TALLINNA TEHNIKAÜLIKOOL
EESTI MEREAKADEEMIA

Merenduskeskus

Helena Rattus

Elektrooniliste mereveodokumentide küberturvariskid ja nende võimalik vähendamine

Lõputöö

Juhendaja: lektor Yrjö Saarinen

Tallinn 2018

Olen koostanud töö iseseisvalt.
Töö koostamisel kasutatud kõikidele teiste autorite töödele,
olulistele seisukohtadele ja andmetele on viidatud.
Helena Rattus ……
(allkiri, kuupäev)
Üliõpilase kood: 141240VDSR
Üliõpilase e-posti aadress: helena.rattus@gmail.com

Juhendaja lektor Yrjö Saarinen:
Töö vastab lõputööle esitatud nõuetele
……
(allkiri, kuupäev)

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

SISUKORD

KASUTATUD LÜHENDID **5**

ANNOTATSIOON **6**

SISSEJUHATUS **7**

1. ÜLEVAADE MEREVEODOKUMENTIDEST **10**

1.1 Mereveodokumentide ajalugu **11**

1.2 Mereveodokumentide käsitlus tähtsamates õigusaktides **12**

1.2.1 Haagi reeglid 12

1.2.2 Haag-Visby reeglid 13

1.2.3 Hamburgi reeglid 14

1.2.4 Rotterdami reeglid 15

1.3 Elektrooniliste mereveodokumentide ajastu algus **16**

1.3.1 Elektrooniliste mereveodokumentide süsteemid 18

1.4 Mereveodokumentide areng ja tulevik **21**

1.4.1 Plokiahela ja hajusraamatu süsteemide kasutus 23

2. MEREVEODOKUMENTID JA KÜBERTURVARISKID **27**

2.1 Küberturvariskid merenduses **28**

2.1.1 Digitaliseerimine 29

2.1.2 Inimfaktor 31

2.1.3 Õigusloome 32

2.2 Mereveodokumentidega seotud küberrünnakud ja pettused **33**

2.2.1 Küberrünnakute ja pettuste näited 34

3. KÜBERVALDKONNA OHTUDE UURIMINE **36**

3.1 Sisulise osa töömeetodi seletus **36**

3.2 Intervjuu **37**

3.2.1 Valim ja läbiviimine 37

3.2.2 Küsimused ja analüüs 38

4. KÜBERTURVARISKIDE VÕIMALIK VÄHENDAMINE **40**

4.1 Elektrooniliste mereveodokumentide küberturvariskide vähendamise võimalused **40**

4.1.1 Küberturvalisuse teadvustamine 40
4.1.2 Rünnakutest teatamine ja koostöö tegemine 41
4.1.3 Elektrooniliste mereveodokumentide andmete kaitse 42

KOKKUVÕTE 44

SUMMARY 47

VIIDATUD ALLIKAD 49

KASUTATUD LÜHENDID

ABS – *American Bureau of Shipping* – klassifikatsiooniühing ABS
BIMCO - *The Baltic and White Sea Conference* – Balti ja Rahvusvaheline Merendusnõukogu
COLREG – *International Regulations For Preventing Collisions* – Rahvusvaheliste laevakokkupõrgete vältimise eeskiri
EMDE - *Estonian Maritime Document Exchange* – Elektrooniline mereinfosüsteem
FAL - *Facilitation Convention* – Rahvusvahelise mereliikluse hõlbustamise konventsioon
ILO – *International Labour Organisation* – Rahvusvaheline Tööorganisatsioon
IMO - *International Maritime Organization* – Rahvusvaheline Mereorganisatsioon
ISM - *International Safety Management Code* - Rahvusvaheline meresõiduohutuse korraldamise koodeks
MARPOL - *The International Convention for the Prevention of Pollution from Ships* - Rahvusvaheline laevade põhjustatava merereostuse vältimise konventsioon
NSW - *National Single Window* – Elektrooniline andmevahetussüsteem
P&I Clubs - *Protection and indemnity insurance* - vastastikuse kindlustuse klubi
RIA - *Information System Authority* – Riigi Infosüsteemi Amet
SOLAS – *Safety of Life at Sea Convention* - Rahvusvaheline konventsioon inimelude ohutusest mere
STCW - T*he International Convention on Standards of Training, Certification and Watchkeeping for Seafarers* - Meremeeste väljaõppe, diplomeerimise ja vahiteenistuse aluste rahvusvaheline konventsioon

ANNOTATSIOON

Kaupade mahud ja väärtused merendussektoris on olnud pidevas tõusutrendis. Seeläbi on pidanud muutuma ka töövõtted kaupadega töötamisel. See tähendab, et tööle kulutatav aeg, mis on suunatud kaupadega seonduvale dokumentatsiooni täitmisele ja teised logistilised planeerimistegevused, on muutunud ajaliselt lühemaks ja effektiivsemaks. Seetõttu on loodud merendusettevõtetele andmete kogumiseks, töötlemiseks, edastamiseks ning jagamiseks erinevaid tarkvarasid ning programme, mis on igati loomulik areng tänapäeva infoühiskonnas ja selles toimuta arengute käigus.

Laevandus oli üks esimesi sektoreid maailmas, kus rakendati ülemaailmselt kasutusel olevaid rahvusvahelisi regulatsioone nagu näiteks: COLREG, SOLAS, MARPOL, ILO, STCW, ISM jpt. Nende väljatöötamine ja rakendamine on reeglina toimunud peale tõsisemaid laevaõnnetusi, mis on kaasa toonud kas suured inimohvrid või ulatusliku keskkonnareostuse. Küberturvalisusele pole seni tõsisemat tähelepanu veel pööratud ning ühtegi kehtivat rahvusvahelist või riiklikku regulatsiooni jõustunud. (Heering 2017,13-14)

Seetõttu tuleb tuua uuendusi sisse dokumentide täitmisel, edastamisel ja vastuvõtmisel. Tehnoloogia areng on kiire ning seeläbi peavad ka inimesed kiiremini kohanema uute, paremate ja kiiremate tööviisidega kui ka võimalike ohtudega, mis tehnoloogiaga kaasneb. Kuna kõrgtehnoloogia, süsteemid ning uudsed töövõtted ei ole pikalt kasutuses olnud siis pole riskid ning küberturvalisuse veel kõigil valdkonnas töötajatel selged. Tähendades, et töö, andmete ning info ei ole alati kaitstud. Seega tuleb välja selgitada, mis on need suurimad riskid küberuumis.

Lõputöö eesmärgiks on välja selgitada küberturvariskid elektroonilistel mereveodokumentidel ning töö käigus pakkuda teoreetilisi lahendusi ilmnenud probleemidele. Selleks uurides praeguseks hetkes loodud küberturvalisust ning elektroonilisi mereveodokumente piiravaid ja määratlevaid määruseid, seaduseid ja konventsioone.

Võtmesõnad: elektroonilised mereveodokumendid, küberturvariskid, elektrooniline andme-edastus

SISSEJUHATUS

Tihti on kaubanduslike merevedude puhul tegemist suurte vahemaadega, mitmete osapoolte ning suurte kaubakogustega, sõltub õigeaegne ja probleemideta kauba sihtkohta jõudmine mitmete osapoolte sujuvast koostööst ja üksteise usaldamisest. Veelgi enam, esmatähtsaks muutub kaupade kohaletoimetamise ajaline täpsus, kindlus ja efektiivsus, mis võimaldaks nii ettevõtjatel kui ka kaupmeestel vähendada laovarude mahtu ja kulusid ning vältida tühisõitude või tühjade konteinerite vedamist. (Üksik 2014, 3)

Meretransport omab maailma majanduses väga olulist rolli. Ligi 90% rahvusvahelistest kaubavedudest tehakse meritsi. 2015. aastal ületas kaubavedu laevadega rekordilise 10 miljardi tonni piiri. Meretransporti võib tinglikult nimetada ka maailmakaubanduse ja -majanduse selgrooks, mille halvamine võib endaga kaasa tuua tõsiseid tagajärgi. (Heering 2017, 10)

Antud lõputöö teema: "Elektrooniliste mereveodokumentide küberturvariskid ning nende võimalik vähendamine" valiku põhjuseks on üha enam merenduses esiletõusev probleem küberturvalisuse valdkonnas. Tänapäeval, kus väga suur osa infovahetusest toimub läbi küberruumi on seetõttu suurenenud ka oht ja võimalus, et infot ei näe ja halda alati vaid isikud, keda arvatakse volitatud olema. Nüüdisajal on kõige olulisem teadmine ja vara igasugune info, selle omamine, valdamine ja haldamine. Seega igasugune info lekkimine, selle manipuleerimine ning ka süsteemide tahtlik rikkumine võib merenduses tuua kaasa suuri rahalisi kaotusi kui ka lausa inimelude ohtuseadmise võimaluse.

Antud valdkond on suurema tähelepanu keskmes viimaste aastate jooksul üha enam. Küll mitte väga aktiivselt Eestis, kuid siiski on hakatud koostama erinevaid materjale, uudiseid, teadustöid antud valdkonna kohta ning selle mõju üle merenduses. Hetke seisuga on eesti keelse materjalina võimalik taustsüsteem selgeks teha Dan Heering koostatud magistritööga "Küberturvalisuse tagamine laevanduses Eesti laevaomanike näItel ning ettepanekud riskide maandamiseks", millega tutvudes ning praktikat sooritades sai alguse huvi uurida lähtuvalt mereveonduse erialast lähtuvalt küberturvalisuse teemat.

Merenduse ettevõtetes on küberrünnakute arv suurenenud ja teadlikkus tõusnud ning nendest juhtumitest on rohkem hakatud teatama. Seetõttu võib pidada antud lõputöö tähtsuseks anda ülevaade elektrooniliste mereveodokumentide põhiliste küberturvariskide kohta, mis võivad mõjutada merendussektorite erinevaid osapooli.

Lõputöö eesmärgiks on välja selgitada teoreetilised küberturvariskid elektroonilistel mereveodokumentidel ning lõputöö käigus pakkuda välja lahendusi ilmnenud probleemidele. Selleks uurides praeguseks hetkes loodud küberturvalisust ning elektroonilisi mereveodokumente piiravaid ja määratlevaid reegleid ja konvensioone. Lisaks anda hinnang, kas antud seadusloome on piisav tagamaks kontrollitud ja turvaline elektroonilisi mereveodokumente edastus. Samuti välja selgitada lõputöö käigus, kui palju on mereveodokumendid kasutusel just elektrooniliselt ning palju on teavitatud küberturvariskidest kasutajaid. Lisaks uurides valdkonnas töötavatelt osapooltelt nende tähelepanekuid, arvamusi ja teadmisi antud teema kohta.

Elektroonilised mereveodokumentidega seoses on probleemiks nende võimalik ohustatus küberriskidest, millega on võimalik mõjutada ettevõtte, laeva ja terminali tööd kaasaarvatud inimeste ohutust töö tegemisel. Seetõttu on lõputöö hüpoteesina välja toodud, et elektroonilised mereveodokumendid ja nendes sisalduv info ei ole piisavalt kaitstud küberrünnakute eest ja on kergesti mõjutatavad. Samuti pole tööjõud, kes mereveodokumentidega tegeleb saanud piisava väljaõppe antud valdkonna ohtude osas.

Töö eesmärgi selgitamiseks püstitatud uurimisküsimused:

- Kas ja kui palju on elektroonilised mereveodokumendid merenduses kasutusel?
- Milline on õiguslik raamistik elektroonilistel mereveodokumentidel?
- Kui palju on reglementeeritud õigusloome abil erinevate elektrooniliste mereveodokumentide koostamine, edastamine, jagamine ja vastuvõtmine?
- Millisel viisil on võimalik veel parandada elektrooniliste dokumentide kasutamist ning nende turvalisust küberruumis?

Lõputöö eesmärgi välja uurimiseks kasutatakse kvalitatiivset uurimismeetodit, millest tulenevalt on püstitatud järgmised uurimisülesanded:

- Selgitada mereveodokumentide all mõeldavaid termineid, dokumente, nende ajalugu ja arengut.
- Selgitada välja elektrooniliste mereveodokumentide eripärad võrreldes traditsioonilisete paberkujul olevate dokumentidega.
- Analüüsida elektrooniliste mereveodokumentidega seotud reguleerivaid määruseid, seaduseid ja konventsioone.
- Koostada lõputööd toetava taustinfoga intervijuud merenduse valdkonnas elektrooniliste mereveodokumentidega kokkupuutuvate osapooltega.
- Anda kokkuvõttena tagasiside mereveodokumentide võimalike küberturvalisuse nõrkade kohtade üle.

Antud lõputöö on kirjutatud neljaks osaks, kus esimene osa annab teoreetilise ülevaate ja selgituse mereveodokunetidest. Kirjeldades, mis on mereveodokumendid, kuidas neid määratleda. Andes taustainfo, kes neid kasutavad ning mis põhimõtetel. Samuti on selgitatud elektrooniliste mereveodokumentide puhul, mis moodi alguse said ning kuidas arenenud ning mis on tuleviku suunad.

Töö teine osa on teoreetiline - uuriv osa, milles antakse ülevaade üldiselt küberturvariskidest merenduses. Lisaks kirjeldatakse lähemalt suurimaid võimalikke probleeme seonduvalt elektrooniliste mereveodokumentidega ja küberruumiga. Samuti tutvustatakse mereveodokumentidega seonduvalt pettuste ja rünnakute põhjuseid ning tuuakse välja ka näiteid antud teemal.

Kolmas osa annab ülevaate töö jaoks koostatud intervjuudest. Selgitades vestluste eesmärke, käiku ning andes ülevaate arvamustest merendusvaldkonnas töötavatelt osapooltelt, kes puutuvad töös kokku elektrooniliste mereveodokumentidega ja nende võimalike kaasnevate probleemidega.

Neljandas peatükk on töö kokkuvõttev osa, mis annab ülevaate antud lõputöö teema problemaatikast ehk küberturvariskidest mereveodokumentidega seoses. Tulenevalt intervjuudest ning lõputöö käigus uuritud materjalist tehakse järeldused ning pakutakse lahendusi, et tagada parem küberturvalisus.

