TALLINNA TEHNIKAÜLIKOOL
Eesti Mereakadeemia
Merenduskeskus

Dan Heering

KÜBERTURVALISUSE TAGAMINE LAEVANDUSES EESTI LAEVAOMANIKE NÄITEL NING ETTEPANEKUD RISKIDE MAANDAMISEKS

Magistritöö

Juhendaja: dotsent Anatoli Alop

Tallinn 2017

Olen koostanud töö iseseisvalt.
Töö koostamisel kasutatud kõikidele teiste autorite töödele,
olulistele seisukohtadele ja andmetele on viidatud.

Autor: Dan Heering
E-posti aadress: dan@mereblog.com

.....
(allkiri, kuupäev)

Juhendaja: dotsent Anatoli Alop
Töö vastab magistritööle esitatud nõuetele.

.....
(allkiri, kuupäev)

Kaitsmiskomisjoni esimees:
Lubatud kaitsmisele

.....
(ametikoht, nimi, allkiri, kuupäev)

SISUKORD

KASUTATUD MÕISTED JA LÜHENDID

Kasutatud mõisted

Eesti keeles	Inglise keeles	Kirjeldus
	F-Secure	Soome andmeturbefirma
Harpuunimine	Spearphishing	Kalastamise eriliik, mis on sihikindlalt suunatud ühele organisatsioonile ning püüab ärilistel, sõjalistel või poliitilistel eesmärkidel saada juurdepääsu konfidentsiaalsetele andmetele, kus-juures kalastussõnumi saatja näib kuuluvat samasse organisatsiooni (enamasti mingil tähtsal ametikohal). Manipuleerimise eelduseks on teave organisatsiooni struktuuri ja töötajate kohta.
Häkker	Hackers	Raadioamatööride hulgas tekkinud sõna tähistab innukat ja oskuslikku tehnikahuvilist. Arvutialase rõhu andsid talle enne arvutite laia levikut Massachusettsi Tehnoloogiainstituudi kõrg-professionaalsed programmeerijad ja süsteemi-arendajad. Praeguseks on laienenud see ka pool-professionaalidele, kes moodustavad oma huvi-alaseid kogukondi.
Kriitiline infrastruktuur (KI)		See on vara, süsteem või nende osa, mis on hädavajalik eluliselt tähtsate ühiskondlike toimingute toimimiseks. Näiteks tervishoiu, turvalisuse, julgeoleku, inimeste majandusliku ja sotsiaalse heaolu toimimiseks. See on infra-struktuur, mille kahjustada saamine või hävimine mõjutaks oluliselt riiki.
Kriitiline informatsiooni infrastruktuur (KII)		See on info- ja kommunikatsioonisüsteemid, mille toimimine, töökindlus ja turvalisus on olulised riigi toimimise seisukohast. KII on osa KIst.
Küberruum	Cyberspace	ISO/IEC 27032 infoturbes: inimeste, tarkvara ja teenuste interaktsiooniga internetis temaga ühendatud tehniliste vahendite ja võrkude abil tekitatav liitkeskkond, mis ei eksisteeri mingil füüsilisel kujul.
Küberspionaaž	Cyber espionage	Julgeoleku, äri, poliitika või tehnoloogia nimel sooritatavad tegevused sellise teabe leidmiseks,

		mis peaks jääma salajaseks. Ei pruugi olla tingimata sõjaline.
Küberrünnak	Cyber attack	Küberruumi vahenditega ja küberruumi vastu toimuv rünnak eesmärgiga peatada teenuste osutamine või vähendada nende käideldavust või rikkuda andmete terviklust või konfidentsiaalsust.
Käidutehnoloogia	Operational technology (OT)	Riistvara, tarkvara, personal ja ta tegevus, mis füüsiliste seadmete, protsesside ja sündmuste otsese seire ja/või juhtimise teel avastab või põhjustab muudatuse tööstusprotsessis.
Läbistustestimine	Penetration testing	Sissetungirünnete imiteerimine turvameetmete toimivuse kontrollimiseks, sageli tehakse süsteemi sertifitseerimistestimise osana.
Ründevektor	Attack vector	Arvutisüsteemi tungimiseks ja/või sinna kahjustava lasti (troojani, nuhkvara vms) paigutamiseks süsteemi nõrkuse ärakasutamise tee või vahend: meilimanus, hüpikaken, jututuba, inimestega manipuleerimine.
SMBv1 protokoll		Võrguprotokolliga, mida kasutatakse võrgu-ressursside jagamiseks (sealhulgas failide jagamine ja printimine).
Vaba tarkvara	Free software	"Vaba" tähendab, et kasutajal on vabad käed selle kasutamiseks ja suvaliseks muutmiseks (õiguseid võidakse küll ka mõnevõrra piirata litsentsiga).

Kasutatud lühendid

Lühend	Inglise keeles	Eesti keeles
ABS	American Bureau of Shipping	Klassifikatsiooniühing ABS
AIS	Automatic Identification System	Laeva automaatne identifitseerimissüsteem
BIMCO	Baltic and International Maritime Council	Balti ja Rahvusvaheline Merendusnõukogu
BIOS	Basic Input-Output System	Arvuti emaplaadil välkmälus (varem püsimälus) talletatav vanemaid operatsioonisüsteeme toetav alglaadimis- ja seadmeliidestusprogramm, mille funktsioonid on osaliselt või täielikult siirdunud ja siirdumas operatsiooni-süsteemidele ja/või uuematele algkäivitusprogrammidele.
BNWAS	Bridge navigational watch alarm system	Navigatsioonivahi alarmsüsteem
BSA	Business Software Alliance	Mittetulunduslik organisatsioon, mis on loodud tarkvaratööstuse ja nende riistvaratootjatest partnerite eesmärkide saavutamiseks. Tegemist on turvalise ja õiguspärase digitaalse maailma edendamisele enim pühendunud organisatsiooniga.
CCR	Cargo control room	Kauba kontrollruum
CCTV	Closed-circuit television	Sisetelevisioon
CIH		Ajalooline arvutitele operatsiooni-süsteemiga MS Windows 95, 98 või ME suunatud tugevalt kahjustav viirus.
CLC	International Convention on Civil Liability for Oil Pollution Damage	Rahvusvaheline konventsioon tsiviilvastutusest naftareostusest põhjustatud kahjustuste korral.
CRM	Cyber risk management	Küberriskide juhtimine.
DNS	Domain name system	Domeeninimede süsteem
DP	Dynamic Positioning	Laeva dünaamiline positsioneerimise süsteem.
ECDIS	Electronic Chart Display and Information System	Elektronkaartide kuvamise- ja infosüsteem
ENISA	The European Network and Information Security Agency	Euroopa Liidu Võrgu- ja Infoturbeamet
FAL	Facilitation Committee	Mereliikluse hõlbustamise komitee

GMDSS	Global Maritime Distress and Safety System	Ülemaailmne merepääste ja –ohutussüsteem
GPS	Global Positioning System	Ülemaailmne positsioneerimissüsteem
HITSA		Hariduse Infotehnoloogia Sihtasutus
ICS	International Chamber of Shipping	Rahvusvaheline Laevanduskoda
IKT		Info- ja kommunikatsioonitehnoloogia
IMO	International Maritime Organization	Rahvusvaheline Mereorganisatsioon
IoT	Internet of Things	Värkvõrk või esemevõrk
ISM Code	International Safety Management Code	Rahvusvaheline meresõiduohutuse korraldamise koodeks
IT	Information Technology	Infotehnoloogia
KKÜ		Kaitseliidu küberkaitse üksus
M2M	Machine-to-machine	Masinalt masinale suhtlus
MSC	Maritime Safety Committee	Meresõiduohutuse komitee
OPA 90	Oil Pollution Act	Naftareostuse seadus
PMS	Property Management System	Varahaldusüsteem
RIA		Riigi Infosüsteemi Amet
SMS	Safety Management System	Meresõiduohutuse korraldamise süsteem
SSAS	Ship Security Alert System	Laeva valvesignalisatsiooni süsteem
STCW	The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers	Meremeeste väljaõppe, diplomeerimise ja vahiteenistuse aluste rahvusvaheline konventsioon
TEU	Twenty-foot Equivalent Unit	Standardühik erimahuliste konteinerite loendamiseks ja konteinerlaevade või konteineriterminaalide mahutavuse väljendamiseks. 20 jala pikkune ISO-konteiner võrdub ühe TEU-ga, 40 jala pikkune ISO-konteiner võrdub kahe TEU-ga.
TTÜ		Tallinna Tehnikaülikool
VDR	Voyage Data Recorder	Reisiinfo salvestussüsteem
VLAN	Virtual local area network	Virtuaalne kohtvõrk
VoIP	IP-telefon	Metoodika ja tehnoloogiaharu kõneside- ja multimeediumiseansside korraldamiseks IP-protokollil põhinevates arvutivõrkudes, eriti internetis.
VPN	Virtual private network	Virtuaalne privaatvõrk

ABSTRAKT

Merendussektoris on seni keskendutud meresõiduohutuse tõhustamisele hoidmaks ära inimelude, kauba ja vara kaotust ning vähendades keskkonnale tekitatavat kahju. Küberturvalisus on seni jäänud tahaplaanile. Laevandusettevõtete jaoks on küberturvalisus muutunud aina suuremaks probleemiks. Samas ei kuule uudiseid küberrünnakutest sadamate või laevafirmade vastu eriti tihti. See võib olla tingitud mitmest aspektist. Peamised põhjused võivad seisneda selles, et ettevõtted ei ole teadlikud nende vastu toimunud rünnakutest ja tekitatud kahjudest või on nad nendest teadlikud, kuid ei ole informeerinud vastavaid ametkondi, koostööpartnereid ja kliente. Küberrünnakutega kaasnevaid kahjusid on võimalik ära hoida või mingil määral vähendada, kui ettevõtete juhtkonnad teadvustaksid olukorra tõsidust ning võtaksid kasutusele vajalikud meetmed.

Magistritöö eesmärgiks oli välja selgitada, millisel määral on küberturvalisus puudutanud Eesti laevandussektorit ja kuidas on laevaomanikud seda ohtu enda jaoks teadvustanud ning selleks ette valmistunud. Autori hinnangul ei ole Eesti laevaomanike teadmised piisavad küberruumis varitsevatest ohtudest ning seetõttu ei ole ka vajalikke kaitsemeetmeid rakendatud. Autor kasutas oma magistritöös uurimismeetodina küsitlusuuringut, mille tulemused on ära toodud käesoleva lõputöö teises peatükis. Küsimustik saadeti elektrooniliselt 16 ettevõttele, kellest 9 andis tagasisidet autorile. Uuringus osalenud ettevõtete laevastikku kuuluvad järgmised laevatüübid: kauba- ja reisilaevad, parvlaevad, ro-ro laevad, puksiirlaevad, avamererajatiste teeninduslaevad ja majutuslaevad.

Uuringu tulemustest selgus, et mitmed Eesti laevaomanikud on küberrünnakutega kokku puutunud ning selle tulemusena ka kahju saanud. Samuti ilmnes, et suur osa laevaomanikke ei ole küberturvalisust tõsise riskina oma ettevõtte jaoks veel teadvustanud ning ainult kahes ettevõttes on töötajad läbinud küberhügieeni koolituse.

Eestikeelses meedias ja kirjanduses ei ole laevandussektorit varitsevatest küberohtudest kirjutatud ning autori teada ei ole sellekohast uuringut ka läbi viidud.

Võtmesõnad: küberturvalisus, laevandus, küberhügieen

SISSEJUHATUS

"There are only two types of companies: those that have been hacked, and those that will be."
Robert S. Mueller, III, FBI director 2001 - 2013

Meretransport mängib maailma majanduses väga olulist rolli. Ligi 90% rahvusvahelistest kaubavedudest tehakse laevadega. 2015. aastal ületas kaubavedu meritsi rekordilise 10 miljardi tonni piiri (Review of Maritime Transport 2016). Meretransporti võib tinglikult nimetada ka maailmakaubanduse ja -majanduse selgrooks, mille halvamine võib endaga kaasa tuua tõsiseid tagajärgi.

Täna seilab meredel juba üle 51 000 kaubalaeva (The Statistics Portal 2016). Kui arvestada juurde ka reisilaevad, puksiirlaevad ja erinevad eriotstarbelised laevad, siis ületab laevade arv maailmameredel 90 000 piiri (Review of Maritime Transport 2016). Kaubavedu laevadega on kõige ökonoomsem ja keskkonnasäästlikum transpordiviis, mis võimaldab liigutada suuri koguseid pikkade vahemaade taha.

Digitaalne revolutsioon on endaga kaasa toonud uued võimalused teenuste arenguks ning protsesside efektiivsemaks muutmiseks. Digitaalne innovatsioon juhib globaalset arengut hämmastaval kiirusel, mis luues uusi võimalusi arenguteks ja uuendusteks, toob endaga kaasa ka uued ja laevandusele senitundmatud ohud.

Nii nagu kiirelt arenev tehnoloogia on jõudnud meie majapidamistesse maismaal, on see aina enam ja enam rakendatav ka laevanduses. Nii on tõusnud laevade sõltuvus infotehnoloogiast (*information technology*) ja käidutehnoloogiast (*operational technology*). Kasutusele on võetud lahendused, mis pakuvad mõõduka hinna eest kõrget funktsionaalsust. Juba täna sõltuvad sadamad, terminaalid, laevad ning avamererajatised internetivõrku ühendatud info- ja käidutehnoloogiast (kommunikatsioon, navigatsioon, logistika, ohutusseire, turvalisus, mehhanismide juhtimine jne).

Lisaks on lähitulevikus oodata omavahel võrku ühendatud ning teineteisega suhtlevate autonoomsete masinate arvu tõusu. See on juba praegu juhtumas õhus nn droonide näol ja

maismaal isesõitvate autode kujul. Autonoomsete laevade võidukäik meredel ei ole enam kaugel (Merendussektori majandusmõju uuring I etapp 2016).

Eesmärk ja metoodika

Käesoleva magistritöö teemaks on valitud „Küberturvalisuse tagamine laevanduses Eesti laevaomanike näitel ning ettepanekud riskide maandamiseks“. Teema valik lähtub autori huvist laevandussektori ja IT valdkonna vastu. Kui merendus on rahvusvaheliselt väga reguleeritud valdkond, siis on üllatav fakt, et küberturvalisusele pole seni tõsisemat tähelepanu veel pööratud ning ühtegi kehtivat rahvusvahelist või riiklikku regulatsiooni jõustunud.

Olles uurinud erialast kirjandust sai autor aru, et laevandussektorile suunatud küberturvalisuse alast informatsiooni eesti keeles ei olegi. Lisaks ilmnes, et suur osa laevaomanikke maailmas ei ole küberturvalisust seni suureks ohuks lugenudki. Tundub, et laevaomanike arvates puudutab see teema ainult maismaal asuvaid ettevõtteid ning infosüsteeme. Samas on hiljuti läbi viidud uuringud näidanud, et teadlikkus küberohtudest on tõusmas ning esimesed tõsisemad küberrünnakud ja –juhtumid on pannud ettevõtjaid oma riske ümber hindama (KMPG 2016). Seetõttu süvenes autori soov uurida, kuivõrd tuttavad on Eesti laevaomanikud sektoris varitsevate küberohtudega ning kas ja milliseid samme on ette võetud, et neid riske vähendada.

Autor püstitab oma töös hüpoteesi, et Eesti laevandusettevõtetes ei ole küber-turvalisusele piisavalt tähelepanu pööratud ning see on endaga kaasa toonud kahjujuhtumeid ettevõtete jaoks. Kahjud võivad olla vigastused laevale, kaubale või meeskonnaliikmetele, keskkonnareostus, ettevõtte andmete lekkimine ning maine kahjustumine, märkimisväärne finantsiline kahju vms.

Magistritöös kasutatud peamiseks uurimismeetodiks on valitud küsitlusuuring, mis viiakse läbi Eesti laevaomanike seas. Autor toob oma magistritöös välja ka soovitused, millised võimalused on laevaomanikel olemas küberriskide vähendamiseks.

Magistritöö struktuur

Tulenevalt magistritöö temaatikast on autor jaganud käesoleva töö kolmeks peatükiks. Esimeses peatükis annab autor kokkuvõtliku ülevaate laevanduse arengust ning käsitleb küberturvalisust ja laevandussektoris varitsevaid küberohtusid. Teine peatükk keskendub Eesti laevaomanike seas läbi viidud küsitlusele ja selle tulemustele ning kolmandas peatükis tuuakse välja soovitused, kuidas laevaomanik suudaks võimalikke küberriske maandada ning tekkivaid kahjusid ära hoida või vähendada.

Käesoleva uurimise tulemustest võib kasu olla eelkõige laevaomanikele ja sadama-operaatoritele, aga ka tulevikus sarnaste uuringute läbiviijatele. Autor ei välista ka võimalust, et jätkab õpinguid Tallinna Tehnikaülikooli ja Tartu Ülikooli juurde loodud küberkaitse magistriõppes ning käsitleb küberturvalisuse teemat laevanduses edasi oma järgmises magistritöös.

Magistritöö autor tänab juhendajat Anatoli Alopit. Autor on tänulik ka heade nõuannete ja abi eest hr Enn Kreemile, Ronnie Jaanholdile ja Erkki Leegole, kes käesoleva töö valmimisele on kaasa aidanud. Samuti tänab autor kõiki laevandusettevõtete esindajaid, kes vastasid magistritöö küsimustikule. Lõpetuseks tänab autor oma abikaasat, kelle toetuseta ei oleks see magistritöö valminud.

1. LAEVANDUSSEKTOR JA KÜBERTURVALISUS

Järgnevas peatükis annab autor ülevaate laevandussektori hetkeolukorrast ja arengutest ning selgitab, mis on küberturvalisus ning kuidas see mõjutab laevandussektorit.

1.1 Laevandus maailmas

Nagu autor sissejuhatuses mainis, siis ligi 90% maailma kaubavedudest tehakse merd mööda (International Chamber of Shipping 2017). Kaubalaevastikku omab üle 150 riigi (CIA 2010) ning kokku töötab laevadel ligikaudu 1 647 500 meremeest (BIMCO, ICS 2015). Seoses maailmalaevastiku kasvuga suureneb vajadus ka laevapersonali järele (vt Tabel 1). BIMCO ja ICS poolt 2015. aastal läbiviidud uuringust selgus, et laevaohvitseride puudujääk suureneb järgnevate aastatega ulatused 2025. aastal juba 147 500 ohvitserini (Ibid.).

Tabel 1. Laevaohvitseride hinnanguline tulevikuvajadus 2015–2025

	2015	2020	2025
Olemasolev tööjõud	774 000	789 500	805 000
Tulevikuvajadus	790 500	881 500	952 500
Puudujääk	-16 500	-92 000	-147 500

Allikas: (BIMCO, ICS 2015)

Laevandus on ka üks esimesi sektoreid maailmas, kus rakendati ülemaailmselt kasutusel olevaid rahvusvahelisi regulatsioone. Nende väljatöötamine ja rakendamine on reeglina toimunud peale tõsisemaid laevaõnnetusi, mis on kaasa toonud kas suured inimohvrid või ulatusliku keskkonnareostuse.

Alljärgnevalt on ära toodud mõned laevaõnnetused, mis mõjutasid riike ja organisatsioone suurendama turvalisust ja ohutust laevadel:

a) RMS Titanic – uppumatuks loetud reisilaev põrkas 1912. aastal Atlandi ookeanis kokku jäämäega viies endaga merepõhja 1517 inimest. Selle laevaõnnetuse järgselt töötati välja ning võeti vastu 1914. aastal Rahvusvaheline konventsioon inimelude ohutusest merel (SOLAS - *The International Convention for the Safety of Life at Sea*).
b) SS Morro Castle – tulekahju 1934. aastal teekonnal Havannast New Yorki nõudis 137 reisija ja meeskonnaliikme elu. Toimunud õnnetus sundis konventsiooni üle vaatama ning sisse viima uued ja rangemad tuleohutust puudutavad reeglid laevaehituses ja meeskondade väljaõppes.
c) SS Torrey Canyon – tankeri madalikule sõitmine Inglismaa edelarannikul 1967. aastal põhjustas suure keskkonnareostuse Inglismaa lääneranniku l ja Prantsusmaa põhjarannikul. Juhtunud katastroof andis tõsise tõuke rahvusvahelise koostöö tõhustamisele merekeskkonna reostamise vältimise, vähendamise ja kontrolli valdkonnas. Rahvusvaheline konventsioon tsiviil-vastutusest naftareostusest põhjustatud kahjustuste korral (CLC - *The International Convention on Civil Liability for Oil Pollution Damage*) võeti vastu 1969. aastal ja jõustus 1975. aastal ning rahvusvaheline laevade põhjustatava merereostuse vältimise konventsioon (MARPOL - *The International Convention for the Prevention of Pollution from Ships*) jõustus 1983. aastal.
d) Tanker Amoco Cadiz – laev sõitis madalikule, murdus mitmeks osaks ja uppus mõne miili kaugusel Prantsusmaa põhjarannikust 1978. aastal. Laevaõnnetus andis sisendi MARPOLi uuendustele ning tõuke Pariisi vastastikuse mõistmise memorandumi (Paris MOU) loomiseks ja sadamariigi laevakontrolli (*Port State Control*) asutamiseks.
e) MS Herald of Free Enterprise – 1987. aastal Zeebruggest lahtise vööriluugiga väljunud autopraam uppus mõne minuti jooksul peale sadamast väljumist. Uppus 193 reisijat ja meeskonnaliiget. Antud juhtum tõstatas küsimuse, kuidas oli selline õnnetus võimalik vaatamata sellele, et ainult seitse aastat varem ehitatud laev oli varustatud kaasaegsete seadmetega ning mehitatud

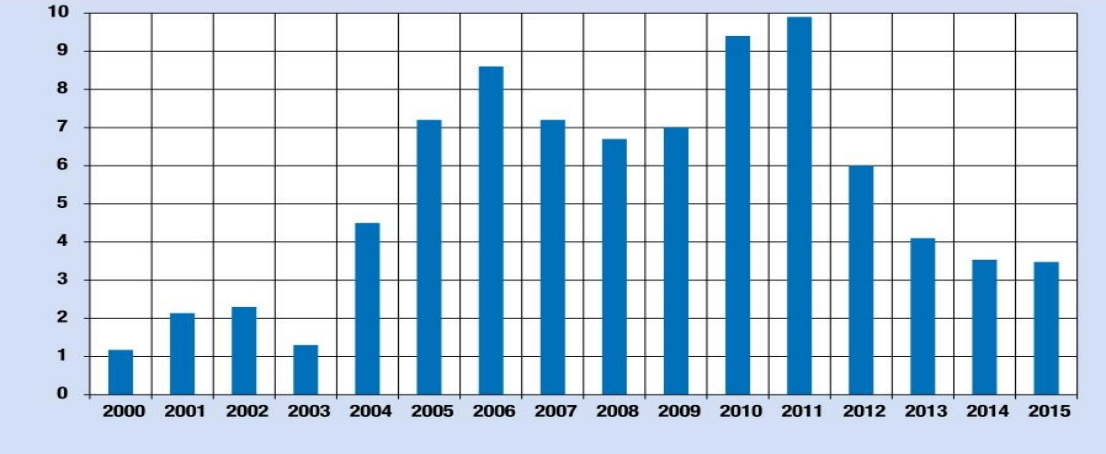
professionaalse meeskonnaga. Õnnetus autopraamiga Herald of Free Enterprise andis tõuke Rahvusvahelise meresõiduohutuse korraldamise koodeksi (*ISM Code*) ja meresõiduohutuse korraldamise süsteemi väljatöötamiseks.

f) Tanker Exxon Valdez – 1989. aastal Alaska rannikul madalikule sõitnud tanker põhjustas suure merereostuse, kui 40000 tonni toornaftat valgus merre. Pärast seda õnnetust võeti vastu Ameerika Ühendriikides naftareostuse seadus (OPA 90), mis muuhulgas keelas ühekerelistel tankeritel siseneda USA sadamatesse.

g) Ro-ro parvlaev Estonia – 1994. aastal Läänemeres toimunud õnnetus tõi endaga kaasa mitmed muudatused ro-ro parvlaevade konstruktsioonile.

h) Tanker Erika (1999) ja tanker Prestige (2002) – kahe laevaga juhtunud õnnetused Prantsusmaa ja Hispaania rannikute lähedal reostasid ulatuslikult ümbruskonna rannad ning halvasid pikaks ajaks kohaliku majanduse. Õnnetused andsid tõuke ühepõhjaliste tankerite keelustamisele lähitulevikus ning tekitasid aluspinnase Euroopa Meresõiduohutuse Ameti (EMSA - *European Maritime Safety Agency*) loomiseks.

