cybersecurity awareness. These suggestions are as follows:

- simulator training,
- computer knowledge,
- traditional navigation methods.

Even though cybersecurity is not compulsory according to STCW code, it is still necessary knowledge for deck- and engine officers to ensure ship's safety. Maritime educational institutions need to gradually start providing cybersecurity education before it is made compulsory. With this thesis, author has provided one way for maritime educational institutions, but also for seafarer training companies and other stakeholders, to provide specific cybersecurity education for ship's officers.

Viidatud allikad

2017 Cybercrime Report. (2017). / ed. S.Morgan. https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf (18.01.2018)

Adamson, D.K. (2016). Knowledge is Power. – *The Navigator*, Issue no.12, 4-5.

Becker-Heins, R. (2014). ECDIS Basics: A Guide to the Operational Use of Electronic Chart Display and Information Systems. Lemmer : Geomares Publishing.

BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF, IUMI. (2017). The Guidelines on Cyber Security Onboard Ships, Version 2.0. http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16 (11.12.2017)

Blake, T. (2017). Shipping must confront onboard systems' cyber vulnerabilities. https://fairplay.ihs.com/safety-regulation/article/4294531/shipping-must-confront-onboard-systems%E2%80%99-cyber-vulnerabilities (12.02.2018)

Boyes, H., Isbell, R. (2017). Code of Practice: Cybe Security for Ships. London : Institution of Engineering and Technology.

CCTV+. (2017). World's first certified smart ship delivered in Shanghai. http://www.cctvplus.com/news/20171205/8067914.shtml#!language=1 (19.02.2018)

Centre for Cyber Security. (2017). Threat Assessment: The cyber threat against the maritime sector. https://fe-ddis.dk/cfcs/CFCSDocuments/The_Cyber_Threat_to_the_Maritime_Sector_march.pdf (12.02.2018)

Cimpanu, C. (2017). To Nobody's Surprise, Ships Are Just as Easy to Hack as Anything Else. – *BleepingComputer*. https://www.bleepingcomputer.com/news/security/to-nobodys-surprise-ships-are-just-as-easy-to-hack-as-anything-else/ (01.03.2018)

Coffer, J.D., Rolli, J. GPS and Shipping: Countering the Threat of Interference. – *Issues in Maritime Cyber Security*, 2017. Washingdon DC : Westphalia Press, 397-405.

CyberKeel (2014). Maritime Cyber-Risks. https://docs.wixstatic.com/ugd/2d153e_46bd931729324d4b81723567d9e7d288.pdf (12.01.2018)

Drias, Z., Serhtouchni, A., Vogel, O. (2015). Analysis of Cyber Security for Industrial Control Systems. – *2015 International Conference on Cyber Security of Smart cities, Industrial Control System and Communications (SSIC) : 5-7 Aug. 2015, Shanghai, China, 1-8*. DOI: 10.1109/SSIC.2015.7245330

Dyryavyy, Y. (2014). Preparing for Cyber Battleships – Electronic Chart Display and Information System Security. https://www.nccgroup.trust/globalassets/our-research/uk/whitepapers/2014-03-03_-_ncc_group_-_whitepaper_-_cyber_battle_ship_v1-0.pdf (05.04.2018)

EUROPOL. (2014). The Internet Organised Crime Threat Assessment (iOCTA) 2014. DOI: 10.2813/16.

Evans, P.C., Annunziata, M. (2012). Industrial Internet: Pushing the Boundaries of Minds and Machines. https://www.ge.com/docs/chapters/Industrial_Internet.pdf (16.04.2018)

Fruhlinger, J. (2017). What is Stuxnet, who created it and how does it work? https://www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html (23.04.2018)

Furuno Voyager, the next-generation bridge system. http://www.furuno.com/en/merchant/voyager/#brochure (21.04.2018)

Goward, D. (2017). Mass GPS Spoofing Attack in Black Sea? https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#gs.4LzEocs (20.04.2018)

Goward, D.A. (2017). Hackers took ‘full control’ of container ship’s navigation systems for 10 hours - IHS Fairplay. https://www.linkedin.com/pulse/hackers-took-full-control-container-ships-navigation-systems-goward (29.04.2018)

Grant, A., Williams, P., Shaw, G., Voy, D.M., Ward, N. (2011). Understanding GNSS availability and how it impacts maritime safety. – *Proceedings of the 2011 International Technical Meeting of The Institute of Navigation, San Diego, CA, January 2011, pp. 687-695.* https://rntfnd.org/wp-content/uploads/GNSS-Maritime-GLA.pdf (18.04.2018)

Guidelines on Maritime Cyber Risk Management. (2017). – M*SC-FAL.1/Circ.3.* http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-

%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20%28Secretariat%29.pdf (10.01.2018)

Harp, D.R., Gregory-Brown, B. IT/OT Convergence: Bridging the Divide. https://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf (18.03.2018)

Hart, D. (2004). An approach to vulnerability assessment for Navy Supervisory Control and Data Acquisition (SCADA) system : master's thesis. Naval Postgraduate School : Monterey, CA.

Heering, D. (2017). Küberturvalisuse tagamine laevanduses Eesti laevaomanike näitel ning ettepanekud riskide maandamiseks : magistritöö. TTÜ Eesti Mereakadeemia : Tallinn.

Hellenic Shipping News. (2017). New cybersecurity rules explained. https://www.hellenicshippingnews.com/new-cybersecurity-rules-explained/ (01.05.2018)

Hughes, M. (2017). Welp, even ships are hackable now. https://thenextweb.com/insider/2017/07/18/welp-even-ships-are-hackable-now/ (29.04.2018)

Inductive Automation. (2016). IIoT: Combining the Best of OT and IT – Why Industrial Organizations Need to Bridge the Gap. http://pages.inductiveautomation.com/WhitePaperIIoTCombiningBestofOTIT_Page.html (24.03.2018)

International Chamber of Shipping. (2011). "Manila Amendments" to the STCW Convention - A Quick Guide for Seafarers. http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/manila-amendments-to-the-stcw-convention.pdf?sfvrsn=6 (28.04.2018)

IMO Model Courses. http://www.imo.org/en/OurWork/HumanElement/TrainingCertification/Documents/list%20of%20IMO%20Model%20Courses.pdf (26.04.2018)

Jain, N., Shrivastva, V. (2014). Cyber crime changing everything - an empirical study. – *International Journal of Computer Application*, 1(4), 76-87. http://rspublication.com/ijca/2014/FEB14/8.pdf (14.01.2018)

Jones, K.D., Tam, K., Papadaki, M. (2016). Threats and Impacts in Maritime Cyber Security. – IET Digital Library: Engineering & Technology Reference. DOI:10.1049/etr.2015.0123

Jones, M. (2017). Spoofing in the Black Sea: What really happened? http://gpsworld.com/spoofing-in-the-black-sea-what-really-happened/ (23.04.2018)

JWC International. Maritime Cyber Security Awareness Programme. https://www.maritimecybertraining.online/ (13.02.2018)

Kenney, M. (2015). Cyberterrorism in a Post-Stuxnet World. – Cyberspace: Malevolent Actors, Criminal Opportunities, and Strategic Competition. Carlisle : The United States Army War College Press, 131-171.

Kongsberg Maritime (2015). K-Chief 700 Retrofit. https://www.km.kongsberg.com/ks/web/nokbg0397.nsf/AllWeb/F25FC8991E666A7DC12580CE00489DAD/$file/KM_K-Chief-700_Retrofit.pdf?OpenElement (22.04.2018)

Lunenburg, F.C., Irby, B.J. (2008). Writing a Successful Thesis or Dissertation. Thousand Oaks : Corwin Press, Inc.

MAIB. (2016). Report on the investigation of the grounding of Muros. https://www.iims.org.uk/wp-content/uploads/2017/10/MAIBInvReport22_2017.pdf (22.03.2018)

Mapchart.net. https://mapchart.net/ (21.04.2018)

Maritime Cyber Risk Management in Safety Management Systems. (2017). – Resolution MSC.428(98). http://www.imo.org/en/OurWork/Security/WestAfrica/Documents/Resolution%20MSC.428%2898%29%20-%20Maritime%20Cyber%20Risk%20Management%20in%20Safety%20Management%20Systems.pdf (10.01.2018)

Marsh & McLennan Companies. (2017). MMC Cyber Handbook 2018: Perspectives on the next wave of cyber. https://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/mmc-cyber-handbook-2018.pdf (22.03.2018)

Meremeeste väljaõppe, diplomeerimise ja vahiteenistuse koodeksi Manila konverentsi muudatused. – *Riigi teataja* II, 23.08.2013, 1. https://www.riigiteataja.ee/akt/223082013001 (01.05.2018)

Mihanović, L., Ristov, P., Belamarić, G. (2016). Use of new information technologies in the maintenance of ship. – *Scientific Journal of Maritime Research*, 30, 38-44. https://hrcak.srce.hr/file/236735 (13.04.2018)

Mimoso, M. (2017). Maersk Shipping Reports $300M Loss Stemming from NotPetya Attack. https://threatpost.com/maersk-shipping-reports-300m-loss-stemming-from-notpetya-attack/127477/ (25.02.2018)

Moskoff, D.B., Kaag, W.G. (2015). Threats to Global Navigation. – *Issues in Maritime Cyber Security*, 2017. Washingdon DC : Westphalia Press, 3-16.