1. ÜLEVAADE MEREVEODOKUMENTIDEST

Mereveodokumendid võib defineerida, kui dokumente, mis kinnitavad, määravad või annavad õiguse kauba suhtes selle saatjale, ostjale kui ka vedajale näiteks ostu-müügi, omandi õiguse või veoviisi kinnitamiseks. Samuti kuuluvad mereveodokumentide alla ka selliseid dokumente, mis määratlevad kaubaveo ümber toimuvat tegevust ja selle juriidilist õigsust. Veodokumentide definitsiooni piiritlemise muudab veelgi keerulisemaks asjaolu, et erinevate transpordiliikide puhul on nõutud veodokumentide hulk erinev. Seejuures võlaõigusseadus §211 kommentaarid selgitavad, et transpordidokumentideks ehk veodokumentideks on dokumendid, mille omamine on vedajalt kauba kättesaamise eelduseks ning on vajalikud asja ehk kauba käsutamiseks. (Üksik 2014, 18)

Kõige tähtsamaks mereveodokumentideks on konossement (*bill of lading*) ja mereveokiri (*sea waybill*). Peale eelnevalt mainitud dokumente esineb meretranspordis ka teisi tähtsaid ning vajalikke dokumente. Lõputöö käigus on kasutusel mõiste mereveodokumendid mille all on mõeldud sellised dokumendid: konossement, mereveokiri ja prahileping. Need on dokumendid, ilma milleta merevedu ei saaks toimuda.

Lõputöö teema keskendub elektrooniliste mereveodokumentidele. Tänaseks päevaks on võimalik enamus dokumente nii koostada kui ka edastada elektroonilisel teel. Samuti on olemas erinevaid tunnustatud keskkondi, kus vajalikke õigusakte luua ja jagada vajalike osapooltega. Seda kõike tänu mõningastele täiendustele eelnevalt paika pandud konventsioonides ja reeglites. Samuti on peale suurt digitaalsete töövõtete levikut kasvanud arusaam vajaduse järgi luua elektrooniliste dokumentide kasutamiseks üha täpsemaid ja täiustatumaid reeglistikke.

Nüüdseks ajaks on olemas üsna mitmeid konventsioone ja rahvusvaheliselt vastuvõetud reegleid (näiteks FAL konventsioon, Rotterdami reeglid), mis annavad täpseid juhiseid elektrooniliste dokumentide osas. Samuti on loodud NSW, mille kaudu on võimalik vahetada ja jagada elektrooniliselt dokumente liinil kallas-laev. Lisaks on loodud ka täiesti uued dokumendi baasvormid, mida kasutatakse ainult elektroonilise vormi puhul.

1.1 Mereveodokumentide ajalugu

Kakssada aastat tagasi erines rahvusvaheline kaubandus kardinaalselt sellest, mida me teame tänapäeval. Üheksateistkümnenda sajandi teisel poolel hakkas kaubandus juba vähehaaval meenutama tänapäeva. Arengu edasilükkavaks jõuks oli vaieldamatult suur osapoolte soov kaubandust mugavamaks ja effektiivsemaks muuta, kuid areng oli soovitust aeglasem. Peale tehnoloogilise arengu ja uute lepinguvormide oli vajalik ka seadusandlusesse muudatuste sisseviimine. Sellest tulenevalt sai konossementidist võtmedokument ja täidab seda rolli kuni tänase päevani. (Todd 2007, 1-2)

Uute kaubandusvormide kasutusele võtmisega suurenesid osapoolte riskid, mis olid mõningal määral leevendatud teiste kaubadokumentide kasutamisega. Kahekümnenda sajandi alguseks oli selle protsessi loogiline areng jõudnud tänapäeval kasutatava kaubadokumentide alusbaasini. Viimased 20 kuni 30 aastat on möödunud uute lepingute ja dokumentide väljatöötamise ning muudatuste tegemisele õiguslikus raamistikus. Need lahendused on omakorda leevendanud mõnda, kuid mitte mingil juhul kõiki probleeme. Seega meretranspordi seadusandluse põhitalad tuginevad üsnagi tugevalt rahvusvahelistel konventsioonidel, reeglitel ja määrustel, mida on üritatud ühtlustada ning parendada juba 20.sajandist. (Ibid, 1-2)

Erinevate riikide kaubandussektoris mõisteti juba varakult, kui väärtuslik on efektiivse majanduse tagamiseks omada ühtset piiriülest õiguslikku raamistikku, mis jagaks vastutuse ja riski lepingulistes suhetes ning suurendaks sellega ettenähtavust, kindlust ning stabiilsust. Nii kaupmeeste kui ka meremeeste tavasid on püütud rahvusvahelises kaubanduses kaupade meritsi veol nii riiklikul kui ka rahvusvahelisel tasandil ühtlustada ning kodifitseerida mitmetel erinevatel ajaperioodi, alates klassikalise ajajärgu mereõiguslike normide kogust Lex Rhodia kuni tänaseni. (Üksik 2014, 12-13)

Suuremad ühtlustamiskatsed rahvusvaheliste konventsioonide puhul algasid alles pärast esimest maailmasõda, vajadusest tasakaalustada vedaja ning kauba saatja ja -saaja vahelisi õigusi ja kohustus. Sealhulgas tõsta konossementide, kui väärtpaberite, usaldatavust ja väärtust, mis aitaks ühtlustada unifitseeritud dokumentatsiooni kasutuselevõttu, mis omakorda kiirendaks lepingute koostamise ja analüüsimise protsessi ning muudaks selle ühesemalt

mõistetavaks mõlemale lepingupoolele. Esimesena sõlmiti 25. augustil 1924 aastal Brüsselis Haagi reeglid, millele järgnesid ja mida täiendasid Haag - Visby, Hamburgi ja Rotterdami reeglid. (Ibid, 13)

1.2 Mereveodokumentide käsitlus tähtsamates õigusaktides

Esimesed katsed koostada konossementide kohta unifitseeritud reegleid tehti rohkem kui sada aastat tagasi. Tulemuseks oli konossemendi nii nimetatud Liverpooli konverentsivormi väljatöötamine, mis kinnitati 1882 aastal Rahvusvahelise Õiguse Assotsiatsiooni poolt Liverpoolis ja kuulutati välja 1883 aastal New Yorgis. Seisukohtade kokkulengevust erinevate riikide vahel siiski ei saavutatud ja need jätkasid oma konossementide küsimusi reguleerivate reeglite väljatöötamist. (Eidast 2007, 177)

Rahvusvaheliste mereõiguse õigusaktide unifitseerimiseks asutas Rahvusvaheline Õiguse Assotsiatsioon 1896 aastal Rahvusvahelise Merekomitee, mis jätkas konossementide tingimuste väljatöötamist ja arendamist. 1921 aastal võeti Haagi konverentsil vastu nii nimetatud Haagi Reeglid. Nende põhilised seisukohad, milliseid küll muudeti ja täiendati 1924 aastal Brüsselis ning ka hiljem, on säilinud tänapäevani. Hetke seisuga on kolm suuremat ja tähtsamat konvensiooni, mis reguleerivad kaupade merevedusid: Haagi reeglid, Haag-Visby reeglid ja Hamburgi reeglid. (Ibid, 177)

Eesti jaoks on oluline ka Põhjamaade koostöö tulemusena Põhjamaades (Soomes, Norras, Rootsis ja Taanis) 01.10.1994 aastal jõustunud mereseadus. Eestis reguleerib meritsi kaubaveo lepinguid kaubandusliku meresõidu seadus. Eesti Vabariik ei ole ühegi mereveolepinguid käsitleva konventsiooniga tänaseni ühinenud, kuigi vastutuse osas jälgib kaubandusliku meresõidu seaduse kohaselt Haagi-Visby reegleid. (Suursoo, Eidast 2016, 367)

1.2.1 Haagi reeglid

Haagi reeglid võeti vastu 1921 aasta Rahvusvahelise Mereõiguse Assotsiatsiooni konverentsil. Nendesse tehti mõningad täiendused 1922 aasta Rahvusvahelise Merekomitee Londoni konverentsil. Antud reeglid reguleerivad mereveo küsimusi välja arvatud elusloomade ja tekil veetava lasti vedu, kui konossemendis pole kokku lepitud teisiti. Samuti

korraldavad antud reeglid konossementide vormistamist, kuid reeglite kasutamise eelduseks on osapoolte kokkulepe. Konventsiooni eesmärgiks oli ka standardiseerida vedaja vastutust kauba osas ning panna paika klauslid, mille puhul ja mis ulatuses vastutatakse. Selle konventsiooni eesmärgiks oli vähendada vedaja vastutust ja standardiseerida teda vastutusest vabastavaid klausleid. Seda just seetõttu, et vedajad olid aegade jooksul konossementidesse sisse kirjutanud kauba oleku eest mitte vastutamise ning sihtsadamasse jõudes ei pruukinud olla kaup sobivas seisukorras tingituna hoopis mitte halbadest ilmastikuoludest mereveo ajal, vaid hoopis vähesest mehitatusest alusel, ebapiisava või vähesest kauba kinnitamisest.

Haagi reegleid on täiendatud ka omakorda Brüsseli konventsiooniga, mis võeti vastu 1924 aastal ja jõustusid 1931 aastal. Täiendamise tingisid konteinerite kasutusele võtmisest tulenenud probleemid. Nende erinevuseks on asjaolu, et kui Haagi reeglid kehtivad osapoolte kokkuleppel siis Brüsseli konventsioon on kohustuslik kõigis selle ratifitseerinud riikides. See tähendab, et ühinenud riigid olid kohustatud konventsiooni nõuded riigi õigusloomesse lisama ja sobitama. Tähelepanu väärne on aga see, et seda on teinud põhiliste punktide osas ka mitteratifitseeritud riigid. Eesti Vabariigi valitsus oli Haagi reeglite väljatöötamisel kaasatud ja allkirjastas konventsiooni, kuid konventsioon jäi Riigikogus ratifitseerimata. Seetõttu ei ole Eesti Vabariik juriidiliselt konventsiooni osaline. (Eidast 2007, 33)

1.2.2 Haag-Visby reeglid

Haag-Visby reeglid võeti vastu 1968 aastal ning kujutavad endas põhiliselt Haagi reeglite taaskordset laiendamist. Haagi-Visby reeglid eelistavad veolepingus vedaja huve ja on seega vedajakesksed. Juhul, kui vedaja oli täitnud oma põhilise kohustuse ehk näidanud üles nõutavat hoolsust ja andnud veo alguseks meresõidukõlbliku ja kaubaveoks sobiliku, vajalikult mehitatud ja varustatud laeva, siis reisi ajal juhtunu osas ta reeglina kahju tekitamisest kaubale või selle kaotamise eest vastutust ei kanna. (Suursoo, Eidast 2016, 366)

Reeglites olid veel tähtsad täiendused järgmiste punktide kohta: konossementide andmeid tuleb vaadelda kui lõplikku tõestust millised ei kuulu vedaja poolt ümberlükkamisele, kui konossement anti edasi heaperemehelikule kolmandale osapoolele. Samuti hagi esitamiseks võidakse aega pikendada, ehk et ei piirduta ühe aastaga, kui pooled on kokku leppinud mõne muu ajalise piiri. Kuid samas võib peale aastase piiraja möödumist rakendada regressiõigust,

kui seda menetlev kohus seda otsustab. Lisaks vaadeldakse kilogrammi alternatiivina koha- või kaubaühikuna ning vedaja vastutus tõsteti kuni 10 000 Poincare frangini, võrreldes varasema 100 kuldnaela ühiku eest või 30 Poincare frangiga 1 kilogrammi eest. (Eidast 2007, 34)

1969 aastal võeti Brüsselis vastu veel üks protokoll konvensiooni kohta, mis asendas Poincare'i frangi rahvusvahelise valuutafondi ühikuga SDR, ehk *special drawing rights*. Esialgu oli SDR ühiku väärtuseks 0.888671 grammi puhast kulda, mis oli täpselt 1 USD väärtus. SDR väärtus aga kaasajal on hoopis teine. Praegusel hetkel on selle all 5 eri valuutat. (Ibid, 34)

1.2.3 Hamburgi reeglid

Hamburgi reeglid kirjutati alla diplomaatilisel konverentsil 1978 aastal. Sisuliselt kujutavad need Haag - Visby reeglite nii täiendamist kui ka muutmist vedaja vastutuse suurendamise suunas. Hamburgi reeglid jõustusid 1992 aastal, kuid selles osalevad suhteliselt madala majandusliku arengutaseme ja merendusega riigid. Seega Hamburgi reeglid on küll suuremas osas vastu võetud, kuid praktilist kasutamist väga ei leia.