Kiire areng laevaehituses ning tehnoloogias on võimaldanud ehitada aina suuremaid, võimsamaid, ökonoomsemaid ja kiiremaid laevu. See on muutnud kauba transportimise laevadega odavamaks ja kiiremaks. Kaubalaevade kandevõime maht maailmas suureneb iga aastaga. 2015. aastal suurenes kandevõime maht 12 kuuga 3,48%, mis on ligikaudu 1,8 miljardit tonni (vt Joonis 1).



Joonis 1. Laevastiku kasv maailmas 2000-2015 (kandevõime mahu tõus protsentuaalselt)
Allikas: (Review of Maritime Transport 2016, 30)

Antud lõputöö kirjutamise hetkel andis Lõuna-Korea laevaehitaja Daewoo Shipbuilding & Marine Engineering üle maailma ühe suurema konteinerlaeva Madrid Maersk, mille pikkus on 399 meetrit, laius 58 meetrit ning mahutavus 20 568 TEU'd (vt Joonis 2). Laevandusettevõte Maersk Line tellis üksteist selle klassi (*2nd generation Triple-E*) laeva. (Maersk Line 2017)

Joonis 2. Maailma suurim konteinerlaev Madrid Maersk
Allikas: (Maersk Line)

12. mail 2017. aastal ristiti pidulikult Samsung Heavy Industries (SHI) laevatehases konteinerlaev OOCL Hong Kong mahutavusega 21 413 TEU'd. See laev on lõputöö kirjutamise hetkel maailma suurim konteinerlaev. Laeva pikkus on 399,87 m ja laius 58,8 m. Orient Overseas Container Line (OOCL) tellis kuus selle klassi laeva.

See on juba kolmas konteinerlaev, mis on paari kuu jooksul ületanud 20 000 TEU piiri. Eelnevad olid MOL Triumph (20 150 TEU) ja ülalmainitud Maersk Madrid (20 568 TEU).

1.2 Laevanduse olukord Eestis

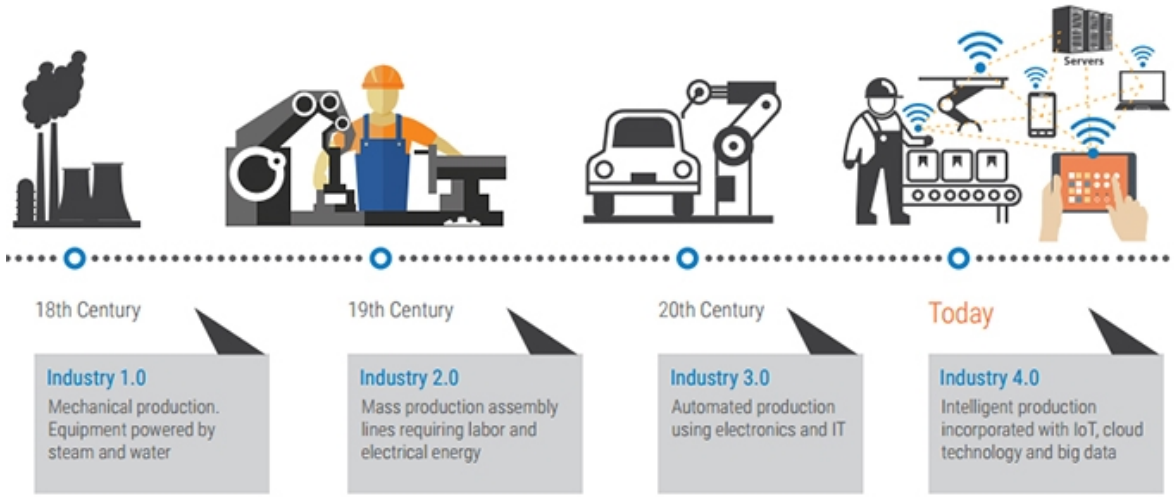
Eesti lipu all sõitvate kaubalaevade arv on viimased kümme aastat olnud langustrendis. Kui 2003. aastal oli Eesti lipu all veel 17 kaubalaeva, siis 2012. aastal oli see näitaja vaid 8. Viimane kaubalaev üle 500 GT lahkus Eesti lipu alt mõned aastad tagasi. Loodetavasti on olukord paranemas tulevikus, kui realiseerub Veeteede Ameti plaan laevade Eesti lipu alla toomiseks. Samas soovib autor rõhutada, et Eesti laevaomanikud ega laevad ei ole kuhugi kadunud, vaid edasi opereeritakse juba välislippude all (Küpros, Malta, Panama jt), kus laevaomanikele pakutakse soodsamaid tingimusi. Kui Eesti lippu kandva kaubalaevastiku olukord vajab kõrgendatud tähelepanu Eesti valitsuse poolt, siis reisilaevandus on näidanud kasvutrendi. Tänu AS Tallink Grupi ja TS Laevad OÜ investeeringutele sõidavad Läänemerel ja saartevahelistel liinidel Eesti lipu all täna uued ja moodsad laevad.

1.3 Autonoomsed laevad

Lloyd's Register, ettevõte QinetiQ ja Southamptoni ülikool avaldasid 2015. aastal visiooni võimalikest tehnoloogilistest arengutest aastaks 2030 (Global Marine Trends 2030). Uuring hõlmas kommertslaevandust, sõjalaevandust ja mereruumi kasutust. Kokku hinnati 56 tehnoloogiat, millel võib olla arengupotentsiaali merendussektoris. Nendest valiti välja 18, mis jõuavad kõige tõenäolisemalt lähitulevikus tarbijateni. Hindamise kriteeriumideks olid äriline teostatavus, turustatavuse potentsiaal ning positiivne mõju uuendustele. Lloyd's Register valis neist välja kaheksa tehnoloogiat, mis hakkavad mõjutama kommertslaevandust kõige enam lähitulevikus. Nendeks on (Ibid.):

1) uued kõrgtehnoloogilised materjalid,
2) suurandmete analüütika,
3) robootika,
4) sensorid,
5) satelliitside,
6) integreeritud laevaehitus,
7) hübriidsed käitursüsteemid,
8) targa laeva projektid.

Uuringust ilmneb, et targad laevad on laevandussektori järgmine tehnoloogiline revolutsioon. Neljas tööstusrevolutsioon ehk Tööstus 4.0 (*Industry 4.0*) võimaldab tarkadel seadmetel asendada inimeste rolli protsesside ja seadmete juhtimisel ja optimeerimisel (vt Joonis 3). Sellest tulenevalt mängivad olulist rolli ka uuringus välja toodud tehnoloogiad, mida rakendatakse tarkade laevade välja töötamisel (robootika, sensorid, suurandmed, satelliitside ja kõrgtehnoloogilised materjalid).



Joonis 3. Tööstusrevolutsioon 1.0 – 4.0 (inglise keeles)
Allikas: (BCM Advanced Research, bcmcom.com/solutions_application_industry40.htm)

Arengut liikumisel autonoomsete laevade poole nähakse uuringus kahes etapis. Lühi- kuni keskpikas perspektiivis toimub areng digitaalselt laevanduselt intelligentsema poole. Selles protsessis omavad suurt rolli suurandmete analüütika ja satelliitside, mis lubavad laevade ehitamisel, hooldamisel ja ekspluateerimisel rakendada reaalajas arukaid ning ennetavaid meetmeid. Keskpikas ja pikas perspektiivis toimub areng intelligentselt laevanduselt autonoomsele laevandusele. Siin mängivad suurt rolli sensor- ja robootika-tehnoloogia, mis võtavad töö üle praegustelt inimoperaatoritelt. See võimaldab järkjärgult üle minna nn poolautomaatsetele laevadele, kus enam pole vajadust näiteks laevamehaanikute järele laeva pardal ning kaugemas plaanis kasutusele võtta juba täisautonoomsed laevad, mille puhul kontrolli ja juhtimist teostatakse kaldalt. Seda toetavad tööstusrevolutsiooni 4.0 põhikomponendid on ära toodud joonisel 4.

Joonis 4. Tööstusrevolutsioon 4.0 põhikomponendid
Allikas: (BCM Advanced Research, bcmcom.com/solutions_application_industry40.htm)

Seetõttu ei saa Lloyd's Registri poolt ära nimetatud kaheksat tehnoloogiat vaadelda kui eraldiseisvaid, üksteisest isoleeritud tehnoloogiaid. Kõik need on omavahel seotud ja integreeritavad.

Kui vaadelda tulevikuprognoose küberturvalisuse seisukohalt, siis esitab see nii laeva- kui ka infotehnoloogiainseneridele suured väljakutsed. Informatsiooni võrgustikud ning info juhtimine ja haldamine muutub laevanduses üliolulisek. Süsteemid on vaja ehitada selliselt, et need suudaksid iseseisvalt vastu pidada välistele sissetungidele nagu viirused, küberterrorism ja küberpiraatlus. Informatsiooni haldamine ja kaitsmine toob tõsiseid katsumusi laevandusettevõtetele.

2017. aasta veebruaris Londonis toimunud iga-aastasel avamere (*offshore*) teemalisel konverentsil *Annual Offshore Support Journal Conference 2017* tutvustasid merendussektoris tuntud ettevõtted nagu Kongsberg Maritime, Rolls-Royce, Damen Shipyards ja DNV GL oma ootuseid autonoomsete laevade osas. Nimelt on Kongsberg Maritime kõige lähedamal sellele, et vette lasta maailma esimene autonoomne laev Hrönn (Automated Ships Ltd...2016). Koostöös Suurbritannia ettevõttega Automated Ships Ltd projekteeritakse ja ehitatakse laev Norras ning ekspluatatsiooni loodetakse alus saata juba 2018. aastal (vt Joonis 5).

Joonis 5. Mehitamata ja täisautonoomne laev Hrönn
Allikas: (Kongsberg Maritime)

Laeva testimispiirkonnaks on Norra linna Trondheimi lähedal asuv fjord, mis 2016. aasta sügisel avati maailma esimese veealana mehitamata veesõidukite testimiseks. Kongsberg Maritime oli üks olulisemaid ettevõtteid selle eripiirkonna avamisprotsessis.

Esimese autonoomse laeva tööülesanneteks saavad olema energiasektori avamererajatiste teenindamine, hüdrograafilised tööd ja teaduslikud uuringud ning kalafarmide teenindamine. Samuti on Hrönn võimeline toimima allveerobotite (ROV – *remotely operated vessel*) ja (AUV – *autonomous underwater vehicle*) baaslaevana ning vedama ka kergemakaalulist kaupa avamererajatistele.

2017. aasta mais sõlmisid Kongsberg ja Norra väetisetootja YARA kokkuleppe maailma esimese null-emissiooni ja täisautomaatse fiiderlaeva ehitamiseks (YARA and Kongsberg...2017). YARA Birkeland alustab opereerimist Breviku ja Larviku sadamate vahel 2018. aasta teises pooles. Esialgu alustab laev tööd mehitatud meeskonnaga. Täisautonoomselt hakkab laev töötama aastal 2020. Laeva mahutavus on 100–150 TEU. Kauba laadimine ja lossimine hakkab elektrikraanasid kasutades toimuma automaatselt. Lisaks varustatakse laev automaatse sildumissüsteemiga. Esialgsete andmete järgi on laeva pikkus kuni 70 m ja laius 15 m ning ekspluatatsiooniline kiirus hakkab olema 6 sõlme.

1.4 E-navigatsioon

Digitaalse maailma sisenemine laevandusse toob endaga kaasa ka uued võimalused mereinformatsiooni paremaks ärakasutamiseks meresõiduohutuse seisukohast. See võimaldab ohutumat ja turvalisemat meresõitu ning vähendab riske merekeskkonnale.

Aastatel 2009-2011 osales lõputöö autor Veeteede Ameti esindajana Läänemere piirkonna riikidevaheline koostöö programmi 2007-2013 raames (*Baltic Sea Region Programme 2007-2013*) rahvusvahelises lipuprojektis EfficienSea (www.efficiensea.org), mille üheks ülesandeks oli välja töötada erinevate e-navigatsiooni teenuste prototüübid.

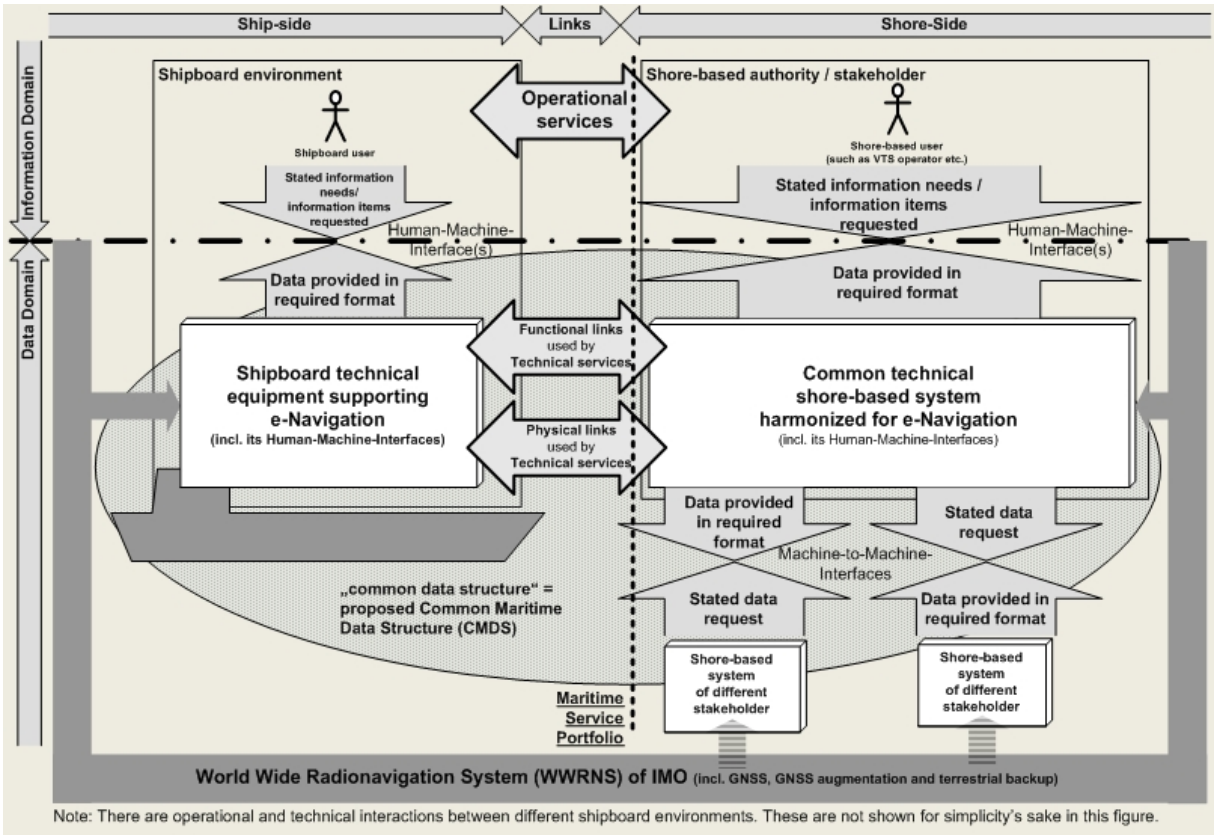
E-navigatsioon on meresõiduks vajaliku informatsiooni kogumise, edastamise, analüüsi ja esitamise kooskõlaline integreerimine elektroonikavahendite abil laeva pardal ja maal selleks, et parandada meresõidu ja vastavate maapealsete teenistuste kvaliteeti ning meresõidu ohutust, turvalisust ja merekeskkonna kaitset. (E-navigation 2017)

Rahvusvaheline Mereorganisatsioon (IMO) kinnitas 2014. aasta novembris e-navigatsiooni strateegia rakendusplaani (SIP – *The e-navigation Strategy Implementation Plan*). See dokument sisaldab hulka ülesandeid, mis on vajalikud e-navigatsiooni viie olulise tingimuse täitmiseks (Ibid.):

1) täiustatud, kooskõlastatud ja kasutajasõbralik laevasilla tehniline lahendus,
2) standardiseeritud ja automatiseeritud raporteerimissüsteem,
3) laevasillaseadmete ja navigatsiooniinfo täiustatud töökindlus ja terviklikkus,
4) erinevate sidevahendite kaudu kättesaadava informatsiooni integratsioon ja esitamine kuvaritel,
5) täiustatud laevaliikluse korraldamise süsteemi (VTS – *vessel traffic service*) teenuste pakkumine sidevahendite abil.

IMO loodab, et 2019. aastaks on ülaltoodud tingimuste täitmiseks lahendused leitud ning organisatsioon on võimeline avaldama kooskõlastatud informatsiooni e-navigatsiooniga seotud toodete ja teenuste projekteerimiseks.

Joonisel 6 (inglise keeles) võib näha IMO poolt viimase paari aasta jooksul välja töötatud kasutaja vajaduste ja võimalike e-navigatsiooniteenuste kokkuvõtet.



Joonis 6. E-navigatsiooni võimalikud teenused ja kasutajate vajadused (inglise keeles)
Allikas: (International Maritime Organization)

Autor on veendunud, et e-navigatsiooni lahenduste väljatöötamisel on küberturvalisus väga olulise tähtsusega ning see peab olema seatud teenuste loomisel kesksele kohale. Erinevate süsteemide omavaheline vastastikune seotus e-navigatsiooni teenuste puhul tõstab ka küberrünnakute riski. Selle probleemi lahendamisega tegeleb hetkel EL teadusuuringute ja innovatsiooni raamprogrammist Horisont 2020 rahastuse saanud jätkuprojekti EfficienSea2 (http://efficiensea2.org), kus osaleb ühe partnerina ka Eesti Veeteede Amet.

Autor sai lõputöö kirjutamise ajal kinnituse projekti EfficienSea 2 liikmelt, et küber-turvalisus on olulisel kohal. Projekti raames arendatakse välja uudne lahendus *Maritime Cloud* (http://maritimecloud.net), mis võimaldab turvalist, efektiivset ja usaldusväärset informatsioonivahetust merendussektoris. Lahenduse kontseptsioon on ära toodud joonisel 7 (inglise keeles).

Joonis 7. *Maritime Cloud* kontseptsioon (inglise keeles)
Allikas: (www.efficiensea2.org)

1.5 Küberjulgeoleku areng Eestis

Autori esimene kokkupuude arvutiviirusega leidis aset 1980. aastate lõpus, kui Loksa I Keskkool sai omale esimesed, „Estroni“ tehases valminud mikroarvutid „Juku“. Sellel ajal väga populaarse arvutimänguga „Indiana Jones“ kandusid edasi 5,25" diskettidega ka lihtsamad viirused. Suuremat rahalist kahju tõi autorile tõsisem kontakt arvutiviirusega CIH (ka *Chernobyl* või *Spacefiller*) 1998. aastal, mis hävitas arvuti BIOS'i. Oma looja, Chen Ing-hau järgi nime saanud viirus nakatas üle maailma ligi 60 miljonit arvutit tekitades kahju umbes 1,6 miljardit USA dollari väärtuses (Beck 2013).

Suurem diskussioon küberturvalisuse teemal tekkis Eestis ja ka terves maailmas kümme aastat tagasi, kui 2007. aasta aprillis ja mais peale nn Pronkssõduri teisaldamist Tallinna kesklinnast Kaitseväe kalmistule tabas Eestit ennenägematu küberrünnak. Suuremahulised teenusetõkestusrünnakud pandi toime Eesti valitsusasutuste, pankade ja päevalehtede veebilehtede vastu. Kolmenädalane küberrünnakute laine NATO liikmesriigi vastu oli organiseeritud rünnak, mis pärines Botnet-võrgustiku vahendusel IP-aadressidelt Venemaal, Jaapanis, Hiinas, Egiptuses ja USAs. F-Secure eksperdi Mikko Hyppöneni sõnul võis küberrünnak olla hoiatus, tekitamaks eestlastes hirmu. Kui eesmärk oleks olnud

korraldada tõeline kübersõda Eesti vastu, siis oleks sihtmärgiks võetud sõjaväe süsteemid (Boyd 2010).

Peale 2007. aasta küberintsidente on küberjulgeolek ja küberkuritegevuse vastane võitlus olnud Eesti jaoks põhiprioriteetide hulgas. Küberjulgeoleku strateegia 2014-2017 kiideti heaks 2014. aastal. Peamised valdkonnad, millele küberjulgeoleku strateegia keskendub, on elutähtsate teenuste tagamine ja küberkuritegevuse vastase võitluse tõhustamine ning riigi kaitsevõimete arendamine. Täiendavad nende eesmärkide saavutamiseks kavandatud meetmed on õigusraamistiku vormimine, rahvusvahelise koostöö ja kommunikatsiooni edendamine, teadlikkuse suurendamine ning spetsialistide väljaõppe tagamine ja samuti tehniliste lahenduste arendamine. (MKM 2014)

Majandus- ja Kommunikatsiooniministeerium (MKM) koordineerib küberjulgeoleku strateegia elluviimist Vabariigi Valitsuse julgeolekukomisjoni juurde 2009. aastal loodud küberjulgeoleku nõukogu kaudu. Selle ülesanne on aidata kaasa ametkondade koostöö toimimisele ja teha järelevalvet küberjulgeoleku strateegia eesmärkide elluviimise üle.

Riigi Infosüsteemi Ametile (RIA) anti 2010. aastal valitsusasutuse staatus ning ametile anti volitused ja vahendid riigi info- ja kommunikatsioonitehnoloogia (IKT) infrastruktuuri kaitse korraldamiseks ning infosüsteemide turvalisuse üle järelevalve teostamiseks. 2010. aastal käivitas RIA kriitilise informatsiooni infrastruktuuri kaardistamise projekti, mille käigus tuvastati elutähtsate teenuste sõltuvused infosüsteemidest. Selle põhjal töötati välja turvanõuded riigi toimimiseks vajalikele elutähtsatele infosüsteemidele.

2011. aastal moodustati riigi- ja erasektori koostöö arendamiseks kriitilise informatsiooni infrastruktuuri kaitse komisjon (KIIK). Elutähtsat teenust osutavate asutuste küberturbe- ja IT-juhte koondava komisjoni tegevuse eesmärk on vahetada operatiivselt teavet, tuvastada probleeme ning teha ettepanekuid riigi elutähtsa infrastruktuuri küberjulgeoleku parandamiseks.