Munro, K. (2017). OSINT from ship satcoms. https://www.pentestpartners.com/security-blog/osint-from-ship-satcoms/ (20.04.2018)

Mägi, K. (2017). Küberturvalisuse baaskoolituse videosalvestus. https://www.ttu.ee/ttu-uudised/uudised/siseveeb/vaata-kuberturvalisuse-baaskoolituse-videosalvestust/ (25.04.2018)

Nelson, E. S. (2012). Maritime Terrorism and Piracy: Existing and Potential Threats. – *Global Security Studies*. 3(1), 15-28. https://pdfs.semanticscholar.org/8686/5608ae0a3eb237f114351c5dd782d9b9573f.pdf (01.03.2018)

NSSLGlobal. (2017). NSSLGlobal survey demonstrates worrying lack of maritime cybersecurity training amongst crews. http://www.nsslglobal.com/index.php?idPage=2&n=58 (05.02.2018)

OCIMF. About TMSA. https://www.ocimf.org/sire/about-tmsa/ (03.03.2018)

Passeri, P. (2018). 2017 Cyber Attacks Statistics. https://www.hackmageddon.com/2018/01/17/2017-cyber-attacks-statistics/ (28.04.2018)

Pipkin, D.L. (2002). Halting the Hacker: A Practical Guide to Computer Security. 2nd ed. New Jersey : Prentice Hall.

Ponemon Institute LLC. (2017). 2017 Cost of cyber crime study: Insights on the Security Investments that make a Difference. https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50 (18.01.2017)

Russell, K. (2018). Carnival and SES Set New Bandwidth Capacity Record at Sea. https://www.satellitetoday.com/mobility/2018/02/26/watch-ses-ceo-setting-new-bandwidth-capacity-record/ (16.05.2018)

Safety4Sea. (2018). Maritime cyber reporting sees progress. https://safety4sea.com/maritime-cyber-reporting-sees-progress/ (15.05.2018)

SKEMA. (2009). Navigation systems including developments in e-Navigation. http://www.eskema.eu/DownloadFile.aspx?tableName=tblSubjectInfo&field=Skema%20Study%20Filename1&idField=subjectInfoID&id=60 (12.04.2018)

Smith, M. (2013). Not cyber myths: Hacking oil rigs, water plants, industrial infrastructure. https://www.csoonline.com/article/2225104/microsoftsubnet/not-cyber-myths--hacking-oil-rigs--water-plants--industrial-infrastructure.html (29.04.2018)

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82, 2. – *National Institute of Standards and Technology.* http://dx.doi.org/10.6028/NIST.SP.800-82r2 (20.03.2018)

Sulpice, G. (2011). Study on Seafarers Employment: Final Report. https://ec.europa.eu/transport/sites/transport/files/modes/maritime/studies/doc/2011-05-20-seafarers-employment.pdf (21.04.2018)

Swanbeck, S. (2015). Coast Guard Commandant Addresses Cybersecurity Vulnerabilities on Offshore Oil Rigs. https://www.csis.org/blogs/strategic-technologies-blog/coast-guard-commandant-addresses-cybersecurity-vulnerabilities (29.04.2018)

Tam, K., Jones, K. (2018). MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment. – *CSCAN with University of Plymouth.* https://www.cscan.org/download/?id=1093 (20.04.2018)

Textor, J. (2017). New OCIMF pre-fixture tanker vetting cyber requirement. http://www.gard.no/web/updates/content/24478791/new-ocimf-pre-fixture-tanker-vetting-cyber-requirement (03.03.2018)

Tracy, P. (2016). Industrial internet of things maritime use cases. https://www.rcrwireless.com/20160727/internet-of-things/maritime-industrial-internet-things-tag31-tag99 (01.05.2018)

Toova, T. (2015). MS Windows'i operatsioonisüsteemid – IFI6045 : Loengukonspekt. Tallinn : Tallinna Ülikool.

UK Chamber of Shipping. (2014). A Master's Guide to Cyber Security. Edinburgh: Witherby Seamanship.

UNCTAD. (2017). Review of Maritime Transport 2017. http://unctad.org/en/PublicationsLibrary/rmt2017_en.pdf (24.04.2018)

Watchwood. (2017). Shipping must confront onboard systems' cyber vulnerabilities. http://www.watchwood.com/news/shipping-must-confront-onboard-systems-cyber-vulnerabilities/ (03.04.2018)

Wärtsilä. (2015). Wärtsilä Engine efficiency monitoring service. https://cdn.wartsila.com/docs/default-source/Service-catalogue-files/Genius-Services/w%C3%A4rtsil%C3%A4-engine-efficiency-monitoring.pdf?sfvrsn=0 (11.04.2018)

Lisad

Lisa 1. Kasutatud mõistete loetelu

Eesti keeles	Inglise keeles	Selgitus
Eksploidipakk	Exploit kit	Brauserite ja nende kaudu käivitatavate programmide ründe instrumendikomplekt, mis automatiseerib klientpoole nõrkuste ärakasutamist.
Hajus ummistusrünne	Distributed denial-of-service attack	Ummistusrünne, milles kasutatakse sihtsüsteemi või -võrgu liikluse mahu tunduvaks suurendamiseks suurt arvu ründavaid süsteeme, eriti zombivõrke.
Halvang	Disruption	Süsteemi või olulise rakenduse käideldavuse ettekavatsematu kadu lubamatult pikaks ajaks mingi ootamatu sündmuse tõttu
Harpuunimine	Spearphishing	Kalastamise eriliik, mis on sihikindlalt suunatud ühele organisatsioonile ning püüab ärilistel, sõjalistel või poliitilistel eesmärkidel saada juurdepääsu konfidentsiaalsetele andmetele, kusjuures kalastussõnumi saatja näib kuuluvat samasse organisatsiooni (enamasti mingil tähtsal ametikohal).
Hilistus	Delay	Sündmuse iseeneslik soovimatu hilinemine.
Juurkratt	Rootkit	Juurkasutaja õigustega kahjurvara, mis käivitub süsteemi igal buutimisel enne operatsioonisüsteemi täielikku laadimist ja on seetõttu raskesti avastatav.
Juurutama	Deploy	Haarab kõiki uue tarkvara või riistvara töölepanekuga seotud protsesse - installeerimist, konfigureerimist, käitamist, testimist ja vajalike muudatuste tegemist.

Lisa 1 järg

Kahjurvara	Malware	Sihilikult infosüsteemi talitluse või kasutaja otseseks või kaudseks kahjustamiseks või häirimiseks, tundliku teabe kogumiseks, lubamatu juurdepääsu saamiseks või konfidentsiaalsuse, tervikluse või käideldavuse ründamiseks määratud programm, koodilõik, skript, makro vms vahend.
Kalastus	Phishing	Petturlik protsess, millega elektroonilises suhtluses usaldatavat olemit teeseldes püütakse saada privaatset või konfidentsiaalset teavet, kasutades selleks suhtlusosavust või tehnilist pettust.
Kaugpääs	Remote access	Pääs infosüsteemi välisvõrgu kaudu.
Kinnisründeoht	Advanced persistent threat	Võimaliku peamiselt mingi välisriigi poliitilistest, majanduslikest või sõjalistest huvidest lähtuva, ettemääratud eesmärgi saavutamisele suunatud sihikindla kohanduva ulatuslike ressursside ja erioskustega kestusründe oht.
Kohtvõrk	Local area network	Kasutaja territooriumil piiratud geograafilisel alal (enamasti ühes hoones) paiknev arvutivõrk.
Konfidentsiaalsus	Confidentiality	Andmete omadus, mis näitab, millises ulatuses need andmed ei ole volitamatutele isikutele, protsessidele või muudele olemitele kättesaadavad ega avalikustatud.
Koorimine	Data scraping	Andmete ekstraheerimine teise programmi inimloetavast väljastisest, eeskätt veebilehelt - käsitsi kopeerimise teel või eritarkvaraga.
Käideldavus	Availability	Iseloomustab teabe, IT-süsteemide, inimeste ja protsesside teovõimet ja kättesaadavust sel ajal, mil organisatsioon neid vajab.
Küberfüüsiline süsteem	Cyber-physical system	Arvutipõhiste algoritmidega juhitav või jälgitav ning Interneti ja selle kasutajatega tugevalt integreeritud tehniline süsteem.

Lisa 1 järg

Käidutehnoloogia	Operational technology	Riistvara, tarkvara, personal ja ta tegevus, mis füüsiliste seadmete, protsesside ja sündmuste otsese seire ja/või juhtimise teel avastab või põhjustab muudatuse tööstusprotsessis.
Küberohutus	Cybersafety	Inimeste või varade kaitstust mingi tervisekahjustust või majanduslikku kahju põhjustava sündmuse või ohule avatuse eest küberruumis.
Küberruum	Cyberspace	Inimeste, tarkvara ja teenuste interaktsioo–niga Internetis temaga ühendatud tehniliste vahendite ja võrkude abil tekitatav liitkesk–kond, mis ei eksisteeri mingil füüsilisel kujul.
Küberrünne	Cyber attack	Küberruumi kaudu sooritatav rünne, mis on suunatud küberruumi kasutamisele organisatsioonis ning püüab häirida, pärssida, hävitada või kahjustavalt valitseda andmetöötluse keskkonda või taristut, rikkuda andmete terviklust või varastada reguleeritud teavet.
Küberturve	Cybersecurity	Teabe konfidentsiaalsuse, tervikluse ja käideldavuse säili(ta)mine küberruumis.
Lunavara	Ransomware	Kahjurvara (enamasti troojan), mis rikub nakatatud süsteemi käideldavust (näiteks mingite failide krüpteerimise teel).
Majakpete	Meaconing	Navigatsioonisignaalide püük ja muudetult retransleerimine samal sagedusel vastase navigatsiooni eksitamiseks.
Manipuleerimisvõtted	Social engineering	Mittetehniline ründevahend, hõlmab veenvat teesklust, valesid, altkäemaksu, ähvardusi jms, peamiselt konfidentsiaalse või tundliku teabe saamiseks.
Masina kasutajaliides	Human-machine interface	Klaviatuurid, näidikud, sõrmistikud, puuteekraanid jms seadmed, mis võimaldavad inimese interaktsiooni süsteemiga.