Hamburgi reeglid kehtestavad vedaja vastutuse presumptsiooni hooletuse korral ühes vastupidise tõendamiskoormisega. Vedaja loetakse süüdi olevaks ning vastutavaks kahju tekitamise eest mitte ainult lasti puudujäägi, vigastamise või riknemise eest, vaid ka hilise kohaletoimetamise korral, välja arvatud siis, kui ta suudab tõendada, et tema või ta agent (sadamas), kelle kontrolli all oli last, on teinud kahju vältimiseks kõik mõistlikkuse piires nõutava. Vedajal lasub täiendav risk veel seetõttu, et ta hakkab vastutama kauba sadamas viibimise ajal, millal kaup pole reaalselt tema või vedaja agentide kontrolli all. Samuti lisandus muutusena asjaolu, et vedaja vastutuse periood suurendati kahe aastani. Lisaks annuleeritud on niinimetatud navigatsioonivea erandid ja piiratud on ka erandlikud seosed tulekahjudega. (Suursoo, Eidast 2016, 366)

Ühinemise soov Hamburgi reeglitega eeldab aga riikidel Haagi reeglite asendamist ning kasutamist leiab see kõikide reeglitega ühinenud riikide vahelistel tšartervedudel. Kusjuures vastutust kauba eest kannavad nii lepinguline kui ka tegelik vedaja. Lisades veel juurde, et

vedajale esitatud pretensioonide puhul on konossement otsustavaks tõenduseks ka selle edasiandmisel kolmandale osapoolele. (Eidast 2007, 34-35)

1.2.4 Rotterdami reeglid

Intermodaalsete vedude, seehulgas konteinervedude jätkuv kasv ja areng viis selleni, et rahvusvahelisele kaubandusele tavalisest sadamast-sadamani teenusest osutus vajalikumaks uksest-ukseni teenus, kus tootja või müüja laost veetakse konteiner ostja lattu ning peale meretranspordi kasutatakse veel mitmeid teisi transpordiliike. Taolised intermodaalsed veod on keerulised ning eriti vaidluste ja kahjunõuete menetlemine komplitseeritud, kuna eri liiki transpordivahendite puhul kehtivad erinevad reeglid, vedajate vastutuse piirmäärad on kordades erinevad, mistõttu palju energiat ja kulutusi tekib ainuüksi kahju tekkimise hetke kindlaksmääramisest. Seetõttu koostati rahvusvahelise kaubanduse kaasaegsetele nõuetele vastav konventsioon, mida hakati nimetama Rotterdami reegliteks. (Suursoo, Eidast 2016, 367)

Allakirjutamise tseremoonia toimus Rotterdamis 23.septembril 2009 aastal, kus allkirjastasid konventsiooni 16 osalisriiki. Rotterdami reeglite toetajate ja teostajate hulka kuuluvad näiteks CMI, BIMCO, ISC. Allkirjastanud riikide hulgas on paljud soliidsed merendusriigid, seehulgas USA, Holland, Prantsusmaa, Taani. Paraku on ratifitseerimisprotsess takerdunud. Seda kuna paljud kardavad selle reeglistiku kasutuselevõttu, sest see on mahukas, keeruline erinevate transpordimooduste kohta ja ka üsna raskelt rakendatav.

Rotterdami reeglid on sisult küllaltki imperatiivse iseloomuga, mille osapooleks saamisel tuleb denonsseerida osalisriigiks olemine, kas Haag - Visby ja/või Hamburgi reeglites, mille jõustumise momendist hakkab uus valik seejärel kehtima. Mingeid reservatsioone Rotterdami reeglite artiklitele teha pole lubatud. Rotterdami reeglite puhul on tegemist 17 000 sõnast koosneva põhjaliku uuendusega kaupade veol nii multimodaalselt, koos meritsi veoga, kui ka vaid meritsi. Mahukas dokument, mille koostamiseks kulus aastaid ja mille vastuvõtmist survestasid eelkõige kaubasaatjad ja omanikud, pole siiani veel korralikku käivitamist saanud.

Lisaks eelnevad rahvusvahelised konventsioonid ja reeglid otseselt ei reguleerinud elektrooniliste mereveodokumentide kasutust, õigusi ning kohustusi siis merenduse

organisatsioonid üritasid sellele lahendust leida, kokkupannes Rotterdami reeglistikku. Reeglid reguleerivad ka lisaks elektrooniliste mereveodokumentide kasutamist ning annavad neile samaväärsed õigused agu paberist vormidel on. Erinevate uuendustega, näitekst seoses e-kaubanduse ja e-dokumentatsiooniga, vähendab see oluliselt paberimajandust ning lepingutega seonduvaid kulusid.

1.3 Elektrooniliste mereveodokumentide ajastu algus

Paberkujul konossemendid on olnud kasutuses maailmas ja mõjutanud kogu kaubandust mitmete sajandite vältel. Vaatamata tänapäeva maailmas levivale digitaliseeritusele on paberkujul konossement jäänud ilma suuremate muutuse sisseviimiseta. See on siiamaani kasutusel kauba vastuvõtukviitungi, tõendina mereveolepingu tingimuste kohta ja kaubaväärtpaberina. Just need funktsioonid on kuni praeguse ajani takistanud paberkujul konossementi asendamist digivariandiga. (Underhill, Bibby 2016)

Konossement on olnud kasutuses paberkujul juba sajandeid, kuid ka sellel on omad vead, mis on andnud põhjuse vaadata positiivsema pilguga elektrooniliste dokumentide kasutamise ja arendamise suunas. Eelised elektroonilise dokumendi vormil paberist versiooni ees on nii mõnigi. Üheks suureks ja tähtsamaiks eeliseks võib pidada dokumendi liikumise kiirust. Tänapäeval on see sageli problemaatiline, sest veo kiirused ja kauba kogused on kasvanud ja kaubalast võib olla mitu korda edasi müüdud vedamise ajal. Selle tulemusena konossement ei pruugi jõuda lastisaajani õigeaegselt ja vedaja on sunnitud vastu võtma kaubasaatja garantiikirja lasti puuduste kohta. Garantiikiri aga ei vabasta vedajat vastutusest vastavalt konossemendile ja lisab administratiivset tööd koos veo kallinemisega. Seda kõik ainult seetõttu, et vedajad on kohustatud lossima kaupa vastavalt väljastatud konossemendi originaalile, kuid antud dokumendi saatmine paber kujul võib olla üsna ajakulukas. Seeläbi elektroonilist konossementi on võimalik saata hetkeliselt üle maailma, mis väga suures osas vähendab administratiivset koormust, eriti, kui lasti omanik korduvalt vahetub. Igasuguseid parandusi on tunduvalt lihtsam ja odavam sisse viia. Elektroonilised makseviisid ja turvalisusega seotud edusammud teevad süsteemi tunduvalt turvalisemaks võrreldes pabervariandiga, kuid seda vaid sinnamaani kuni tuleb küberturvalisuse teema arutusele.

Elektroonilise konossomendi peamiseks aeglaselt levimise põhjuseks on see, et seda ei kohelda samal viisil õiguslikult konventsioonides ja reeglites, kui paberkujul konossementi (v.a Rotterdami reeglid). Peamiseteks põhjusteks on asjaolud, et paberkonossement on ametlik dokument, mida saab kasutada läbirääkimistel ja on tõendina kauba omamisese tõestamiseks. See ei pruugi olla nii aga elektroonilise konossemendiga. Lisaks rakenduvad Haagi-Visby konventsiooni veolepingu reeglite punktid ainult paber konossemendile või muu samaväärse ametliku paberdokumendile. Praegu pole see veel elektroonilisele konossemendile laienenud. Samas pärast digitaalse konossemendi klausli lisamist BIMCO NYPE 2015 ajatšarteri vormi ja P&I klubide heakskiitu algas hulgaliselt elektroonilise konossemendi kasutus ning pabervormi kasutamine on jäänud järjest vähemaks. (Underhill, Bibby 2016)

Ühe võimaliku lahendusena Haag - Visby reeglist tuleneva elektrooniliste dokumentide mitte tunnistamisele probleemile oleks osapoolte omavaheline leping. Selle jaoks peavad osapooled aga kokkuleppima ühesuguste reeglite kasutuselevõtus, mida kõik osapooled oleksid kohustatud täitma ja järgima. Selle süsteemi heaks näiteks on elektrooniliste veodokumentide süsteem BOLERO, mis on olnud kasutuses alates 1990ndatest ja töötab ainult osapoolte vahel, kes kasutavad sellele süsteemile omaseid ühtseid reeglistiku. Kui elektroonilise veodokumentide süsteemi kasutaja sõlmib tehingu mitte elektroonilise veodokumentide süsteemi kasutajaga, siis elektroonilist süsteemi ei ole võimalik kasutada ja koostatakse paberkonossement. Kuigi see süsteem on kasutajate vahel sõlmitavate tehingute mõsites mugav siis see funktsioon takistab laialdast elektrooniliste veodokumentide kasutuselevõttu, sest nende efektiivsus on proportsionaalne kasutajate arvule.

Elektrooniliste kaubadokumentide kasutus oli ka varasemalt olemas merenduses, kuid BIMCO poolt tunnustatud alates 2015 aasta NYPE vormi uuendamisest. Sinna lisatud elektroonilise konossemendi klauslitega öeldakse kokkuvõtvalt, et elektroonilise kaubadokumentide süsteemi kasutamine on võimalik tšarteri valikul. Samuti saavad omanikud tellida tšarteri poolt valitud elektrooniliste dokumentide süsteemi, eeldusel, et süsteem on tunnustatud rahvusvahelise P&I klubide grupi poolt. Sellisel juhul maksavad tšarterid kõik kulud, mis kaasnevad omanike poolt valitud süsteemi valikuga. Samuti tšarterid

hüvitavad omanikele valitud süsteemi kasutusest tulenevad kulutused, kuid ainult juhul, kui kulutused pole tekkinud omaniku hooletusest.

Praegusel ajal on elektrooniliste veodokumentide plussid nähtavad konteinervedude puhul, sest sageli on eraldi konossoment vajalik iga konteineri jaoks. Elektrooniliste kaubadokumentide süsteemide kasutus ei piirdu samas ainult konteinervedudega. Suured kaubafirmad, finantsautused ja naftasaaduste tootjad kasutavad selliseid süsteeme ja on selge, nende tähtsus merenduses kasvab tulevikus veelgi.

1.3.1 Elektrooniliste mereveodokumentide süsteemid

Rahvusvahelise P&I Clubs poolt on heaks kiidetud kolm elektroonilist kaubadokumentide süsteemi: BOLERO, essDOCS ja E-title. See tähendab seda, et kindlustus juhtumite puhul on kahjud kaetud samasugustel tingimustel nii paber- kui elektroonilise konossemendi kasutamisel.

Elektrooniliste kaubadokumentide süsteemide kasutusega kaasnevad mitmed riskid: häkkimised, süsteemi kokkuvarisemine, e-vargus ja viirused. Ükski neist juhtudest ei ole tavaliselt P&I klubide poolt kaetud ja vajab seega eraldi kindlustust. Sellega seoses essDOCS, mis on kasutuses 71 riigis üle 3000 firma poolt, võib olla kindlustatud kuni USD $20 miljonit elektoonilise konossomendi kohta. Nimetusega “eRiskid” kindlustus hõlmab enda all sealhulgas elektroonilist kuritegevust ja süsteemitõrked.

Samuti teevad elektrooniliste dokumentide süsteemide arendajad pidevat tööd turvalisuse osas. süsteem on turvaline ja konossemendi võltsimine võrreldes paberkandja konossemendiga on tunduvalt keerukam. BOLERO ja essDOCS rakendavad süsteemis kõigeima tehnoloogilise turvalisuse taseme. Seega ohtu, et keegi tungib süsteemi ja muudab konossemendi sisu on minimaalne. Paber konossemendi omand on asendatud «ainukontrolliga» elektroonilise dokumendiga. BOLERO kasutab digitaalseid sertifikaate, mis annab krüptitud, unikaalse allkirja, samal ajal kui essDOCS tugineb kahe faktoriga autoriseerimis süsteemile. (Lichman 2016, 19)

Vanim neist elektrooniliste dokumentide süsteemidest on BOLERO, siis essDOCS ja uusim E-Title. Lisaks turul on hulk teisi süsteeme, mis baseeruvad juba olemasolevatel eelpool mainitud süsteemidel. Kõigi kolme, BOLERO, ESS ja E-Title´i puhul on vaja kõigil kasutajatel sõlmida mitme osapoolega leping selleks, et elektrooniline süsteem oleks juriidiliselt aktsepteeritav. Juhul, kui üks osapooltest ei ole elekrtoonilise süsteemi kasutaja, tuleb väljastada paberkujul konossement, mis vähendab olulisel määral elekrtoonilise süsteemiga kaasneva kasu.

BOLERO on avatud IT süsteem, mis kergendab dokumentidel kogu kaubandusketi läbimise. BOLERO opereerib nelja valdkonna abil: reeglite raamat – õiguslik raamistik; digitaalsete allkirjade/sertifikaadide asutused; standartsed dokumendid ja erapooletu omand. Rahvusvahelisel turul tegutsevatele ettevõttetele pakkub BOLERO teenuseid viies valdkonnas: vahetada standartiseeritud kommerts-, finants- ja ametlikud dokumendid õiguslikult seotud ja kinnitatud formaadis; avaliselt standartiseeritud dokumentatsioon; integreeritud tagavara infosüsteem; parandab tarneahela efektiivsust; ja kasutada avatud süsteemi kauplemiseks erinevate pankade keskkonnas. (Lichman 2016, 19)

Aastal 2005 asutatud CargoDocs on tänaseks üks suuremaid ettevõteid, kes pakub erinevatele ettevõtetele võimalust minna üle elektroonilisele dokumentatsioonile. CargoDocs oli aastal 2014 ümber nimetatud essDocsiks. Ettevõtel on üle 3400 kliendi, 72 riigis tehakse süsteemi kasutamise katsetusi ja paljudes riikides on süsteem juba ka kasutusele võetud. Ettevõtte poolt pakutava süsteemiga on liitunud 27 maailmapanka. Ettevõte teeb aktiivset koostööd FIATAga (*International Federation of Freight Forwarders Associations*), mis võimaldab neil väljastada elektroonilisi Fiata Konossemente. essDocs kasutavad paljud ettevõted väga erinevates valdkondades, kuid viimastel aastatel keskendub ettevõte põhiliselt neljale turuosale ja nendeks on: metallid ja mineraalid, energia, kemikaalid ja põllumajandus. Samuti on liitunud ka paljud pangad ja transpordiettevõted. (Ibid, 21)

E-title™ on nendest elektrooniliste mereveodokumentide süsteemidest kõige uuem. See on väljatöötatud spetsiaalselt fookusega laevaliinide, logistika teenuse pakkujatele ning kommertsettevõtetele. Süsteem on ülesseehtitatud korralikule õiguslikule alusele, mis võimaldab edastada elektroonilisi konossemente ja mereveokirju. Vähendades sellega

igasuguseid kulusid pabervormiga seonduvate kuludele. Süsteemi funktsioonid lubavad suhelda ning edastada dokumente muretult kõikidel osapooltel.