2012. aastal koondati Politsei- ja Piirivalveameti (PPA) küberkuritegude uurimise võimekus ühte talitusse. Samuti on loodud PPA juurde veebikonstaabli ametikohad, kelle ülesandeks on tõsta inimeste teadlikkust interneti turvalisusest ning kaitsta lapsi ja noori internetis.

2011. aastal loodi Eesti küberruumi kaitsmiseks Kaitseliidu küberkaitse üksus (KKÜ), mille liikmeteks on vabatahtlikud IT-spetsialistid. KKÜ missioon on kaitsta Eesti

kõrgtehnoloogilist eluviisi, kaitstes informatsiooni infrastruktuuri ning teostades seeläbi laiapõhjalise riigikaitse eesmärke. (Kaitseliit 2017)

Küberjulgeoleku valdkonna peamine koolitaja ja teadlikkuse tõstja Eestis on Hariduse Infotehnoloogia Sihtasutus (HITSA), kes korraldab koolitusi juba eelkooliealistele ja vanematele lastele.

2009. aastal avati Tallinna Tehnikaülikooli ja Tartu Ülikooli koostöös rahvusvaheline küberkaitse magistriõppekava ning 2014. aastal avati Tallinna Tehnikaülikooli Küber-kriminalistika ja Küberjulgeoleku Keskus.

1.6 Küberturvalisuse mõiste

Küberturvalisuse all võib lühidalt mõista tehnoloogiate, protsesside ja harjumuste kogumit, mis on mõeldud võrgu- ja infosüsteemide, arvutite ja andmete kaitseks rünnakute, vigastuste või keelatud ligipääsu vastu. Kübermaailmaga on meie igapäevane elu väga tihedalt seotud. Me kasutame nutitelefone, arvuteid, nutikaid televiisoreid, suhtleme avatult sotsiaalmeedias, laadime üles fotosid ja dokumente, loeme ja saadame päevas kümneid ja kümneid e-kirju. Kui kasutaja arvab, et teda see teema ei puutu ning temaga midagi ei juhtu, siis ta eksib. Küberrünnakute ohvriteks võivad sattuda nii eraisikud, ettevõtted kui ka riigid. Kui 2016. aastal oli internetiga seotud üle 3,4 miljardi inimese, siis aastaks 2025 ennustatakse, et see arv tõuseb 5 miljardini. Selline massiline internetiga ühendumine soodustab plahvatuslikku uute teenuste, rakenduste ja seadmete loomist ja internetiga ühendamist. Võttes arvesse senist esemevõrgu (IoT – *Internet of Things*) arengut ja tehnoloogia evolutsiooni ning majanduse ja demograafia trende, hinnatakse 2025. aastaks esemevõrgu majanduslikku mõju 3,9 – 11,1 trillionit dollarit aastas (McKinsey Global Institute 2015).

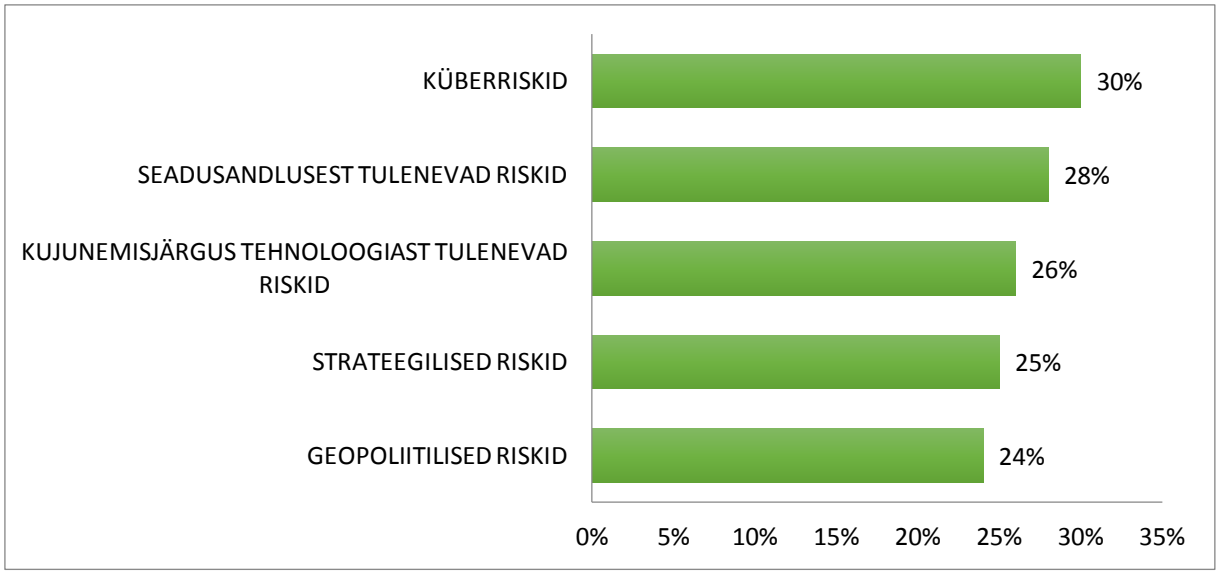
Samal ajal, kui digitaliseerumine, arenev esemevõrk, pilveteenused ja suurandmed pakuvad uusi võimalusi teenuste arendamiseks ning protsesside reaalajas jälgimiseks ja optimeerimiseks, toovad need endaga kaasa ka uued ja täiendavad turvaohud suurendades süsteemse riski keerukust. Kuna esemevõrk toimib justkui sillana kübermaailma ja füüsiliste süsteemide vahel, võib rikutud või tahtlikult moonutatud esemevõrk põhjustada enamat, kui ainult andmete kadumist või hävimist. Halvemal juhul võib see halvata olulisi tööprotsesse ja teenuseid ning tekitada vigastusi inimestele.

Mõningaid näiteid selle kohta võib tuua lähiminevikust:

a) 2010. aastal nakatati Iraani tuumaelektrijaama arvutid viirusega, mis manipuleeris tsentrifuugide kiirust kontrollivaid Siemens arvutisüsteeme ja lõhkus arvutite kontrollitud seadmeid. Stuxnet'i nimeline viirus toodi sisse USB mälupulgaga. Viiruse koodi keerukust hinnates arvavad eksperdid, et sellise rünnaku taga sai olla riik, mitte üksik küberkurjategija (Schneier 2010).
b) Ukrainas langesid mitmed energiaettevõtted (kriitiline infrastruktuur) küberrünnaku alla 23. detsembril 2015. aastal. Koordineeritud rünnak Ukraina kriitilise infrastruktuuri vastu jättis ligi 700 000 tarbijat külmal perioodil elektrita (Groll 2016).
c) Maailma kõige ulatuslikum küberrünnak leidis aset 12. mail 2017. aastal. Lunavara nimega WannaCry nakatas ligi 150 riigis üle 200 000 masina nõudes andmete tagasisaamiseks lunaraha. Muuhulgas oli tugevasti häiritud Suurbritannia tervishoiusüsteem ning erinevate riikide pankade ja telekommunikatsiooniettevõtete toimimine.

Uuringud on näidanud, et paljude ettevõtete juhid on hakanud mõistma, et küberturvalisus on midagi, mida ei saa ega tohi ignoreerida. Teadlikumad ettevõtted on võtnud kasutusele ennetavad meetmed ja koolitanud oma personali, et kaitsta oma võrgu- ja infosüsteeme võimalike rünnete vastu. Sellised sammud võivad olla mingil määral piisavad, kuid toimunud küberintsidendid näitavad, et isegi kõige suuremad ja küberturvalisusesse suuri investeeringuid teinud ettevõtted ei suuda vastu panna järjekindlale ja hästi rahastatud rünnakule.

KPMG poolt 2016. aastal ligi 1300 tegevjuhi seas läbi viidud uuring näitas, et kõige suuremaks riskiks oma ettevõtte vastu näevad nad täna küberturvalisusest tulenevaid riske (Now or never...2016). Viie kõige suurema riski jagunemine on ära toodud joonisel 8.



Joonis 8. Viis suuremat riski ettevõtjate jaoks
Allikas: (2016 Global CEO Outlook, KPMG International)

Tänapäeva kiirelt arenevas digitaalses maailmas on võimalus pahavaraga nakatuda aina suurem. Eriti näitavad tõusutrendi lunavara kaudu erinevad väljapressimised. E-kirjade ja veebilehtede kaudu leviv lunavara pakkus 2016. aastal palju kõneainet nii maailmas kui ka Eestis.

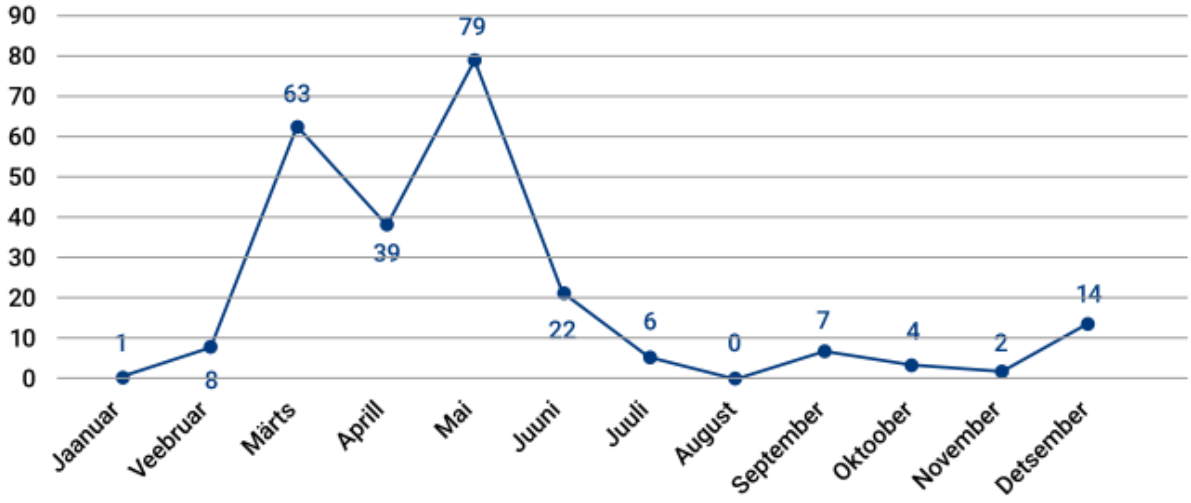
12. mail 2017. aastal üle maailma puhkenud ulatuslik lunavaraga nakatumine puudutas ca 200 000 seadet ligikaudu 150 riigis (Goldman 2017). Küberrünnaku alla sattusid haiglad, sideoperaatorid, autotootjad, pangad, energiafirmad, raudteefirmad, riigiasutused jt. Ajaloo suurim lunavararünnak viidi läbi kasutades krüptolunavara WannaCry (või Wcry), mida seostatakse USA riikliku julgeolekuameti (NSA – *National Security Agency*) serveritest häkkimise käigus varastatud informatsiooniga turvaaukudest SMBv1 protokollis.

Tüüpiline lunavara saadetakse tavaliselt ühele isikule. E-kiri on reeglina korrektselt kirjutatud ja vormistatud ning sisaldab manusena kas CV-d, arvet või muud usaldusväärsena näivat dokumenti. Kui selline manuses olev lunavara sisaldav dokument avada, siis krüpteerib käivitunud fail arvutis ja ligipääsetavatel võrguketastel asuvad failid. Seejärel teavitatakse arvutikasutajat, kuidas on võimalik osta andmete lahtikrüpteerimiseks vajalik võti. Juhul, kui ohver etteantud tähtajaks lunaraha ei maksa, jäävad failid kättesaamatuks (vt Joonis 9).

Joonis 9. Pahavara CryptoLocker infoaken
Allikas: (http://myspybot.com/)

Lunavara levitajaks on sageli „elukutselised" kurjategijad ning kuna nende tulu sõltub nende töö professionaalsusest, on lunavara sisaldavad e-kirjad tihtipeale hästi koostatud, need mõjuvad legitiimsena ning kirja saatja kasutab ära organisatsiooni tavapäraste tööprotsesside toimimist – näiteks arvete saatmist meilitsi. Viirustõrjest möödapääsemiseks töötatakse lunavarast välja uusi versioone. Neil põhjustel ei ole lunavaraga nakatumist võimalik alati vältida. Seda enam on oluline, et kasutaja oleks lunavaraohtudest teadlik ning käituks vastutustundlikult nii isiklikke kui tööseadmeid kasutades. (Riigi Infosüsteemi Ameti küberturvalisuse...2016)

Joonisel 10 on näha, et CERT-EE poolt registreeritud lunavaraintsidentide kõrgaeg Eestis jäi 2016. aasta kevadesse.



Joonis 10. CERT-EE registreeritud lunavaraintsidendid Eestis 2016
Allikas: (Riigi Infosüsteemi Amet)

Ettevõtetel on võimalik ära hoida kulukaid lunavaraintsidente. See eeldab lihtsate, kuid toimivate tegevuste järgimist (The Ultimate Checklist...2016):

a) tee oma andmetest varukoopiaid;
b) uuenda regulaarselt tarkvara;
c) koolita oma töötajaid ära tundma võimalikke küberohtusid;
d) kaitse oma ettevõtte (side)võrkusid;
e) segmenteeri ligipääsu ettevõtte võrkudele;
f) jälgi ettevõtte võrguliiklust;
g) tõkesta pahavara sissetung rakendades ennetavaid meetmeid;
h) piira seadmete kasutust ettevõtte sisevõrgus ja rakenda minimaalõiguste printsiipi;
i) ole kursis, millised ohud kübermaailmas varitsevad;
j) ütle „EI“ väljapressimistele.

Ülalnimetatud meetmete rakendamine eeldab autori hinnangul ettevõtte juhtkonna pühendumist küberkaitsele ning samuti probleemide olemasolu teadvustamist. Kui vaadata soovitust „a) tee oma andmetest varukoopiaid“, siis tihtipeale ettevõtted seda ei järgi ning sellisel juhul ei jää muud üle, kui alluda küberkurjategijate nõudmistele ning maksta olulise

informatsiooni tagasisaamiseks lunaraha, mis võib jääda 500 kuni 100 000 dollari vahele. Erinevate raportite hinnangul maksab ligi 30-40% ettevõtetest lunaraha ära.

2016. aastal avastati ligi 638 miljonit lunavarajuhtumit, mille puhul ainult 42% ohvriks langenud ettevõtetest olid võimelised taastama kaotatud informatsiooni varukoopiatelt. Võrreldes aastaga 2015 tõusis avastatud lunarahajuhtumite arv koguni 167 korda. (SonicWall 2017)

1.7 Küberturvalisus laevandussektoris

Küberrünnakutest ei ole jäänud puutumata ka transpordisektor. Digitaalse tehnoloogia arenguga on muutunud sihtmärgiks ka laevad. Põhjuseid, miks korraldada küberrünnakuid transpordisektori vastu, on mitmeid. Kuna kaupade liikumine sõltub suuresti erinevatest transpordiliikidest, siis on võimalik rünnakutega mõjutada kaubavedu üldiselt või suunata rünnakud spetsiifilise kauba või transpordiliigi vastu. Rünnakud raudtee vastu võivad pidurdada või peatada kaupade jõudmise sadamatesse. Sadama vastu suunatud rünnakud võivad halvata kaupade sisse- ja väljaveo riigist. Turismisektorit on lihtne negatiivselt mõjutada küberrünnakutega lennujaamade vastu.

Küberrünnakuid laevanduse vastu võib vaadelda kui moodsat mereblokaadi. Ainus vahe on selles, et täna kulub blokaadi tekitamiseks ainult murdosa sellest, mis kulus 100-200 aastat tagasi. Samas on ka saavutatud kasu või tekitatud kahju palju suurem. Vaatamata sellele, et laevandus on üks vanemaid tööstussektoreid maailmas, on sadamate ja kaubalaevade tehnoloogiline mahajäämus küberturvalisuse valdkonnas võrreldes teiste sektorite infosüsteemidega ligi 10-20 aastat.

Informatsiooni küberrünnakute kohta laevanduse ja transpordisektori vastu üldisemalt on vähe. Põhjus võib peituda selles, et ettevõtted ei ole huvitatud teavitama avalikkust ega vastavaid ametkondi toimunud intsidentidest oma maine säilitamiseks ja sellest tulenevate võimalike täiendavate finantsiliste kahjude vältimiseks (Wagstaff 2014).

Kui vaadata, millised grupid on laevanduses ohustatud küberrünnakute poolt, siis jagaks autor need järgmiselt: laev ja ohutu navigatsioon, automaatne identifitseerimise süsteem, satelliitside, radarisüsteemid ja kaupade jälgimise süsteem.

Alljärgnevalt toob autor ära infosüsteemid, andmed ja tehnoloogiad, mis võivad muuta laeva haavatavaks küberrünnakute puhul (The Guidelines on Cyber Security...2016):

1) Sidesüsteemid:
    a) satelliitside seadmed;
    b) IP-telefon (VoIP);
    c) traadita kohtvõrk;
    d) valjuhääldiside ja üldine ohusignalisatsioon.

2) Sillasüsteemid:
    a) positsioneerimissüsteemid (GPS jms);
    b) elektronkaartide kuvamise- ja infosüsteem (ECDIS);
    c) laeva dünaamiline positsioneerimise süsteem (DP);
    d) süsteemid, mis ühenduvad elektroonilise navigatsioonisüsteemi ja jõuning manööverdussüsteemidega;
    e) automaatne identifitseerimissüsteem (AIS);
    f) ülemaailmne merepääste ja –ohutussüsteem (GMDSS);
    g) radar;
    h) reisiinfo salvestussüsteemid (VDR);
    i) muud jälgivad ja andmeid koguvad süsteemid.

3) Jõu- ja elektriseadmete süsteemid:
    a) peamasina pöörete regulaatorid;
    b) toitehaldus;
    c) ühtne kontrollsüsteem;
    d) alarmsüsteemid;
    e) hädaolukordadele reageerimise süsteemid.

4) Ligipääsu kontrollsüsteemid:
    a) valvesüsteemid (nt sisetelevisioon CCTV);
    b) navigatsioonivahi alarmsüsteemid (BNWAS);
    c) laeva valvesignalisatsiooni süsteemid (SSAS);
    d) elektroonilised "personal-pardal" süsteemid.

5) Kaupade jälgimise süsteemid:
    a) kauba kontrollruum (CCR);
    b) taseme näidikusüsteemid;
    c) klappide kaugjuhtimisseadmed;
    d) vee sissepääsu alarmsüsteemid;
    e) ballastvee süsteemid;
    f) gaasi vedeldamine.

6) Reisijate teenindamise ja juhtimise süsteemid:
    a) varahaldusüsteemid (PMS);
    b) tervisekontrolli kaardid;
    c) reisijate ja meeskonnaliikmete pardalepääsu süsteemid;
    d) infrastruktuuri toetavad süsteemid nagu domeeninimede süsteem (DNS) ja kasutaja autentimise süsteemid.

7) Reisijatega seotud võrgud:
    a) reisijatele mõeldud WiFi või kohtvõrk
    b) reisijate meelelahutussüsteemid;
    c) kommunikatsioon.

8) Tuumiktaristu süsteemid:
    a) ruuterid;
    b) lülitid;
    c) tulemüürid;
    d) virtuaalsed privaatvõrgud (VPN);
    e) virtuaalsed kohtvõrgud (VLAN);
    f) sissetungi vältimise süsteemid;
    g) turvasündmuste logimise süsteemid.

9) Administratiivsed ja laeva meeskonnale mõeldud süsteemid:
    a) administratiivsed süsteemid;
    b) meeskonna WiFI või kohtvõrgud, kuhu nad saavad ühendada oma seadmed.

2016. aasta suvel IHS Markit ja BIMCO poolt läbi viidud uuring näitas, et tagasisidet andnud 300 merendussektoris tegutsevast ettevõttest 21% oli langenud küberrünnaku ohvriks ning 22% ei soovinud sellekohast informatsiooni avaldada (Good 2016). Uuring kestis neli nädalat ning küsitletute seas oli laevaomanikke (26%), sadamaid (2%), laevatehaseid (2%) ja teisi merendusega seotud ettevõtteid. Kõige tavalisemad rünnakutüübid olid kahjurvaraga nakatamine (77%), informatsiooni õngitsemine (57%), volituste vargus (25%) ja sihikindel kalastamine ehk harpuunimine (23%). Kui uuriti, millist kahju ettevõte rünnakute tagajärjel sai, siis jagunesid vastused järgnevalt: IT süsteemide kahjustumine (67%), ettevõtte andmete kadu (48%), finantsiline kahju (21%) ning laevasüsteemide kahjustumine (4%). Neljandikule ohvritest tekitati rünnakuga kahju 5 000 kuni 50 000 USD, kahele vastanule aga üle 500 000 USD.

Ettevõtetelt uuriti, millised laevasüsteemid on nende arvates kõige ründealtimad, siis jagunesid viis kõige haavatavamat süsteemi järgnevalt: laeva positsioneerimissüsteem (52%), ECDIS (51%), jõuseadmete kontroll (40%), kauba juhtimissüsteem (36%) ja ülemaailmne merepääste ja –ohutussüsteem (24%).

Mis puudutab küberturvalisuse suuniste jälgimist, siis ainult 16,8% laevaomanikest tunnistas, et on rakendanud meetmeid laevade ohutusjuhtimissüsteemides ning ainult 22% vastanutest kinnitas, et nende töötajad on saanud küberhügieeni koolitust.

Samuti toob autor välja juba varasemalt mainitud fakti, et laevaomanikud ei ole huvitatud teavitamast kolmandaid osapooli sellest, et nad on langenud küberrünnaku ohvriks. Uuringus vastanutest ainult 45% ettevõtetest teavitas oma töötajaid toimunud rünnakust ning ainult 11% informeeris oma kindlustusseltsi!

1.8 Laevanduses toimunud küberintsidendid

Küberrünnakud laevandussektori vastu toimuvad, kas laevaomanikud seda tunnistavad või mitte – on juba teine teema. Küberohud võivad varitseda ettevõtte pangaandmeid, logistikatarkvara, kirjavahetust, navigatsioonisüsteeme jms. Järgmistes alapeatükkides toob autor ära laevandussektori vastu toime pandud küberrünnakuid ja mõned simuleeritud rünnakud.

1.8.1 Rünnak Houstoni sadama arvutisüsteemide vastu (2001)

20. septembril 2001. aastal langesid Houstoni sadama arvutid ummistusründe (DoS – *denial of service*) alla. See kukutas kokku sadama süsteemid, mis sisaldasid sadamas tegutsevate ettevõtete jaoks olulist informatsiooni laevade liikumiste, sildumiste ja ilmastiku kohta. Rünnaku korraldas Suurbritanniast pärit 19-aastane noormees Aaron Caffrey, kelle esmane eesmärk oli tegelikult rünnata Lõuna-Aafrikast pärit isikut nimega „Bokkie“, kes ühises jututoas kirjutas USA vastaseid kommentaare. Valesti suunatud rünnaku tõttu sai kannata Houstoni sadam.

Jututoa logid paljastasid, et Aaron kasutas rünnakuks uuendamata tarkvaraga serverite nimekirja, mille abil oli võimalik üle võtta arvutid ning suunata ummistusrünnak „Bokkie“ peale. (McCue 2003)

1.8.2 „Conficker“ viirus Prantsusmaa ja Suurbritannia mereväe arvutites (2009)

2009. aastal sattus viirus nimega Conficker Prantsusmaa mereväe arvutisüsteemidesse (Willsher 2009). Viirus nakatas andmebaasid, mistõttu ei saanud lennukid alla laadida lennuplaane ega tõusta õhku. Mitu kuud varem hoiatas Microsoft, et selline viirus on liikvel ning soovitas võtta kasutusele vastavad meetmed. Prantsusmaa merevägi seda ei teinud. Arvatakse, et viiruse tõi sisse mõni töötaja oma USB mälupulgaga.