Lisa 1 järg

Masinõpe	Machine learning	Protsess, millega funktsionaalüksus täiustab oma talitlust uue teadmuse või uute oskuste omandamise või seniste ümberkorraldamise teel.
Omandtarkvara	Proprietary software	tarkvara, mida ta õiguste omanik litsentsib kasutamiseks: - (tavaliselt lähtekoodita), - teatud tingimustes, - teatud kitsendustega.
Ohtlik süsteem	Safety-critical system	Süsteem, mille rikke või häire korral võib tekkida otsene oht isikutele, keskkonnale ja/või materiaaltehnilistele vahenditele [AAP-6 tõlge].
Paik	Patch	Tarkvaratoote suhteliselt väikeseks muutmiseks, näiteks programmivea või nõrkuse kõrvaldamiseks määratud koodi- ja/või andmekogum,
Programmeeritav kontroller	Programmable logic controller	Tööstusautomaatikas jm mitmesuguste tehniliste protsesside juhtimiseks määratud eriotstarbeline mikroarvuti, programmee–ritava mikroprotsessoriga juhtseade.
Puhvri ületäitumine	Buffer overflow	Andmete salvestuse siirdumine väljapoole nende ajutiseks talletuseks määratud puhvrit, seda vältiva mehhanismi puudumise, vigasuse või ründega rikkumise tõttu
Pühkur	Wiper	Ründeobjekti kettasisu kustutav kahjurvara.
Pääsumandaat	Access credentials	Olemi (näiteks kasutaja või süsteemi) väidetava identiteedi tõendamiseks (autentimiseks) edastatavad andmed (näiteks parool).
Pääsuõigus	Access right	Kasutajaile, programmidele või tööjaamadele antavad õigus või eesõigus andmete ja failide loomiseks, muutmiseks, kustutuseks või vaatamiseks süsteemis, määratletult andmete omanike ja infoturvapoliitika kehtestatud reeglitega.

Lisa 1 järg

Rikketaluvus	Fault tolerance	Määr, mille ulatuses süsteem, toode või komponent töötab kavatsetud viisil, hoolimata ta riistvarariketest või tarkvara–defektidest.
Rikkumine	Defacement	Võõra veebilehe sisu pahatahtlik muutmine vandalismina või mingil (näiteks poliitilisel) eesmärgil.
Segamine	Jamming	Saate vastuvõttu ja/või elektrooniliste seadmete või süsteemide tööd häirida püüdev rünne elektromagnetenergia kiirgamise, tagasikiirgamise või peegeldamisega teatud kanalil või sagedusel.
Sild	Bridge	Kaht sama või sarnase võrguarhitektuuriga arvutivõrku ühendav funktsionaalüksus.
Skriptinaga	Script kiddy	Võhiklik arvutikasutaja, kes sooritab ründeid teiste väljatöötatud ja kergesti leitava kahjurvaraga, sageli alaealine.
Superviisorsüsteem	SCADA	(= supervisory control and data acquisition, "superviisorjuhtimine ja andmehõive") Liik tehnojuhtimissüsteeme, automatiseerib tehniliste protsesside järelevalvet ja nende hierarhilise juhtimise ülataset, teenindades andmeside ja kaugjuhtimise abil operaatori–keskusi.
Teenusetõkestus; ummistus	Denial of service	Volitatud juurdepääsu tõkestamine süsteemiressursile või süsteemi töö viivitamine, mille tulemusena kaob volitatud kasutajail süsteemi käideldavus.
Tehnojuhtimissüsteem	Industrial control system	Tööstuslike tootmisprotsesside, tehnoteenuseprotsesside jt tehniliste protsesside juhtimiseks määratud arvutipõhine automatiseeritud süsteem.
Terviklus	Integrity	Õigsus ja täielikkus, st infovara lubamatute muudatuste puudumine.
Troojan	Trojan	Andmete volitamatut kogumist, võltsimist või hävitamist võimaldavat ründeloogikat sisaldav näiliselt kahjutu programm.

Lisa 1 järg

Uss	Worm	Liik kahjurvara: programmikood, mis paljundab end massiliselt (näiteks nakatatud arvuti aadressiraamatu abil) võrgu kaudu ja sageli sooritab kahjulikke toiminguid, näiteks saadab rämpsposti või korraldab ummistusründeid.
Vaalapüük	Whaling	"Suure kala" (tippjuhi, poliitiku, lavatähe) püügile suunatud kalastus kaalukate andmete saamiseks; pettetekst koostatakse ohvri rolli arvestavas stiilis, näiteks kliendi kaebusena, kohtukutsena, sisemise märgukirjana
Vahendusrünne	Man-in-the-middle attack	Rünne, mille sooritaja on võimeline salaja lugema, lisama ja muutma sõnumeid kahe poole vahel.
Vahetatavus	Interchangeability	Komponendid A, B, C,... on omavahel vahetatavad, kui süsteemis saab ta üldisi omadusi ja käitumist muutmata kasutada ükskõik millist neist.
VSAT-side	VSAT	Satelliitside tehnoloogia ja maajaam paraboolantenni läbimõõduga 50-100 lainepikkust: Ka-sagedusalal alla 2m, Ku-alal alla 4m ja C-alal alla 8m.
Võltsimine	Spoofing	Magistritöö kontekstis GNSS signaali võltsimine
Õhkeraldus	Air gap	Arvutivõrgu turbe meetod: elutähtsa võrgu füüsiline, elektriline ja elektromagnetiline eraldamine teistest võrkudest.
Ühilduvus	Compatibility	Kahe või mitme süsteemi või komponendi võime vahetada informatsiooni.
Zombi	Bot	Võrgustatud arvuti häkkerite kaugjuhtimise all, sageli troojani abil õõnestatud

Lisa 2. Küberturbe teadlikkuse kursuse tunnistus

JWC
INTERNATIONAL

THIS IS TO CERTIFY THAT

Lauri Roolaid

HAS SUCCESSFULLY COMPLETED THE
MARITIME CYBER SECURITY AWARENESS (MCSA)
PROGRAMME AT AWARENESS LEVEL

Certificate Number JWC/MCSA 1072
February 13th 2018 17:22
Score 100 %

First Name	Lauri
Last Name	Roolaid
Date Of Birth	June 22nd 1986
Home Address	[redacted]
Postal Or Zip Code	
City	Tallinn
Country	Estonia
E-mail Address	lauriroolaid@gmail.com
Contact Number	+37256648814

Valid for three years from February 13th 2018
Queries regarding the authenticity of this certificate should be addressed to:

Training & Certification Department
JWC International, Castledown Business Park, Wiltshire, United Kingdom, SP11 9FA
Authorised training centre representative: Jordan Wylie
info@jwcinternational.com
+44 (0) 1264 847 817

CCHQ Certified Training
mca
APMG International
Accrediting Professionals

MCSA certificate 'Lauri Roolaid' | February 14th 2018

JWC

Lisa 3. Õppeasutuste nimekiri ja põhiandmed

Tabeli selgitused:

- (O)OW – vahitüürimees
- (E)OOW – vahimehaanik
- (ET)O – elektrimehaanik
- (R)Eng. – külmutusseadmete mehaanik
- KT – küberturvalisus
- Info puudub – õppekavas puudusid väljundid
- Väljund puudub - väljundite all polnud küberturvalisust mainitud
- Üldine – küberturbe üldine käsitlus
- Spetsiifiline – küberturbe erialaspetsiifiline käsitlus

Lisa 3 järg

Nr.	Riik	Kooli nimi	Õppekavad	Arvutiõpetus	KT koduleheküljel
1	Belgia	Antwerp Maritime Academy	O/E	Jah	Väljund puudub
	Kooli kodulehekülg: https://www.hzs.be/nl/ Õppekavad OOW: https://www.hzs.be/images/documenten/BACH_NauticalSciences_1718.pdf EOOW: https://www.hzs.be/images/documenten/BACH_ME_1718.pdf				
2	Bulgaaria	Nikola Vaptsarov Naval Academy	O/E/ET	Jah	Info puudub
	Kooli kodulehekülg: http://www.naval-acad.bg/en/				
3	Bulgaaria	Technical University Varna	O/E/ET	Jah	Info puudub
	Kooli kodulehekülg: http://fs.tu-varna.bg/ Õppekavad OOW: http://www.tu-varna.bg/tu-varnaumo/images/stories/uchebni_planove/bak_mag_sled_sredno/kv_br.pdf EOOW: http://www.tu-varna.bg/tu-varnaumo/images/stories/uchebni_planove/bak_mag_sled_sredno/kmm_br.pdf				
4	Eesti	TTÜ Eesti Mereakadeemia	O/E/ET/R	Jah	Üldine
	Kooli kodulehekülg: https://www.ttu.ee/asutused/mereakadeemia/ Õppekavad OOW: https://www.ttu.ee/asutused/mereakadeemia/sisseastujale-40/erialad-20/laevajuhtimine-2/ EOOW, ETO ja REng.: https://www.ttu.ee/asutused/mereakadeemia/sisseastujale-40/erialad-20/laevamehaanika-2/				
5	Gruusia	Batumi State Maritime Academy	O/E/ET	Jah	Info puudub
	Kooli kodulehekülg: http://www.bsma.edu.ge/index.html?lang=en Õppekavad OOW: http://www.bsma.edu.ge/text_files/en_file_90_1.pdf EOOW: http://www.bsma.edu.ge/text_files/en_file_91_1.pdf ETO: http://www.bsma.edu.ge/text_files/en_file_92_1.pdf				
6	Hispaania	University of Cadiz	O/E	Jah	Väljund puudub
	Kooli kodulehekülg: http://www.uca.es/?lang=en Õppekavad OOW: http://asignaturas2.uca.es/wuca_fichasig_asignaturas_xtitulacion?titul=41414 EOOW: http://asignaturas2.uca.es/wuca_fichasig_asignaturas_xtitulacion?titul=41413				