1.4 Mereveodokumentide areng ja tulevik

Meretranspordi sektor on tänapäeval pidevalt muutuv ja pikaajalised perspektiivid on mõõdetavad kuudes – 60 kuud on ettekujuldematu, 24 kuud on arvatavasti maksimumaeg, mida saaks ennustada ning majanduslikus mõttes plaane seada. Selline arusaadav lühiajalisus dikteerib strateegilist otsustusvõimet. (Clayton 2018)

Merenduse valdkond pole kunagi olnud esimene erinevate uuenduste väljatöötamise, ülevõtmise ja kasutamisega. Kuna aga maailmas on tehnoloogia areng üsna kiire ning, et valdkond ka tulevikus jätkusuutlik oleks, tuleb merendusel traditsoonilistest lahendustest edasi liikuda uute ning tehnoloogiliste lahenduste suunas.

Pärast elektrooniliste konossomentide klausli kaasamise BIMCO uusimasse NYPE vormi on selge, et elektrooniliste kaubadokumentide süsteemide kasutus suureneb. Samuti on peale NYPE vormi uuendamist järgnenud ka teiste lepinguvormide uuendused, just elektrooniliste mereveodokumentide osas. Paratamatult on esmaste ilmnevate probleemide seas oodata probleeme elektrooniliste kaubadokumentide süsteemide kasutuselevõtuga seotud juriidilised probleemid tööstuses. Lisaks eelnevale probleemile kaasnevad ka mured küberriskidega, on siiski saadav kasu liiga suur, et mitte kasutada elektroonilisi võimalusi. (Underhill, Bibby 2016)

Peale küberriskide, mis tänapäeval tundub nii ilmne probleem, on veel ka teisi takistusi, mida elektrooniliste mereveodokumentide puhul tuleks ületada. Üks suurimaid ja tähtsamaid ülesandeid on muuta elektroonilised dokumendid õiguslikult ja regulatiivselt võrdväärseks paberkonossemendiga. Tulevad need probleemid just elektrooniliste kaubadokumentide süsteemide ülesehituse ja regulatsioonide tõttu. Nimelt saavad süsteemide kasutajad sõlmida elektroonilisi dokumente, vaid süsteemide kasutajate vahel, et dokument oleks juriidiliselt aksepteeritav. Vastasel juhul tuleb sõlmida süsteemi kasutaja ja mittekasutaja vahel paber vormil dokumendid, et need oleks õigluslikus mõttes kehtivad, see aga tühistab igasuguse digitaalse dokumendi vormide kasutamise.

Vaatamata aastakümnete jooksul toimunud aeglasele omaks võtmisele, on viimasel paaril aastal elektrooniliste veodokumentide süsteemide poolt täheldatud nende platvormide

märgatavat kasutuse suurenemist. Kasutuse suurenemise taga on aravatavasti mitmeid põhjuseid, kuid peamised on merendussektori suurem tunnustus, sest didgitaalse tehnoloogia kasutuselevõtt on tulevikus vältimatu. Lisaks rahvusvahelise P&I klubide ja teiste mõjukate assotsiatsioonide nagu BIMCO heakskiit, mis kindlasti annab elektrooniliste mereveodokumentide kasutusel hoogu juurde. Hea näitena võib tuua, et valdkonna suurtegijad võtsid kasutusele elektrooniliste dokumentide süsteeme, oli see heaks eeskujuks väiksematele tegijatele. Näiteks 61% maailma tankerilaevastikust kasutab juba CargoDocs süsteemi. See julgustab ka teisi sektoreid kaasa minema uuendustega.

Kui kaua võtab aega näiteks ühe mereveodokumendina tuntuma, paberkonossementide, asendamine elektrooniliste konossementidega suuremas osas maailma merenduses pole veel selge. Edasine areng toimub edasi tõenäoliselt sektori kaupa ja laevandussektoris on mõni sektor, mis näib olevat vastuvõtmiseks küps. LNG on üks väga hea näide. Elektrooniliste konossementide ksutuselevõtt on LNG sektoris olnud siiani aeglane. Näiteks ESS´i elektrooniliste dokumentide süsteemi avaldatud infost on LNG sektor võtnud kasutusele CargoDocs´I elektrooniliste konossementide süsteemi suhteliselt hiljuti, septembril 2016. Arvestades firmade vähesust LNG sektoris ja piiratud LNG terminalide arvu kogu maailmas ja seda, et last võib olla korduvalt edasimüüdud enne sihtpunkti jõudmist, on selge, et LNG sektor on sobiks hästi elektrooniliste konossementide laiemaks kasutamiseks. Just seetõttu, et see on üsna noor valdkond ning seda saaks arendada siis juba koos uudse dokumendite vormide ja süsteemidega. (Underhill, Bibby 2016)

Positiivsena võib näha ka prognoosi, et tehnoloogia areng võib tuua tulevikus üha enam noori inimesi juurde merenduse valdkonda. Seda läbi infotehnoloogia valdkonna arengu ja põiumumise antud valdkonnas, kus paratamatult palju süsteeme on seotud infotehnoloogiliste lahendustega. Samas tuleb mõista, et noorte uuendusmeelsed mõtted ja ideed on ehk kasuks lugupidamist vääriva eaga valdkonnal. Eelmine aasta merenduses investeeriti umbes 65 miljardit dollarit uutesse tehnoloogilistesse lahendusestesse ja süsteemidesse. Kui väike osa sellest investeeritaks noortesse inimestesse, selleks, et muuta asju paremaks, oleks tulemus ette kujuldamatu - see oleks hiiglaslik. (Walia 2018)

1.4.1 Plokiahela ja hajusraamatu süsteemide kasutus

Üha enam teevad erinevad valdkonnad koostööd. Seda ilmselgemalt, kuna tehnoloogiad arenevad ning pole mõistlik üksinda jalgratast leiutada. Loogilise jätkuna näeme, et IT-valdkond on laienenud ka merendussektorisse. Seega ei saa vaadelda tuleviku teemat ilma, et jälgiks infotehnoloogia arengusuundi. Viimaste tehnoloogiasüsteemide suurim ja järjest enam leviv lahendus on plokiahel (ingl.k. *block chain)*. Plokiahela tehnoloogia võimaldab kaubanduspartneritel vahetada transpordidokumente ilma vahendajateta ja ilma paberita. Sellel eesmärgil testivad hetkel mitmed laevafirmad plokiahela süsteemil saadetavaid mereveodokumente, selleks, et saatmis protsesse sujuvamaks muuta. Sellised mereveodokumendid oleksid saadetud automatiseeritud süsteemis ja baseeruksid detsentraliseeritud turvalises võrgukeskkonnas. Tehnoloogia võib hõlbustada ka tarnijate, turustajate ja reguleerivate asutuste vahelisi turvalisi koostoimeid. Samuti on see võimalus siduda makseprotsessi plokiahelaga, saavad tarnijad olla kindlad, et neile makstakse. (Underhill, Bibby 2016)

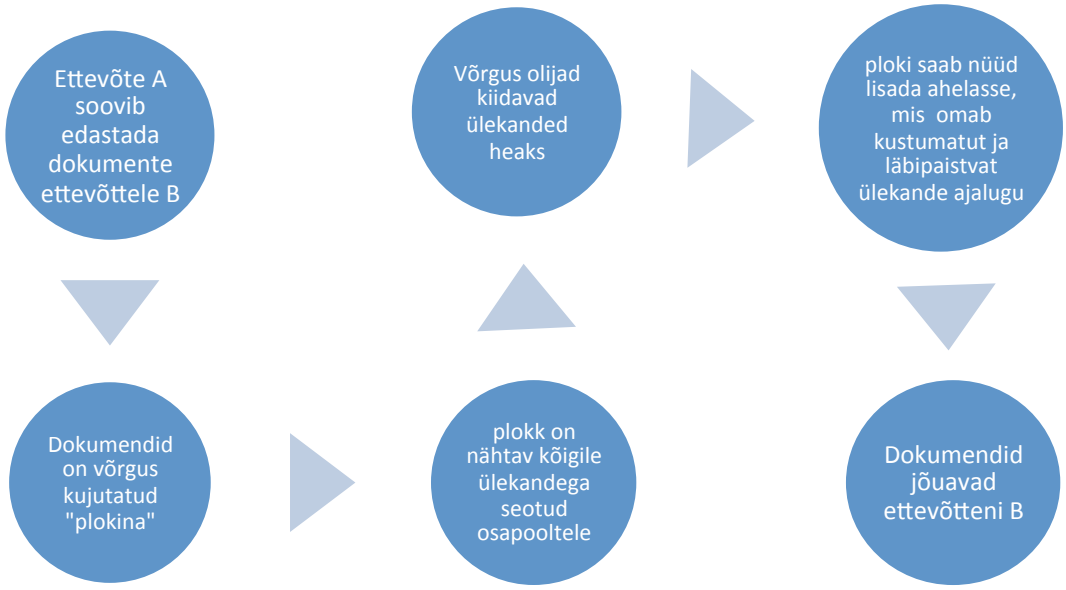
Elektrooniliste mereveodokumentide taga oleva tehnoloogia areng ning arendus on olnud viimastel aastatel hämmastavalt kiire. Üks huvipakkuv valdkond, mis tulevikus võib mängida suurt rolli elektrooniliste mereveodokumentide suuremal vastuvõtmisel merenduse valdkonnas on elektrooniliste dokumentide süsteemid, mis kasutavad lepinguid ja plokiahelat ja jagavad hajusraamatu (ingli.k. *ledger technology*) lahendusi.

Plokiahel on järjestikustest andmeplokkidest koosnev andmestruktuur. Plokiahela iga järgmine plokk luuakse iga fikseeritud ajavahemiku möödudes. Plokkide sisu esitab kokkulepitud viisil kodeeritud registreeritud sündmusi, millel võib olla informatiivne, äriline või õiguslik tähendus. Plokiahela terviklust kaitstakse iteratiivse räsimisega. Räside endi tervikluse kaitseks kasutatakse: digitaalsignatuuride, seetähendab avalike võtmete kaudu või volitatud isikute digitaalallkirjadega; räsitud ajatembeldusega; interaktsioonita ajatembeldust, mis seisneb plokkide erilistes vormingureeglites. (RIA 2018, 17)

Plokiahelat säilitatakse ja hallatakse tavaliselt hajusraamatu kujul, kus mitu osapoolt haldab koopiat. Mitme dokumendi halduri korral nimetatakse seda teostust hajusraamatuks. Kasutajate saadetud kirjed jõuavad sel juhul, kas otse või kaudselt kõigi halduriteni, kes

sõltumatult haldavad. Hajususraamatu peamised kaks põhjust miks seda kasutatakse on järgmised. Esiteks usaldus, kuna üksikut haldurit ei loeta piisavalt usaldusväärseks lahenduseks, arvestades võimalikku korruptsiooni. Teiseks töökindlus, sest üksiku halduriga lahendust ei loeta piisavalt töökindlaks, arvestades võimalusega, et üks haldur võib muutuda side- ja muude probleemide tõttu teistele kättesaamatuks. (Ibid, 17)

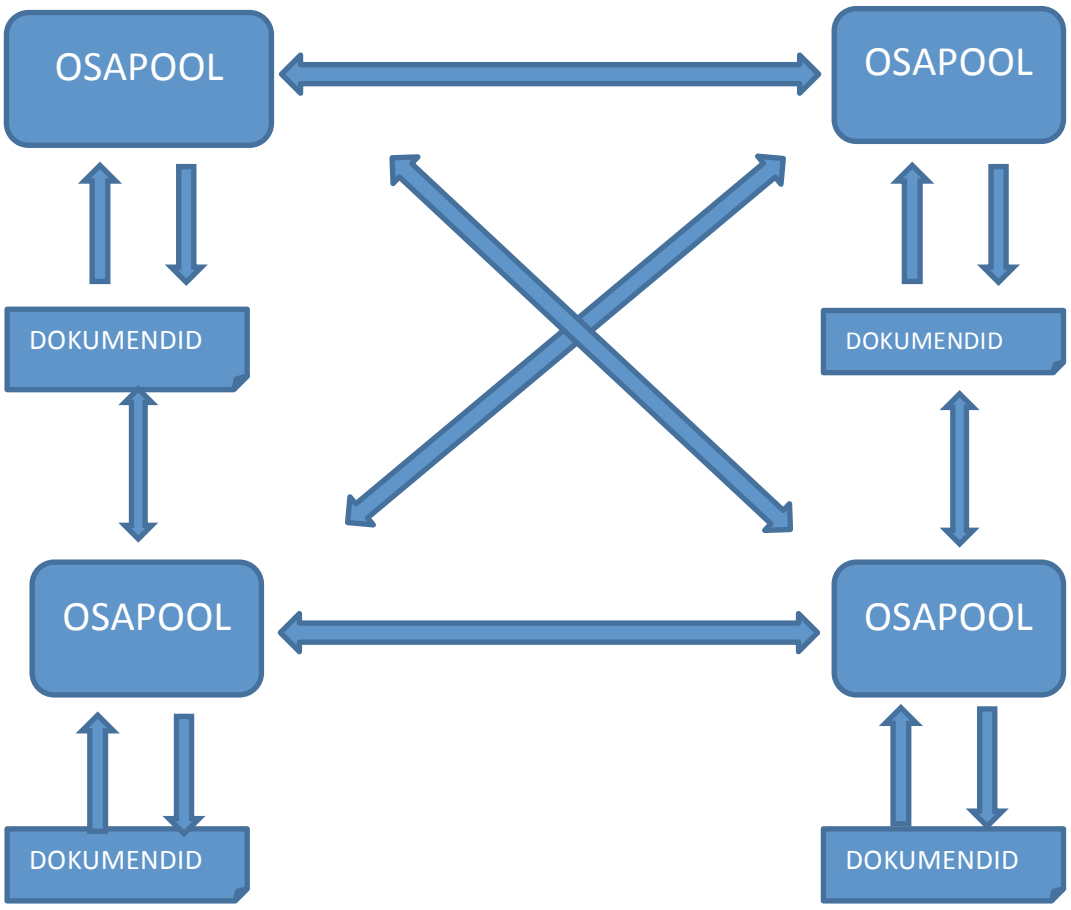
Plokiahela ja hajusraamatu süsteem on digitaalne. Selle toimimist võib kirjeldada lihtsustatud kujul, et identsed dokumnedid, mis paiknevad erinevates arvutites on võimalik jagada üle süsteemi ning kinnitada kõikidel osapooltel korraga. Samuti saab dokumente jagada vaid nende osapooltega, kellele see info vajalik. Need tehnoloogia platvormid pakuvad mitmeid võmalusi lepingute automatiseerimisel kasutades "tarkasid" lepingumudeleid. Kuigi nende lahenduste potensiaalne kasutusele võtmine võib olla veel mõnda aega lahtine, kuna elektroonilised mereveodokumendid on valdkond, kus tuleb enne kasutamist testida ning proovida kõik versioonid korralikult läbi. Seda seetõttu, et vältida tulevikus ebaõnnestumisi ja majanduslikke kaotusi, kuna tehnoloogilised süsteemid ei toimi. (Underhill, Bibby 2016)



Joonis 2. Plokkahela süsteemi seletus dokumendi edastuse näitel
Allikas: Autori koostatud

Joonis 2. kujutab piltliku seletust, kuidas toimib dokumendi edastus plokiahela kaudu. Juhul, kui ettevõte A soovib edastada ettevõttele B elektroonilisi dokumente ja need teiste vajalike

osapooltega kooskõlastada. Dokumendid on kujutatud ahelas plokina. Seda plokki näevad kõik võrgus olevad osapooled. Kõigi vajalikud osapooled saavad dokumendi kinnitada või võtta infoks ning peale seda lisatakse plokk ahelasse. See ahel omab ülekannete ja tegevuste ajalugu mis on kustumatu ning läbipaistev kõigile osapooltele, et tagada ausad võtted kõigi poolt. Peale seda tegevust on vajalikud dokumendid kinnitatud ning edastatud siht osapooleni, kes saab need turvaliselt kätte. Ükskord plokiahelasse sisestatud info püsib seal igavesti ega ole tagantjärele muudetav. Plokiahela rakendused loovad turvalise infovahetuse, salvestamiseks ja jagamiseks nii omavahel usaldusväärset suhet juba omavate kui seda veel mitte omavate osapoolte vahel.