Sama aasta alguses langes Conficker viiruse ohvriks ka Suurbritannia merevägi, kus kuuldavasti ligi 75% laevastikust nakatus (Wattanajantra 2009).

1.8.3 Iraani laevaomaniku laevad küberrünnaku all (2011)

2011. aasta augustis pandi ulatuslik küberrünnak toime Iraanile kuuluva laevandusettevõtte IRISL vastu (Torbati, Saul 2012). Häkkerid ründasid ettevõtte servereid kahjustades andmeid kaupade, laadimiste, saabumisaegade jms kohta. Rünnaku tulemusena puudus ettevõttel ülevaade, kus mingi kaup antud hetkel asus. Suur hulk kaupa toimetati valesse sihtpunkti ning osa kaubast jäigi kadunuks.

1.8.4 Kummituslik kaubavedu läbi Antwerpeni sadama (2011-2013)

Antwerpeni sadama juhtum on hea näide konventsionaalsete kurjategijate ja arvutihäkkerite koostööst. Kahe aasta jooksul (2011–2013) vedas Hollandist pärit kuritegelik organisatsioon narkootilisi aineid Lõuna-Ameerikast Belgiasse läbi Antwerpeni sadama kasutades ära häkkerite abil saadud ligipääsu sadama terminaalidele (Bateman 2013). Heroiin ja kokaiin peideti ära legitiimse kauba nagu banaanid ja metsamaterjal vahele.

Belgiast palgatud häkkerid suutsid sisse tungida vähemalt kahe Antwerpeni sadamas tegutseva ettevõtte arvutisüsteemidesse, mis igapäevaselt haldavad tuhandete läbi sadama liikuvate konteinerite vedu, ladustamist ja edasi saatmist. See võimaldas neil saada vajalikku informatsiooni kaubakonteinerite, nende asukoha kui ka turvaandmete kohta. Saadud informatsiooni ära kasutades saatsid kurjategijad sadamasse oma veoautod, mis kindlad konteinerid peale võtsid ning sadamast välja viisid enne, kui kauba õigusjärgne omanik neile järele jõudis tulla.

Et pääseda ligi vajalikele andmetele, saatsid häkkerid sadamas tegutsevate ettevõtete töötajatele e-kirjaga kuritahtliku tarkvara (*malicious software*), mis võimaldas neile kaugligipääsu (*remote access*) terminaali süsteemidele. Pärast kauba kättesaamist ning sadamast välja vedamist kustutati süsteemidest andmed seotud konteinerite kohta. Kui ettevõtted rünnaku avastasid, eemaldati pahavara ning paigaldati tulemüürid.

See aga ei takistanud kurjategijail edasi tegutsemast. Sadamas asuvatesse ettevõtetesse murti füüsiliselt sisse ning paigaldati arvutite külge seadmed raadiosilla (*wireless bridge*) tekitamiseks, mis võimaldas kurjategijatele otsepääsu operatsioonisüsteemidele ja kauba informatsioonile. Joonistel 11 ja 12 on näha, milliseid vahendeid kasutati süsteemidele ligi pääsemiseks.

Joonis 11. Antwerpeni sadamas kaugligipääsu saamiseks kasutatud elektroonilised vahendid
Allikas: (BBC)

Joonis 12. Antwerpeni sadamas kaugligipääsu saamiseks kasutatud elektroonilised vahendid
Allikas: (BBC)

Kokku tegutsesid Hollandi ja Belgia kurjategijad selliselt kaks aastat, kuni laevaomanikud ja sadamaoperaatorid avastasid süstemaatilise konteinerite kadumise. Politsei konfiskeeris operatsioonide käigus üle tonni kokaiini, relvi ning rohkem kui 1,3 miljonit eurot sularahas. Kui palju tegelikult salakaupa sellel liinil liikus, on teadmata.

Antud juhtum andis aimu uuest kuritegevuse liigist logistikasektoris. Teadaolevalt on see esimene avastatud „kummituslik kaubavedu“. Antwerpeni sadama intsident näitas, et andmetele ligipääs ja nendega manipuleerimine on võimalik kõrgeimal ligipääsu tasemel. See ei välista, et lisaks salakaubale oli kurjategijatel ligipääs ka teistele väärtuslikele või tundlikele kaupadele ja informatsioonile.

1.8.5 Küberspionaaž ThyssenKruppi vastu (2016)

Tööstuskonglomeraat ThyssenKrupp langes küberrünnaku ohvriks 2016. aasta alguses. Maailma üks suurimaid terasetootjaid teavitas avalikkust 2016. aasta augustis, et grupi alla kuuluvate ettevõtete vastu pandi toime ulatuslik organiseeritud küberrünnak, mis ekspertide arvates oli pärit Kagu-Aasiast. Vaatamata sellele, et rünnakud leidsid aset sama aasta veebruaris, suutsid ettevõtete IT-töötajad lekkele jälile jõuda alles aprillis. Oma avalduses ThyssenKrupp nendib, et rünnakute eesmärgiks oli saada ligipääs tehnoloogilisele oskusteabele ja erinevatele uuringutele. Samas avalduses tunnistab ettevõte, et ei suuda usaldusväärselt hinnata rünnaku tõttu tekitatud kahjusid (intellektuaalse omandi vargus) ning samuti on teadmata, milline informatsioon ründajateni jõudis. (thyssenkrupp 2016)

Kuna tegemist on ettevõttega, kes ehitab ka allveelaevasid ja sõjalaevu erinevatele riikidele, siis spekuleeriti ka selle üle, kas ründajate kätte võis sattuda informatsiooni antud hetkel Iisraeli mereväele ehitatavate allveelaevade projekti kohta (Cohen 2016). ThyssenKrupp kinnitas oma avalduses, et küberrünnak ei ulatunud meresüsteemide üksuseni ning informatsiooni laevade projektide kohta kurjategijate kätte ei sattunud.

ThyssenKrupp rõhutas ka avalikkusele saadetud sõnumis, et toime pandud küberrünnak ei võinud saada võimalikuks ettevõtte IT süsteemides esinevate puuduste ega inimliku vea tõttu. Rünnakut kirjeldati, kui väga organiseeritult ja professionaalselt läbi viidud operatsiooni. Ekspertide sõnul on väga keeruline suurtes ettevõtetes, kus kasutatakse komplitseeritud infotehnoloogilisi süsteeme, vastu seista taolistele küberrünnakutele. Nende vastu aitab rünnete varajane avastamine ning kohene vastumeetmete rakendamine.

1.8.6 Küberspionaaž DCNS vastu (2016)

Sarnaselt ThyssenKrupp juhtumiga langes Prantsusmaa ettevõte DCNS küberrünnaku ohvriks (Siegel, Irish 2016). DCNS grupp on spetsialiseerunud sõjalaevade ehitamisele. 2016. aasta augustis tunnistas ettevõte, et tema arvutisüsteemid on langenud rünnaku alla ning enam kui 22 000 lehekülge kuue India mereväele ehitatava Scorpene-klassi allveelaeva projekti kohta on lekkinud. Allveelaevad ehitatakse Indiale kuuluvas laevatehases Mumbais.

1.8.7 GPS signaali häirimine (2016)

Lõuna-Korea süüdistas 2016. aastal Põhja-Koread GPS signaali segamises, mis mõjutas enam kui 700 laeva ja 1 000 lennukit (Kim, Saul 2016). Tõsisemaid intsidente õnneks ei juhtunud, kuid seadis siiski ohtu laevade navigeerimise. Seetõttu kaalub Lõuna-Korea taas ellu äratada dubleeriva navigatsioonisüsteemi eLoran loomise projekti, mida oleks väga keeruline segada ja häkkida.

Lõuna-Korea algatas eLorani projekti juba 2011. aastal, kuid oli sunnitud selle peatama konflikti tõttu USA tarnijaga. Seekord plaanitakse kaldajaamad üles seada 2019. aasta lõpuks.

1.8.8 Superjahi ülevõtmine Londoni konverentsil (2017)

Campbell Murray, küberkuritegevuse ekspert ettevõttest BlackBerry, tõestas 2017. aasta maikuus Londonis toimunud superjahtide konverentsil, et lühikese aja jooksul on võimalik sülearvutit kasutades üle võtta laev, mis on varustatud moodsa ja kaasaegse tehnikaga (Neate 2017). Ainult 30 minutit kulus IT-spetsialistil aega, et üle võtta laeva traadita interneti võrk (WiFi – *wireless high- fidelity*), pääseda ligi e-kirjadele ning neid kustutada ja isegi muuta. Lisaks pääses Murray ligi superjahi omaniku finantsandmetele ning võttis kontrolli laeva valvekaamerate, satelliitside ja navigatsiooniseadmete üle. Tehniliselt oli ta võimeline kai pealt superjahi sadamast välja juhtima.

1.9 Standardid ja suunised

Vaatamata sellele, et küberturvalisus on muutunud kõige suuremaks riskiks ettevõtetele, ei ole Rahvusvaheline Mereorganisatsioon, mis reguleerib rahvusvahelist laevandust, veel välja arendanud ega rakendanud kohustuslikke meetmeid laevandussektorile. See protsess võtab aega ning nõuab eelnevat olukorra analüüsi. IMO esialgsed soovituslikud juhised (*Interim guidelines on maritime cyber risk management*) aga kinnitati 2016. aasta mais toimunud IMO mereohutuse komitee istungil ringkirjaga MSC.1/Circ. 1526 (Interim guidelines...2016). Lisaks IMO suunistele märgib autor ära veel mõned juhised, mis on välja antud teiste merendusorganisatsioonide poolt:

a) The Guidelines on cyber security onboard ships (BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO);
b) Code of Practice. Cyber Security for Ports and Port Systems. (Institution of Engineering and Technology);
c) The application of cybersecurity principles to marine and offshore operations. Volume 1: Cybersecurity (American Bureau of Shipping);
d) Cybersecurity implementation for the marine and offshore industries. ABS CyberSafety Volume 2. (American Bureau of Shipping);
e) Data integrity for marine and offshore operations. ABS CyberSafety Volume 3. (American Bureau of Shipping);
f) Cyber security resilience management for ships and mobile offshore units in operation. (DNV GL);
g) Cyber-enabled ships. Deploying information and communications technology in shipping – Lloyd's Register's approach to assurance. (Lloyd's Register);
h) Social Media Guidance for Seafarers. (INTERTANKO).

Kõik nimetatud dokumendid on allalaaditavad aadressilt cybersecurity.mereblog.com. Lisaks soovituslikele suunistele võivad laevaomanikud rakendada oma ettevõttes ka infoturbealaseid põhimõtteid, mis on ära toodud küberturvalisust käsitlevates standardites nagu näiteks Eesti riigi ja kohalikes omavalitsustes kasutatav ISKE (infosüsteemide kolmeastmeline etalonturbe süsteem), ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO/IEC

15408-1:2009 või USA Riikliku Standardi- ja Tehnikainstituudi (NIST – *National Institute of Standards and Technology*) poolt välja antud juhendmaterjalides.

1.10 Euroopa Liidu isikuandmete kaitse üldmäärus 2016/679

Alates 25.05.2018 hakatakse Euroopa Liidus kohaldama uut isikuandmete kaitse üldmäärust (Euroopa Parlamendi ja nõukogu määrus 2016/679). See muudab kehtetuks andmekaitsedirektiivi 95/46 (Euroopa Parlamendi ja nõukogu direktiiv 95/46/EL) ja sellel põhineva isikuandmete kaitse seaduse (Isikuandmete kaitse seadus 2007). Uus üldmäärus sisaldab palju uusi sätteid, millel on oluline mõju isikuandmete kogumisele ja töötlemisele ettevõttes.

Juhul, kui laevandusettevõte kogub ja kasutab tundlikku isikuteavet ning toimetatakse suurte andmemassiividega, viib läbi ulatuslikku kaamerajälgimist ning automaat-profileerimist, tuleb kindlasti üle vaadata ettevõtte töökorraldus, käitumismustrid, infosüsteemid ja dokumendipõhjad. Kuna üldmääruse läbiv joon on riskipõhine lähenemine, siis on reeglid seda karmimad mida tundlikum andmetöötlus. Üldmääruse kohaselt mõistetakse isikuandmete all ka seadmete, tööriistade ja protokollide jagatavaid võrguidentifikaatoreid nagu näiteks IP-aadressid, küpsised (*cookies*) ning asukohateave.

Juhul, kui Eestis tegutsevad laevandusettevõtted ei ole selle üldmäärusega veel tutvunud, siis on autori arvates praegu viimane aeg vaadata üle ettevõtte protsessid ning hinnata nende vastavust üldmääruse nõuetele. Suure tõenäosusega vajavad ettevõtted abi andmekaitsespetsialistidelt. Selle jaoks tuleb vajadusel välja koolitada inimene oma ettevõttest või leida usaldusväärne nõustaja, kes oskab sidustada andmekaitse ja infoturbe nõudeid reaalselt laevandusettevõtte tööprotsesside ja infosüsteemidega.

Uue muudatusena peavad kõik isikuandmete töötlejad 25. maist 2018. aastal kehtima hakkava isikuandmete kaitse üldmääruse artikli 33 kohaselt edastama informatsiooni isikuandmetega seotud rikkumistest Andmekaitse Inspektsioonile.

„Vastavalt üldmääruse artiklile 33(1) peab teavitamine toimuma põhjendamatu viivituseta ja võimaluse korral 72 tunni jooksul pärast rikkumise teada saamist. Seda siis ka juhul, kui kõik rikkumise põhjused ei ole veel teada või pole lõplikult selge näiteks rikkumist puudutavate isikute arv“ (AKI Rikkumisteated 2017).

Kuigi üldmäärus annab andmetöötlejale õiguse hinnata, millal on tegu ohuga füüsiliste isikute õigustele ja vabadustele, selgitavad üldmääruse põhjenduspunktid 75, 76 ja 85, et erineva tõenäosuse ja tõsidusega ohud füüsiliste isikute õigustele ja vabadustele võivad tuleneda isikuandmete töötlemisest, mille tulemusel võib tekkida füüsiline, materiaalne või mittemateriaalne kahju, eelkõige juhtudel, kui (AKI Rikkumisteated 2017):

a) Töötlemine võib põhjustada diskrimineerimist, identiteedivargust või -pettust, rahalist kahju, maine kahjustamist, ametisaladusega kaitstud isikuandmete konfidentsiaalsuse kadu, pseudonümiseerimise loata tühistamist või mõnda muud tõsist majanduslikku või sotsiaalset kahju.
b) Andmesubjektid võivad jääda ilma oma õigustest ja vabadustest või kontrollist oma isikuandmete üle.
c) Töödeldakse isikuandmeid, mis paljastavad rassilist ja etnilist päritolu, poliitilisi vaateid, religioosseid või filosoofilisi veendumusi ning ametiühingusse kuulumist, samuti geneetilisi andmeid, andmeid tervise, seksuaalelu ning süüteoasjades süüdimõistvate kohtuotsuste ja süütegude ning nendega seotud turvameetmete kohta.
d) Hinnatakse isiklikke aspekte (nt isiku vaated, seisukohad, isikuomadused, sotsiaalne staatus), eelkõige töötulemuste, majandusliku olukorra, tervise, isiklike eelistuste või huvide, usaldusväärsuse või käitumise, asukoha või liikumisega seotud aspektide analüüsimisel või prognoosimisel, et luua või kasutada isiklikke profiile.
e) Töödeldakse kaitsetute füüsiliste isikute, eriti laste isikuandmeid.
f) Töötlemine hõlmab suurt hulka isikuandmeid ning mõjutab paljusid andmesubjekte.

Autor soovib ära mainida veel paar olulist muudatust, mis kaasneb uue üldmäärusega. Nimelt viiakse sisse ülisuured trahvid isikuandmete kaitse üldmääruse rikkumise eest. Väiksemate eksimuste puhul on see kuni 10 miljonit eurot või 2% ettevõtte eelmise aasta käibest ja suurte eksimuste puhul kuni 20 miljonit eurot või 4% ettevõtte eelmise aasta käibest (sõltuvalt sellest, kumb number on suurem). Trahvi määramise õigus on järelevalveasutusel, Andmekaitse Inspektsioonil. Trahvi suuruse otsustab amet iga juhtumi puhul eraldi, võttes arvesse kõiki asjaolusid antud juhtumi puhul.

Lisaks kaasneb ettevõtetele uue üldmäärusega kohustus võimaldada inimestel oma isikuandmed kanda ühelt andmetöötlejalt teisele. Andmete ülekandmist tuleb kohaldada ainult nendele andmetele, mille töötlemise aluseks on kas inimese nõusolek või inimese ja andmetöötleja vahel sõlmitud leping (Mida tähendab...2017). Juhul, kui on oodata selliseid päringuid, siis soovitab autor laevandusettevõtetel oma infosüsteemid üle vaadata ning vajadusel viia sisse nõutavad muudatused.

2. PRAKTILINE UURING JA SELLE TULEMUSED

Magistritöö teine peatükk käsitleb magistritöö raames läbi viidud uuringut Eesti laevaomanike seas. Autorile teadaolevalt ei ole varasemalt küberturvalisuse teemal uuringut Eesti laevaomanike seas läbi viidud. Seetõttu ei ole võimalik ainult antud uuringu tulemuste põhjal täiel määral hinnata küberturvalisuse teadlikkuse arengutendentsi.

Magistritöö praktilise uuringu eesmärgiks on välja selgitada:

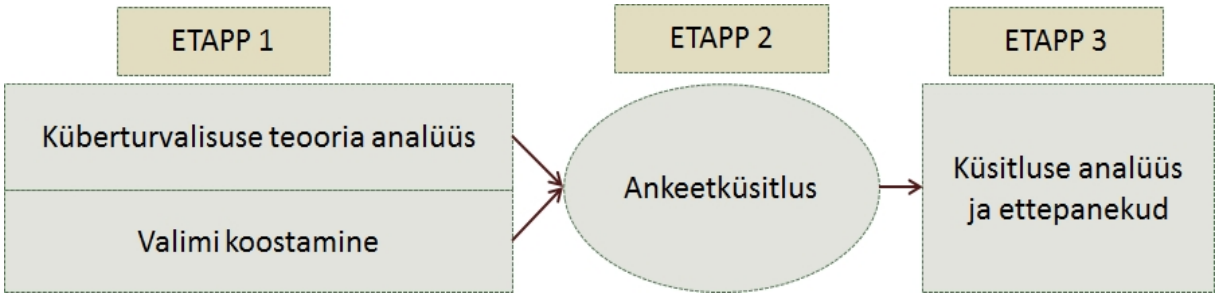
a) Eesti laevaomanike teadlikkus kübermaailmas varitsevatest ohtudest ning millistest allikatest informatsiooni saadakse;
b) ettevõtete valmidus küberrünnakutega toimetulekuks;
c) ettevõtete varasem kokkupuude küberrünnakutega;
d) kas ettevõtete töötajad ja laevapersonal on saanud küberhügieeni alast koolitust;
e) milliseid standardeid, metoodikaid või parimaid praktikaid kasutavad Eesti laevaomanikud küberturvalisuse tagamiseks oma ettevõtetes ja laevades;
f) laevaomanike informeeritus 25. mail 2018. aastal kehtima hakkavast Euroopa Liidu isikuandmete kaitse üldmäärusest.

2.1 Uuringu metoodika ja valimi kirjeldus

Autor kasutas magistritöö uuringu läbi viimiseks küsitlusmeetodit. Küsitluse koostamise jaoks kasutas autor veebipõhist programmi *Google Forms* (forms.google.com), mis võimaldas ettevõtete esindajatel elektrooniliselt küsimustele vastata. Laekunud vastuste analüüsimiseks kasutas autor andmetöötlustarkvara *Microsoft Office Professional Plus 2010*.

Töö käigus teostatud uuring koosneb kolmest etapist. Esimeses etapis tegeles autor taustainfo kogumisega küberturvalisuse valdkonnas ning küberrünnakute esinemisest laevandussektoris. Paralleelselt küberturvalisuse teooria analüüsiga kaardistas autor võimalikud Eesti laevandusettevõtted. Teine uuringu etapp, küsitlusmeetod, põhines küber-

turvalisuse teooria ja ettevõtetelt saadud andmete analüüsil. Kolmandas etapis toob autor välja küsitluse tulemused ning esitab ettepanekud küberturvalisuse riskide maandamiseks laevandusettevõtetes. Uuringu etapid on ära toodud joonisel 13.



Joonis 13. Magistritöö uuringu etapid
Allikas: (autor)

Uurimuse algetapiks oli taustandmete kogumine ja hetkeolukorra kaardistamine. Autor kasutas selle jaoks internetis leiduvat informatsiooni, teostatud uuringuid ning teema kohta kirjutatud raamatuid. Olukorda kaardistades ilmnes, et küberturvalisuse teema kohta on eesti keeles informatsioon internetis küll saadaval, kuid ühtegi analüüsi või teaduslikku artiklit laevandussektorit puudutavate ohtude kohta ei ole ilmunud. Küll on põgusalt kirjutanud võimalikust küberpiraatluse ohust autonoomsete laevade puhul tehnikaportaal Geenius.ee (Lõugas 2017) ja merendusportaal Mereblog.com (cybersecurity.mereblog.com). Teostatud küberturvalisuse teooria ja valdkonna analüüs andis autorile sisendi ankeetküsitluse välja töötamiseks.

Et valdkonda paremini tundma õppida ning olla kursis viimaste arengutega, osales lõputöö autor neljal valdkonnaga seotud seminaril ning konsulteeris ka nelja IT- turvalisusega tegeleva ettevõtte esindajaga (vt Tabel 2).

Tabel 2. Autori osalemine seminaridel ja kohtumistel

Kohtumine või seminar	Ettevõtte nimi	Kuupäev
Küberturbeeksperdi Mikko Hyppönen'i avalik loeng	BCS Koolitus, F-Secure	10.04.2017
Kohtumine	Security Software	21.04.2017
Kuidas olla IT halduses 3 sammu ees?	3 Step IT	27.04.2017
Kohtumine	Leego Hansson	27.04.2017
Euroopa Liidu uus isikuandmete kaitse määrus.	CGI Eesti ja Fondia	28.04.2017
Kohtumine	CGI Eesti ja Fondia	28.04.2017
Kohtumine	TTÜ Küberkriminalistika ja Küberjulgeoleku Keskus	11.05.2017
TMSA 3 and how to comply with KPIs on Cyber Security	DNV GL	15.05.2017

Allikas: (Autori koostatud)

Selgitamaks välja, milline on Eesti laevaomanike teadlikkus küberturvalisuse teemal ja kas ettevõtted on astunud samme riskide maandamiseks, viis autor läbi internetipõhise ankeetküsitluse, mille struktuur ja sisu on esitatud käesoleva lõputöö lisas 1.