Lisa 3 järg

7	Hispaania	University of Oviedo: Escuela Superior de la Marina Civil de Gijon	O/E	Jah	Väljund puudub
	Kooli kodulehekülg: http://marina.uniovi.es/ Õppekavad OOW ja EOOW: http://marina.uniovi.es/infoacademica/calendarios				
8	Hispaania	University of Coruna: School of Nautical Science and Marine Engineering	O/E	Jah	Info puudub
	Kooli kodulehekülg: http://www.nauticaymaquinas.es/web2009/index.asp Õppekavad OOW: http://www.nauticaymaquinas.es/galeria/docs/TRIPTICO_GNTM_%202pag_v05_SIN_ING_.pdf EOOW: http://www.nauticaymaquinas.es/galeria/docs/TRIPTICO%20GRADO%20TEC%20MARINA%202%20PAG_v04.pdf				
9	Hispaania	University of La Laguna	O/E	Jah	Väljund puudub
	Kooli kodulehekülg: https://www.ull.es/ Õppekavad OOW ja EOOW: https://e-guia.ull.es/nautica/				
10	Hispaania	University of Basque Country	O/E	Jah	Väljund puudub
	Kooli kodulehekülg: https://www.ehu.eus/es/grado-nautica-y-transporte-maritimo Õppekavad OOW: https://www.ehu.eus/es/grado-nautica-y-transporte-maritimo/creditos-y-asignaturas-por-curso EOOW: https://www.ehu.eus/es/grado-marina/creditos-y-asignaturas-por-curso				
11	Hispaania	Polytechnic University of Catalonia	O/E	Jah	Väljund puudub
	Kooli kodulehekülg: https://www.fnb.upc.edu/ Õppekavad OOW: https://www.fnb.upc.edu/es/node/1131 EOOW: https://www.fnb.upc.edu/es/node/1132				
12	Holland	Rotterdam University of Applied Sciences	O/E	Jah	Info puudub
	Kooli kodulehekülg: https://www.hogeschoolrotterdam.nl/ Õppekavad OOW: https://search.nvao.net/files/4de396f4f095a_rapport%20HRO%20hbo-ba%20Maritiem%20Officier.pdf EOOW: https://search.nvao.net/files/51a8877f8b033_advies%20STC%20hbo-ba%20Scheepsbouwkunde-Maritieme%20Techniek.pdf				

Lisa 3 järg

13	Holland	NHL Stenden University	O/E	Info puudub	Info puudub
	Kooli kodulehekülg: https://www.nhlstenden.com/en Õppekavad OOW/EOOW: https://www.nhlstenden.com/hbo-opleidingen/maritiem-officier#algemeen				
14	Holland	Maritieme Academie Holland	O/E	Info Puudub	Info puudub
	Kooli kodulehekülg: http://www.maritiemeacademieholland.nl/ Õppekavad OOW/EOOW: http://www.hva.nl/opleiding/maritiem-officier/maritiem-officier.html?origin=SuQm%2FlB%2BQ0%2BV%2Fx7b7T%2BJPw				
15	Horvaatia	International University of Rijeka - Faculty of Maritime Studies	O/E/ET	Jah	Väljund puudub
	Kooli kodulehekülg: http://www.pfri.uniri.hr/web/en/index.php Õppekavad OOW: http://www.pfri.uniri.hr/web/hr/studij_pre_N.php EOOW: http://www.pfri.uniri.hr/web/hr/studij_pre_BS.php ETO: http://www.pfri.uniri.hr/web/hr/studij_pre_EL.php				
16	Horvaatia	University of Dubrovnik	O/E/ET	Jah	Spetsiifiline
	Kooli kodulehekülg: http://www.unidu.hr/index_eng.php Õppekavad OOW: http://www.unidu.hr/datoteke/129izb/Studijski-program-NAUTIKA-2014-2015-15.02.14-FINAL.pdf EOOW: http://www.unidu.hr/datoteke/130izb/Studijski-program-BS-2014-2015-15.02.14-FINAL.pdf ETO: http://www.unidu.hr/datoteke/635izb/elektrotehnika_rgb.pdf				
17	Horvaatia	University of Split - Faculty of Maritime Studies	O/E/ET	Jah	Info puudub
	Kooli kodulehekülg: http://www.pfst.unist.hr/en/ Õppekavad OOW, EOOW ja ETO: http://www.pfst.unist.hr/red_predavanja/2017-2018/red_predavanja_2017_2018_redoviti.pdf				
18	Horvaatia	University of Zadar - The Maritime Department	O/E	Jah	Info puudub
	Kooli kodulehekülg: http://www.unizd.hr/promet-pomorstvo Õppekavad OOW ja EOOW: http://www.unizd.hr/promet-pomorstvo/studijski-programi-pomorskog-odjela/redovi-predavanja				

Lisa 3 järg

19	Iirimaa	National Maritime College of Ireland	O/E/ET	Ei	Info puudub
	Kooli kodulehekülg: https://www.nmci.ie/ Õppekavad OOW: https://courses.cit.ie/index.cfm/page/course/code/CR_SNASC_7 EOOW: https://courses.cit.ie/index.cfm/page/course/code/CR_EMARE_7 ETO: https://courses.cit.ie/index.cfm/page/course/code/CR_EMAEL_7				
20	Island	Technical College Reykjavík - School of Navigation	O/E	Info puudub	Info puudub
	Kooli kodulehekülg: https://tskoli.is/				
21	Itaalia	Istituto Nautico Cristofaro Mennella Forio	O/E	Info puudub	Info puudub
	Kooli kodulehekülg: http://www.ismennellaischia.gov.it/				
22	Kreeka	Merchant Marine Academy of Syros	O	Jah	Üldine
	Kooli kodulehekülg: http://www.aensyrou.edu.gr/ Õppekavad OOW: http://www.aensyrou.edu.gr/index.php?option=com_k2&view=itemlist&layout=category&task=category&id=20&Itemid=114&lang=gr				
23	Küpros	Cyprus Maritime Academy	O/E/ET	Jah	Info puudub
	Kooli kodulehekülg: https://www.cyma.ac.cy/ Õppekavad OOW: https://www.cyma.ac.cy/programmes/maritime-studies/nautical-science/ EOOW: https://www.cyma.ac.cy/programmes/maritime-studies/marine-engineering/ ETO: https://www.cyma.ac.cy/programmes/maritime-studies/marine-electrotechnology/				
24	Küpros (Põhja)	Grine American University Marine School	O	Jah	Info puudub
	Kooli kodulehekülg: http://marine.gau.edu.tr/en Õppekavad OOW: http://marine.gau.edu.tr/en/deck_department.html				
25	Leedu	Lithuanian Maritime Academy	O/E/ET	Jah	Info puudub
	Kooli kodulehekülg: http://www.lajm.lt/en/studies.html Õppekavad OOW: https://www.aikos.smm.lt/_layouts/15/asw.aikos.registersearch/objectformresult.aspx?o=prog&f=prog&key=3926&pt=of EOOW: https://www.aikos.smm.lt/_layouts/15/asw.aikos.registersearch/objectformresult.aspx?o=prog&f=prog&key=3925&pt=of ETO: https://www.aikos.smm.lt/_layouts/15/asw.aikos.registersearch/objectformresult.aspx?o=prog&f=prog&key=9374&pt=of				