Joonis 3. Hajusraamatu tööpõhimõtte selgitus dokumendi edastuse näitel
Allikas: Autori koostatud

Joonis 3. iseloomustab piltlikult seletust hajusraamatu süsteemile. Samuti ka see joonis on tehtud dokumendi edastuse näitel. Selle süsteemi eeliseks on, et edastatavad dokumendid on nähtavad kõigile samuti redigeeritavad kõigile ning võimalik liigutada mitte kindlas

järjekorras vaid soovitud liikumissuunas osapoolte vahel. Samuti on võimalik seda süsteemi rakendada erinevate maksete sooritamiseks, ilma et peaks mõne osapoole kinnitust ootama.

Näitena ülal toodud infotehnoloogilistele süsteemide kasutamisest ja arendamisest on võimalik tuua uudis jaanuarist 2018. Nimelt teatasid Maersk ja IBM koostööst plokiahela turvatehnoloogia alal selleks, et tõsta efektiivsust kogu tarneahela ulatuses. Projekti on juba kaasatud hulk organisatsioone, sealhulgas Houston´i sadam ning Ameerika Ühendriikide Toll ja Piirivalve. Eraldiseisva pilootprojektina kasutas Iisraeli konteinerfirma ZIM edukalt plokiahea põhist süsteemi elektroonilise konossemendi saatmiseks. Lisaks kasutab klassifikatsiooniühing DNV GL plokiahela tehnoloogiat selleks, et "suurendada tehasest saadavate toodete läbipaistvust ja jälgitavust tarbijale". (SKF Marine 2018)

Lisaks näitena on BIMCO'l maailmatasemel standardlepingud ja klauslid kasutuses olnud merendusvaldkonnas juba üle sajandi ja on tunnustatud üle maailma, kehtestades standardeid rahvusvahelises kaubanduses. BIMCO näeb erinevaid võimalusi just detsentraliseeritud plokiahela tehnoloogias, mis võib kiirendada elektrooniliste konnosomentide kasutust. Samuti koos teiste tehnoloogiatega saab koostada tšartereid plokiahela platvormil ning ka edastada sama tehnoloogilist võtet kasutades. Plokiahela rakendamiseks nähakse erinevaid võimalusi, nagu näiteks logistilised tarneahelad – konteinerid; punkerdamine; laevade varuosad; jne. Mitmed suured konteinerifirmad teevad juba koostööd erinevate IT lahenduste pakkujatega selleks, et leida võimalikke plokiahelal baseeruvaid lahendusi. BIMCO´l on selles tõusvas tehnoloogias juhendaja roll, tuues kokku võtmetähtsusega liikmeid sidusrühmadesse; informeerimine; soovitamine ja informatsiooni jagamine, standardite järgimine ja kontroll, mis tahes uue vormi prahilepingute ja muude lepingute puhul.

Inimesed on hakanud mõistma, et plokiahelal on potentsiaali erinevate ülekannete tegemisel, eriti nendel, kus kasutatakse usaldatud vahendajat. Usaldus mängib merenduses suurt osa, kuid praegusel hetkel põhineb see suuresti tsentraliseeritud süsteemidel, nagu pangad, kes kontrollivad tehinguid. Tsentraliseeritud süsteemid võivad olla korrumpeerunud ja neid on võimalik häkkida, kuid plokiahel on detsentraliseeritud ja võib tulevikus pakkuda ülimalt turvalisi lahendusi. (Papagiannopoulos 2017)

2. MEREVEODOKUMENTID JA KÜBERTURVARISKID

Ajajärgul, kus järjest enam seadmeid on ühendatud internetiga on muutumas üha enam kaitsetuks küberrünnakute eest. Valdkonnad nagu merendus ja energiatööstus ühendab laevu, konteineried ja naftapuurplatvorme arvutivõrkudega, mida on võimalik häkkeritel muuta ja segada töötamist. Näiteks ründasid häkkerid ujuvpuurplatvormi arvutivõrku ajades aluse piisavalt kreeni, et katkestada töö. Selleks, et alus töökõlblikuks saada, läks 19 päeva otsimaks pahavara üless. Samuti juhtum lähiminevikust, kus häkkerid sisenesid Antwerpeni sadama arvutisse ning pikaajaliselt toimetasid illegaalseid kaupu riigist läbi. Lisaks eelmistele näidetele on teada, et Somaalia piraadid kasutavad internetist saadavat navigatsiooni ja aluste infot valimaks välja enda sihtmärke. (Wagstaff 2014)

Tänapäeva ühiskond koos oma tähtsate e-teenustega ei saa toimida ilma küberturvalisuse tagamiseta. Küberruum on uudne keskkond, mis nõuab süsteemset ja kõikehõlmavat kaitset rahvusvahelisel, riiklikul, valdkondlikul ja personaalsel tasandil. Eelmiste näidete põhjal on selgesti näha, et paratamatu osa tänapäeva tehnoloogia arenguga seoses on ka negatiivsed pooled, milleks on erinevad pahavarad ning sellega seonduvad probleemid. Kuna inimesed merenduses on alles kasutusele võtmas elektroonilisi lahendusi, ei osata veel mõelda ega arvestada veel vähem ennast ettevalmistada erinevateks ohtudeks. Samuti ei osata ettekujutada, kuidas näeb üldse küberrünnak välja ning mida see endast täpsemalt võib kujutada ning kaasatuua.

Joonis 1. Küberkuritegevuse põhilised põhjused
Allikas: Boyes, H. ;Roy, I. ;Luck, A. (2016)

Joonis 1. on välja toodud tähtsamad põhjused ja põhjustajad küberkuritegevuses. Need on jaotatud gruppidena, kellele toovad küberrünnakud mingil viisil kasu. Üheks suurimaks grupiks, kes küberrünnakuid toime panevad on kuritegevusega seotud üksused, kes illegaalsete toimingute jaoks ründavad, et saada infot või seda muuta. Sinna hulka kuuluvad ka finantspettuseid sooritavad isikud ja grupeeringud. Peale organiseeritud kuritegevuse panevad toime küberrünnakuid ka erinevad valdkonna aktiivsemad grupid, näiteks häkkerid. Need grupid võib jagada üldjoones kaheks, need kes soovivad küberrünnakuga tõestada ja näidata süsteemi nõrki kohti ja teised, kes üritavad n.ö nõrki kohti ära kasutades saada lühiajalist tähelepanu, muutes näiteks infot kodulehtedel.

Eelmistest põhjusest edasi tulevad joonis 1. küberrünnakute sooritajad, kelle eemärk on palju konkreetsem ning spetsialiseeritud. Nendeks on sõjandus üldisemalt ning ka terrorism ning spionaaž. Neid tegevused on sõjaväelise või tööstusliku taustaga. Kindlasti on nende eesmärgid palju suuremad, kui lihtsalt infot muuta mõnel ettevõtte kodulehel.

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. Esemevõrk toimib kui sild 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. (Heering 2017, 25)

2.1 Küberturvariskid merenduses

Küberturvalisus on üha enam teemaks tänapäeval, olenemata valdkonnast. Seda soosib tehnoloogia kiire areng ning ühiskonnas uute süsteemide ja lahenduste kiire kasutusele võtmine. Nii mõnelgi juhul toimub üleminek tehnoloogilistes lahendustes ilma eelnevate teadmisteta ohtudest, mida võib antud muudatus endas peita.

Suurimad riskid küberturvalisuses peituvad teadmiste ja oskuste taga. Teadmised, kogemused ning ka oskused on inimesel, kes on kõige tehnoloogilise tarbija ja kasutaja. Seega on kõige suurem riskiallikas just inimene. Vaadeldes seda probleemi näitlikult siis läbi inimese, kes on

küberkurjategija saavad alguse pahateod küberruumis ning need on suunatud just tehnoloogia kõige nõrgema lüli suunas, kes on kasutaja ning ka inimene.

Küberturvariske põhjustavate teguritena võib käsitleda ka lisaks inimfaktorile ka mitmeid teisi täitsaid punkte, mis kõik on omavahel mingil viisil seotud. Näidetena võib välja tuua: üha rohkem erinevate toimingute ning tegevuste digitaliseeriumist; uudsuse tõttu tingitud teadmatusest; küberturvariske, küberturvalisust ning – rünnakuid reguleerivaid õiguslikke määrustike vähesust. Need kõik annavad väga hea võimaluse küberrünnakute sooritamiseks.

2.1.1 Digitaliseerimine

Tehnoloogia areneb ja üha enam võetakse kasutusele elektroonilisi süsteeme ning järjest rohkem muudetakse erinevat infovahetust digitaalseks. 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. (Heering 2017, 30)

Digitaliseerimine on võtnud sihi merenduse suunas ning teeb seda üsna kiire tempoga. Just digitaliseerimine ja sellega kaasnevad tehnoloogiad pakuvad suurepäraseid võimalusi, muutes elu ja töö palju lihtsamaks, tõhusamaks ning kiiremaks. Kuid tähele tuleks ka panna tõsiasi, et digitaliseerimisega kaasnevad ka ohud, millele tähelepanu mitte pööramine võib ettevõttele väga suuresti kättemaksta.

Tänapäeval on üsna sage nähtus, kus mõni tehnoloogiline lahendus või termin on hakanud laialdaselt levima üle kogu regiooni või isegi maailma, mis toob sinna punkti, et mingi hetk on antud teemal rohkem kõlapinda ja tähelepanu. Näiteks võib tuua: küberturvalisus, Bitcoin ja nüüd on selleks mõisteks saanud digitaliseerimine ja plokiahel. Plokiahel ei ole teaduslikus mõistes üldsegi uus tehnoloogia. See arenes välja tegelikult krüptovaluutast. Samuti on küberkuritegevus olnud tegev sama kaua kui inimesed küberruumis tegutsenud, kuid tähelepanu on saanud alles nüüd rohkem. Seda seetõttu, et üha suureneva kasutajate võrgu tõttu on ka rünnakuid järjest enam.

Digitaliseerimisel on potentsiaali tuua dramaatilisi muudatusi merendusse. Mõned neist muudatustest võivad olla põnevad võimalused ja mõned neist võivad olla tõsised väljakutsed. Merendus võib muutuda leebemaks ja läbipaistvamaks. Kuid see võib muuta ka merenduse haavatavamaks. Selle vältimiseks tuleb hoolikalt juhtida ja võtta meetmeid küberriski leevendamiseks. (Papagiannopoulos 2017)

Viimastel aastatel on merenduses toimunud tehnoloogiline areng, kuigi selle edenemine ei ole alati olnud lineaarne. Plokiahel, internet ja tehisintellekt võimaldaksid merendussektoril koordineerida ning kasutada kogutud informatsiooni meretranspordi valdkonnas. Laevaomanikud ja teised merendusvaldkonna esindajad peavad olema ettevaatlikud, sest nende käes on suure väärtusega informatsiooni, mida tahtlikult ei soovi keegi teistega jagada. Sellisel juhul ei pruugi olla abi isegi plokiahelast. Info, mis ei ole ärisaladus, saaks olla hallatud sõltumatute andmetarnijate poolt. Kaubandust läbiva digitaliseerimise lainega on paralleelselt kasutuses ka tehisintellekt, mille algoritmide abil analüüsitakse informatsiooni ja sellest lähtuvalt võetakse vastu otsuseid.

Veel üks väljakutse merenduse valdkonnale on erinevate süsteemide ühilduvus, mille abil saaks edastada andmied laevadelt kaldale ja vastupidi. Sõltuvus digitaliseerimisest ja sellega kaasnevad muutused on väljakutseks kõigile osapooltele. Ainuüksi motiveerivaks mõttekohaks on see, et digitaliseerides tööprotsesse ning kasutades elektroonilisi mereveodokumente on võimalik merenduse sektoris kokku hoida suurtes kogustes paberit. Arvestatavalt 5-10% aastasest kaubamaksumusest kulub paberi ja sellega seonudvate süsteemide kasutamisele ressursse.

Koos erinevate digitaliseerumistega ning tehnoloogiate arendamisega on merenduses hakanud tegema ka koostööd sellised ettevõtted, kelle toodetavad teenused, tooted, tehnoloogiad või süsteemid võiksid üksteist täiustada, arendada või hoopis midagi uut tehnoloogiat arendada. Näiteks satelliitside teenuseid pakkuv Inmarsat hakkas strateegilisi partnersuhteid looma selliste sidevahendite arendajate ja tootjatega nagu JRC, Cobham ja Intellian. Sellised partnerlussuhted on paindlikumad, võimaldades mastaapset juurdepääsu mõlemale partnerile. Näitena võiks tuua veel Transas/Wärtsilä koostöö, kus Transase ECDIS ja Rolls-Royce masinad koguvad ja vahetavad informatsiooni.