Võttes arvesse küberturvalisuse teema uudsust ning arvestades, et antud vastused võivad sisaldada ettevõtete jaoks delikaatset informatsiooni, jättis autor mõned küsimused ettevõtte jaoks vabalt vastatavaks:

a) Ettevõtte nimi.
b) Vastaja e-posti aadress.
c) Vastaja telefoni number.
d) Milline on teie ametikoht ettevõttes?
e) Milline on töötajate arv ettevõttes?
f) Mitu laeva on ettevõttel?
g) Milline on IT-ga seotud inimeste arv ettevõttes?
h) Küberturvalisuse auditi teostanud ettevõtte nimi?
i) Kas teie ettevõte on kokku puutunud võimaliku küberrünnakuga?
j) Kui teie ettevõte on langenud küberrünnaku ohvriks, siis millist tüüpi rünnaku(te)ga on tegemist olnud?
k) Kui teie ettevõte on varasemalt küberrünnaku ohvriks langenud, siis millist kahju see tekitas?

l) Kas ettevõte on kaalunud küberriskide katmist kindlustuspoliisi sõlmimisel?
m) Milline on teie ettepanek küberturvalisusega seotud informatsiooni paremaks levitamiseks?
n) Milline on teie ettepanek küberturvalisuse tõhustamiseks laevafirmas?

Lisaks võimaldas autor mõne küsimuse puhul märkida vastusevariandiks „Ei soovi vastata“:

a) Kui teie ettevõte on langenud küberrünnaku ohvriks, siis millist tüüpi rünnaku(te)ga on tegemist olnud?
b) Kui teie ettevõte on varasemalt küberrünnaku ohvriks langenud, siis millist kahju see tekitas?
c) Kas teie ettevõtte poolt sõlmitud kindlustuspoliisid katavad küberrünnaku tõttu tekitatud kahjud (k.a. kolmandatele osapooltele)?

Lähtuvalt magistritöö teemast ja uurimisküsimustest kasutas autor ankeetküsitluse levitamisel eesmärgistatud valimit. Uurimustöö sihtgrupiks on Eestis tegutsevad laevaomanikud, kes opereerivad kauba- ja reisilaevadega, kalalaevadega ning puksiirlaevadega. Esialgse laevaomanike nimekirja sai autor Eesti Laevaomanike Liidu tegevjuhilt, hr Enn Kreemilt (vt Lisa 2). Kuna mitmest faktorist põhjustatuna ei ole Eesti lipp atraktiivne kaubalaevastikku omavate laevaomanike seas, siis tuli autoril täiendada valimit ettevõtetega, kes on Eestis küll registreeritud, kuid omavad laevu teiste riikide lippude all nagu Küpros, Malta, Panama (UNCTAD Merchant fleet...2016). Selle jaoks kasutas autor internetiotsingut ning uuris erinevate laevandusega seotud ettevõtete kodulehti.

Magistritöö uuring puudutab ettevõtete jaoks suhteliselt tundlike teemade käsitlemist. Seetõttu on kvalitatiiv-kvantitatiivsel segameetodil ülesehitatud uurimistöö käigus saadud andmed anonüümsed ning tagatud on igakülgne konfidentsiaalsus, millest autor informeeris vastajaid koos küsimustikuga saadetud kaaskirjas.

Autor saatis ankeetküsitluse 16 laevandusettevõttele laiali kõigepealt e-kirjaga, mis sisaldas magistrandi tutvustust ja kontaktandmeid, uuringu eesmärki ja lühikirjeldust, valimi selgitust, vastamisele kuluvat orienteeruvat aega ja linki küsitlusele veebikeskkonnas *Google Forms*. Mõne päeva möödudes võttis autor ettevõtetega ühendust telefoni teel, et kindlaks teha, kas e-kiri ankeetküsitlusega on jõudnud kohale ning kas ta saab pakkuda abi selle

täitmisel. Paar päeva enne tähtaega saatis autor veelkord meeldetuletuskirja palvega küsimustikule vastata. Autor viis küsitluse läbi ajavahemikus 18.–27.04.2017. Kokku laekus elektroonilisi vastuseid üheksalt ettevõttelt. Ühe ettevõttega toimus väga lühike intervjuu telefoni teel, kuid selle tulemusi ei ole kajastatud antud uuringus. Ettevõte ei soovinud kommentaare anda, kuid enne kõne järsku lõpetamist kinnitas, et tema laevad on väga hästi kaitstud igasuguste küberrünnakute vastu ning nemad abi ei vaja.

2.2 Uuringu tulemused

Nagu autor eelnevalt mainis, saadeti ankeetküsitlus e-kirjaga 16 ettevõttele. Vaatamata sellele, et küsitlusele vastamise tähtaeg oli 27. aprill, sai autor tagasisidet 9. mail veel kahelt ettevõttelt. Võttes arvesse teema uudsust ja tundlikkust ning teades valimisse sobivate ettevõtete arvu piiratust, siis on lõputöö autor rahul saadud tagasiside hulga ja informatsiooniga.

Konsulteerides erinevate infoturbe spetsialistidega, mõistis autor, et tagasiside saamine ettevõtetelt lõputöö teemal võib olla raskendatud. Ettevõtted reeglina ei tunnista, et nemad võivad olla küberrünnakute sihtmärgiks. Kui küberintsident on siiski juhtunud, siis sellest ei soovi ettevõtted rääkida.

Küsitlus algas kolme küsimusega laevandusettevõtte nime ja ankeetküsitluse täitja kohta. Nendele küsimustele võis ettevõtte esindaja vastata vabatahtlikult. See võimaldas autoril mõista, miks vastati edasistele küsimustel nii nagu seda tehti.

Järgneva nelja küsimusega tundis autor huvi, kui palju töötab laevandusettevõttes inimesi kontoris ja laevadel ning milliste laevadega ettevõte opereerib. Saadud vastused andsid autorile ettekujutuse ettevõtte suurusest ja laevastikust.

Edasi tundis autor huvi, kas ettevõttes on korraldatud IT riskijuhtimine, mitu inimest on määratud selle peale ning kas on rakendatud erinevate organisatsioonide poolt välja töötatud standardeid ja suuniseid küberriskide haldamiseks. Autor loetles vastusevariantides ära mitmed laevandussektorile loodud suunised ning infoturbe halduse standardid. Lisaks võimaldas autor vastata küsimusele „Milliseid standardeid ja suuniseid kasutate ettevõttes ja laevades küberriskide haldamiseks?“ vastustega „ei kasuta ühtegi standardit ega suunist“ ning „muud standardid või suunised“.

Järgmise küsimusega paluti vastajal teada anda, milliseid elementaarsemaid tehnilisi vahendeid ja lahendusi on laevandusettevõte rakendanud, et tagada küberturvalisus laevadel ja kontoris. Autor pakkus välja ka mõned vastusevariandid. Juhul, kui ettevõttes rakendatakse lisaks muid meetmeid, sai vastaja seda kirjeldada kommentaari kastis.

Küsimustega „Kas olete teadlikud laevanduses varitsevatest küberohtudest?“ ja „Kas teie ettevõtte planeerib muudatusi seoses suurenenud küberohuga?“ soovis autor teada saada, kuivõrd teadlik on laevandusettevõte laevandussektoris varitsevate küberohtudega. Lihtsama vastuseversiooni „jah-ei“ asemel pakkus autor välja veel kolmanda variandi. Esimesele küsimusele oli võimalik vastata „mõningal määral, aga soovime rohkem teada“ ja teisele küsimusele oli võimalik veel vastata „planeerime, kuid täpne plaan puudub“. Nagu küsitluse tulemustest hiljem selgus, siis oli nende vastusevariantide lisamine õigustatud ning andsid parema ülevaate ebakindlast olukorrast ettevõtetes. Mõlema küsimuse puhul üle pooled vastanud ettevõtetest valisid vastusevariandid „mõningal määral, aga soovime rohkem teada“ ja „planeerime, kuid täpne plaan puudub“.

Järgmise küsimusega soovis autor teada saada, kas ettevõte planeerib seoses suureneva küberohuga laevandussektoris võtta lähiajal juurde lisatööjõudu.

Edasi palus autor vastajatelt informatsiooni, kas ettevõttes on viidud läbi turvaaudit hindamaks ettevõtte ja laevade süsteemides kasutatavate kaitsevahendite efektiivsust, tuvastada turvaaugud ning kaardistada muud võimalikud ohud. Vastused antud küsimusele peegeldavad autori hinnangul hästi laevandusettevõtte teadlikkust küberturvalisusest ning valmisolekut küberintsidentideks.

Samuti toetab üldpildi kujunemist järgmine küsimus, mis uurib, kas ettevõttes on koostatud küberrünnaku intsidendiplaan (hädaolukorra lahendamise plaan). Autori arvates on parim kaitse küberruumist tuleneva rünnaku vastu infoturbeteadlikkus ning valmisolek ja oskus juhtunud intsidentidega koheselt tegeleda.

Järgmise kolme küsimusega uuris autor ettevõtete kogemust küberrünnakutega: kas on langetud rünnaku ohvriks, millist tüüpi on rünnakud olnud ning millist kahju on ettevõttele selle läbi põhjustatud. Reeglina kaasnevad eduka küberrünnakuga kahjud ettevõtte jaoks. Need võivad olla

a) vigastused laevale, kaubale või meeskonnaliikmetele;
b) keskkonnareostus;
c) ettevõtte andmete lekkimine;

d) maine kahjustumine;
e) märkimisväärne finantsiline kahju.

Vastamine kõigile kolmele küsimusele oli vabatahtlik. Autor andis ette vastuse-variandid küsimustele „Kui teie ettevõte on langenud küberrünnaku ohvriks, siis millist tüüpi rünnaku(te)ga on tegemist olnud?“ ja „Kui teie ettevõte on varasemalt küberrünnaku ohvriks langenud, siis millist kahju see tekitas?“. Vastused nendele kolmele küsimusele on olulise tähtsusega. Saadud vastustest selgub, kas küsitlusele vastanud ettevõtetes on toimunud küberintsidente ja kuidas on see ettevõtet mõjutanud.

Kindlustusettevõtted pakuvad täna juba võimalust soetada küberriskide kindlustuse poliisi, mis võimaldab tegeleda rünnaku tulemusena tekkinud kahjudega. Seetõttu uuris autor järgmise kahe küsimusega, kas laevandusettevõtted on selle võimaluse peale mõtelnud või seda ka kasutanud.

Küsimusega „Milliseks hindate küberrünnaku võimalust enda ettevõtte vastu?“ palus autor ettevõtte esindajal hinnata skaalal 1-5 võimalust, et nende ettevõte võib langeda küberrünnaku ohvriks.

Järgnevalt uuris autor kahe küsimusega, kas ettevõtte töötajad on juba saanud küberhügieeni koolitust ning kas nad vajaksid seda.

2018. aastal kehtima hakkav Euroopa Liidu isikuandmete kaitse üldmäärus puudutab kõiki ettevõtteid, kes koguvad, talletavad või kasutavad isikuandmeid. Järgmise küsimuse eesmärk oli selgitada välja, kas küsitlusele vastanud ettevõtted on uue üldmääruse kehtima hakkamisest teadlikud ning kas plaanitakse seoses sellega midagi muuta.

Edasi huvitas autorit, millistest allikatest saavad ettevõtted informatsiooni küber-intsidentide ja küberturvalisuse kohta laevandussektoris ning kas vajatakse seda rohkem.

Viimase kahe küsimusega ootas autor ettevõtetelt ettepanekuid küberturvalisusega seotud informatsiooni paremaks levitamiseks ning küberturvalisuse tõhustamiseks laevandus-ettevõttes.

Järgnevalt esitatakse kokkuvõte uuringu tulemustest. Autor saatis e-kirja teel ankeetküsitluse 16 laevandusettevõttele, kellest 9 vastasid elektrooniliselt. Ühe ettevõtte esindajaga vestles autor lühidalt telefoni teel, kui pakkus oma abi ankeetküsitluse täitmisel. Kahjuks ei olnud ettevõtte esindaja nõus ankeeti täitma ega telefoni teel informatsiooni andma. Kategooriliselt kinnitades, et nende ettevõttes on kõik korras ning küberrünnakud neid

ei ohusta, lõpetati kõne. Kokku kvalifitseerus seega üheksa korrektselt täidetud ankeeti. Tabelis 3 on ära toodud lühikokkuvõte ankeetküsitluse üldinfo osast.

Tabel 3. Lühikokkuvõte ankeetküsitluse üldinfo osast

Ettevõtete arv, kellele ankeetküsitlus saadeti	16
Elektrooniliselt saabunud vastuste arv	9
Küsimuste arv ankeetküsitluses	33
Vastanud isiku positsioon ettevõttes	tippjuht – 55,6% keskastmejuht – 33,3% spetsialist – 11,1%
Ettevõtete laevastiku suurus	1-16 laeva
Küsitluses avaldatud laevade arv	52 laeva
Laevade tüübid ettevõtetes	kaubalaev, reisilaev, ro-ro laev, parvlaev, multifunktsionaalne laev, avamererajatiste teeninduslaev, majutuslaev, puksiirlaev

Allikas: (Autori koostatud)

Kolmele esimesele küsimusele, mis puudutasid ettevõtte nime ja küsitluse täitja kontaktandmeid, vastamine kohustuslik ei olnud. Sellega soovis autor tagada vastaja anonüümsust ning võimaldada informatsiooni vabamalt jagada. Ainult viis vastajat pani kirja esindatava ettevõtte nime ning kolmel juhul täideti ära ka vastaja e-posti aadressi ja telefoni lahtrid.

Töötajate arvu nimetamine ettevõttes ja laevadel oli vabatahtlik. Sellele küsimusele andsid tagasisidet kõik üheksa vastajat. Tabelis 4 on näidatud ettevõtete jagunemine inimeste arvu järgi ettevõttes ja laevadel. Analüüsist selgub, et üle poole vastanud ettevõtete kontoris töötab enam kui 50 inimest.

Tabel 4. Ettevõtete jagunemine töötajate järgi

Töötajate arv ettevõttes	
1-10	1
11-30	2
31-50	1
51-100	3
101-300	1
301 ja enam	1
Töötajate arv laevadel	
1-10	0
11-30	1
31-50	2
51-100	3
101-300	1
301 ja enam	2

Allikas: (Autori koostatud)

Tabelis 5 on ära toodud ettevõtete laevastiku andmed. Küsimusele „Mitu laeva on ettevõttel?“ oli vastamine vabatahtlik, kuid laevatüüpide nimetamine kohustuslik. See võimaldas saada ettekujutuse, milliste laevadega vastanud ettevõtted opereerivad. Oma laevastiku arvu nimetas ära kaheksa ettevõtet üheksast. Üks vastaja kas unustas või ei soovinud infot avaldada. Kokku oli avaldatud laevastiku suuruseks 52 laeva.

Tabel 5. Ettevõtete laevastiku suurus

Ettevõtte laevastiku suurus	
vastanud ettevõte	laevade arv
1	1
2	2
3	3
4	6
5	6
6	10
7	14
8	16

Allikas: (Autori koostatud)

Lisaks autori poolt etteantud laevade tüüpidele, märkis kaks ettevõtet kommentaarides ära oma laevastikus esinevad laevatüübid, mida autor ei osanud ette näha: ro-pax laev, majutuslaev, avamererajatiste teeninduslaev ja nn „*walk-to-work*“ laev, mida kasutatakse avamererajatiste meeskondade abistamiseks (vt Tabel 6).

Tabel 6. Ettevõtete laevastik

Ettevõtete laevade tüübid		
laeva tüüp	ettevõtete arv, kellel nimetatud laevatüübid esinevad	
Kaubalaev	3	33,3%
Reisilaev	4	44,4%
Ro-ro laev	2	22,2%
Parvlaev	3	33,3%
Puksiirlaev	2	22,2%
Multifunktsionaalne laev	1	11,1%
Majutuslaev	1	11,1%
Ro-pax laev	1	11,1%
Avamererajatiste teeninduslaev	1	11,1%
Walk-to-work“ laev	1	11,1%

Allikas: (Autori koostatud)

Järgnevalt palus autor vabatahtlikult nimetada infotehnoloogiaga tegelevate inimeste arv ettevõttes. Uuringu tulemusena selgub, et kolmel ettevõttel on palgal üks IT spetsialist, ühes ettevõttes töötab kaks inimest, ühel ettevõttel on eraldi IT osakond ligi 50 inimesega ning ülejäänud kasutavad emafirma poolt pakutud IT teenust (vt Tabel 7).

Tabel 7. IT-ga seotud inimeste arv ettevõttes

Ettevõte	Inimeste arv	Kommentaar
1	1	
2		Teenust ostetakse emafirmalt sisse
3	2	
4	1	Kõik töötajad on mingil määral IT-ga seotud
5		Teenust pakub emafirma, ostetakse IT teenust ka Eestist
6	50	Ettevõttel on enda IT osakond
7	1	IT tuge pakub emafirma
8	1	
9		Kasutatakse kontserni tsentraalset teenust

Allikas: (Autori koostatud)

Küsimus, mis puudutas IT riskijuhtimist ettevõttes, oli kohustuslik ning sellele vastas positiivselt kaheksa ettevõtet. Ainult üks vastaja märkis ära, et nende ettevõttes IT riskijuhtimine ei ole korraldatud. Autor märgib ära ühe IT riskijuhtimise kohta tehtud kommentaaridest: „Korraldus kaldub olema pigem formaalne“. Ülejäänud kommentaarid täiendasid antud vastuseid lisainfoga, et IT riskijuhtimine toimub emafirma kaudu.

Tabelis 8 on ära toodud ettevõtete hinnangud IT riskijuhtimise vajaduse kohta. Selgub, et mitte kõik ettevõtted ei loe seda väga oluliseks. Ühe ettevõtte puhul märgiti see lausa mittevajalikuks.

Tabel 8. IT riskijuhtimise vajalikkus ettevõttes

Vajaduse hinnang	Ettevõtete jagunemine	
Väga vajalik	5	55,6%
Mõningal määral vajalik	3	33,3%
Vajadus puudub	1	11,1%

Allikas: (Autori koostatud)

Tänasel päeval ei ole Rahvusvaheline Mereorganisatsioon (IMO) veel välja töötanud ühtseid rahvusvahelisi standardeid küberriskide haldamiseks. Samas IMO ja mitmed teised

organisatsioonid avaldanud soovituslikud suunised laevaomanikele riskidega tegelemiseks. Autor palus ettevõtetel ära märkida etteantud variantidest, milliseid suuniseid või standardeid on firmas rakendatud. Tabelis 9 on ära toodud tulemused. Vastamine oli kohustuslik.

Tabel 9. Standardite ja suuniste kasutamine ettevõttes ja laevades küberriskide haldamiseks

Dokument	Ettevõtete arv	
IMO Interim Guidelines on Maritime Cyber Risk Management	1	11,1%
The Guidelines on Cyber Security onboard Ships (BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO)	1	11,1%
Cyber security resilience management for ships and mobile offshore units in operation (DNV GL)	1	11,1%
ISO/IEC 27001:2013	1	11,1%
Ei kasuta ühtegi	4	44,4%
Muud standardid või suunised	3	33,3%

Allikas: (Autori koostatud)

Tulemustest järeldub, et 44% vastanud ettevõtetest ei ole rakendanud ühegi suunise või standardi soovitusi küberriskide haldamiseks. Ettevõtted, kes vastasid „muud standardid või suunised“ ei olnud kindlad, kas ja milliseid suuniseid kasutatakse, kuna sellega tegeleb emaettevõte. Üks ettevõte kinnitas kommentaarides, et „otseselt ei jälgi ühtegi sõna-sõnalt, küll aga põhimõtteid“. Üks vastanud ettevõte märkis vastusevariantides ära, et neil on rakendatud nii BIMCO *The Guidelines on Cyber Security onboard Ships* kui ka standardi ISO/IEC 27001:2013 põhimõtted.

Küberturvalisuse tõstmiseks ettevõttes ja laevadel on olemas lihtsad moodused, mida rakendada. Autor palus ettevõtetel vastata, milliseid neist meetmetest on nad kasutusele võtnud. Vastamine sellele küsimusele oli kohustuslik. Kokkuvõttest selgus, et üle 75%

vastanutest kasutavad ja teostavad perioodilist kontrolli arvutitesse installeeritud viirusetõrje ja tulemüüri programmidega. Samuti teeb perioodiliselt tagavarakoopiaid andmetest üle 77% vastanutest. Kui vaadata tagavarakoopiate hoidmist mitmes eksemplaris ja erinevatel andmekandjatel, siis näeb autor siin arenguruumi. Näiteks lunavarast, mis krüpteerib arvutites põhjustatud kahjude vältimiseks või vähendamiseks tuleks kasutada 3-2-1 reeglit (Leopando 2013):

a) tee vähemalt kolm tagavarakoopiat;
b) tee koopiad kahele erinevale andmekandjale;
c) hoia üks tagavarakoopia asukohas, mis asub eemal algandmetest ning ei ole ühendutud ühegi võrguga.

Teatavasti ei liigu viirused ja pahavara mitte ainult interneti teel. Seda kantakse edasi inimeste poolt ka USB-pulkade ja väliste kõvaketastega. Seetõttu tegi autorit eriti murelikuks tagasiside küsimusele „Piirame USB mälupulkade ja USB laadijate (telefon, e-sigaretid jms) kasutamist ettevõtte ja laevade arvutites“. Ilmnes, et ainult ühel ettevõttes on olemas reeglistik USB-pesade kasutamise kohta. Ülejäänud kaheksa ettevõtet ei märkinud oma vastuses ära, et neil oleks mingi piirang USB seadmete kasutamiseks. Autor märgib ära kaks kommentaari, mis jäeti käesoleva küsimuse alla:

a) Tulemüür on serveris. Arvutites on sisseehitatud tulemüür. Praktiliselt on USB-pulkade kasutamist kohati raske piirata (*cargoplans*, sadamate külastused, prahtijate külaskäigud).
b) Laeva kriitilistele süsteemidele (*power management system*, *integrated bridge system*, *dynamic positioning system*, etc.) on juurdepääs tugevalt piiratud. Muudatuste tegemisel sellistes süsteemides tuleb läbida FMEA testid veendumaks töökindluses.

Vastuste kokkuvõte on ära toodud tabelis 10. Rakendatavad meetmed on järjestatud tabelis nende kasutuse järgi ettevõtetes kasvavas järjekorras.

Tabel 10. Laevades rakendatavad meetmed küberturvalisuse tõstmiseks

Rakendatavad meetmed	Vastanute arv	
Piirame USB mälupulkade ja USB laadijate (telefon, e-sigaretid jms) kasutamist ettevõtte ja laevade arvutites	1	11,1%
Ettevõtte töötajatele ja laevapersonalile tuletatakse võimalikest küberohtudest perioodiliselt meelde	4	44,4%
Tagavarakoopiaid hoiame mitmes eksemplaris ja erinevatel andmekandjatel	6	66,7%
Tulemüüri tarkvara kasutamine arvutites perioodiline kontroll	7	77,8%
Perioodiliselt uuendame tarkvara laevade arvutites	7	77,8%
Perioodiliselt teeme vajalikust informatsioonist tagavarakoopiaid	7	77,8%
Ettevõtte töötajad ja laevapersonal kasutavad erinevaid e-posti aadresse isiklikuks ja tööalaseks suhtluseks	7	77,8%
Perioodiliselt uuendame tarkvara kontori arvutites	8	88,9%
Arvutites on seadistatud kasutajatele põhjendatud juurdepääsuõigused	8	88,9%
Viirusetõrje tarkvara kasutamine arvutites ja perioodiline kontroll	9	100%
Muu	2	22,2%

Allikas: (Autori koostatud)

Autor uuris, kas laevaomanikud on teadlikud laevanduses varitsevatest küberohtudest. Vastamine oli kohustuslik. Ainult kolm vastajat arvas, et neil on piisavalt informatsiooni võimalikest küberohtudest. Viis vastajat kinnitasid, et nad on mõningal määral teadlikud, kuid sooviksid rohkem informatsiooni selle kohta. Üks vastaja kinnitas, et tal puudub ülevaade küberohtudest.