Lisa 3 järg

26	Läti	Latvian Maritime Academy	O/E/ET	Jah	Info puudub
	Kooli kodulehekülg: http://www.latja.lv/ Õppekavad OOW, EOOW ja ETO: http://www.latja.lv/bakalauriem/				
27	Malta	Malta College of Arts Science and Technology	O/E	Info puudub	Info puudub
	Kooli kodulehekülg: http://www.mcast.edu.mt/ Õppekavad OOW: http://www.mcast.edu.mt/course/1013 EOOW: http://www.mcast.edu.mt/course/1052				
28	Montenegro	University of Montenegro - Faculty of Maritime Studies Kotor	O/E/ET	Jah	Info puudub
	Kooli kodulehekülg: http://www.pfkotor.me/en				
29	Norra	The Norwegian University of Science and Technology (NTNU)	O	Jah	Väljund puudub
	Kooli kodulehekülg: https://www.ntnu.edu/ Õppekavad OOW: https://www.ntnu.no/studier/studieplan#programmeCode=353MN&year=2017				
30	Norra	University College of Southeast Norway	O/E	Jah	Info puudub
	Kooli kodulehekülg: https://www.usn.no Õppekavad OOW: https://www.usn.no/studier/studie-og-emneplaner/#/studyplan/3NA_2018H EOOW: https://www.usn.no/studier/studie-og-emneplaner/#/studyplan/3MD_2018H				
31	Norra	Western Norway University of Applied Sciences (HVL)	O/E	Ei	Info puudub
	Kooli kodulehekülg: https://www.hvl.no/ Õppekavad OOW: https://www.hvl.no/studier/studieprogram/2017h/nab/utdanningsplan/ EOOW: https://www.hvl.no/studier/studieprogram/2017h/mmt/utdanningsplan/				
32	Norra	The Arctic University of Norway	O	Jah	Info puudub
	Kooli kodulehekülg: https://uit.no/startsida Õppekavad OOW: https://uit.no/utdanning/program/282924/nautikk_ingenior_-_bachelor				

Lisa 3 järg

33	Poola	Gdynia Maritime University	O/E/ET	Jah	Info puudub
	Kooli kodulehekülg: https://am.gdynia.pl/ Õppekavad EOOW: http://wm.am.gdynia.pl/programy-studiow ETO: http://www.we.am.gdynia.pl/programy-studiow				
34	Poola	Maritime University of Szczecin	O/E	Jah	Info puudub
	Kooli kodulehekülg: https://www.am.szczecin.pl/ Õppekavad OOW: https://www.am.szczecin.pl/plany-zajec/441-studia-stacjonarne-wydzial-nawigacyjny EOOW: https://www.am.szczecin.pl/plany-zajec/442-studia-stacjonarne-wydzial-mechaniczny				
35	Portugal	Escola Náutica Infante D. Henrique	O/E/ET	Jah	Info puudub
	Kooli kodulehekülg: http://www.enautica.pt Õppekavad OOW: http://www.enautica.pt/en/courses-4/undergraduated-courses--9/deck-and-bridge-operations-12/ EOOW: http://www.enautica.pt/en/courses-4/undergraduated-courses--9/marine-engineering-13/ ETO: http://www.enautica.pt/en/courses-4/undergraduated-courses--9/marine-electrotechnical-engineering-31/				
36	Prantsusmaa	Ecole Nationale Supérieure Maritime	O/E	Info puudub	Info puudub
	Kooli kodulehekülg: https://www.supmaritime.fr OOW ja EOOW: https://www.supmaritime.fr/en/engineer-level-seafarer-merchant-marine-first-class-officer.html				
37	Rootsi	Linnaeus University: Kalmar Maritime Academy	O/E	Ei	Info puudub
	Kooli kodulehekülg: https://lnu.se/mot-linneuniversitetet/Organisation/fakulteten-for-teknik/sjofartshogskolan/ Õppekavad OOW: https://kursplan.lnu.se/utbildningsplaner/utbildningsplan-YGSKP-2.pdf EOOW: https://kursplan.lnu.se/utbildningsplaner/utbildningsplan-YGSIP-2.pdf				
38	Rumeenia	"Mircea cel Batran" Naval Academy	O/E/ETO	Jah	Info puudub
	Kooli kodulehekülg: https://www.anmb.ro/eng/ Õppekavad OOW: https://www.anmb.ro/ro/files/structura/fnmn/d_ntn.html EOOW: https://www.anmb.ro/ro/files/structura/fnmn/d_imnp.html ETO: https://www.anmb.ro/ro/files/structura/fim/d_ieen.html				

Lisa 3 järg

39	Rumeenia	Romanian Nautical College	O/E/ET	Ei	Info puudub
	Kooli kodulehekülg: http://nauticalcollege.org/ro/ Õppekavad OOW: http://nauticalcollege.org/wp-content/uploads/2017/02/CURRICULA-HND-NAUTICAL-SCIENCE-2016-2017-1.pdf EOOW: http://nauticalcollege.org/wp-content/uploads/2017/02/CURRICULA-HND-MARINE-ENGINEERING.pdf ETO: http://nauticalcollege.org/en/uk-hnd-officers-programs/experienced-electrician-to-electro-technical-officer/				
40	Rumeenia	Constanta Maritime University	O/ET	Jah	Info puudub
	Kooli kodulehekülg: https://cmu-edu.eu/ Õppekavad OOW: https://cmu-edu.eu/wp-content/uploads/2016/02/Plan-Invatamant-Navigatie.pdf ETO: https://cmu-edu.eu/wp-content/uploads/2016/02/Plan-Invatamant-Electrotehnica-zi.pdf				
41	Saksamaa	Jade University of Applied Sciences	O	Jah	Info puudub
	Kooli kodulehekülg: https://www.jade-hs.de/ Õppekavad OOW: https://www.jade-hs.de/unsere-hochschule/fachbereiche/seefahrt-und-logistik/studiengaenge/nautik-und-seeverkehr/				
42	Saksamaa	Flensburg University of Applied Sciences	O/E	Jah	Info puudub
	Kooli kodulehekülg: https://hs-flensburg.de Õppekavad OOW: https://hs-flensburg.de/node/1667 EOOW: https://hs-flensburg.de/node/1662				
43	Saksamaa	University of Applied Sciences Emden/Leer	O	Jah	Info puudub
	Kooli kodulehekülg: https://www.hs-emden-leer.de Õppekavad OOW: https://www.hs-emden-leer.de/fileadmin/user_upload/vb/2017/VB_Nr._49_2017_BPO_Nautik_und_Seeverkehr_06062017_endg.pdf				
44	Saksamaa	Wismar University of Applied Sciences Technology, Business and Design	O/E/ET	Jah	Väljund puudub
	Kooli kodulehekülg: https://fiw.hs-wismar.de/ Õppekavad OOW: https://tinyurl.com/yabh5uga EOOW: https://tinyurl.com/yclcaav3 ETO: https://tinyurl.com/y7nq25t7				

Lisa 3 järg

45	Sloveenia	University of Ljubljana - Faculty of Maritime Studies And Transport	O/E	Jah	Väljund puudub
	Kooli kodulehekülg: https://www.fpp.uni-lj.si/ Õppekavad OOW: https://www.fpp.uni-lj.si/studij/studijski_program_1stopnje/navtika_vss/predmetnik/ EOOW: https://www.fpp.uni-lj.si/studij/studijski_program_1stopnje/ladijsko_strojnistvo_vss/predmetnik/				
46	Soome	Åland University of Applied Sciences	O/E/ET	Jah	Väljund puudub
	Kooli kodulehekülg: https://www.ha.ax/ Õppekavad OOW: https://www.ha.ax/bo-studera/kursbeskrivningar/sjokapten-kurser/ EOOW: https://www.ha.ax/bo-studera/kursbeskrivningar/maskinteknik-kurser/ ETO: https://www.ha.ax/bo-studera/kursbeskrivningar/elektoteknik-kurser/				
47	Soome	South-Eastern Finland University of Applied Sciences	O/E	Jah	Väljund puudub
	Kooli kodulehekülg: https://www.xamk.fi/ Õppekavad OOW: https://opinto-opas.xamk.fi/index.php/fi/28/fi/6841/MKKT18SP/year/2018 EOOW: https://opinto-opas.xamk.fi/index.php/fi/28/fi/6839/MIKT18SP/year/2018				
48	Soome	Novia University of Applied Sciences	O	Jah	Info puudub
	Kooli kodulehekülg: https://www.novia.fi/ Õppekavad OOW: https://www.novia.fi/utbildning/ansokan-och-studier/laroplaner/lp2017/?id=11267				
49	Soome	Axxell Vocational Institute	O/E	Jah	Info puudub
	Kooli kodulehekülg: https://www.axxell.fi Õppekavad OOW ja EOOW: https://tinyurl.com/y94bnb27				
50	Soome	Satakunta University of Applied Sciences	O/E	Ei	Väljund puudub
	Kooli kodulehekülg: https://www.samk.fi/ Õppekavad OOW: https://samk.solenovo.fi/opsnet/disp/fi/ops_KoulOhjOps/tab/tab/sea?ryhma_id=15673858&koulohj_id=14402717&valkiel=en&stack=push EOOW: https://samk.solenovo.fi/opsnet/disp/fi/ops_KoulOhjOps/tab/tab/sea?ryhma_id=15628463&koulohj_id=13588913&valkiel=fi&stack=push				
51	Suurbritannia	City of Glasgow College	O/E/ET	Info puudub	Info puudub
	Kooli kodulehekülg: https://www.cityofglasgowcollege.ac.uk/				