Tekib küsimus, mis hetkel areneb digilahendusi tootvatate firmade konkurents üle koostööks. Kas Wärtsilä suudaks tulevikus nii suurt kogemust digivaldkonnas omandada, et suudaks ise digilahendusi luua? Või on tulevik ikkagi strateegiliste partnerlussuhete päralt? Uute tehnoloogiate puhul tuleb olla valmis huvitavatest võimalustest kinni haarama ning kaasa minema sellega mida uudsed võimalused digitaliseerimisega luuakse. (Clayton 2018)

2.1.2 Inimfaktor

Riski, ressursside ja turvalisuse mõtelises ühises kogumis on kõige olulisem ülesanne inimesel, kes küberruumis tegutseb. Kui vaadelda inimest riski ja turvalisuse narratiivides, on tegemist passiivse osapoolega, kes vajab kaitsmist. Vaadeldes aga inimest läbi ressursside narratiivide, on tegemist aktiivse tegutsejaga ning seda aktiivsust võiks kasutada ka küberturvalisuse parandamiseks. (Kirch 2013, 2)

Ühe suurima muret tekitava punktina nähakse tõsiasja, et kuigi tehnoloogia areneb, erinevad programmid muudavad töö kiiremaks ja tulemuslikumaks sooritamiseks arenevad siis inimeste teadlikus, kuidas neid süsteeme hallata ohutult on siiski üsna kesised. Veel viimase ajani kipunud stereotüüpne arvamus olema paljudel ettevõtetel, et milleks kulutada summasid töötajate koolituseks ohutu küberruumi kasutamise osas, kui ettevõttel on tihtipeale olemas oma isik, kes vastutab infotehnoloogiliste küsimuste eest. Osalt tänu sellisele suhtumisele on ka nii mõndeki ettevõtted saanud korralike kahjusid tunda rahalisel, andmete lekkimise või kadumise kaudu.

Küberrünnakute sihtmärgid on tihtipeale inimesed, läbi kelle saab edasi ligipääsu ettevõtetele. Kurjategijad on nutikad ja valivad rünnatavaks just sellise lüli, mis on kõige nõrgem. Kuna ettevõtete süsteemid on enamasti kindlalt ja hästi kaitstud ning sealt turvaauku leida on aeganõudev ning keeruline siis on leitud sild üle selle piltlikult väljendatud müüri. Palju levinud skeem on väga lihtne. Töötaja kasutab oma töö ja eraelu asjaajamisteks ühte arvutit, mälupulka, telefoni või mõnda muud tehnikaseadet. Seade nakatub pahavaraga, peale kahtlase sisuga meili, ebaturvalistel interneti lehekülgedel käimist, allalaadides faile mitte turvalistelt lehekülgedelt. Peale pahavaraga nakatumist ja näiteks ettevõtte süsteemiga ühendamist on võimalik pahavaral ligipääseda firma siseinfole. Edasine stsenaarium suuresti sõltub

kurjategija plaanidest, hallates siis ettevõttes töö, tootmise, varastades andmed või hoopis muutes neid endale vajalikuks.

Murekoht küberturvalisuse teemal ning inimfaktorist põhjustatuna rünnak on mitmetes valdkondades, mitte ainult merenduses. Ei saa võrrelda, milline valdkond oleks kõige enam mõjutatav küberrünnakute poolt, kuid kindlasti ei saa öelda, et merendus, eesotsas laevandusega oleks just vähem mõjutatav. Piisab inimeselt teha ühekordne hooletusest või laiskusest tulenev viga ning see võib mõjutada tervet ettevõtet. Mõttekoht on, et kui küberrünnakutega suudetakse sisse saada laevas olevatesse süsteemidesse siis ega kaldal sadamad, terminalid, laod keerulisema ülesehitusega süsteemid pole ning rünnakute tagajärjed võivad on väga tõsised.

2.1.3 Õigusloome

Küberturvalisus on tähtis ning selle tagamine üsna kulukas, keeruline ning aeganõudev. Suureneva digitaliseerumise tõttu ning inimfaktorit, kui võimalikku ohtu turvalisusele on üha enam üritatud keskentuda õiguslikku raamistiku loomisele antud teema ümber. Antud olukord, kus puudub konktreetne ja ühtne reeglite raamistik, millest väljenduvad kindlad kohustused, õigused ja võimalused võib pidada küberturvariskiks.

Viimaste aastate jooksul toimunud küberrünnakud on pannud merenduse valdkonda vaatama arusaamasid küberruumi ning selle kasutamise ning kasutusele võtmise osas kriitilise pilguga üle. Kindalsti pole teadaolevad rünnakud ainukesed, vaid võib arvata, et nii mõnedki ettevõtted, kas pole teadlikud pahavara olemasolust või pole sellest teatanud.

Suurtest ohtudest lähtuvalt on erinevad merenduse organisatsioonid, liidud ja isegi ettevõtted hakanud koostama erinevaid juhiseid ning infomaterjale küberturvalisuse kohta, sellest nii kaldal kui ka laevas. Kõike seda selle nimel, et inimeste teadlikust tõsta ning mitte sattuda rünnaku alla. Lisaks on tänapäeva võimaluste juures on võimalik enda kaupa, laeva või ettevõtet ka küberrünnakute eest kindlustada.

Kuritegevus on juba ammuste seadustega riikides karistatav. Küberkuritegevuse suunas liigutakse sama rada, seega seda nähakse, kui pahategu teise suhtes. Kindlasti on küberruumis

sooritatavaid kuritegusid palju raskem jälitada ning leida vastutaja. Seetõttu isegi, kui on olemas regulatsioonid karistamaks küberkurjategijaid siis seda reaalselt teha on ülimalt keeruline. Samas on Eesti Vabariigi karistusseadustikus olemas juba paragrahvid, mis karistavad erinevate küberruumis sooritatud kuritegude eest. Näiteks § 213, mis käsitleb arvutikelmust sätestab, et varalise kasu saamise eest arvutiprogrammide või andmete sisestamise, vahetamise, kustutamise, sulustamise või muul viisil andmetöötlusprotsessi sekkumise teel, kui sellega on mõjutatud andmete töötlemise tulemust, - karistatakse rahalise karistuse või kuni viieaastase vangistusega.

Tugeva näitena, kus on astutud samm turvalise küberruumi poole ning andes mõista, et ka seal toimepandud kuritegusid karistatakse võib pidada Euroopa Liidu kokkulepet liikmesriikidega, kus perioodil 2013-2015 karmistati küberkuritegevuse eest määratud karistusi. Enne seda oli kõigil liikmesriikidel eraldi seadused selleks ning suurimaks erinevuseks oligi määratavad karistused, leppe abil ühtlustati neid üleliiduliselt.

Elektroonilised mereveodokumendid pole merenduse valdkonnas siiani suuresti kanda kinnitanud, mille üheks põhjuseks mitmetest võib tuua ebaselge ja puuduliku juriidilise raamistiku. Seeläbi pannes kaks suurt küberturvariski kokku, kus on vähekasutatud dokumendi vorm, mida paljud veel ei tea ning teisalt puudulik õiguslik raamistik on taaskord koht, mida võivad pettusteks ja omakasuks kurjategijad ära kasutada.

Suurem õiguslik reguleeritus ei tähenda ekspertide hinnangul suuremat küberruumi turvalisust – ekspertide arvates ei parandaks õiguslik regulatsioon küberruumi turvalisust. Eksperdid leiavad, et küberturvalisuse legitimeerimine eeldab lisaks õiguslikule regulatsioonile ka olulisel määral küberturvalisusega seonduvate asjaolude selgitamist. (Kirch 2013, 2)

2.2 Mereveodokumentidega seotud küberrünnakud ja pettused

Küberturvalisuse valdkonda võib pidada praegusel hetkel üsna nooreks ja uueks valdkonnaks. Kuigi on üritatud üha rohkem, paremaid ja kiiremini erinevaid tehnoloogiaid arendada ja parandada siis ründajad arenevad samas või kiiremas tempos samuti kaasa. Praegusel hetkel on kurjategijad võimelised ründama näiteks merenduse ettevõtet nii, et jälgides kogudes või lausa muutes infot suudetakse antud rünnak korraldada ka enne kui neile üldse jälile saadakse.

Üha enam on ka merenduse valdkond liikumas sinnasuunas, et on mõstma hakanud küberohutuse vajalikust ning teavad millised tõsised tagajärjed võivad küberrünnakuga järgneda.

Tihti leiab aset situatsioon, et erinevatele ettevõtetele suuantud küberrünnak ei jõua avalikuseni või isegi mitte ametlike asutusteni. Seda võib seletada mitmete põhjendustega, nimelt esiteks ei tea ettevõte üldsegi, et teda on rünnatud ning andmed või informatsioon pole enam salajased. Antud juhtum on tõenäoline nendes ettevõtetes, kus pole suurt rõhku pööratud töötajate teavitustööle ja koolitusele küberturvalisuse valdkonnas.

Teise suure põhjusena võib tuua välja olukorra, et ettevõtted ei teata enda vastu suunatud küberrünnakust kuna võtavad seda, kui maine rikkumist ettevõtte suunas. Isegi, kui küberkurjategijad nõuavad raha siis ka sellest vaikitakse. Seetõttu jäävad paljud rünnakud märkimata ning ka kurjategijad leidmata. Tavaline praktika siiski soosib kohesest teatamist vastavalt riiklikele määrustele vastavatele ametkondadele.

Kuna digitaalsete süsteemide kasutamise mõttega kaasnevad paljudel suured hirmud küberrünnakute eest siis on üks põhjuseid miks siiani pole digitaalsed dokumentide vormid saavutanud edu paberist vormide ees. Osati on ka kahtlustel põhjust, kuna paljud organisatsioonid on küberrünnakuid iseloomustanud kui tänapäeva piraatlust, mis on merelt edasi levinud ka tehnoloogiasse. Just neid kahtluseid iseloomustavad ja toovaid näiteid reaalsetest juhtumitest, mis on seotud mereveodokumentide küberrünnakute ja pettustega.

2.2.1 Küberrünnakute ja pettuste näited

2016 aastal teatas turvateenuseid pakkuv firma G4S, et kinnipeetud kuritegelik grupeering oli 3D printeriga kopeerinud konteineri avamiseks vajaliku seadme. Uurimine tuvastas, et sadamas tegutsenud kriminaalid olid loonud ideaalse koopia avamaks üldtuntud lukustussüteeme. Tänu sellele oli kurjategijatel võimalik peita jälgi ning jätta mulje, kui röövi mitte toimumisest. Selline võimalus saab tõenäoliseks, kuna tänapäeval saavad kõik soetada paari tuhande dollari eest 3D printeri ning internetist saadavad info, jooniste ja piltide abil on võimalik luua peaaegu ideaalne koopias pea ükskõik mis esemest. (Grey 2017)

Glencore ja MSC kohtuasi on heaks näiteks, et elektrooniliste kaubadokumentide süsteemide kasutamisel. Lasti üleandmine peab toimuma ainult vastavalt veolepingule ja peab olema tõendatud konossemendiga, isegi siis, kui elektrooniline kaubaüleandmise süsteem on kasutuses. Antud näite puhul oli kaup üle antud PIN koodide ettenäitamisel, vaatamata konossomendis puuduvatele sätetele. Pärast tuli samas aga välja, et kaks üle antud lastisaadetist oli kahjustatud. Tänu sellele võeti vedaja vastutusele.

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. Keelatud ained peideti ära legitiimse kauba nagu banaanid ja metsamaterjal vahele. (Heering 2017, 35)

27.juuni 2017 langes küberrünnaku ohvriks rahvusvaheliselt merenduses tuntud Taani ettevõte A.P. Moller Maersk. Lunavara nimega NotPetya küberrünnak halvas põhiliselt konteinerlaevadega opereeriva Maerski elektoonilised süsteemid, mis haldasid erinevaid andmeid ja dokumentatsiooni . Tagajärjena olid raskendatud klientidel esitada ning näha infot kauba kohta ning ettevõttel jooksvalt klaarida dokumente erinevate osapooltega, tagamaks kaupade liikumine. Seetõttu lisaks lunavara nõudele andmete tagastamise eest sai ettevõte ka kahjunõudeid erinevatelt sadamatööga seotud osapooltelt, kuna töö oli halvatud ning tegevused seisid. Lisaks kaotas ettevõte ka mitmeid lepinguid. Võttes kokku kõik rahalised kohustused, sai ettevõtte kahju ekspertide sõnul ligi 850 miljonit dollarit, millest 200-300 miljonit läks lunavara nõude makseks. (Gronholt-Pedersen 2017)

3. KÜBERVALDKONNA OHTUDE UURIMINE

Antud peatükk koos alapeatükkidega on koostatud andmaks ülevaade lõputöö uurimis osa kohta. Selgitades, millised olid töömeetod, uurimismeetod, millistel viisidel koguti andmeid. Samuti andes ülevaate ühe andmete kogumisviisi, intevjuude - valiku valimi, küsimuste põhjenduse ja selgituste kohta.

3.1 Sisulise osa töömeetodi seletus

Empiirilise töö eesmärgiks on mingi nähtuse või objektidega seonduvate probleemide väljaselgitamine ja lahenduste otsimine, olemasolevate teoreetiliste ja empiiriliste allikate analüüsimine, empiirilise uuringu teostamine, tulemuste analüüsimine ning hinnangu andmine.