Edasi uuris autor, kas ettevõtted planeerivad muudatusi seoses suureneva küberohuga. Küsimusele vastamine oli kohustuslik. Kindlat plaani omab ainult kaks ettevõtet, kellest üks lisas küsimuse alla veel järgmise kommentaari: „Lähme üle ühtsele renditarkvarale automaatsete uuendustega, korrastame ligipääse kasutajatele“. Viis ettevõtet mõtlevad muudatuste peale, kuid kindel plaan puudub. Kaks ettevõtet ei plaani midagi ette võtta.

Autor selgitas küsitlusega välja, et ainult kaks ettevõtet planeerib palgata lisatööjõudu lähitulevikus seoses aina suureneva küberohuga. Kommentaarina lisas üks ettevõte, et selle jaoks vajadus puudub, kuna teenust ostetakse sisse. Teine ettevõte märkis kommentaaris ära, et hetkel puuduvad vahendid uue inimese palkamiseks küberturvalisuse peale.

Küsimusele, kas ettevõte on tellinud oma infosüsteemide hetkeolukorra analüüsi või auditi, et hinnata olemasolevate kaitsevahendite efektiivsust, tuvastada turvaaugud ning kaardistada muud ohud. Saadud vastustest selgus, et ainult kaks laevandusettevõtet on tellinud hetkeolukorra analüüsi ning ühel ettevõttel on see plaanis. Eitavalt vastas küsimusele kuus vastajat, kellest kolm täpsustasid kommentaarides, et nad ei ole teadlikud analüüsi läbiviimisest.

Autorit üllatas mõningal määral positiivselt, et küberrünnaku intsidendiplaan on olemas neljal ettevõttel. Viiel vastanud ettevõttel see puudub.

Järgneva kolme küsimusega tundis autor huvi, kas ettevõtted on langenud küberrünnaku ohvriks ning millist kahju see neile põhjustas. Nendele küsimustele vastamine oli vabatahtlik. Saadud vastused kinnitasid autori esitatud hüpoteesi, et mõned Eesti laevaomanikud on tõepoolest juba langenud küberrünnakute ohvriks ning tekitatud on ka reaalset kahju. Tabelist 11 selgub, et küberrünnakud on puudutanud vähemalt kolme küsitlusele vastanud ettevõtet.

Tabel 11. Ettevõtete kokkupuude küberrünnakutega

Vastus	Vastanute arv	
Jah	3	33,3%
Ei	4	44,4%
Ei tea	2	22,2%

Allikas: (Autori koostatud)

Tabelis 12 toob autor ära laevandusettevõtete poolt tuvastatud küberrünnakute tüübid. Nimekirja kuuluvad nii arvutite nakatumine kahjurvaraga, meiliteesklus (*email spoofing*), lunavaraga nakatumine kui ka GPS signaali häirimine. Kolm ettevõtet ei soovinud avaldada infot, millise rünnakutüübi ohvriks nad langesid.

Tabel 12. Küberrünnakute tüübid

Rünnaku tüüp	Vastanute arv	
Meiliteesklus (*e-mail spoofing*)	2	28,6%
GPS signaali häirimine	1	14,3%
Arvutite nakatamine kahjurvaraga	3	42,9%
Lunavara (*ransomware*)	2	28,6%
Kalastus (*phishing*)	3	42,9%
Ei soovi vastata	3	42,9%
Muu	1	14,3%

Allikas: (Autori koostatud)

Küberrünnakutega kaasnevad alati mingid kahjud. Autor palus oma küsitluses ettevõtetel võimaluse korral ära nimetada, millist kahju nad kannatasid. Tabel 13 näitab ära neli põhilist küberrünnakute põhjustatud kahju. Kõige enam sai kannatada ettevõtete maine (2 juhtumit) ning kahjustati IT süsteeme (2 juhtumit).

Nii nagu kolm ettevõtet ei avaldanud andmeid küberrünnakute tüüpide kohta, ei jaganud samad ettevõtted informatsiooni ka tekitatud kahjude kohta.

Tabel 13. Küberrünnakute tõttu tekitatud kahjud

Rünnaku tüüp	Vastanute arv	
Ettevõtte andmete leke	1	14,3%
Mõõdetav finantsiline kahju	1	14,3%
IT süsteemide kahjustumine	2	28,6%
Maine kahju	2	28,6%
Ei soovi vastata	3	42,9%
Muu	1	14,3%

Allikas: (Autori koostatud)

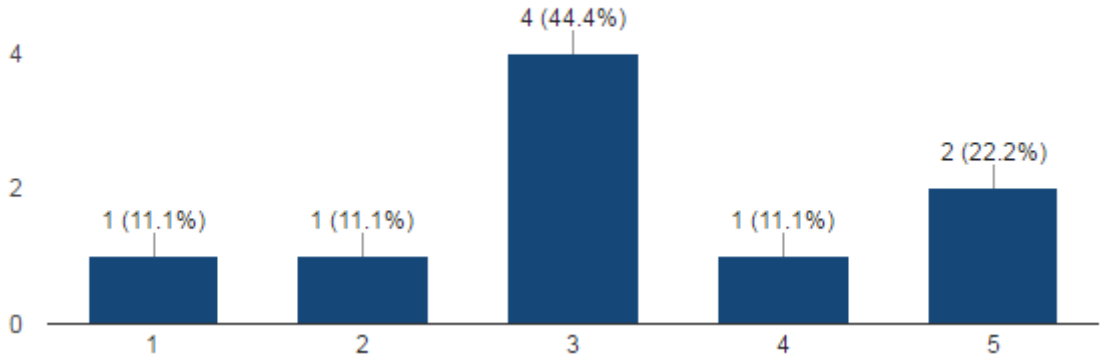
Järgmise kahe küsimusega uuris autor, kas ettevõtetel on sõlmitud küberriskide kindlustuse poliis. Kui mitte, siis kas on seda plaanis teha. Tabel 14 näitab üllatuslikult, et kolm ettevõtet on sõlminud vastava poliisi. Kolmel ettevõttel küberriskide kindlustus puudub ning kolm vastajat ei soovinud infot jagada. Küsimustele vastamine oli vabatahtlik.

Tabel 14. Küberriskide kindlustus

Vastus	Vastanute arv	
Jah	3	33,3%
Ei	3	33,3%
Ei soovi vastata	3	33,3%

Allikas: (Autori koostatud)

Autor palus ettevõtete hinnangut küberrünnaku võimaluse kohta oma ettevõtte vastu. Üllatuslikult hindasid võimalust kõrgeks ainult kolm ettevõtet. Ülejäänud kuus ettevõtet andsid hinded ühest kolmeni (vt Joonis 14).



Joonis 14. Hinnang küberrünnaku võimalusele ettevõttes (1 = madal ja 5 = kõrge)
Allikas: (Autor)

Järgnevate küsimustega, millele vastamine oli kohustuslik, tundis autor huvi, kas ettevõtte töötajad ja laevapersonal on saanud küberhügieeni alast koolitust ning kas ettevõtte hinnangul oleks seda vaja. Saadud vastused autorit ei üllatanud. Ainult kaks ettevõtet on oma töötajatele koolitust pakkunud (vt Tabel 15).

Tabel 15. Töötajad on saanud küberhügieeni alast koolitust

Vastus	Vastanute arv	
Jah	2	22,2%
Ei	7	77,8%

Allikas: (Autori koostatud)

Vähem kui pooled vastanutest leidsid, et küberhügieeni koolitust pole ettevõtte töötajatele hetkel vaja (vt Tabel 16).

Tabel 16. Ettevõtte vajadus küberhügieeni koolituse järgi

Vastus	Vastanute arv	
Jah	4	44,4%
Ei	5	55,6%

Allikas: (Autori koostatud)

Autorit huvitas, kas laevandusettevõtted on kursis 2018. aastal kehtima hakkava Euroopa Liidu isikuandmete kaitse üldmäärusega ning kas on planeeritud ka mingisugused tegevused sellega seoses. Küsimusele vastamine oli kohustuslik. Neli ettevõtet vastas, et nad ei ole teadlikud uuest määrusest. Sama palju ettevõtteid kinnitas, et nad on teadlikud uuest määrusest ning plaanivad ette võtta vajalikud tegevused. Üks ettevõte teatas, et nad on teadlikud uue määruse kehtima hakkamisest, kuid ei plaani hetkel midagi ette võtta.

Lisaks uuris autor laevandusettevõtetelt, millistest infoallikatest saavad nad informatsiooni küberintsidentide kohta laevandussektoris ning kas vastavat infot oleks vaja rohkem. Vastamine küsimustele oli kohustuslik ning autor andis vastusevariandid ette. Tulemused on ära toodud tabelis 17. Autor toob siinkohal ära ka ühe kommentaari, mis jäeti ühe vastaja poolt: „Info peaks olema selline, mille olemasolu võimaldab hoida ära või vähendada küberriskidest tulenevaid õnnetus- või vahejuhtumeid. Seni on see olnud piisav, kuid uute asjaolude või praktikate esiletulek võib seda seisukohta muuta“.

Tabel 17. Infoallikad küberturvalise teemadel ning ettevõtete vajadus info järele

Allikas	Vastanute arv	
Klassifikatsiooniühing	5	55,6%
Uudised internetist	5	55,6%
Mereadministratsioon	4	44,4%
Lipuriik	3	33,3%
Laevaomanike liit	2	22,2%
Ajakirjad ja ajalehed	6	66,7%
Riigi Infosüsteemi Amet	4	44,4%
Andmekaitse Inspektsioon	5	55,6%
Muu	2	22,2%
Kas vajatakse rohkem informatsiooni?	Vastanute arv	
Jah	4	44,4%
Ei	5	55,6%

Allikas: (Autori koostatud)

Eelviimase küsimusega uuris autor laevaomanikelt, millised on nende arvates paremad moodused küberturvalisusega seotud informatsiooni levitamiseks. Vastamine oli vabatahtlik. Autor toob allpool ära kolm olulisemat tehtud ettepanekut:

a) Küberturvalisuse rikkumisega seotud õnnetus- või vahejuhtumid oleks mõistlik avalikustada. Usun, et seda ka jõudumööda tehakse.
b) Klassifikatsiooniühing, laevaomanike liit ja lipuriik (eesti). Lisaks informatsioon veebilehtedel ja ajakirjades.
c) Teemaga läbinisti kursis oleva, aga samas sõltumatu organisatsiooni meililist. Lühikesed kampaaniad fokuseeritud praktilistele valukohtadele.

Saadud tagasiside kattub osaliselt autori soovitustega, mida ta käsitleb järgmises peatükis.

Küsitluse lõpus palus autor laevaomanikel teha ettepanekuid, kuidas laevafirmas tõhustada küberturvalisust. Küsimusele vastamine oli vabatahtlik. Mõned kommentaarid toob autor allpool ära:

a) USB kasutamist tuleks tõesti piirata, kasutada tuleb ühtlustatud ja *up-to-date* tarkvara. Kasutajad ja andmete salvestus peavad olema reglementeeritud.
b) Teadlikkuse tõstmine ja koolitused.
c) Kui tekib kohustus tõhustada küberturvalisust, siis on seda ka lihtsam laiaulatuslikult rakendada.

Praktilise uuringu käigus veendus autor, et mitte kõikides laevandusettevõtetes ei pöörata tähelepanu küberturvalisusele. Olenemata sellest, kas ettevõte on väike või suur, on oht sattuda küberrünnaku ohvriks väga reaalne. Lunavarajuhtumite puhul võetakse sihikule tavaliselt väiksema ja keskmise suurusega ettevõtted, kelle puhul on oodata lunaraha tasumist andmete tagasisaamiseks. Suurtel ettevõtetel on olemas võimekus küberintsidentideks valmis olla ning tekkivate probleemidega tegeleda. Uuringust selgub, et neli ettevõtet ei kasuta ühtegi laevandussektorile suunatud juhendit küberriskide maandamiseks ning kolm ettevõtet ei ole kindlad, kas järgitaksegi mõnda juhendit! Autor hindab küberhügieeni taset uuringus osalenud ettevõtetes väga madalaks. Ainult kahes ettevõttes on töötajad saanud mingisugust koolitust, kuidas turvaliselt internetis käituda ning arvuteid ja infosüsteeme kasutada. Vaatamata sellele, et aina rohkem võib meediast kuulda ja lugeda, et küberrünnakud on tõusutendentsis ning puutumata ei jää tõenäoliselt ükski ettevõte, leiab üle poole vastanud ettevõtetest (55,6%), et küberhügieeni koolitus ei ole antud hetkel vajalik oma töötajatele. Lisaks sellele ei ole seitsmel ettevõttel veel kindlat plaani, kuidas lähitulevikus võimalike küberintsidentidega tegeleda: plaanis ei ole palgata lisatööjõudu ning puudub ettevõtte infotehnoloogia turvariskide analüüs. Lisaks puudub koguni viiel ettevõttel küberintsidendi hädaolukorra lahendamise plaan!

Tundub, et ettevõtted tegelevad probleemidega nende tekkimise järjekorras, mitte ei läheneta tõenäolisele ohule või isikuandmete kaitse uutele nõudmistele süsteemselt ja ennetavalt. Autori väidet kinnitab ka ühe ettevõtte esindaja kommentaar vastustes: „Lahendame küsimused nende tekkimise järjekorras“.

Uuringust järeldub, et suuremad laevandusettevõtted ning ettevõtted, kes on varasemalt kokku puutunud küberrünnakutega, on täna paremini ette valmistunud. Neil on suurem IT personal, nad on rohkem teadlikud võimalikest küberohtudest, nende töötajad on saanud või saavad lähiajal küberhügieeni alast väljaõpet ning neil on olemas küberintsidentide hädaolukorra lahendamise plaan.

3. SOOVITUSED KÜBERTURVALISUSE TÕHUSTAMISEKS

Alljärgnevalt annab autor soovitused, mida saavad laevaomanikud rakendada küberriskide maandamiseks. Sellega seoses, et laevadel võetakse aina enam kasutusele seadmeid ja tarkvarasid, mis on ühenduses interneti, sisevõrkude ja teiste seadmetega, tuleb arvesse võtta erinevaid aspekte võimalike küberohtude vältimiseks.

Meetmed, mida ettevõte saab rakendada, sisaldavad laeva- ja infosüsteemide ning infrastruktuuri kaitsmist, ettevõtte töötajate koolitamist, kasutajaõiguste piiramist süsteemidele, ettevõtte dokumentatsiooni käsitlemist vastavalt selle tundlikkusele, laeva ja kalda vahelise side turvalisemaks muutmist.

Autor jagab soovitused kaheks grupiks. Esimesse gruppi kuuluvad ettepanekud, mida saab laevaomanik rakendada lühi- ja pikaajaliselt ning teise gruppi kuuluvad üldised ettepanekud, mida võiks tulevikus arutada ja võtta koostöös mereharidusasutuste ja küberturvalisuse järelevalveorganitega kasutusele.

Esimesse gruppi kuuluvad autori soovitused:

a) küberohtude ja probleemide teadvustamine juhtkonna tasemel,
b) küberhügieeni koolitused ettevõtte töötajatele,
c) olemasolevate suuniste ja standarditega tutvumine,
d) hetkeolukorra hindamine ja riskianalüüsi läbiviimine
e) küberrünnaku intsidendiplaani koostamine,
f) ettevõtte süsteemide läbistustestimine,
g) küberturvalisusega seotud õppuste korraldamine laevas ja ettevõttes,
h) rakendada ettevõttes kõikidele arusaadav küberturvalisuse reeglistik,
i) legaalse tarkvara kasutamine ettevõtte arvutites,
j) küberriskide kindlustamine,
k) valmistumine EL isikuandmete kaitse üldmääruse rakendumiseks,
l) küberturvalisusega seotud infoportaalide jälgimine.

Teise gruppi kuuluvad järgmised ettepanekud:

a) järelevalveasutuse teavitamine turvaintsidentidest anonüümselt ning meililisti koostamine Eesti laevandussektori jaoks küberturvalisuse ja -intsidentidega seotud informatsiooni jagamiseks,
b) infopäevade korraldamine laevandusettevõtetele küberturvalisuse teemal,
c) meremeeste väljaõpe vajab muutuseid.

Järgnevates alapeatükkides selgitab autor täpsemalt tema tehtud soovitusi.

3.1 Küberohtude ja probleemide teadvustamine juhtkonna tasemel

Osaledes mitmel küberturvalisust käsitleval seminaril, tutvudes uurimistöö käigus küberturvalisuse teooriaga ning viies läbi küsitlusuuringu Eesti laevaomanike vahel, veendus autor, et kõige olulisem esimene samm ettevõttes on probleemide ja ohtude teadvustamine juhtkonna tasemel. See võimaldab tuua probleemid ja ohud lauale ning neist avatult rääkida. Siit on võimalik edasi astuda juba järgmiseid samme tõstmaks ettevõtte küberturvalisus uuele tasemele. See sisaldab turvalisuse auditi läbiviimist, arenguplaanide koostamist koos vajaliku tegevusplaani ja eelarvega.

Tänapäeval on infotehnoloogia muutunud üheks osaks äriprotsessidest. Seetõttu algab ka ettevõtte küberturvalisus pihta juhtkonnast, mitte laeva turvaülemast või IT osakonnast. Infoturbe teema võib tunduda ettevõtte juhile ebameeldiv. Seda eriti olukordades, kus on vaja vastu võtta infoturbega seotud otsuseid. Kui ettevõtte protsessid ja tegevused sõltuvad suuresti infotehnoloogiast, siis tasub kaaluda selle jaoks tööle võtta eraldi inimene või osta teenust sisse pädevalt ettevõttelt. Infoturbejuht on see inimene, kes hindab ettevõtte infosüsteemide kaitstust, koostab turvameetmete rakendamise plaani koos selleks vajalike ressurssidega ning informeerib juhtkonda toimunud intsidentidest. Soovitavalt võiks hoida infoturbe spetsialisti töökoht eraldi IT osakonnast.

3.2 Küberhügieeni koolitused ettevõtte töötajatele

Tänapäeval vajavad autori hinnangul juba kõik arvuteid ja infosüsteeme kasutavad töötajad väljaõpet. See peab sisaldama informatsiooni, kuidas hoiduda küberohtudest, kuidas ära tunda petukirjad ning kuidas käituda, kui rünnak on juba toimunud. Olenemata sellest, et täna ei ole vastavad koolitused laevapersonalile veel kohustuslikud, soovitab autor siiski laevandusettevõtetel tõsiselt kaaluda oma töötajate teadlikkuse tõstmist küberturvalisusest. Magistritöö raames läbi viidud uuring näitas, et enamus ettevõtteid, kes langesid küber-rünnaku ohvriks, ei ole oma töötajatele küberhügieeni koolitust pakkunud.

Autorile teadaolevalt teevad mitmed välismaised IT- ja koolitusettevõtted koostööd rahvusvaheliste merendusorganisatsioonidega laevandussektorile mõeldud küberhügieeni e-õppe kursuste välja töötamiseks. Seagull Maritime (https://www.seagull.no/maritime) on näiteks kasutusele võtnud klassifikatsiooniühingu DNV GL küberturvalisuse e-õppe moodulid oma treeningprogrammides, SOFTimpact (http://www.soft-impact.com) on välja töötanud küberhügieeni õppeprogrammi laevapersonalile ning uudiseid võib lähiajal oodata ka suurelt koolitusfirmalt Videotel (http://videotel.com/). Lisaks saab laevaomanik tutvuda veebi-keskkonnas https://www.maritimecybertraining.online/ asuva küberhügieeni kursusega.

Autor soovitab laevaomanikel tõsiselt kaaluda ka uue küberhügieeni e-õppe platvormi kasutusele võtmist, mis on välja töötatud Eesti ettevõtte CybExer Technologies OÜ poolt (E-õpe suurendab...2017). Loodud platvormi abil on võimalik testida ja parandada töötajate teadlikkust ohtudest digitaalses ruumis.

3.3 Olemasolevate suuniste ja standarditega tutvumine

Autor soovitab ettevõtetel tutvuda olemasolevate suuniste ja standarditega, mis on ära toodud käesoleva lõputöö peatükis 1.9 (lk 41). Need on koostatud kindla eesmärgiga – aidata laevaomanikku, vähendada riske ning tõhustada meresõiduohutust. Suunised ei ole laevaomanikule kohustuslikud, kuid nendega tutvumine ja läbi töötamine aitab kindlasti tõsta töötajate ja laeva meeskondade teadlikkust probleemidest.

2016. aasta jaanuaris avaldasid BIMCO, CLIA, ICS, INTERCARGO ja INTERTANKO suunised „*The Guidelines on Cyber Security onboard Ships*“, mille eesmärk

on anda laevaomanikele ja –operaatoritele juhised, kuidas hinnata laevade tegevusega kaasnevaid küberriske ning rakendada küberturvalisuse meetmeid laevadel.

3.4 Hetkeolukorra hindamine ja riskianalüüsi läbiviimine

Autor soovitab laevaomanikel kaaluda tõsiselt oma ettevõtte ja laevade IT süsteemide hetkeolukorda hindamist kompetentse spetsialisti või ettevõtte poolt. See annab põhjaliku ülevaate infosüsteemide olukorrast, kaitsevõimest ning puudustest. Koostatud ülevaade võimaldab esitada ettepanekud IT valdkonna arenguvajadusteks ning infosüsteemide turvalisemaks ja töökindlamaks muutmiseks.

Laevandusettevõte võib läbi viia ka ise esialgse olukorra kaardistuse, mille raames vaadatakse üle kõik infosüsteemid ja protseduurid. Siinkohal tuleks kindlasti arvesse võtta ka inimfaktor, mis on üheks suuremaks küberintsidentide põhjustajaks.

Autor soovitab ettevõtte juhtkonnal analüüsida olukorda, kus infotehnoloogia eest vastutav inimene lahkub töölt ning asemele tuleb uus töötaja. Millise raskusastmega on uus IT töötaja võimeline saama kohest ülevaadet ettevõttes ja laevades kasutatavatest info- ja võrgusüsteemidest ning arengukavadest?

3.5 Küberrünnaku intsidendiplaani koostamine

Laevandusettevõtte peab koostama ning tegema kõikidele töötajatele kättesaadavaks hädaolukorra plaani küberintsidentide jaoks. Laeva või kontori infosüsteemide vastu toime pandud rünnakutele reageerimisel ei piisa tõenäoliselt ainult ettevõtte kompetentsist seoses rünnakute keerukuse ja tõsidusastmega. Sellistel juhtudel on vaja kaasata abi väljastpoolt ettevõtet. Vastasel juhul võivad tehtud otsused ja tegevused ainult raskendada andmete ja süsteemide taastamist ning hävitada võimalikud asitõendid rünnaku kohta.

Intsidendiplaan peab sisaldama informatsiooni, kellel on õigused teha tekkinud olukorras otsuseid, millal tuleb ühendust võtta välisekspertidega ning milliseid kommunikatsioonivahendeid kasutatakse. Laevaga seotud intsidendiplaan peab sisaldama juhendavat infot olukordade kohta, kus elektroonilised navigatsioonivahendid või laeva juhtimissüsteemid ei ole enam kasutatavad. Lisaks võib see sisaldada infot, kuidas teha

kindlaks, kas arvatava rünnaku tõttu on kriitiline informatsioon veel alles ning kuidas käituda lunavaraga nakatumise korral.

Oluline on see, et asjassepuutuv personal on teadlik, kuidas käituda küberrünnaku puhul. Autor rõhutab veel üle, et intsidendiplaan peab olema kättesaadav personalile ka paberkandjal, nii laevas kui ka kontoris.

