Sisekaitseakadeemia

Sisejulgeoleku instituut

Margus Kukkur

KÜBEROLUKORRATEADLIKKUS JA SELLE TÕHUSTAMISE VÕIMALUSED EESTI ELUTÄHTSA MAKSETEENUSE JA SULARAHARINGLUSE OSUTAJATE NÄITEL

Magistritöö

Juhendaja:
Piret Pernik, MA

Kaasjuhendaja:
Anne Valk, MBA

Tallinn 2019

ANNOTATSIOON

Sisejulgeoleku instituut	Kaitsmise kuu ja aasta: 06.2019
Töö pealkiri eesti keeles: Küberolukorrateadlikkus ja selle tõhustamise võimalused Eesti elutähtsa makseteenuse ja sularaharingluse osutajate näitel Töö pealkiri võõrkeeles: Cyber threat intelligence and its development possibilities at the example of Esonian vital payment and cash circulation service providers. Lühikokkuvõte: Magistritöö on kirjutatud eesti keeles, võõrkeelne resümee on inglise keeles. Töö koosneb 80 leheküljest, millest põhiosa moodustavad 63 lehekülge. Töös on kasutatud 105 eesti ja inglisekeelset allikat. Töö sisaldab 5 tabelit, 8 joonist ja 3 lisa. Magistritöö eesmärk on välja selgitada küberolukorrateadlikkuse loomise ja rakendamise tõhustamise võimalused. Töö eesmärgi saavutamiseks püstitati neli uurimisülesannet: tuvastada inglisekeelse termini „cyber threat intelligence“ parim eestikeelne vaste; analüüsida küberolukorrateadlikkuse loomise ja rakendamisega seotud dokumente; Analüüsida organisatsioonide küberolukorrateadlikkuse loomist ja rakendamist ning selgitada välja organisatsioonide vajadused; Analüüsida küberolukorrateadlikkuse teoreetilist käsitlust ning empiirilise uuringu tulemusi ja esitada ettepanekuid küberolukorrateadlikkuse parandamiseks. Magistritöö eesmärgi saavutamiseks ja uurimisülesannete täitmiseks kasutati uurimisstrateegiana juhtumiuuringut. Magistritöö andmekogumisemeetoditeks olid dokumendianalüüs ja poolstruktureeritud intervjuud. Kvalitatiivse sisuanalüüsi teostamiseks kasutati andmeanalüüsiprogrammi NVivo 12 Pro. Magistritöö tulemusel selgusid küberolukorrateadlikkuse tõhustamise suunad, mille põhjal tegi magistritöö autor kolm praktilist rakendatavat ettepanekut küberolukorrateadlikkuse parandamiseks.	
Lisasid: Ei ole	
Võtmesõnad: küberkaitse, küberjulgeolek, küberohud, küberohipilt, küberohuteadlikkus, küberohuluure teave, küberohumaastik, küberolukorrateadlikkus.	
Võõrkeelsed võtmesõnad: cyber threat intelligence, cyber threat, situatuional awareness, cyber defence, cyber security.	
Säilitamise koht: Sisekaitseakadeemia raamatukogu	
Töö autor: Margus Kukkur Olen koostanud lõputöö iseseisvalt. Kõik lõputöö koostamisel kasutatud teiste autorite tööd, seisukohad, kirjalikest allikatest ja mujal allikates saadud info on nõuetekohaselt viidatud. Olen nõus oma lõputöö avaldamisega elektroonilises keskkonnas. Allkiri:	
Vastab lõputöö nõuetele Juhendaja: Piret Pernik	Allkiri:
Vastab lõputöö nõuetele Kaasjuhendaja: Anne Valk	Allkiri:
Kaitsmisele lubatud Instituudi juhataja: Erkki Koort	Allkiri:

SISUKORD

MÕISTED JA LÜHENDID

APT – *(Advanced Persistent Tvthreat)* Kinnisründeoht, mida iseloomustab ettemääratud eesmärgi saavutamiseks suunatud sihikindla kohanduva ulatusliku ressursside ja erioskustega kestusründe oht.

CERT – *(Computer Emergency Response Team)* Üksus, mis tuvastab, jälgib ja lahendab arvutivõrkudes toimuvaid turvaintsidente, teavitab ohtudest ja korraldab ennetustegevusi (Riigi Infosüsteemi Amet, 2018b).