Lõputöö on koostatud kvalitatiivset uurimismeetodit kasutades. See tähendab, et andmed, nende töötlemine ja järelsused ei ole seotud arvuliste näitajatega. Kvalitatiivse uurimise käigus keskendutakse ühe objekti süvaanalüüsile. uuritakse toimuva sisu. Kvalitatiivse uurimuse korral püütakse vastata küsimustele miks ja kuidas ning tegeletakse sõnaliste karakteristikutega ja objektide kirjeldustega. Samuti uuritakse inimesi või süsteeme neid jälgides ja saadakse andmeid vaatluse, intervjuu ja sõnalise suhtlemise kaudu. Tulemuseks on „oma lugu“, mis on näidiseks või üksikuks juhtumiks mingist laiemast protsessist. (Laherand 2008)

Kvalitatiivse uurimuse tüübiks on valitud tegevusuuring. Seda mõistetakse, kui loomulikus keskkonnas tehtavaid väikeseid sekkumisuuringuid, kus uuritakse sekkumise üldisemat mõju. Objektiks on aga sotsiaalset laadi praktika. Selle abil püütakse lahendada tegelikke probleeme, mõista töökollektiivi sotsiaalset praktikat ja käitumist. (Ibid)

Kvalitatiivsete andmete kogumine on tehtud ühe osana andmete kogumisega internetist. Uuriti peale erialaste raamatute, teadustööde ka internetist saadavaid materjale. Enamus neist olid inglise keeles ning põhilised allikad olid erinevad uudislood, arvamuslood, kõned, intervjuud eriala ekspertide poolt. Internetist andmete kogumise positiivseteks külgeteks võib pidada andmetele kergemat ligipääsu sõltuvalt teemast, info ja faktide kontrollimise võimalus,

parema tervikpildi saamise võimalus. Samas kui problemaatilisteks kohtadeks võib pidada võimalikke teksti originaal autori mitte viitamine, keelelised vead just erialaste sõnade tõlkes, võimalik kallutatus.

3.2 Intervjuu

Kuna ainult internetist andmete kogumisega usaldusväärset lõputöö põhimaterjali ei saa koguda, just selle võimaliku ühekülgse arvamuse kallutatuse tõttu, siis otsustas autor koguda andmeid intervjuudega lisaks. Põhiline eemärk vestlustega on toetada ning kommenteerida internetist kogutud materjale.

Intervjuu on viis, mis annab infot selle kohta, mida inimene mõtleb. Just seeläbi on antud lõputööl mõlemad andmete kogumise viisid tähtsad, sest vestluste käigus on arvamust avaldanud isikud, kes on töö käigus kokkupuutumas lõputööd käsitlevate teemadega.

Antud lõputöö raames viis autor läbi kolm intervjuud, mis olid tüübilt poolstruktureeritud. Poolstruktureeritud intervjuu tüüpi kasutatakse siis kui on ühekordne intervjueerimise võimalus. Intervjuu jaoks valmistatakse ette põhiküsimused ning tehakse intervjuu plaan. Intervjuu käigus lastakse informandil rahulikult küsimusele vastata. Informanti suunatakse vajadusel teema juurde tagasi. (Viires 2013)

3.2.1 Valim ja läbiviimine

Intervjuude valimi valikuks analüüsis autor eelnevalt saadud kirjalikke materjale. Kirjutades lõputööd tekkisid põhilises kolmes suunas küsimused, mille järel otsustas just neid suundasid autor vestluste käigus uurida ja kommentaare küsida. Seda seetõttu, et autor ei leidnud materjale ning soovi tõttu saada teada, mida arvavad ning teavad inimesed, kes antud valdkonnas huvipakkuva teemaga tegelevad.

Küsimuste suundasid arvestades otsustas autor, et iga valdkonna suuna kohta teeb ühe intervjuu. Kuna tegemist oli kommentaaride saamise eesmärgil tehtava intervjuuga, mitte tulemuslikel, mille jaoks oleks olnud vaja suurt tagasiside, mida merenduse valdkonnas on saada pigem keeruline.

Intervjuude kolmeks suunaks olid elektroonilste mereveodokumentide võimalikud küberturvariskid ja nende võimalik vähendamine lähtuvalt: 1) õigusliku, järelvalve valdkonna esidaja; 2) agenteerimine; 3) ekspedeerimine.

Intervjuud viidi läbi esitades kõigile intervjueeritavatele kolm küsimust. Vestluse teema ja küsimused saadeti kõigepealt meili teel tutvumiseks. Kuna vastajad leidsid, et kõige mugavam ning effektiivsem on vastata meili teel siis saadeti küsimusete vastused tagasi autorile. Märkusena tuleb lisada, et autor ei saanud päris kõigile küsimustele otseseid vastuseid, mida ka peale küsimuse täpsustamist ei muudetud.

Lisaks lepiti kõigi vestelnutega kokku, et nimesid ja ettevõtteid ei nimetata töös. Seetõttu on töös vastuste eristamiseks lihtsalt nimetatud valdkond, milles tegeletakse.

3.2.2 Küsimused ja analüüs

Esimene intervjuu oli õigusloome ja järelvalve valdkonna esindajale. Nende küsimustega soovis autor saada teada erialase inimese arvamust tehnoloogia mõjust merendusektorile, ning kuidas see mõjutab. Lisaks arvamust küberturavlisuse küsimuste osas. Teise küsimusele olid juures ka lähtuvalt vastusest lisa küsimus suunamise eesmärgil. Küsimused:
1) Kas merendussektori arengule mõjub kiire tehnoloogilistele võimaluste arendamine pigem positiivselt või negatiivselt? Miks nii?
2) Kui suur probleem on üldse küberturvalisus merenduses, lähtudes Teie ametist vaadatuna?
- Kui ei, siis mis on hetkel tähtsamad murekohad merenduses?
- Kui jah, siis kuidas antud probleemiga tegeletakse?
3) Kui ohutuks annab merendussektorit muuta küberturvalisuse osas just õigusloomega?

Teine intervjuu pühendati agenteerimise valdkonna küsimustele. Uurides lähemalt elektroonilisi mereveodokumente ning nende võimalikke küberturvalisust. Teise küsimusele olid juures ka lähtuvalt vastusest lisa küsimus suunamise eesmärgil. Küsimused:
1) Kui suur osa Teie töös edastavates/vastuvõetavatest dokumentidest on elektroonilised mereveodokumendid?
2) Kas elektrooniliste mereveodokumentide edastamine on Teie arvates ohutu?
- Jah, siis milles see ohutu edastamine täpsemalt peitub?

- Ei, mida saaks muuta või parendada?
3) Kas Teie arvates vajab küberturvalisus merenduses suuremat tähelepanu? Miks?

Kolmas intervjuu suunati ekspedeerimise valdkonnale. Küsimustega üritas autor saada kommentaare üldise hulga üle elektrooniliste mereveodokumentide kasutatavuse kohta töös. Samuti küberturvalisuse tähtsuse ja teadlikkuse osas. Teise küsimusele olid juures ka lähtuvalt vastusest lisa küsimus suunamise eesmärgil. Küsimused:
1) Kui suur osa Teie töös edastavatest/vastuvõetavatest dokumentidest on elektroonilised mereveodokumendid?
Kas see hulk on suurenenud/vähenenud või hoopis muutusteta võrreldes viimaseid aastaid?
2) Kas seoses elektrooniliste mereveodokumentide kasutamisega olete rohkem töös tähelepanu pööranud ka küberturvalisusele?
- Ei, kas plaanite seda teha tulevikus?
- Jah, mida olete antud hetkes teinud, et töös tagada suurem küberturvalisus?
3) Kas küberturvalisus on ainuke probleem elektrooniliste mereveodokumentidega seoses?

Korraldatud intervjuudest saadud informatsiooni ja lõputööd kirjutades välja tulnud probleemide analüüsimisel moodustas autor neljanda peatüki. Järgnev analüüsiv peatükk toob välja põhilised järeldused ning võimalikud lahendused antud tähelepanekutele. Intervjuud, mis olid tehtud ainult lõputöö raames aitasid aru saada, selgitada ning tähelepanna kitsaskohti ning võimalikke lahendusi nii mitmetelegi esinenud probleemidele.

4. KÜBERTURVARISKIDE VÕIMALIK VÄHENDAMINE

Küberturvariskide võimalik vähendamine on kõigi küberruumi heatahtlike kasutajate huvides. Sellest ei võida ainult ettevõtted, kellel asub võimalus kõrgete küberturvariskide tõttu sattuda rünnaku ohvriks ning kaotada andmed, raha ning ka võimalik, et peatada töö. Võimalikult väheste küberturvariskide olemasolu annab kogu sektorile võimaluse tegutseda julgemalt ning suunata energiat teenuste pakkumisse ja äritegevuse tegemisse. Küberturvalisuse probleemi vähendamist vajab ka merenduse sektor, et oleks võimalik edasi liikuda ning uusi tehnoloogiaid kasutusele võtta.

4.1 Elektrooniliste mereveodokumentide küberturvariskide vähendamise võimalused

Lõputöö käigus koostatud ja läbiviidud intervjuudest ning lisaks eelnevalt läbitöötatud materjalist leidis autor kolm suuremat küberturvariski, millele pakub välja võimalikke vähendamise lahendusi. Samuti annab peatükk järelduse, kas autori püstitaud hüpotees vastab tõele või ei. Töö hüpoteesiks on seatud, et elektroonilised mereveodokumendid ja nendes sisalduv info ei ole piisavalt kaitstud küberrünnakute eest ja on kergesti mõjutatavad. Samuti pole tööjõud, kes mereveodokumentidega tegeleb saanud piisava väljaõpet ohtude osas.

4.1.1 Küberturvalisuse teadvustamine

Küberturvariske ei saa muuta madalamaks, kui inimeste üldine teadmine ohtudest on kasin. Nagu ka intervjuude käigus selgus siis küberrünnakute uudised on meedia kaudu jõudnud kõigile valdkonnas kohale. Samas teadmised, mis konkreetselt juhtus, mis süsteemide läbi ning millised olid võimalikud kahjud jäävad tihtipeale arusaamatuks. Seda kõike just seetõttu, et siiani pole panustatud inimeste informeerimisse küberturvalisuse teemadel ning kes ise huvi ei tunne, ei saagi teadma, et just ta võib olla väga suur küberturvarisk ettevõttele.

Tähtis on ennetustöö juba seetõttu, et nii mitmedki ettevõtted on asunud kasutama ainult elektroonilisi süsteeme edastamaks ning vahetamaks elektroonilisi dokumente. Samuti on kasutusel ka erinevad pilvesüsteemid, mis arhiveerivad dokumente. Samas tõdeti, et

küberturvalisuse teema ning tulenevate ohtude seletamine jäi kasinaks. Seega rünnaku korral on ohustatud ainuüksi ühe ettevõtte puhul äärmiselt suur hulk andmeid.

Intervjuudest selgus, et kindlasti suurim osa teadvustamise tööst on kanda ettevõtetel endil, kellel on esmatähtis, et andmed oleks kaitstud ning töö sujuks ilma tõrgeteta. Ühtlaselt on see variant ka kõige kiirem, kui ettevõte panustab ise koolitustesse seeläbi õpetades just nende süsteemide ja tehnoloogiate põhjal küberturvalisust, mis antud ettevõttes kasutusel. Seega lahendusena siinkohal pakuti välja, et ettevõtted peaksid korraldama koolitusi, seminare ja ka koostama õppematerjalid ning hädajuhuks ka kindlalt kokkulepitud käitumismustri ning tegevuse järjekorra.

Samuti on oluline, et haridusasutused mõistaksid, et erialade õppekavade kaasajastamine vastavalt reaalsetele vajadustele on äärmiselt tähtis. Seetähendab, et õppekavasse võiks kuuluda õppeained, millest saadud teadmised on tarvilikud sektoris hetkel ja ka tulevikus, mitte õpetada aineid, mis olid vajalikud minevikus. Pakkudes tudengitele õppida erialaaineid integreerides info- ja kommunikatsioonitehnoloogia valdkonnaga annab see tulevikuks tudengitele lisandväärtuse tööturul.

4.1.2 Rünnakutest teatamine ja koostöö tegemine

Küberrünnaku toimumise järgselt on äärmiselt tähtis teavitada lähtuvalt seadustest vajalikke instantse. Lõputöö teoreetilises osas väljendunud arusaam, et nii mitmetki inimesed ning ettevõtted ei teavita üldjuhul rünnakutest põhjustel, mis võivad olla valehäbi ning võimalik maine halvenemine on valed ja mitte jätkusuutlik käitumisviis. Üha enam üritavad erinevad merendusorganisatsioonid teadvustada, et teatamine rünnakust on äärmiselt vajalik. Seeläbi on võimalus teistel ettevõtetel olla veel ettevaatlikumad ning tugevdada ettevaatusabinõusid.

Ettevõtete hallatavate suurte andmekogude tõttu, mis rünnakute korral oleks katastroofiline on jõutud järeldusteni, et andmeid kogudes, töödeldes ning kasutades peab olema taustsüsteem ehk õigusraamistik väga konkreetselt paigas. Nimelt alates 2018 aastast hakatakse Euroopa Liidus kohaldama uut isikuandmete kaitse üldmäärust, mis määrab igasuguse andmete kogumise, andmetöötlusel kasutatava tegevuse ning ka arhiveerimise.

Samuti kehtestab üldmäärus uue muudatusena, et kõik peavad isikuandmete töötlejad kehtima hakkava isikuandmete kaitse üldmääruse artikli 33 kohaselt edastama informatsiooni isikuandmetega seotud rikkumistest Andmekaitse Inspektsioonile. Vastavalt üldmäärusele 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. (Heering 2017, 40)

Intervjuudest tuli välja asjaolu, et lisaks erinevatele määrustele ja seadustele nii riigi siseselt kui ka rahvusvaheliselt rünnakutest teatamise osas on siiski tuntav vajadus koostööle rünnakutest ennetamise suhtes, konkreetsete tegevuste osas peale rünnakut ning ka süsteemide ülesehituse osas kuna informatsiooni haldamine ja kaitsmine on tõsine katsumus merenduse ettevõttele.