Läbiviidud uuringust selgus, et ainult kolmel küsitlusele vastanud laevandusettevõttel on olemas mingisugune tegevusplaan võimaliku küberrünnaku korral.

3.6 Ettevõtte süsteemide läbistustestimine

Läbistustestimiseks (*penetration testing*) nimetatakse sissetungirünnete imiteerimist turvameetmete toimivuse kontrollimiseks (Andmekaitse ja infoturbe leksikon 2017). Sellised testid võimaldavad hinnata, kas süsteemide tegelik küberkaitsevõime vastab ettevõtte ootustele. Tavaliselt viiakse simuleeritud läbistustestimised läbi kolmanda osapoole poolt, kes kasutavad selle jaoks infotehnoloogilisi lahendusi, manipuleerimisvõtteid (*social engineering*) ning isegi füüsilist sekkumist ettevõtte strateegilisele infrastruktuurile.

Testi tulemused annavad laevaomanikule ülevaate, kas tema ettevõtte süsteemid on haavatavad ning milline kaitse vajab üle vaatamist. Tulemused on abiks ka edasiste arenguplaanide ja eelarvete koostamisel.

3.7 Küberturvalisusega seotud õppuste korraldamine laevas ja ettevõttes

Autor soovitab ettevõtetel korraldada regulaarseid õppuseid küberturvalisuse testimiseks nii ettevõttes kui ka laevas. Reaalsete küberintsidentide läbi mängimine annab hea ettekujutuse laevaomanikule ja personalile, kuidas ollakse valmis toime tulema olukordadega, mis võivad tegelikkuses ka juhtuda.

Nii nagu laevameeskond on kohustatud regulaarselt osalema paadi-, tuletõrje- ja laeva mahajätmise õppustel, peaksid nad osa võtma ka küberturvalisusega seotud õppustel. Autor mõistab, et seni, kuni taolised õppused ei ole laevaomaniku jaoks tehtud kohustuslikuks, neid vabatahtlikult korraldama ei hakata. Samas on digitaalne maailm laevandussektoris muutunud

kiiremalt, kui regulatsioonid järgi jõuavad. Seega on tekkinud reaalne vajadus selliste õppuste jaoks.

Küberturvalisuse õppus laevas võib sisaldada näiteks järgmiseid stsenaariumeid: tiheda liiklusega alas sõitev laev kaotab kontrolli ECDISe või GPSi üle, arvutites avastatakse lunavara, mis krüpteerib kõik andmed jne. Kui laevas tehakse perioodiliselt varukoopiaid andmetest, siis kas on keegi meeskonnast suuteline taastama neid andmekandjalt?

Täna peavad laevade meeskonnad valmis olema sellisteks ootamatuteks olukordadeks ning teadma, mida tekkinud olukorras teha, millised on järgmised sammud ning keda peab tekkinud probleemist teavitama.

3.8 Kõigile arusaadava küberturvalisuse reeglistiku rakendamine

Üheks võimaluseks maandada küberriske ettevõttes on kindla küberturvalisuse reeglistiku välja töötamine ning selle perioodiline meeldetuletamine. See võib sisaldada reegleid, kuidas:

a) võivad töötajad kasutada isiklikke andmekandjaid (väline kõvaketas, USB mälupulk jms) töö juures ja laevas;
b) on paika pandud isikliku ja tööalase e-posti aadressi kasutamine;
c) laadida telefone, akupankasid, e-sigarette jms kontori ja laeva arvutitega;
d) peavad töötajad endale paroole looma (nn „paroolipoliitika“) ja kui tihti seda muutma.

Lõputöö uuringust selgus, et mõnel laevandusettevõttel juba eksisteerivad reeglid, mis reguleerivad näiteks tööalase ja isikliku e-posti aadressi kasutamist ettevõttes. Samas märkis ainult üks vastaja, et nende ettevõttes piiratakse USB mälupulkade ja USB laadijate kasutamist arvutites.

3.9 Legaalse tarkvara kasutamine ettevõtte arvutites

Kriitilise tähtsusega on ettevõtja jaoks teadmine, et tema sisevõrgus paigaldatud ja kasutatav tarkvara on legaalne koopia ning saadud usaldusväärsest allikast. Sama kehtib ka ettevõtte sisevõrgus olevate töötajate isiklike arvutite kohta, mille puhul on suurem võimalus, et paigaldatud võib olla illegaalne tarkvara koos sinna lisatud pahavaraga.

Samuti tuleb olla kindel vaba tarkvara kasutamisel, et selle päritolu on usaldusväärne. Ka vaba tarkvara võib levida erinevates piraattarkvara levitavates kanalites, kus sellele lisatakse külge pahavara. Vaba tarkvara käivitades aktiveeritakse ka sellesse lisatud pahavara, mis muudab arvutis ja sellega seotud sisevõrgus oleva informatsiooni küberkurjategijale kättesaadavaks.

3.10 Küberriskide kindlustamine

Eestis on aina rohkem levima hakanud küberriskide kindlustamine. Kui traditsiooniliselt on küberkindlustus olnud populaarsem IT-ettevõtete, finantsasutuste ja tootmisettevõtete seas, siis aina rohkem on hakanud küberkindlustust tellima ka teiste sektorite ettevõtted. Lõputöö uuringu tulemustest selgub, et ka kolm küsitlusele vastanud ettevõtet on sõlminud küberriskide kindlustuse (vt Tabel 14, lk 61).

Küberkaitse kindlustus ei kaitse ettevõtet küberintsidentide eest, kuid aitab tegeleda selle tagajärgedega. Eestis pakub laevandussektorile küberriskide kindlustust IIZI Kindlustusmaakler AS. Kindlustusfirma kodulehelt võib lugeda küberriskide hüvitamise kohta järgmist:

„Kindlustustingimused on üles ehitatud „All Risk“ põhimõttel ning on ulatusliku kaitsega. Lühidalt katab küberriskide kindlustus ära varakindlustuse, äri katkemise kindlustuse ja vastutuskindlustuse selle välistuse, mis puudutab andmete, IT-süsteemide jmt seotud kahjud“ (Küberriskide kindlustus 2017).

Autor soovitab laevaomanikel kindlasti kaaluda küberriskide kindlustamist.

3.11 Valmisolek EL isikuandmete kaitse üldmääruse rakendamiseks

25. mail 2018. aastal kehtima hakkav Euroopa Liidu isikuandmete kaitse üldmäärus muudab kardinaalselt seda, kuidas ettevõtted andmetega ümber käivad. Reeglina ei tea ettevõtted antud hetkel, millised andmed neil infosüsteemides on ning millised andmed võimaldavad personaalset identifitseerimist.

Autori hinnangul peavad laevaomanikud juba täna mõtlema selle peale, millised muudatused või täiendused on sisse vaja viia nende organisatsioonides ja infosüsteemides, et need vastaksid uue määruse nõuetele (vt Joonis 15).

Joonis 15. Valmistumine EL isikuandmete kaitse üldmääruse rakendamiseks
Allikas: (KPMG 2016)

3.12 Küberturvalisusega seotud infoportaalide jälgimine

Lihtne moodus, kuidas ennast kursis hoida maailmas toimuvate küberintsidentidega, on jälgida mõnda infoportaali, mis jagab laevaomanikule sobivat informatsiooni. Autor mõistab, et internetis leiduv infoküllus võib olla kurnav ning jälgida veel mõnda temaatilist veebilehte on palju palutud. Tänapäeval võimaldavad enamus uudiste tootmisega tegelevaid veebilehti liitumist nende uudiskirjaga, mida saadetakse lugejatele 1-7 korda nädalas. Saatmissagedus oleneb valdkonnast ning teema pakilisusest.

Autor soovitab kindlasti tutvuda CERT Eesti poolt saadetava kübervaldkonna uudiskirjaga. Uudiskirjaga liitumiseks tuleb saata e-kiri teemaga „*Subscribe*“ aadressile certnews@cert.ee. Eestikeelsetest portaalidest soovitab autor silma peal hoida tehnikaportaalil www.geenius.ee ning merendusportaalil cybersecurity.mereblog.com.

Ingliskeelsetest portaalidest võiks jälgida www.becyberawareatsea.com, mille uudiskiri *Phish & Ships* ilmub kord kuus.

3.13 Turvaintsidentidest anonüümne teavitamine

Eestis tegeleb turvaintsidentide jälgimise, ohtudest teavitamise ja ennetustegevuste korraldamisega Riigi Infosüsteemi Ameti infoturbeintsidentide käsitlemise osakond (CERT-Eesti). Osakonna ülesanded on (Turvaintsidentide käsitlemine...2017):

a) jälgida Eesti infoturbe olukorda, kasutades selleks laekunud raporteid ja kogudes ise infot infoturbeintsidentide kohta;
b) aidata ära hoida turvaintsidente ja vähendada turvariske, seda eelkõige turvateadlikkuse tõstmise ja teavitamise abil;
c) abistada asutusi infoturbeintsidentide asjus ja neid nõustada, kui nad soovivad, et õiguskaitseorganid alustaksid intsidendi uurimist.

CERT Eesti ülesannete hulka kuulub turvaintsidentide käsitlemine, avalikkuse hoiatamine turvaaukude, viiruste leviku ja küberrünnakute kohta, infoturbe alase teadlikkuse tõstmine, abi pakkumine asutuste ja interneti teenusepakkujate süsteemi- ja võrguadministraatoritele ning klienditoele.

Autorile teadaolevalt ei ole viimase kolme aasta jooksul laevandussektori poolt ühtegi raportit võimaliku küberrünnaku kohta laekunud. Lõputöö kirjutamise ajal võttis autor CERT Eestiga ühendust, et uurida, kas on võimalik luua eraldi meililist merendussektori jaoks, mille kaudu levitatakse listiga liitunud ettevõtetele informatsiooni küberintsidentide kohta merenduses nii Eestis kui ka välismaal. See eeldab ettevõtete aktiivset kaasa löömist ja listiga liitumist.

Autor soovitab laevaomanikel teavitada CERT Eestit vähemalt anonüümselt igast juhtumist, et tekiks ülevaade, milliste küberohtudega laevaomanikud silmitsi seisavad. Saadud informatsioon on abiks kõigile listiga liitunud ettevõtetele. Meililisti koostamist võiks autori hinnangul koordineerida Eesti Laevaomanike Liit.

Intsidendiraporti saab ettevõte edastada CERT Eestile teavituskeskkonna raport.cert.ee kaudu. E-kirja teel saab turvaintsidendi raporti saata e-posti aadressile cert@cert.ee. Turvaintsidendi raporti vormi leiab Lisast 3.

3.14 Infopäevade korraldamine laevandusettevõtetele küberturvalisuse teemal

Autori ettepanek on korraldada koostöös Eesti Laevaomanike Liidu, Veeteede Ameti ja TTÜ Eesti Mereakadeemiaga infopäevad Eesti laevandussektorile küberturvalisuse teemal. Lisaks spetsialistidele Eesti Mereakadeemiast tuleb kutsuda küberkuritegevusest rääkima Riigi Infosüsteemi Ameti ja TTÜ Küberkriminalistika ja Küberjulgeoleku Keskuse spetsialistid, praktikud infoturbega tegelevatest ettevõtetest ning küberkindlustust pakkuva seltsi esindaja.

Samuti on oodatud esinema tegevjuhid ettevõtetest, kes on varasemalt langenud küberrünnakute ohvriks ning kes on edukalt suutnud rakendada meetmeid küberturvalisuse tõstmiseks. Selliseid poolepäevaseid infopäevi võib korraldada näiteks TTÜ Eesti Mereakadeemia ruumides kord kvartalis. Sellise tihedusega infopäevade korraldamine aitab hoida „teemad“ õhus ning paremini informatsiooni vahendada osapoolte vahel.

3.15 Meremeeste väljaõpe vajab muutuseid

Meremeeste väljaõppele on autori poolt kaks ettepanekut:

a) Paralleelselt digitaalse tehnoloogia pealetungiga laevandussektorisse tuleb kanda hoolt ka selle eest, et laeva meeskond oleks suuteline adekvaatselt tegelema tekkivate infotehnoloogiliste probleemidega. Juba kümne aasta pärast vajatakse laevadele spetsialiste, kellel on uued oskused ja kvalifikatsioon. See tähendab aga seda, et meremehed vajavad juba praegu teistsugust väljaõpet, et toime tulla uute tehnoloogiliste väljakutsetega. Arvesse võttes ka küberriskide suurenemist laevandussektoris peavad meremehed olema võimelised hindama küberintsidendist tekkinud olukorda ning suhtlema vajadusel ettevõtte või kolmanda osapoole IT spetsialistiga. Koostöös laevaomanike, mereharidus-asutuste ning IT ettevõtetega on võimalik tõsta juba täna meremeeste kvalifikatsiooni infotehnoloogia vallas.

b) Laevandussektori sõltuvus kaasaegsest tehnoloogiast tulevikus ainult suureneb. Viimastel aastatel toimunud juhtumid näitavad, et radar, ECDIS, GPS ja AIS võivad muutuda küberrünnaku tõttu kasutuskõlbmatuks. Sellisteks olukordadeks peavad meeskonnad olema valmis ja välja koolitatud. Tulevaste laevajuhtide väljaõppes peab panema enam rõhku traditsiooniliste navigeerimisoskuste õpetamisele nagu näiteks navigeerimine tähtede järgi.

KOKKUVÕTE

Küberkuriteod on muutunud digitaalse ühiskonna paratamatuks osaks. Ühelt poolt võimaldavad uued tehnoloogilised lahendused erinevate ja uudsete teenuste arengut ning olemasolevate protsesside efektiivsemaks muutmist. Teisest küljest toovad muutused endaga kaasa uued ja senitundmatud ohud. Laevandussektor ei ole erand. Nii on tõusnud ka laevade, sadamate, terminaalide ja avamererajatiste sõltuvus moodsast info- ja käidutehnoloogiast (kommunikatsioon, navigatsioon, logistika, ohutusseire, turvalisus, mehhanismide juhtimine jne). Juba lähitulevikus on oodata omavahel võrku ühendatud ning teineteisega suhtlevate autonoomsete laevade ilmumist maailmameredele.

Selleks, et takistada kurjategijatel küberrünnakute edukat läbiviimist või vähendada nende rünnakutega kaasnevaid kahjusid, on esmalt vajalik teadvustada olemasolevat probleemi ettevõtte kõrgemal tasemel ning edasi juba pühenduda küberturvalisuse tõhustamisele ettevõtte ja laevade info- ning võrgusüsteemides. Kuna Rahvusvahelise Mereorganisatsiooni poolt ei ole laevandussektoris esinevate küberriskide haldamine veel reguleeritud, peavad laevandusettevõtted olema ise aktiivsed oma süsteemide ja infrastruktuuri kaitsmisel.

Antud magistritöö „Küberturvalisuse tagamine laevanduses Eesti laevaomanike näitel ning ettepanekud riskide maandamiseks“ eesmärgiks oli uurida, kui palju on Eesti laevaomanikud pööranud tähelepanu uutele kübermaailmast lähtuvatele ohtudele, kas ettevõtted on langenud küberrünnaku ohvriks ning millist kahju on see tekitanud. Lisaks soovis autor tuua välja soovitused, mida saavad laevaomanikud rakendada küberriskide vähendamiseks.

Autor seadis töö kirjutamisel hüpoteesi, et Eesti laevandusettevõtetes ei ole küberturvalisusele piisavalt tähelepanu pööratud ning see on endaga kaasa toonud kahjujuhtumeid ettevõtete jaoks. Uurimismeetodina kasutas autor küsitlusuuringut. Valimisse kuulusid Eestis tegutsevad laevaomanikud, kes opereerivad kauba-, reisi-, kala- ja puksiirlaevadega. Kokku saadeti ankeetküsitlus e-kirjaga 16 ettevõttele, kellest 9 andis tagasisidet. Küsimustik koosnes 33 küsimusest, millest 14 küsimusele võisid laevaomanikud vastata vabatahtlikult. Arvestades

valimisse sobivate ettevõtete arvu piiratust ning lõputöö teema tundlikkust loeb autor saadud tulemust heaks. Oma laevastiku arvu nimetas ära kaheksa ettevõtet. Üks vastaja ei soovinud infot avaldada. Kokku oli avaldatud laevastiku suuruseks 52 laeva.

Töö esimeses osas annab autor kokkuvõtliku ülevaate laevanduse arengust ning käsitleb küberturvalisust ja laevandussektoris varitsevaid küberohtusid. Teises osas keskendub autor Eesti laevaomanike seas läbi viidud küsitlusele ja selle tulemustele ning kolmandas peatükis toob välja soovitused, kuidas laevaomanik saab võimalikke küberriske maandada ning tekkivaid kahjusid ära hoida või vähendada.

Läbiviidud küsitluse tulemustest selgub, et püstitatud hüpoteesid leidsid selle töö valimi puhul kinnitust. Kolm ettevõtet tunnistas, et on varasemalt langenud küberrünnaku ohvriks ning kaks ettevõtet ei osanud sellele küsimusele vastata. Samuti kannatasid rünnaku alla jäänud ettevõtted kahjusid: ettevõtte andmete leke, mõõdetav finantsiline kahju, IT süsteemide kahjustumine ja maine kahju. Uuringu käigus saadud tulemused võib kokku võtta järgnevalt:

a) paljudes laevandusettevõtetes ei ole seni suurt tähelepanu pööratud küber-turvalisusele;
b) neli küsitlusel osalenud laevandusettevõtet ei kasuta ühtegi laevaomanikele mõeldud soovituslikku suunist küberriskide maandamiseks ning kolm vastajat ei ole kindlad, kas midagi kasutatakse;
c) ainult kahe laevandusettevõtte töötajad on saanud küberhügieeni koolitust ning enam kui pooled vastanutest (55,6%) leiavad, et küberhügieeni koolitus ei ole töötajatele vajalik;
d) ainult ühel ettevõttel on olemas reeglistik piiramaks USB mälupulkade ja USB laadijate kasutamist ettevõtte ja laevade arvutites;
e) ainult kolmel ettevõttel on piisavalt informatsiooni laevanduses varitsevate küberohtude kohta, viis ettevõtet sooviksid rohkem informatsiooni ning ühel ettevõttel puudub ülevaade küberohtudest;
f) ainult kaks ettevõtet on tellinud oma info- ja võrgusüsteemide analüüsi, ühel on see plaanis ning kuuel on see tegemata või ei ole vastajad sellest teadlikud;
g) küberrünnaku intsidendiplaan on olemas ainult neljal ettevõttel;
h) küberrünnaku alla on sattunud kolm laevaomanikku, kaks ettevõtet ei ole selles kindlad ning neli arvavad, et neid ei ole rünnatud;

i) küberriskide kindlustus on sõlmitud ainult kolmel ettevõttel;
j) neli ettevõtet kinnitasid, et nad ei ole teadlikud uuest 2018. aasta mais kehtima hakkavast Euroopa Liidu isikuandmete kaitse üldmäärusest, neli ettevõtet on teadlikud uuest määrusest ning plaanivad ette võtta vajalikud tegevused, üks ettevõte on teadlik uue määruse kehtima hakkamisest, kuid ei plaani hetkel midagi ette võtta.

Lõputöö kolmandas osas toob autor välja 15 soovitust, mida laevaomanikud saavad rakendada ettevõttes või koostöös kolmandate osapooltega. Kõige olulisemateks soovitusteks loeb autor küberturvalisuse teadlikkuse tõstmist juhtkonna tasemel ning ettevõtte töötajate koolitamist, ettevõtte infosüsteemide hetkeolukorra kaardistamist ning arenguplaanide koostamist, küberrünnaku intsidendiplaani koostamist, olemasolevate soovituslike suuniste rakendamist ettevõttes, küberturvalisusega seotud õppuste korraldamist laevas ja ettevõttes ning infopäevade korraldamist laevandusettevõtetele küberturvalisuse teemal.

Kokkuvõtteks väidab autor, et laevaomanikud vajavad rohkem informatsiooni küberohtude ning nendest hoidumise kohta. Seda saab teha koostöös teiste asutustega infopäevade ja seminaride kujul.

SUMMARY

ENSURING CYBER SECURITY IN SHIPPING WITH REFERENCE TO ESTONIAN SHIPOWNERS AND PROPOSALS FOR RISK MITIGATION

Dan Heering

Cybercrime has become part and parcel of our digital society. On the one hand, new technological solutions enable to develop various innovative services and make current processes more efficient. On the other hand, those changes bring along new and unknown threats. Shipping is no exception to the rule. Ships, ports, terminals and offshore facilities are increasingly becoming dependent on modern information and operational technology. Already in the near future we can expect interconnected and intercommunicating autonomous ships operating at sea. To prevent systems being compromised by cyber attacks or to diminish damages, the problem needs first to be acknowledged at the highest management level. Then it is possible to deal with cyber security enhancement in company networks and ship information and intercommunication systems.

The aim of the present master thesis titled „Ensuring Cyber Security in Shipping with Reference to Estonian Shipowners and Proposals for Risk Mitigation“ is to find out how much attention have Estonian shipowners paid to new cyber security risks, whether companies have been victims to cyber attacks and what are the damages cyber attacks have caused. In addition, the author wished to highlight some proposals for shipowners – what they themselves could do for risk mitigation. The author proposes a hypothesis that for Estonian shipping companies cyber security is an issue that deserves little attention and consequently, it has brought about damages for those companies. As a method survey was used. A questionnaire was emailed to 16 shipping companies, 9 of them replied.

In his thesis the author gives a brief overview of the history and the development of shipping, discusses cyber security and cyber threats in the shipping sector, then focuses on the questionnaire conducted among Estonian shipowners and its results.

Finally the author makes 15 relevant proposals for shipowners – how to mitigate possible cyber risks and how to prevent or diminish damages.

The results of the questionnaire reveal that on the basis of the sample the hypotheses were confirmed. Three companies admitted that they have been victims to cyber attacks and two companies could not provide answer to the question. The companies under cyber attack sustained damages such as company data leak, measurable financial damages, damages to their IT systems and company reputation. The results of the questionnaire could be summarized as follows:

a) four companies do not use any guidelines for cyber risk mitigation recommended to shipowners and three respondents were not sure whether any measures are taken;
b) only two companies have trained their employees on cyber hygiene, whereas more than half of the respondents (55,6%) find that cyber hygiene training is not necessary for their employees;
c) only one company has established rules on the usage of USB sticks and chargers in the company and ship computers;
d) only three companies have enough information on cyber threats in shipping, five companies would like to get more information on the subject and one company does not have an overview of cyber threats;
e) only two companies have commissioned an analysis of their information system and networks, one company is intending to do it and six of them have not commissioned such an analysis or the respondents are not aware of it;
f) only four companies have a cyber incident response plan;
g) three shipowners have come under cyber attack, two companies are not aware of any attacks and four think that they have not been under attack;
h) only three companies have bought cyber risk insurance;
i) four companies confirmed that they are not aware of the European Union General Data Protection Regulation that becomes applicable in May 2018, four companies are aware of that regulation and intend to take necessary steps, one company knows that there is such a regulation, but does not intend to anything.

The author considers the following proposals most important: increase awareness at management level and provide relevant cyber hygiene training for employees, map the current situation of the IT systems in companies and draft development plans, draft incident management plans, implement current recommended guidelines, organize cyber security exercises on ships and in companies, and organize briefings on the subject.

In conclusion, the author states that shipowners need more information on cyber threats and relevant prevention methods. This could take the form of briefings and seminars that are organised in cooperation with other agencies.