Lisa 3 järg

52	Suurbritannia	Liverpool John Moores University	O/E	Ei	Info puudub
	Kooli kodulehekülg: https://www.ljmu.ac.uk/about-us/faculties/faculty-of-engineering-and-technology/department-of-maritime-and-mechanical-engineering Õppekavad OOW: https://prodcat.ljmu.ac.uk/KIS/32821-3000002479.pdf EOOW: https://prodcat.ljmu.ac.uk/KIS/32119-3500006804.pdf				
53	Suurbritannia	Scottish Maritime Academy	O	Jah	Info puudub
	Kooli kodulehekülg: http://www.smaritime.co.uk/ Õppekavad OOW: http://www.smaritime.co.uk/public/upload/SMA_infoHNC_NautScie_SCOTTISH_2017.pdf				
54	Suurbritannia	South Tyneside College	O/E/ET	Jah	Info puudub
	Kooli kodulehekülg: Õppekavad OOW: http://www.stc.ac.uk/marine-school/course/foundation-degree-marine-operations-merchant-navy-deck-officer-trainee-scheme EOOW: http://www.stc.ac.uk/marine-school/course/foundation-degree-marine-engineering ETO: http://www.stc.ac.uk/marine-school/course/foundation-degree-marine-electrical-engineering				
55	Suurbritannia	Southampton Solent University	O/E/ET	Jah	Info puudub
	Kooli kodulehekülg: http://www.warsashacademy.co.uk/home.aspx Õppekavad OOW, EOOW ja ETO: https://www.warsashacademy.co.uk/about/brochures-and-gallery/resources/wma-officer-cadet-brochure-2016.pdf				
56	Taani	Copenhagen School of Marine Engineering and Technology Management	E	Info puudub	Info puudub
	Kooli kodulehekülg: https://www.msk.dk/ Õppekavad EOOW: http://kmedok.dk/showpage.php?pageid=36040				
57	Taani	Marstal Navigatsionsskole	O	Jah	Väljund puudub
	Kooli kodulehekülg: http://www.marnav.dk Õppekavad OOW: http://www.marnav.dk/media/sites/3/2017/PDFS/Studieordning-for-Skibsforeruddannelsen-20122017.pdf				

Lisa 3 järg

58	Taani	Svendborg International Maritime Academy	O/E	Jah	Väljund puudub
	Kooli kodulehekülg: http://www.simac.dk/ Õppekavad OOW ja EOOW: https://www.simac.dk/wp-content/uploads/2018/03/Studieordning-Skibsofficer-Version-5.20-af-29.-januar-2018-1612.pdf				
59	Taani	Fredericia School of Engineering	E	Ei	Väljund puudub
	Kooli kodulehekülg: http://www.fms.dk/ Õppekavad EOOW: https://tinyurl.com/y8tbdgtp ja https://tinyurl.com/y96mn9ff				
60	Türgi	Istanbul Technical University	O/E	Jah	Väljund puudub
	Kooli kodulehekülg: http://df.itu.edu.tr/anasayfa Õppekavad OOW: http://www.sis.itu.edu.tr/tr/dersplan/plan/DUI/201410.html EOOW: http://www.sis.itu.edu.tr/tr/dersplan/plan/GMI/201210.html				
61	Türgi	Recep Tayyip Erdogan University	O	Jah	Väljund puudub
	Kooli kodulehekülg: http://denizcilik.erdogan.edu.tr/ Õppekavad OOW: http://bologna.erdogan.edu.tr/organizasyonInfo.php?kultur=tr-TR&mod=1&program=636&yil=2017#anchors				
62	Türgi	Karadeniz Technical University	O	Jah	Väljund puudub
	Kooli kodulehekülg: http://www.ktu.edu.tr/denizduim Õppekavad OOW: http://katalog.ktu.edu.tr/DersBilgiPaketi/matrix.aspx?pid=86&lang=2				
63	Türgi	Piri Reis University	O/E	Jah	Väljund puudub
	Kooli kodulehekülg: https://www.pirireis.edu.tr/ Õppekavad OOW ja EOOW: https://www.pirireis.edu.tr/ders-planlari				
64	Ukraina	Odessa Maritime Academy	O/E/ET	Jah	Info puudub
	Kooli kodulehekülg: http://www.onma.edu.ua/ Õppekavad OOW, EOOW ja ETO: http://www.onma.edu.ua/denna-forma				

Lisa 3 järg

65	Venemaa	Admiral Makarov State Maritime Academy	O/E/ET	Jah	Info puudub
	Kooli kodulehekülg: https://ma.gumrf.ru/ Õppekavad OOW, EOOW ja ETO: https://edu.gumrf.ru/studentam/schedule/				

Lisa 4. Küsimustik mereõppeasutustele

Kaaskiri

Hello!

I'm a student of Estonian Maritime Academy.

I'm writing my master's dissertation on cybersecurity education for future ship's officers in maritime educational institutions.

With the emergence of ever more advanced technologies and increasing connectedness, cybersecurity has become a hot topic in the maritime industry and in the world generally. My goal is to find out if and at what level is cybersecurity education provided for future ship's officers during their training in maritime educational institutions and to give suggestions for the improvement of cybersecurity education.

For this i've created a Google Forms questionnaire consisting of two parts. First part contains general questions to get an overall picture of the situation and second part has specific questions to find out more about the experience of different institutions in this field.

Anonymity is guaranteed - answering questions which reveal your identity is not required!

Completion of this questionnaire will take 5-10 minutes and it will remain accessible until 20.05.2018

Thank you for your help!

If this is not you expertise, please forward this e-mail to someone who can answer these questions.

Should you have any comments or questions, please feel free to contact me at lauriroolaid@gmail.com or +372 56648814.

If you're interested in the results of the survey, please let me know.

Lisa 4 järg

Best regards,
Lauri Roolaid

Master's student
Estonian Maritime Academy of Tallinn University of Technology

Küsimused

General questions:

1. Please state your e-mail address. (voluntary)

2. State the name of your institution. (voluntary)

3. In what country is your institution located? (voluntary)

4. What is your position in this institution? (voluntary)

5. What kind of ship's officer study programmes do you provide?

a) Officer in charge of navigational watch (OOW) 500GT+
b) Engineer officer of the Watch (EOOW) 750kW+
c) Electro-technical officer (ETO)
d) Ship refrigeration engineer
e) Radio officer
f) Other

6. What level of education do you provide for ship's officers? (Based on EQF - European Qualifications Framework)

a) EQF level 4 - (Vocational/trade school etc.)
b) EQF level 5 - (Certificate/diploma of higher education etc.)
c) EQF level 6 - (Professional higher education/Bachelor's degree etc.)
d) EQF level 7 - (Master's degree/Vocational university etc.)
e) Other

Lisa 4 järg

7. Approximately how many students per year receive ship's officer (OOW, EOOW, ETO etc.) certificate of competency at your institution?

8. Does your institution provide cybersecurity training for future ship's officers?

a) Yes
b) No
c) Maybe in the futuure
d) Other

9. Do you think that it is necessary to provide cybersecurity training for future ship's officers?

a) Yes
b) No
c) Maybe in the future
d) Other

10. Please explain your answer to previous question

Specific questions (Continue If you answered “yes” to question 8):

11. In what way is cybersecurity training for ship's officers provided at your institution?

a) As a separate subject
b) Using e-learning platform (like Seagull)
c) As part of another subject (e.g. Information Technology)
d) As a course provided by guest lecturer
e) Other

Lisa 4 järg

12. What kind of cybersecurity training is provided for ship's officers at your institution?

a) Generic cybersecurity awareness training
b) Specific cybersecurity training for ship's officers
c) Simulator training
d) Other

13. Please describe how do you use simulator for cybersecurity training? (Answer only if you use simulator for training)

14. What topics do you cover in cybersecurity training?

a) Cybersecurity basics (terminology, general awareness etc)
b) Basics of computer networking and communications
c) National and international regulations related to cybersecurity
d) Standards related to cybersecurity
e) Maritime industry guidelines related to cybersecurity
f) Ship as a target (who, why and how would attack my ship)
g) Cybersecurity of ship's Information-, communications and operational technology systems
h) Detection of, protection against, response to and recovery from cyber attacks
i) Other

15. Please comment on your experience in providing cybersecurity training for ship's officers (refer to question 10). (Why did you choose this particular study method? What are the considerations to be made when choosing a study method? What kind of problems did you face when implementing this method? Feedback from students etc.)

16. Do you think that the level of cybersecurity training for ship's officers at your institution is sufficient?

a) It's sufficient
b) It needs to be improved
c) Other

Lisa 5. Ekspertintervjuud

Intervjuu 1

Intervjuu kestus: 10:00–10:30

K: Alates 2017/2018 õppeaastast on TTÜ EMERA arvutialaseid alusteadmisi käsitleva õppeaine nimetus kui ka väljundid muutunud. Miks see nii on?
V: See on aine, mis on TTÜ poolt terve ülikooli peale antud. On määratud teatud väljundid, mis tuleb läbi võtta. Esialgu õpetasime me Microsoft Office'it, aga nüüd on teemasid lisandunud – muuhulgas programmeerimise alused, küberturvalisus, pildi-. Heli- ja videotöötlus ning andmebaasid. Esimese kursuse „IT-alused" on nüüd väga mahukas, ja päris raske on neid teemasid väga põhjalikult käsitleda. Selles mõttes on keeruline.

K: Kas see on siis TTÜ nõue?
V: Öeldakse, et sellised õpiväljundid peavad olema, ja selle järgi tuleb ainekava koostada.

K: Kas peale TTÜ kusagilt mujalt ka on tulnud nõudeid käsitleda laevaohvitseride väljaõppes küberturvet? (näiteks Haridus- ja teadusministeerium, Veeteede Amet, mingisugused Euroopa Liidu/Rahvusvahelised nõuded)
V: Minu teada selliseid nõudeid pole tulnud.

K: Kuidas on TTÜ EMERAs korraldatud õppekava koostamine/kinnitamine/muutmine?
V: Mina olen koostanud ainult oma ainekava. Õppekavadega tegelevad programmijuhid.