4.1.3 Elektrooniliste mereveodokumentide andmete kaitse

Küberrünnakute tagajärgedeks võivad olla ulatuslikud andmete kadumised ja elektrooniliste mereveodokumentide süsteemi kasutuskõlbmatuks muutumine. Lahendusena võib olla näiteks paralleelselt ka erineva ja teineteisest sõltumatu elekrtoonilise mereveodokumentide süsteemi kasutamine. Sellisel juhul on suur võimalus, et küberrünnaku tagajärjel langeb üks süsteem rivist välja, kuid teine funktsioneerib edasi. Analoogse näiena võib tuua laevades kasutuses oleva ECDIS'e, kus on kasutuses üksteisest sõltumatuna kaks või enam süsteemi. Lahenduse miinuseks võib lugeda kõrgemat hinda ja andmete dubleerimist.

Eelnevalt väljapakutud lahendusega on võimalik ära hoida ulatuslikke kulutusi küberkurjategijate käest andmete tagasi ostmisele, töö seisust tekkivatele kulutustele, lepingute mittetäitmisest tulenevad trahvid. Seega lisakulutused andmete dubleerimisele mõeldud topelt süsteemide kasutamiseks on igati õigustatud ning tasuvad ära. Lisaks sellele parallelselt kahe süsteemi kasutuselevõtt annaks kasutajale paindlikkust ja võimalust kasutada just seda süsteemi, mis parasjagu vajalik ja sobiv.

Küberturvalisust merenduses on laiem probleem, millega tuleb tegeleda, kuna rohkem ja rohkem on laevad läinud nii öelda küberruumi. See puudutab nii kommunikatsiooni, navigatsiooni ja palju muud. Nende süsteemide halvamine võib põhjustada palju kahjusid, kui

mitte öelda katastroofe. Dokumentide edastamine toimub laeva ja kalda vahel. Andmeedastus toimub üldjuhul satelliitsidet kasutades. Sellest lähtuvalt küberrünnak laevale on vähem tõenäoline ja keskenduda tuleks kaldasüsteemide kaitsele.

KOKKUVÕTE

Merenduse valdkond on viimase kümnendi jooksul arenenud väga jõuliselt. Seda arengut võib vaadelda just tehnoloogilisest poolest. Peamisteks põhjusteks sellisele arengule võib pidada kaubamahtude pidevat suurenemist, tehnoloogia ja erinevate süsteemide väljatöötamist, arendamist ja täiendamist. Sellised arengud tänaseks hetkeks on võtnud aga seisukorra, kus üha enam toimub paberimajanduse digitaliseerimine. Tänu millele muutub töö merenduse valdkonnas just erinevate dokumentatsiooniga töötamisel kiiremaks ja effektivsemaks töödeldavate dokumentide hulga suhtes.

Tehnoloogiad arenevad muutes töö tegemise kiiremaks ja mugavamaks. Samas pole ühtegi head tegurit ilma halva pooleta. Suure digitaliseerumise käigus on palju informatsiooni ja andmeid kolinud ümber küberruumi. Suuresti eesmärkide täitmisele orienteeritud ning käivete suurendamise tuhinas on siiski liigutud üsna rutakalt üle väga olulisest teemast –isiku ja vara ehk andmete kaitsmine küberruumis. Paljud paberkujul dokumendid on saanud võrdväärse digitaalse variandiga ning posti asemel kasutatakse moodsaid süsteeme vajaliku info vahetamiseks vajalike osapooltega.

Praeguseks hetkeks on merenduse valdkond jõudnud punkti, kus üheks suurimaks ja olulisemaks teemaks on küberturvalisus. Seda kõike tänu sagedastele küberrünnakutele ning -pettustele, mis ajaga edasi arenedes järjest ohtlikumaks muutuvad nii kaubale, tehnikale kui ka inimestele endale. Peale mitmeid suuri küberrünnakuid on mõistnud mitmed ettevõtted, et kulutused küberturvalisusele tasuvad ennast ära, sest ohvriks langemine on liiga suur risk ajal, kui kurjategijad on oskuste poolest alati sammu võrra targemad.

Lõputöö eermärgiks oli välja selgitada küberturvariskid elektroonilistel mereveodokumentidel ning töö käigus pakkuda teoreetilisi lahendusi ilmnenud probleemidele eriala teadmiste piires. Lahenduste leidmiseks koostas autor teoreetilises osas ülevaate mereveodokumnetidest üldiselt ning nende arengust. Samuti uuris autor põhilisi küberturvariske merenduses ning kuidas need põhiliselt mõjutavad. Lisaks tuues välja suuremad näited küberrünnakutest ja pettustest, et anda üldine ülevaade, mis suurusjärgus toimub antud valdkonnas tegevus.

Töö hüpoteesiks oli välja toodud, et elektroonilised mereveodokumendid ja nendes sisalduv info ei ole piisavalt kaitstud küberrünnakute eest ja on kergesti mõjutatavad. Samuti pole tööjõud, kes mereveodokumentidega tegeleb saanud piisava väljaõppe antud valdkonna ohtude osas. Hüpoteesi tõestamiseks kogutud materjali kommenteerimiseks korraldas autor intervjuud inimestega, kes töötavad merenduse valdkonnas ning puutuvad kokku igapäevaselt elektrooniliste mereveodokumnetidega. Tulemusena kujunesid välja konkreetsed probleemid, lahendused, mis käsitlesid kübervaldkonna ohtusid. Sellest tingituna leiab autor, et püstitatud hüpotees on väär, kuna elektroonilised mereveodokumendid on täpselt sama turvalised või isegi turvalisemad, kui nendele eelnevalt kasutuses olnud paber vormid. Samas ilmnes, et inimeste teadlikus ohtudest on tõesti madal ning osalt tänu sellele toimuvadki küberrünnakud mille tagajärjed on tõsised.

Põhilisteks küberturvalisuse probleemideks peab autor mereveonduse eriala vaatevinklist järgmiseid punkte:

- Digitaliseerimise mugavus on ka samas üks suurtest ohtudest. Muutes paljud töötegemise viisid digitaalseks millest lähtuvalt muutub töö kiireks ja mugavaks, unustatakse tihti eesmärgile orienteerituna süsteemide turvalisust puudutavad küsimused.
- Ebaselge ja puuduliku juriidiline raamistik rahvusvaheliselt elektrooniliste mereveodokumentidele. Kuigi merendus on küllaltki süsteemselt ja selgelt reglementeeritud siis puudab sealt osa, mis selgitaks elektrooniliste mereveodokumentide kasutamist, õigusi ja kohustusi. Seetõttu võib seda pidada küberturvariskiks.
- Inimeste teadlikus ohtudest. Süsteem on täpselt nii tugev, kui selle kõige nõrgem lüli – ehk mida teadlikumad on töötajad ettevõttes, seda väiksem on risk, et nende kaudu ilmub ettevõtte andmete vahale tegutsema pahavara.

Autori hinnangul elektrooniliste mereveodokumentide küberturvalisuse küsimuste põhjalikuks uurimiseks ei piisa vaid merenduse valdkonna teadmistest. Seega ettepanekuna edaspidiseks tööks tuleks kaasata ka infotehnoloogia valdkonnast teadmisi ja oskusi, leidmaks sisulisi lahendusi riskivabaks elektrooniliste dokumentide jagamiseks vajalike osapooltega.

Kuigi küberturvalisuse probleem on hetkeks olnud üsna palju päevakorras erinevatel merenduse valdkonna konverentisdel, kohtumistel ja seminaridel siis siiani võib kohata arvamust, et küberturvalisus on midagi, mis ei ohusta kõiki ning ei ole midagi nii suur oht. Samas viimaste suuremate küberrünnakute näidete põhjal merenduses on hakanud see eksiarvamus muutuma ning on võetud vastu otsuseid ning samme, et muuta kübermaailm turvalisemaks. Tänu sellele on ehk ka lootus, et merenduse valdkonnas toimub kiirem areng digitaliseerimise alal ja peale laevanduse tehnoloogiate arenevad ka jõudsalt edasi ka maapeal paiknevad infosüsteemid.

SUMMARY

CYBER SECURITY RISKS OF ELECTRONIC SHIPPING DOCUMENTS AND THEIR FEASIBLE MINIMISATSION.

Helena Rattus

Maritime industry has evolved over the past few years thanks to technological advances. The main reasons for this are the continuous increase in the volume of goods, development and upgrading of technology and various systems. Large digitization has taken place with the introduction of technical developments. Previously used paper documents are turned into digitaal form and transferred digitally. This makes work with documents faster and more effective.

During digitization much information and data have moved to cyberspace. Adoption of digitalisation has been rapid and one important aspect has been overseen during this process – data protection in cyberspace. There has been increasing amount of cyber attacs and frauds against cargo, facilities and people. After major cyber attacs, number of companies have understood, that investment in cybersecurity is necessary, because price of damage is too high and criminals are always one step ahead.

The goal of the graduation thesis is to identify cyber threats in electronic maritime documents and to provide theoretical solutions to the problems encountered within the knowledge of the field. In order to find solutions, the author, in the theoretical part, provided an overview of the maritime transport documents and their development in general. The author examined the main cyber threats in the maritime industry and how they can influence cargo documents. Additionally examples of cyber attacs and cyber frauds have been added.

The hypothesis of the work was that electronic maritime transport documents and the information contained therein are not sufficiently protected from cyber attacks and are easily influenced. Also personell working with maritime documents has got no suficient training against cyber threats. As a result, the hypothesis is incorrect, since electronic maritime

transport documents are exactly as safe or even more than the paper forms that were previously used. At the same time, it became apparent that personell awareness of the dangers was not sufficient.

Cyber security issue has been an important topic on different maritime meetings, conferences and discussions. There is still opinions, that cyberthreat is not a real threat. After recent major cyber attacs, the opinions have changed. Decisions and steps have been made to make cyberspace safer. This gives hope, that rapid digitalisation in maritime industry will develop at the same speed as in the shipping industry.

Keywords: electronic freight documents, cyber security risks, electronic data transmission

VIIDATUD ALLIKAD

1. Boyes, H.; Roy, I.; Luck, A. (2016) Code of Practice. Cyber Security for Ports and Port Systems. London: Institution of Engineering and Technology
2. Brewer, J. (2015) Digitalisation and the Cyber Threat in the Maritime Industry. All about shipping, 25.10.2015 http://www.allaboutshipping.co.uk/2015/10/25/digitalisation-and-the-cyber-threat-in-the-maritime-industry/ (24.04.2018)
3. Clayton, R. (2018) Disrupting the disrupters: Why systems solutions might not be solutions at all. Lloyd's List, 14.04.2018 https://lloydslist.maritimeintelligence.informa.com/LL1122196/Disrupting-the-disrupters-Why-systems-solutions-might-not-be-solutions-at-all (22.04.2018)
4. Eidast, A. (2007) Meretranspordi kommertsekspluatatsioon. Tallinn: Tallinna Raamatutrükikoda
5. Grey, E. (2017) Cargo theft: a billion-dollar problem. Ship technology, 30.07.2017 https://www.ship-technology.com/features/featurecargo-theft-a-billion-dollar-problem-5882653/ (24.04.2018)
6. Gronholt-Pedersen, J. (2017) Maersk upbeat on shipping outlook, faces hefty cyber attack bill. Reuters, 16.08.2017 https://www.reuters.com/article/us-maersk-results/maersk-upbeat-on-shipping-outlook-faces-hefty-cyber-attack-bill-idUSKCN1AW0FQ (22.04.2018)
7. Heering, D. (2017) Küberturvalisuse tagamine laevanduses eesti laevaomanike näitel ning ettepanekud riskide maandamiseks: magistritöö. TTÜ Eesti Mereakadeemia: Tallinn
8. Kirch, K. (2013) Küberturvalisuse konstrueerimine ekspertide narratiivides: magistritöö. Tallinna Ülikool: Tallinn
9. Laherand, M.-L (2008) Kvalitatiivne uurimisviis. Saaremaa Ühisgümnaasium, https://www.syg.edu.ee/~peil/ut_alused/kvalitatiivne_uurimisviis.html (22.04.2018)
10. Lichman, E. (2016) Elektrooniline konossement ja mereveokiri: lõputöö. TTÜ Eesti Mereakadeemia: Tallinn
11. Papagiannopoulos, A (2017) ShipIT Conference speech. Bimco, 27.09.2017 https://www.bimco.org/news/bimco/20170928-bimco-president (24.04.2018)
12. Riigi Infosüsteemi Amet (2018) Krüptograafiliste algoritmide elutsükli uuring 2017: tehniline dokument. Riigi Infosüsteemi Amet: Tallinn

13. SKF Marine (2018) A paperless maritime future. Engineering at sea, 19.04.2018 http://engineeringatsea.skf.com/a-paperless-maritime-future/ (22.04.2018)
14. Suursoo, J.; Eidast, A. (2016) Ekspedeerija käsiraamat. Tallinn: Tallinna Tehnikakõrgkool
15. Todd, P. (2007) Bills of lading and banker's documentary credits. Fourth Edition. London: MPG Books
16. Viires, K (2013) Etnograafiline intervjuu. Kadri Viires, 09.06.2013 http://intervjuu.weebly.com/intervjuu-tuumluumlbid-ja-meetodid.html (22.04.2018)
17. Underhill, S. - A.; Bibby, W. (2016) Electronic Bills of Lading. Reed Smith, 14.01.2016 https://www.shiplawlog.com/2016/01/14/electronic-bills-of-lading (22.04.2018)
18. Wagstaff, J. (2014) All at sea: global shipping fleet exposed to hacking threat. Reuters, 24.04.2014 https://www.reuters.com/article/us-cybersecurity-shipping/all-at-sea-global-shipping-fleet-exposed-to-hacking-threat-idUSBREA3M20820140424 (29.04.2018)
19. Walia, I. (2018) SMW: Digitalisation is the way ahead, but challenges loom. Lloyd's List, 23.04.2018 https://lloydslist.maritimeintelligence.informa.com/LL1122313/SMW-Digitalisation-is-the-way-ahead-but-challenges-loom (23.04.2018)
20. Winter, C.; Plaistowe, M. (2018) E-bills of lading. Norton Rose Fulbright, veebruar 2018 http://www.nortonrosefulbright.com/knowledge/publications/163594/e-bills-of-lading (22.04.2018)
21. Üksik, K. (2014) Ostja õiguskaitsevahendid veodokumentidega seotud puuduste korral merevedude näitel: magistritöö. Tartu Ülikool: Tartu