VIIDATUD ALLIKAD

AKI. Rikkumisteated.
http://www.aki.ee/et/andmekaitse-reform/rikkumisteated (13.02.2017)

Analysis of cyber security aspects in the maritime sector. (2011). The European Network and Information Security Agency. https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport

Andmekaitse ja infoturbe leksikon. Cybernetica.
http://akit.cyber.ee/ (2017)

Automated Ships Ltd and Kongsberg to build first unmanned and fully-automated vessel for offshore operations (2016)
https://www.km.kongsberg.com/ks/web/nokbg0238.nsf/AllWeb/65865972888D25FAC125805E00281D50?OpenDocument (01.11.2016)

Bateman, T. Police Warning after Drug Traffickers' Cyber-attack, BBC News
http://www.bbc.com/news/world-europe-24539417 (16.10.2013)

Beck, T. Computing's 11 Smartest Super-Viruses–And The Damage They Wrought.
https://www.fastcompany.com/3015224/computings-11-smartest-super-viruses-and-the-damage-they-wrought (8.02.2013)

BIMCO, ICS (2015). Manpower report – The Global supply and demand for seafarers in 2015. https://www.bimco.org/-/media/bimco/news-and-trends/news/crew-support/2016/manpower_report_2015_executive_summary_final.ashx

Boyd, C. Cyber-war a growing threat warn experts.
http://www.bbc.com/news/10339543 (17.06.2010)

CIA. The World Factbook, Merchant Marine.
https://www.cia.gov/library/publications/the-world-factbook/rankorder/2108rank.html (2010)

Cohen, G., Reuters. German Maker of Israeli Submarines Says Secrets Stolen in 'Massive' Cyberattack. http://www.haaretz.com/israel-news/1.757734 (8.12.2016)

E-navigation. Internation Maritime Organization.
http://www.imo.org/en/OurWork/safety/navigation/pages/enavigation.aspx (2017)

E-õpe suurendab riigitöötajate küberteadlikkust. Riigi Infosüsteemide Amet.
https://www.ria.ee/ee/e-ope-suurendab-riigitootajate-kuberteadlikkust.html (2017)

Equasis (2016). The world merchant fleet in 2015.
http://www.emsa.europa.eu/emsa-documents/latest/download/4429/472/23.html

Euroopa Parlamendi ja nõukogu direktiiv 95/46/EL. Vastu võetud 24.10.1995. –
EÜT L 281, 23.11.1995, lk 31.

Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679. Vastu võetud 27.04.2016. –
http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32016R0679&qid=1476170311681&from=ET
(04.05.2016)

Good, N., IHS Fairplay Maritime Cyber-security Survey – the results.
http://fairplay.ihs.com/article/4275151/ihs-fairplay-maritime-cyber-security-survey-the-results (19.09.2016)

Global Marine Technology Trends 2030 (2015) / Lloyd's Register, Qinetiq, University of Southampton. http://www.lr.org/en/projects/Global-Marine-Technology-Trends-2030.aspx

Goldman, R. What We Know and Don't Know About the International Cyberattack.
https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html?_r=0 (14.05.2017)

Groll, E. Did Russia Knock Out Ukraine's Power Grid? Foreign Policy.
http://foreignpolicy.com/2016/01/08/did-russia-knock-out-ukraines-power-grid/ (08.01.2016)

Interim guidelines on maritime cyber risk management (2016). International Maritime Organization.
http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC.1-CIRC.1526%20%28E%29.pdf (01.06.2016)

International Chamber of Shipping (2017).
http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade

Isikuandmete kaitse seadus. Vastu võetud Riigikogus 15.02.2007 –
RT I 2007, 24, 127

Korstanje, E. M. (2016). Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities. ISBN: 9781522519386. Pennsylvania: IGI Global.

Kaitseliit. Küberkaitse üksus.
http://www.kaitseliit.ee/et/kuberkaitse-uksus (28.04.2017)

Kim, J., Saul, J. South Korea revives GPS backup project after blaming North for jamming.
http://www.reuters.com/article/us-shipping-southkorea-navigation-idUSKCN0XT01T
(01.05.2016)

KPMG. Andmekaitse üldmäärus.
http://kpmglegal.ee/_files/Andmekaitse.pdf (2016)

Küberriskide kindlustus. IIZI Kindlustusmaakler AS.
https://www.iizi.ee/ariklient/kuberriskide-kindlustus/ (2017)

Leopando, J. World Backup Day: The 3-2-1 Rule.
http://blog.trendmicro.com/trendlabs-security-intelligence/world-backup-day-the-3-2-1-rule/
(02.04.2013)

Lõugas, H. Merd hakkavad kündma kaptenita laevad.
https://geenius.ee/rubriik/ole-homseks-valmis/merd-hakkavad-kundma-kaptenita-laevad/
(17.03.2017)

Maersk Line. Maersk Line deploys its first 2nd generation Triple-E.
http://www.maerskline.com/da-dk/countries/int/news/news-articles/2017/05/maersk-line-deploys-its-first-2nd-generation-triple-e (02.05.2017)

Majandus- ja Kommunikatsiooniministeerium (2014). Küberjulgeoleku strateegia 2014-2017.
https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., Aharon, D.
The Internet of Things: Mapping the Value Beyond the Hype .
http://bit.ly/2mm9iH8 (June 2015)

McCue, A. 'Revenge' hack downed US port systems.
http://www.zdnet.com/article/revenge-hack-downed-us-port-systems/ (7.10.2003)

Mida tähendab andmete ülekandmise õigus? Andmekaitse Inspektsioon.
http://www.aki.ee/et/andmekaitse-reform/mida-tahendab-andmete-ulekandmise-oigus
(16.01.2017)

Neate, R. Cybercrime on the high seas: the new threat facing billionaire superyacht owners.
https://www.theguardian.com/world/2017/may/05/cybercrime-billionaires-superyacht-owners-hacking (05.05.2017)

Now or never: 2016 Global CEO Outlook. KPMG.
https://home.kpmg.com/content/dam/kpmg/pdf/2016/06/2016-global-ceo-outlook.pdf (2016)

Riigi Infosüsteemi Amet. Turvaintsidentide käsitlemine CERT Eesti.
https://www.ria.ee/ee/cert.html (25.03.2014)

Riigi Infosüsteemi Ameti küberturbe aastaraport 2016.
https://www.ria.ee/public/Kuberturvalisus/RIA-kuberturbe-aastaraport-2016.pdf

Schneier, B. The Story Behind The Stuxnet Virus.
https://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html (10.07.2010)

SonicWall (2017). 2017 SonicWall Annual Threat Report. https://www.sonicwall.com/whitepapert/2017-sonicwall-annual-threat-report8121810

The Cybercrime Survey Report 2015. KPMG. https://assets.kpmg.com/content/dam/kpmg/pdf/2016/03/Cyber-Crime-Survey-2015.pdf (November 2015)

The Guidelines on Cyber Security onboard Ships. BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO. https://www.bimco.org/-/media/bimco/ships-ports-and-voyage-planning/security/cyber-security/guidelines_on_cyber_security_onboard_ships_version_1-1_feb2016.ashx?la=en (01.02.2016)

The Statistics Portal (2016). https://www.statista.com/statistics/264024/number-of-merchant-ships-worldwide-by-type/ (01.01.2016)

The Ultimate Checklist To Preventing And Fighting Ransomware Attacks (2016). Cisco. http://www.techrepublic.com/resource-library/whitepapers/the-ultimate-checklist-to-preventing-and-fighting-ransomware-attacks/post/?regId=

thyssenkrupp. Statement on the cyber-attack at thyssenkrupp. https://www.thyssenkrupp.com/en/newsroom/dataprotection/ (8.12.2016)

Torbati, Y., Saul, J. Iran's top cargo shipping line says sanctions damage mounting. http://www.reuters.com/article/us-iran-sanctions-shipping-idUSBRE89L10X20121022 (22.10.2012)

Turvaintsidentide käsitlemine CERT Eesti. Riigi Infosüsteemi Amet. https://www.ria.ee/ee/cert.html (2017)

UNCTAD Merchant fleet by country of beneficial ownership (2016). http://unctadstat.unctad.org/wds/TableViewer/tableView.aspx?ReportId=80100

Review of Maritime Transport 2016. UNCTAD. ISSN 0566-7682. http://www.unctad.org/en/PublicationsLibrary/rmt2016_en.pdf

Siegel, M., Irish, J. France's DCNS says India submarine data leak may be 'economic warfare'. http://www.reuters.com/article/us-france-submarines-india-australia-idUSKCN10Z04G?il=0 (24.08.2016)

Wagstaff, J. All at sea: global shipping fleet exposed to hacking threat. http://www.reuters.com/article/us-cybersecurity-shipping-idUSBREA3M20820140424 (23.04.2014)

Wattanajantra, A. An infection on Ministry of Defence systems affects warship communication systems. http://www.itpro.co.uk/609550/royal-navy-systems-hit-by-computer-virus (16.01.2009)

Willsher, K. French fighter planes grounded by computer virus. http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html (07.02.2009)

YARA and Kongsberg enter into partnership to build world's first autonomous and zero emissions ship. Kongsberg. https://www.km.kongsberg.com/ks/web/nokbg0238.nsf/AllWeb/98A8C576AEFC85AFC125811A0037F6C4?OpenDocument (09.05.2017)

LISAD

Lisa 1. Küsimustik laevaomanikele

Lugupeetud vastaja!

Palun leida natuke aega, et vastata allolevale küsimustikule, mis aitab selgitada välja Eesti laevaomanike teadlikkust laevanduses varitsevatest küberohtudest ning uurida, kas ja millised lahendused on kasutusele võetud võimalike küberrünnakute avastamiseks, vältimiseks ning kahjude vähendamiseks.

KPMG poolt 2016. aastal läbi viidud uuringust selgus, et küberrisk muutub tegevjuhtide hinnangul järgmise paari aasta jooksul üheks suurimaks ohuks nende ettevõttele. Samas teatas ainult 28% ligi 1300 küsitletud ettevõtjast oma firma valmisolekust võimalikuks küberintsidendiks.

Küsimustik koosneb 29-st küsimusest. Võimaluse korral palun kommenteerige oma vastuseid. Vastamiseks võib kuluda kuni 30 minutit. Küsitluse tulemusi kasutatakse anonüümselt kokkuvõtvate üldistustena magistritöö valmimisel.

Soovi korral saadan kokkuvõtte uuringu tulemustest.
Selle jaoks palun küsimustiku lõpus ära märkida oma soov ja lisada e-posti aadress.

Küsimustik on aktiivne kuni 27. aprillini.
Olen väga tänulik, kui vastate selleks ajaks kõikidele küsimustele.

Küsimustiku koostas ja küsitluse viib läbi TTÜ Eesti Mereakadeemia magistrant Dan Heering. Kui ankeedi kohta tekib küsimusi, siis palun saata need e-posti aadressile dan@mereblog.com või helistada telefonil 506 2783.

Ette tänades
Dan Heering

Lisa 1 järg

1. Ettevõtte nimi? (vabatahtlik)
2. Vastaja e-posti aadress? (vabatahtlik)
3. Vastaja telefoni number? (vabatahtlik)
4. Milline on teie ametikoht ettevõttes? (vabatahtlik)
    a. tippjuht
    b. keskastmejuht
    c. spetsialist
    d. muu
5. Milline on töötajate arv ettevõttes? (vabatahtlik)
    a. 1-10
    b. 11-30
    c. 31-50
    d. 51-100
    e. 101-300
    f. 301 ja rohkem
6. Milline on laevadel töötajate ligikaudne arv? (kohustuslik)
    a. 1-10
    b. 11-30
    c. 31-50
    d. 51-100
    e. 101-300
    f. 301 ja rohkem
7. Mitu laeva on ettevõttel? (vabatahtlik)
8. Millist tüüpi laevad on ettevõttel? (kohustuslik)
    a. kaubalaev
    b. reisilaev
    c. konteinerlaev
    d. ro-ro laev
    e. tanker
    f. parvlaev
    g. puksiirlaev

Lisa 1 järg

h. jäämurdja
i. multifunktsionaalne laev
j. lootsilaev
k. uurimislaev
l. reostustõrjelaev
m. traallaev
n. krabipüügilaev
o. krevetipüügilaev
p. muu

9. Milline on IT-ga seotud inimeste arv ettevõttes? (vabatahtlik)
10. Kas teie ettevõttes on IT riskijuhtimine korraldatud? (kohustuslik)
    a. ei
    b. jah
11. Milliseks hindate organisatsiooni vajadust IT riskijuhtimise järgi? (kohustuslik)
    a. vajadus puudub
    b. mõningal määral vajalik
    c. väga vajalik
12. Milliseid standardeid ja suuniseid kasutate ettevõttes ja laevades küberriskide haldamiseks? (kohustuslik)
    a. IMO Interim Guidelines on Maritime Cyber Risk Management
    b. The Guidelines on Cyber Security onboard Ships (BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO)
    c. United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Security
    d. Cyber security resilience management for ships and mobile offshore units in operation (DNV GL)
    e. Guide for Cybersecurity implementation for the marine and offshore industries (American Bureau of Shipping)
    f. ISO/IEC 27001:2013
    g. ISO/IEC 27002

Lisa 1 järg

h. BSI Grundschutz
i. IEC-62443-3-3
j. IEC 61162-450:2011
k. ei kasuta ühtegi standardit ega suunist
l. muud standardid või suunised

13. Milliseid tehnilisi vahendeid kasutate küberturvalisuse tagamiseks ettevõttes ja laevades? (kohustuslik)
    a. Viirusetõrje tarkvara kasutamine arvutites ja perioodiline kontroll
    b. Tulemüüri tarkvara kasutamine arvutites perioodiline kontroll
    c. Perioodiliselt uuendame tarkvara kontori arvutites
    d. Perioodiliselt uuendame tarkvara laevade arvutites
    e. Perioodiliselt teeme vajalikust informatsioonist tagavarakoopiaid
    f. Tagavarakoopiaid hoiame mitmes eksemplaris ja erinevatel andmekandjatel
    g. Arvutites on seadistatud kasutajatele põhjendatud juurdepääsuõigused
    h. Piirame USB mälupulkade ja USB laadijate (telefon, e-sigaretid jms) kasutamist ettevõtte ja laevade arvutites
    i. Ettevõtte töötajad ja laevapersonal kasutavad erinevaid e-posti aadresse isiklikuks ja tööalaseks suhtluseks
    j. Ettevõtte töötajatele ja laevapersonalile tuletatakse võimalikest küberohtudest perioodiliselt meelde
14. Kas olete teadlikud laevanduses varitsevatest küberohtudest? (kohustuslik)
    a. ei
    b. mõningal määral, aga soovime rohkem teada
    c. jah
15. Kas teie ettevõtte planeerib muudatusi seoses suurenenud küberohuga? (kohustuslik)
    a. ei
    b. planeerime, kuid täpne plaan puudub
    c. jah, planeerime

Lisa 1 järg

16. Kas teie ettevõte planeerib palgata lisatööjõudu küberturvalisuse tõhustamiseks? (kohustuslik)
    a. ei
    b. jah
17. Kas teie ettevõte on tellinud küberturvalisuse auditi, et hinnata ettevõtte ja laevade süsteemides kasutatavate kaitsevahendite efektiivsust, tuvastada turvaaugud ning kaardistada muud võimalikud ohud? (kohustuslik)
    a. ei
    b. planeerime
    c. jah
18. Kui vastasite eelnevale küsimusele positiivselt, siis palun võimaluse korral ära märkida auditi teostanud ettevõtte nimi. (vabatahtlik)
19. Kas teie ettevõttel on olemas küberrünnaku intsidendiplaan (hädaolukorra lahendamise plaan)? (kohustuslik)
    a. ei
    b. planeerime
    c. jah
20. Kas teie ettevõte on kokku puutunud võimaliku küberrünnakuga? (vabatahtlik)
    a. ei
    b. ei tea
    c. jah
21. Kui teie ettevõte on langenud küberrünnaku ohvriks, siis millist tüüpi rünnaku(te)ga on tegemist olnud? (vabatahtlik)
    a. meiliteesklus (e-mail spoofing), saatja andmete võltsimine meilipäises tegeliku saatja varjamiseks ja kirja saaja vastama peibutamiseks
    b. GPS signaali häirimine (GPS signal interference)
    c. AIS'i töö häirimine
    d. ECDIS'e töö häirimine
    e. arvutite nakatamine kahjurvaraga (malware)

Lisa 1 järg

f. lunavara (ransomware), mis rikub nakatatud süsteemi käideldavust (näiteks failide krüpteerimise teel) või teeskleb mingi kahjurkoodi avastamist ja nõuab käideldavuse taastamise või "kahjurkoodi kõrvaldamise" eest lunaraha
g. kalastus (phishing), mille sooritaja saadab tundliku teabe saamiseks sõnumeid, mis näivad tulevat sotsiaalvõrgust, oksjonisaidist, pangast vm usaldatavast allikast
h. manipuleerimisvõtted (social engineering) - mittetehniline ründevahend, mis hõlmab veenvat teesklust, valesid, altkäemaksu, ähvardusi jms, peamiselt konfidentsiaalse või tundliku teabe saamiseks
i. ei soovi vastata
j. muu

22. Kui teie ettevõte on varasemalt küberrünnaku ohvriks langenud, siis millist kahju see tekitas? (vabatahtlik)
    a. laeva vigastus või kaotus
    b. kauba vigastus või kaotus
    c. vigastused meeskonnaliikmele
    d. keskkonnareostus
    e. ettevõtte andmete leke
    f. mõõdetav finantsiline kahju
    g. IT süsteemide kahjustumine
    h. laevasüsteemide kahjustumine
    i. kahju tekitamine kolmandale osapoolele
    j. maine kahju
    k. ei soovi vastata
    l. muu
23. Kas teie ettevõtte poolt sõlmitud kindlustuspoliisid katavad küberrünnaku tõttu tekitatud kahjud (k.a. kolmandatele osapooltele)? (kohustuslik)
    a. ei
    b. jah
    c. ei soovi vastata

Lisa 1 järg

24. Kui vastasite eelmisele küsimusele „EI“, siis kas olete kaalunud küberriskide katmist kindlustuspoliisi sõlmimisel? (vabatahtlik)
    a. ei
    b. jah
25. Kui teie ettevõte ei ole langenud küberrünnaku ohvriks, siis milliseks hindate küberrünnaku võimalust enda ettevõtte vastu? (kohustuslik)
    a. 1 (madalalt)
    b. 2
    c. 3
    d. 4
    e. 5 (kõrgelt)
26. Kas teie ettevõtte töötajad ja laevapersonal on osalenud küberhügieeni koolitusel? (kohustuslik)
    a. ei
    b. jah
27. Kas teie ettevõte vajab küberhügieeni koolitust oma töötajatele ja laevapersonalile? (kohustuslik)
    a. ei
    b. jah
28. Kas teie ettevõte on teadlik 25. mail 2018. aastal kehtima hakkavast Euroopa Liidu isikuandmete kaitse üldmäärusest (http://www.eugdpr.org/) ning planeerinud vajalikud tegevused? Infoks: üldmääruse teemal korraldab CGI Eesti 28. aprillil hommikuseminari (https://www.facebook.com/events/449267255422639) (kohustuslik)
    a. ei ole teadlik
    b. jah, oleme teadlikud, kuid ei planeeri midagi muuta
    c. jah, oleme teadlikud ning võtame ette vajalikud tegevused
29. Millistest allikatest saate informatsiooni küberturvalisuse kohta merenduses? (kohustuslik)
    a. klassifikatsiooniühing
    b. uudised internetist

Lisa 1 järg

c. mereadministratsioon
d. lipuriik
e. laevaomanike liit
f. ajakirjad ja ajalehed
g. Riigi Infosüsteemi Amet
h. Andmekaitse Inspektsioon
i. muu

30. Kas vajate rohkem informatsiooni küberturvalisuse kohta laevanduses? (kohustuslik)
    a. ei
    b. jah
31. Milline on teie ettepanek küberturvalisusega seotud informatsiooni paremaks levitamiseks? (vabatahtlik)
32. Milline on teie ettepanek küberturvalisuse tõhustamiseks laevafirmas? (vabatahtlik)
33. Soovin saada uuringu kokkuvõtet e-posti aadressile. (kohustuslik)
    a. ei
    b. jah
34. E-posti aadress. (vabatahtlik)

Lisa 2. Eesti Laevaomanike Liidu liikmete nimekiri (seisuga 01.04.2017)

Eesti Laevaomanike Liit (*Estonian Shipowners's Association*)

President (juhatuse esimees):Kalev Järvelill

Peasekretär (tegevdirektor):Enn Kreem

Aadress:Kopli 101, Tallinn 11712

Kontakt:Tel/fax 613 5528, e-posti aadress: reederid@ hot.ee

1) AS Tallink Grupp (Sadama 5/7, Tallinn 10111)
2) Lindaliini AS (Ädala 4a, Tallinn 10614)
3) Eesti Mereakadeemia (Kopli 101, Tallinn 13912)
4) AS Saaremaa Laevakompanii (Kohtu 1, Kuressaare 93812)
5) Alfons Hakans OÜ (Ahtri 6A, Tallinn 10151)
6) AS Eesti Loots (Sadama tee 9, Rohuneeme, Viimsi vald, Harju maakond 74012)
7) DFDS A/S Eesti filiaal (Lõõtsa 2b, Tallinn 11415)
8) AS Kihnu Veeteed (Büroomaja 1, Papiniidu 5, Pärnu 80010)
9) Viking Line Eesti OÜ (Hobujaama 4, Tallinn 10151)
10) TS Shipping OÜ (Uus-Sadama 21/4, Tallinn 10120)
11) TS Laevad OÜ (Sadama 25, Tallinn 15051)
12) Assotsiseerunud liige Consolato del Mare OÜ (Sadama 4, Tallinn 10111)

Lisa 3. Turvaintsidendi raporti vorm (CERT Eesti)

Ettevõte, asutus:		Tel:	
Teate saaja:		Tel:	
Raporti kirjutaja:		E-post:	
Intsidendi nimetus:		Intsidendi nr:	*Täitja asutusesisene numeratsioon*

Intsidendi tüüp	
Käideldavus	
Terviklus	
Konfidentsiaalsus	
Muu	

Intsidendi põhjus			
Tarkvara viga		Kasutajaõiguste haldus	
Riistvara viga		Välise teenusepakkuja viga	
Administreerimise viga		Puudulik testimine	
Rünne		Muu	

Kriitilisus	Madal		Keskmine		Kõrge	

Intsidendi kokkuvõte:	
Intsidendi toimumise aeg (ajavahemik):	
Intsidendi ulatus ja äriline mõju (nt klientide arv):	
Intsidendi kirjeldus ja kronoloogia (mis on ohus, sündmuste jada):	
Võimalik põhjus:	
Võimalik lahendus:	
Soovitused intsidendi vältimiseks tulevikus: (Soovituse juurde märkida selle eeldatav teostamise aeg)	

Lisa 3 järg

Lisaandmed elutähtsa teenuse osutajalt hädaolukorra või selle tekkimise ohu korral: (ei täida ISKE rakendaja, kes ei osuta Hädaolukorra seaduse §34 nimetatud elutähtsat teenust)

Teadaolevad andmed prognoositava kahju kohta varale ja keskkonnale (võimaluse korral rahalises väärtuses)	
Teadaolevad andmed prognoositava mõju kohta elutähtsate teenuste toimepidevusele (millised elutähtsad teenused on mõjutatud, mõjutatud isikute hulk)	
Teadaolevad andmed hukkunute ja kannatanute kohta	
Teadaolevad andmed elanike evakueerimise või selle vajaduse kohta	
Millised isikud on hädaolukorrast või hädaolukorra tekkimise vahetust ohust teavitatud? Millised isikud vajavad teavitamist?	