K: Mismoodi on õppeaine „IT-alused" raames lahendatud väljund „Mõistab küberturvalisuse ja -eetika põhimõtteid."?
V: Üliõpilased peavad vaatama antud teemal videoloenguid, tegema märkmeid ning vastama küsimustele. Moodle'is on selleteemaline valikvastustega test. Test läbitakse arvutiklassis, et raskendada spikerdamist või kellegi abi kasutamist. Niimoodi saab õigemad tulemused.

K: Kas praeguste kogemuste põhjal on tulnud mõte väljaõppes midagi muuta?

Lisa 5 järg

V: Esialgu nii jääb. Kui on plaanis põhjalikumalt teha, siis võiks see olla mõne teise õppeaine raames. Üldaine sees detailseks minna ei saa, sest maht on piiratud.

K: Kui piirangud puuduksid, siis kuidas teie arvates võiks küberturbe õpet kõige paremini korraldada?
V: Sellele oskab programmijuht paremini vastata.

K: Kas arvutiõpetus üldainena on nii laevajuhtidele- kui mehaanikutele sama?
V: Jah.

K: Elektromehaanikute õppekavas on õppeaine „Laeva arvutivõrgud ja andmetöötlussüsteemid“, kuid seal ei ole väljundite all küberturvet käsitletud.
V: Elektromehaanikutele tuleb ilmselt TTÜ peamajast keegi seda asja õpetama. Praegu ei ole see eriala veel käima läinud. Üliõpilased võeti juba vastu, kuid kaks esimest aastat on üldained ja siis hakkab eriala. Seega eriala ettevalmistamiseks on aega veel üks aasta.

K: Kas teie võimaluse korral õppeaine „IT alused“ raames käsitleksite küberturvet rohkem, või muudaksite selles suhtes midagi?
V: Ma pean ennast selle teemaga rohkem kurssi viima. Teema on suhteliselt uus. Selle õppeaasta jooksul on väga palju sellest räägitud, kuid üldist teooriat selle kohta on vähe. Leiab küll inglise keeles, kuid see tuleb läbi töötada ning tõlkida. Uute väljunditega seoses on õppetöö päris pingeline ning mingi uue asja ettevõtmise jaoks on aega väheks jäänud.

K: Kui mina õppisin TTÜ EMERAs, siis oli õppeaine „Informaatika I“ ja peale selle valikaine „Informaatika II“. Kas praegu on võimalus valikainena saada arvutiõpetust laiemalt?
I: Sellist võimalust praegu ei ole. Praegu jääb näiteks programmeerimise osa väga nõrgaks. Õppeaine raames tuleb läbi võtta väga palju teemasid ja programmeerimist selgeks ei saa. Ega ka varasemalt päris selgeks ei saanud, aga vähemalt paremini.

K: Kas õpilastelt on tulnud küberturbe käsitluse kohta antud aine raames ka mingisugust tagasisidet?

Lisa 5 järg

V: Tagasiside aine kohta on olemas, kuid konkreetselt küberturbe kohta küsimust ei olnud.

K: Ma saan aru, et see teema on niivõrd uus ning praegu on niiöelda veel prooviperiood, kuidas „IT-alused“ õppeaine raames küberturbe õpet korraldada.
V: Tulevik näitab mismoodi see asi hakkab olema. Praegu on TTÜs suur ümberkorraldus. Kõik ained tehakse ümber. Kontakttunde võetakse vähemaks ning iseseisvat tööd tuleb juurde, vastavalt 40% ja 60%, ja see juba tekitab mõningaid probleeme.

Intervjuu 2

Intervjuu kestus: 09:30–10:15

K: Kas teie arvates peaksid laevajuhid ja -mehaanikud saama küberturbe haridust erialaspetsiifiliselt?
V: Küberturvet STCW veel ei sisalda ja mudelkursusi selle kohta pole, mistõttu ei ole ka meie seda õppekavasse sisse viinud. See on terves maailmas uus teema. Praegu ei tule ühtegi sellist laevamehhanismide juhtimissüsteemidega seotud juhtumit ette. Laevades on need süsteemid lokaalsed ning juurdepääs neile on kas laevapereliikmetel või seadmete valmistajatel.

K: STCW koodeks annab küll miinimumnõuded, kuid osalisriigid võivad alati laevaohvitsere kõrgemal tasemel õpetada.
V: Seda küll, kuid need miinimumnõuded on küllaltki kõikehõlmavad ning ega enamat ei oskakski juurde panna. Need nõuded katavad tulevaste laevaohvitseride töös kõik vajalikud teadmised ja oskused ära ning ühtegi lõtku seal ei ole..

K: Kuidas käib TTÜ EMERAs õppekavade kinnitamine? Kuidas on sellega seotud Haridus- ja teadusministeerium, VTA ja kutsestandardid?
V: Eesti on IMO liikmesriik ja vabariigi mereadministratsiooni rolli täidab VTA. Kõik laevaohvitseride õppekavad on kooskõlastatud VTA-ga. Seoses TTÜ õppestatuudi muutusega tuli teha tüürimeestele ja mehaanikutele uued õppekavad. Mehaanikute poole

pealt lisandus elektromehaaniku õppekava. Need õppekavad said kooskõlastuse ka VTA-st. Kutsestandardid on küll olemas, aga IMO-l ja VTA-l on nendest ükskõik ja meremeeste diplomeerimist see ei mõjuta mitte kuidagi.

K: Alates sellest õppeaastast lisandus õppeaine „IT-alused“ väljundite alla küberturvalisus.
V: „IT alused“ on meil aegade algusest olnud, aga vähemalt viimaste aastate jooksul on seal käsitletud üksnes kontoritarkvara. Aga kui nüüd seal küberturvet käsitletakse, siis on see väga hea. Päris täpselt ei oska öelda, kui palju on IT meestel pädevust ja teadmisi küberturbe asjus.

K: Elektromehaanikute õppekavas on aine „Laeva arvutivõrgud ja andmetöötlussüsteemid“. Kas selle õppeaine raames käsitletakse küberturvet?
V: Kompetentsinõudeid käsitleb STCW ning nende rakendamiseks on loodud soovituslikud mudelkursused. Sealhulgas ka laeva elektrimehaaniku mudelkursus. Selles mudelkursuses küberturve teema võiks loogiliselt olla eelnimetatud aines, kuid selle jälgi ma sealt küll ei leidnud. Mida see õppeaine täpsemalt endast kujutab, praegu ei oska öelda. Esimesed elektrimehaanikud Mereakadeemias alustasid sügisel ning eriala ained tulevad alles neljandal kursusel. Laevadele toodavad selliseid arvuti- ja elektroonikasüsteeme mitmed firmad ning nende komponendid ja arhitektuur on väga erinevad. Seetõttu selles aines saab anda ainult üldiseid aluseid. Antud õppeaine käsitleb tõenäoliselt siiski lokaalseid võrke ning nendele väljastpoolt sisse häkkida niisama ei saa.

K: Millised võimalused on masinaruumi simulaatoril? Kas on võimalik simuleerida ka rikkeid süsteemide ja seadmete rikkeid? Kas on võimalik mängida läbi küberintsidentidega seotud juhtumeid?
V: Masinaruumi simulaatori õpe on väga oluline osa väljaõppes. See koosneb kahest plokist. Esimene plokk on laevasüsteemide ettevalmistamine ja käitamine normaalse töö käigus. Teise plokina on võimalik sisse sööta kas teatud ajalises järjestuses või eelnevatest tegutsemistest tingitud mitmesuguseid häireid ning siis peab nendele häiretele reageerima, tuvastama põhjuse ning võimalusel kõrvaldama. Küberintsidentide võima

likkust ei oska ma praegu ette kujutada. Küll aga saab läbi mängida stsenaariume, kui mingisugune elektri-, elektroonika- või automaatjuhtimissüsteemi lüli otsad annab.

K: Kuidas teie küberturbe väljaõppe käsitlemise tulevikku näete? Kas seda võiks üldse millalgi käsitleda? Kas peaks võiks seda käsitleda eraldi õppeainena, mingi õppeaine siseselt, e-kursusena või mingil muul viisil?
V: Siin võiks, natukene võibolla ka teie poolt, uurida, kuivõrd on küberohud merenduses reaalsed. Ma tean, et füüsiline turvalisus on küll probleem, aga küberturbe intsidentidest minuni ei ole infot jõudnud. Nõrgem koht laevade puhul on minu meelest sild. Masinasüsteemid on siiski enamjaolt lokaalsed. Laevadel on alati võimalus minna käsitsijuhtimise peale ja see on lausa IMO nõue. Laevajuhtidel on teine probleem. GPS annab täpse asukoha ja see on sillameeste elu teinud mugavaks ja lihtsaks. Juhul kui elektrivarustus kaob ja UPS ei toida, peaks olema võimalik määrata iidsete vahenditega laeva asukohta. Seda aga ei osata, sest neid viise kasutatakse haruharva. Küberturve hakkab päevakorda tõsisemalt tulema tõenäoliselt tulevikus autonoomsete laevade kasutuselevõtuga seoses. Aga see protsess ei lähe väga kiiresti.

Intervjuu 3

Intervjuu kestus: 10:30–10:55

K: Kas teie arvates peaksid laevajuhid ja -mehaanikud saama küberturbe haridust erialaspetsiifiliselt?
V: Vaadates tänapäeva trende ja seda, mis maailmas toimub, siis igal juhul tuleb laevaohvitseride teadlikkust tõsta. Nähes kui palju küberintsidente nii maismaal kui merenduses toimub, oleks see teema kindlasti vajalik.