CROE – (Cyber Resilience Oversight Expectations) Järelevalve ootused küberkerksusele.

CSIRT – *(Computer Security Incident Response Team)* vt CERT.

CVE – (Common Vulnerabilities and Exposures) USA mittetulundusühingu MITRE Corporation toimetatav ja hallatav rahvusvaheline nimekiri avaldatud turvanõrkustest, mille igale avaldatud nõrkusele omistatakse unikaalne numbriline identifikaator, kirjeldus ja vähemalt üks avalik viide.

DDOS – *(Distributed Denial of Service)* Hajutatud teenusetõkestamise rünnak eesmärgiga arvuti või arvutivõrgu ülekoormamine samal ajal suure hulga päringute saatmise teel.

Eksploidi pakid – Kollektsioon tarkvara nõrkuseid ärakasutavatest pahavaradest.

EBA – *(European Banking Authority)* Euroopa Pangandusjärelevalve.

ENISA – *(European Union Agency for Network and Information Security)* Euroopa Liidu Võrgu- ja Infoturbeamet.

FMI – *(Financial Market Infrastructure)* Finantsturu infrastruktuur.

HUMINT – *(Human Intelligence)* Inimluure (Cybernetica 2019b).

IMINT – *(Imagery Intelligence)* Visuaalne luure ehk piltluure (Cybernetica 2019a).

IOC – *(Identification of Compromise)* Kompromiteerimise identifikaatorid.

ISKE – Infosüsteemide kolmeastmeline etalonturbe süsteem, mille väljatöötamisel ja arendamisel on aluseks võetud Saksamaa Küberkaitseameti (BSI) avaldatud infoturbe standard.

Kalastus – *(Phishing)* Petturlik protsess, millega elektroonilises suhtluses usaldatavat olemit teeseldes püütakse saada privaatset või konfidentsiaalset teavet, kasutades selleks suhtlusosavust või tehnilist pettust (Eesti Standardikeskus, 2018).

Kinnisründeoht – vt APT.

Krüptokaevekaaperdus – *(Cryptojacking)* Brauserikaaperdus eesmärgiga rakendada ohvri arvuti ressursse krüptorahakaeveks ja/või krüptoraha varguseks.

Küberintsident – süsteemis toimuv sündmus, mis ohustab või kahjustab süsteemi turvalisust (Küberturvalisuse seadus, 2018).

Küberkerksus – *(Cyber Resilience)* Seisund, olukord või omadus, kus organisatsioon suudab oma teenuseid pakkuda ka pidevate küberrünnakute olukorras ning neile vaatamata.

Küberolukorrateadlikkus – (*Cyber Threat Intelligence- CTI*) Teadlikkus üksikisikut või organisatsiooni ohustavast küberohust, mis võimaldab reageerida ohust tuleneva mõju ennetamiseks, tuvastamiseks ja tõrjumiseks.

Küberruum – inimeste, tarkvara ja teenuste interaktsiooniga Internetis temaga ühendatud tehniliste vahendite ja võrkude abil tekitatav liitkeskkond, mis ei eksisteeri mingil füüsilisel kujul (Cybernetica, 2019d).

Lunavara – Pahavara, mille eesmärk on rikkuda süsteemi käideldavust, nõudes käideldavuse taastamiseks lunaraha.

NIST – *(National Institute of Standards and Technology)* Riiklik Standardi- ja Tehnikainstituut.

Olukorrateadlikkus – (situational awareness) võime läbi küberolukorrateadlikkuse protsessi tuvastada ja mõista potentsiaalseid kahjulikke sündmuseid ning kasutusele võtta meetmeid riski leevendamiseks (CPMI & IOSCO, 2016; ECB, 2018).

OSINT – *(Open Source Intelligence)* (näiliselt salajase) teabe kogumine ja tuletamine avalikest allikatest, näiteks ajalehtedest (Cybernetica 2019c).

Robotvõrk – *(botnet)* kaugjuhitaval teel kontrollitavatest seadmetest koosnev võrk, mida kasutatakse ebaseaduslikeks toiminguteks.

Pahavara – Tarkvara, mille eesmärk on kahju teha.