K: Kas TTÜ EMERA-l on küberturbe hariduse korraldamise suhtes mingisuguseid mõtteid?
V: See teema on meil läbi käinud. Oleme rääkinud, et kas ta peaks olema eraldi õppeaine. Vastavalt TTÜ statuudile peaksid kõik õppeained olema 6 EAP. Kui võtta uue ainena küberturvalisus sisse, võtaks see meeletu mahu õppekavast ära. Selles mõttes on see küsimärk. Võimalus on küll teha valikainena.

Lisa 5 järg

K: Kas merenduses on rahvusvaheliselt juba olemas mingisugune nõue, et küberturvet peab käsitlema?
V: Hetkel ei ole sellisest nõudest kuulnud, et küberturve peaks olema õppeprotsessi osa.

K: Kuidas õppekavad TTÜ EMERAs kinnitatakse?
V: Väikesed muudatused saab teha ära majasiseselt – muuta õppeaine sisu vms. Kui on vaja õppeainet teise ainega asendada, siis peab see minema TTÜ-sse kinnitamisele. Õppekava kiidab heaks VTA. Lisaks on olemas programmi nõukoda, kes tuleb kokku kutsuda, kui on vaja mingi muudatus õppekavasse sisse viia. Sinna kuuluvad näiteks keegi tegevkaptenitest, VTA-st ning üliõpilaste esindaja. Esmalt peaks muudatus programmi nõukojalt heakskiidu saama.

K: Kas laevajuhid ja -mehaanikud peaksid küberturbe haridust saama ühte moodi?
V: See võib olla ühel tasemel. Tänapäeva laevas on kõik omavahel ühendatud. Sild ja masin on ühendatud erinevate arvutite ja sensoritega. Sillast näeb masinate parameetreid ja masinast näeb silla omi samamoodi. Selles mõttes midagi erinevat olema ei pea. Võib täiesti üks ja sama olla. Arvutid on ikka arvutid. Sissetungimiseks peab olema ühendus välismaailmaga. Laeva tuleb internet läbi satelliidi, sealt edasi levib see masinaruumi, silda. Kõik on ühtemoodi koos.

K: Kas sillasimulaatoriga on võimalik mängida läbi küberintsidente?
V: Instruktor saab teha mida iganes. Kõik parameetrid on muudetavad ja nii öelda „häkitavad". Saab sensorid küljest ära võtta, nihkesse panna ja muud moodi süsteemi manipuleerida – sõidad ja järsku on GPS kadunud jne.

K: Millisel kujul oleks teie arvates küberturbe õpet kõige parem läbi viia ja millised piirangud erinevatel võimalustel on? (eraldi õppeaine, e-kursus, loeng väljastpoolt)
V: Küberturvet eraldi õppeainena teha ei saa, sest sellisel juhul peaks see olema 6 EAP. Võimalik on see mingi muu valikainega asendada ning teha see mõne muu õppeaine eeldusaineks, st kui seda valikainet ei läbi, siis teist õppeained deklareerida ei saa. E-kursusena küberturbe läbimise probleem on, et selle eest ei saa õpilasetele anda aine–

Lisa 5 järg

punkte. Pigem ma näen teda teise õppeainega integreerituna. Õppeaines on sellisel juhul kaks õppejõudu. Õppejõuks võib olla käsunduslepingu alusel ükskõik kes.

Intervjuu 4

Küsimused:

1) Do you provide general cybersecurity knowledge as a part of "Information Technology"?

2) Cybersecurity is not required by STCW code nor is it a part of IMO model courses. Why did you decide to add this topic to your curricula?

3) How are ship's officer study programmes created and approved in you school? Were there any requirements from government/maritime administration to add cybersecurity to your curricula?

4) In what way are you planning to add this subject to your curricula and why? (as a separate subject; e-learning course, as a part of another subject etc.)

5) What constraints do you see in providing this kind of training in the school? (e.g. time, not enough material on this topic, teachers have no knowledge about the topic etc.)

6) Will deck officers and engineer officers receive the same cybersecurity training? Do you think cybersecurity training should be different for deck officers and engineer officers?

7) What possibilities do the engine and bridge simulators in your school have? Is it possible to simulate cyber attacks? Are you planning to use simulators in any way during cybersecurity training?

8) In the questionnaire, you did not check " Ship as a target (who, why and how would attack my ship)" as a part of your future cybersecurity training. why?

Lisa 5 järg

Vastus:

As I informed you before, we are at the beginning of the process. Study programm will be prepared taking into account the following list of tecommentations:

- *IMO guidance, MSC-FAL.1/Circ.3, at the moment, these are only recommendations. At the moment there are no obligatory requirements from IMO about cybersecurity.*
- *Resolution MSC.428(98) adopted last year (2017) by The Maritime Safety Committee at its 98th session, contains date (first annual verification after 1 January 2021) for administrations for ensuring that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code). So at present time it's too early to talk about possible requirements from administrations.*
- *The Guidelines on Cyber Security On board Ships form BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI. Good list of tasks about cybersecurity, but again, only as recommendation level.*

The Guidelines on Cyber Security On board Ships are aligned with the IMO guidelines and provide practical recommendations on maritime cyber risk management covering both cyber security and cyber safety. The aim of this document is to offer guidance to ship owners and operators on how to assess their operations and put in place the necessary procedures and actions to maintain the security of cyber systems on board their ships.

At present there are no requirements from Latvian national government or Maritime Administration, and for the moment I simply have no answers for you questions, except Nr.7 - Latvian Maritime Academy has exactly same simulators (NTPro 5000 - navigational and TechSim for engine) as Estonian Maritime Academy, with same functionality and possibilities. Of course, as with using any simulator that contains PC and LAN, it is possible to simulate cyber breaches

Lisa 5 järg

Intervjuu 5

K: I understand that you provide cybersecurity training as a part of another subject. Is it part of "Informatics" (Računalništvo in informatika) or "Maritime Information Systems" (Pomorski informacijski sistemi)?

V: We don't have a special subject about cybersecurity. Cybersecurity is taught as a part of „Security Awareness", which is included into regular syllabus. In this subject we talk about 10–15 minutes about cybersecurity. It includes topics like password security, e-mail security, dangers with opening links and attachments sent via e-mail, dangers with USB flash drive. The subject „Maritime Informaton System" is an elective course and it is a technical subject. We teach students how to send documents required by FAL convention, how to transfer files from GPS to ECDIS. Of course we remind students that onboard ECDIS should be licensed and charts updates from trusted source.

K: Do deck officers and engineer officers receive the same cybersecurity training? Do you think cybersecurity training should be different for deck officers and engineer officers?

V: Yes, they receive the same training, because these are the basic things every seafarer needs to know. Engine room and bridge have different systems, but cybersecurity is the same.

K: Cybersecurity is not required by STCW code, nor is it a part of IMO model courses. Why did you decide to add this topic to your curricula?

V: Small part of „Security Awareness" training requirements is cybersecurity. It is also mentioned in STCW code under „Competences for Seafarers with Desgnated Security Duties" and „Competences for Ship's Security Officer."

K: I understand, you provide general cybersecurity training for your students. But what about specific training i.e. specific risks to ships, diferent attackers and vulnerabilities etc.?
V: This is not the job for seafarers. If somebody attacked GPS signals, what could seafarers do? It's too much to ask from seafarers. The systems need to be protected, but it is no a job for seafarers. They must only keep the systems secured from viruses and so on.

K: How are ship's officer study programmes created and approved in you school? Were there any requirements or constraints from the government/maritime administration in adding cybersecurity to your curricula?
V: If we want to add something new, we must ask firs the University and the Government to change the program. If we explain, that it is necessary to do it, they will accept. The administration looks only STCW and the University looks that everything is according to the Bologna requirements.

K: Have you had any problems in teaching this topic? (e.g. time, money, not enough material on this topic, teachers have no knowledge about the topic etc.)
V: There is no material in Slovenian related to maritime cyber threats, but some of my colleagues have studied about these things – attacks on GPS signal etc. We share information about this.

From informatics perspective this is not a topic related only to the ships, but to everything where computers are used.

K: What possibilities do the engine and bridge simulators in your school have? Is it possible to simulate cyber attacks? Do you use simulators in any way during cybersecurity training?
I don't know if they have this capability, but I think not.

Lisa 5 järg

K: You said in the survey questionnaire that all cybersecurity related topics are covered in non specialised subjects. What subjects are those and in what way is cybersecurity covered in these subjects?

V: We have „Security Awareness“, which is a part of basic training. We discuss this a little bit in „Maritime Information Systems“ and „Electronic Navigation Systems“ e.g don’t use illegaal sources for chart updates and ohter programs.

K: Have you had any further plans to improve cybersecurity training at your school?

V: For the subjects I teach, I think that it is enough. We have discussed with colleagues about cyberattacks and so on, but just what the attackers are capable of and not what the seafarers could do to protect the ship. Im teaching from seafarers perspective and I think that it is not necessary to enlarge this topic. Only what officer’s need to know to perform their everyday duties. It is not the job of a seafarer to protect the ship from cyberattacks, it is the job of somebody else.

K: In general, do you think that cybersecurity something that the ship’s officers need to learn?

V: I think that it is important to be aware. To remind the students to use only legal software, not to open suspicious attachments on e-mail etc. So it would be necessary to improve awareness training. But to teach the how to handle cyberattacks, I think it would be too much work for the officers.