Rakendusliides – reeglid ja vahendid, mida rakendusprogramm kasutab suhtluseks operatsioonisüsteemiga, andmebaasihalduse süsteemiga või muu juhtprogrammiga, samuti sideprotokolliga.

Rämpspost – elektroonilise sõnumside süsteemide kuritarvitus soovimatute massiliste sõnumite valimatuks saatmiseks.

Ründevektor – tee või vahend, mille abil ründaja võib saada juurdepääsu arvutile või võrguserverile pahatahtliku tagajärje tekitamiseks (Eesti Standardikeskus, 2018)

SIGINT – (*Signals Intelligence)* Signaaliluure (Cybernetica 2019f).

STIX – (*Structured Threat Information eXpression)* Struktuurne keel ja formaat küberolukorrateadlikkuse loomiseks ja jagamiseks (Barnum, 2014).

SOC – *(Security Operations Center)* Küberkaitse operatsioonide keskus kui üksust, mis on spetsialiseerunud küberintsidentide lahendamisele.

SQL süst – Rünne andmebaasipõhisele rakendusele (Cybernetica 2019g).

Suhtlusründed – *(Social Engineering)* Inimestega manipuleerimine eesmärgiga panna neid sooritama toiminguid või avaldama konfidentsiaalset teavet.

TAXII – *(Trusted Automated eXchange of Indicator Information)* Rakendatava küberolukorrateadlikkuse jagamise formaat, millega defineeritakse sõnumite vahetus organisatsiooni ja toodete/teenuste tasemel (Davidson & Schmidt, 2014).

TECHINT – (*Technical Intlelligence)* Tehniline luureteave (Cybernetica 2019h).

TTP – *(Tactics, Techniques and Procedures)* Taktikad, tehnikad ja protseduurid, mis kirjeldavad kaitse/ründe käitumismustrit. Taktikad kirjeldavad tegutseja käitumismustrit ründe/kaitse ajal. Tehnikad kirjeldavad ründe elluviimiseks kasutatavaid tehnikaid. Protseduuride käsitluses kirjeldatakse, kuidas taktikaid ja tehnikaid kombineerides edukas rünnak ellu viiakse.

Õngitsemine – vt kalastus.

SISSEJUHATUS

Tänapäeva küberrünnakud asutuste ja ettevõtete infosüsteemide vastu on muutunud läbimõeldumaks ja keerukamaks, mis teeb ka nende avastamise raskemaks. Kümne aasta eest piisas traditsiooniliste kaitsemeetme (viirusetõrje, tulemüür) rakendamisest, kuid nüüd tuleb kaitsele panustada palju rohkem meetmeid ja ressurssi. Ründaja eesmärgiks on tavapärastest meetmetest mööda minna ning leida viise arvuti kompromiteerimiseks või nakatamiseks, mille kaudu rünnakut edasi planeerida. Näiteks kinnisründe ohu kategooriasse klassifitseeruvad ründed (*Adnvanced Persistent Threat*) (Cole, 2013; Chen et al., 2016), mis on olnud riikide luuretegevuse ründemeetodiks (Ask, et al., 2014; Fireeye, 2014; Weedon, 2015, pp. 67-77), leiavad järjest rohkem kasutust küberkurjategijate seas eesmärgiga saada rahaline kasu läbi rünnaku (Buck, et al., 2016).

Euroopa Liidu Võrgu- ja Infoturbeamet (ENISA) toob 2016 aasta raportis välja 15 küberohtu, millel põhinevad erinevad küberrünnakud. Kolm peamist küberohtu on pahavarad erinevates variatsioonides (lunavara, viirused, troojalased jt), veebipõhised rünnakud veebirakendustele (DDOS ehk teenustõkestusrünnak, SQL süstimised, eksploidi pakid jt), andmerikkeohud andmete juhusliku või ebaseadusliku hävingu, kao, muutmise, volitamata avalikustamise või nende juurdepääsu näol (kalastusründed, küberspionaaži jt), mida kasutatakse küberkuritegevuste elluviimisel, sh finantskuritegevustes (ENISA, 2016a). Et suurendada organisatsioonide küberkaitset keerukate rünnakute tuvastamiseks, on üheks kasvavaks trendiks küberolukorrateadlikkuse *(cyber threat intelligence)* loomine ja selle rakendamine, mis võimaldab saadud teadlikkuse põhjal olemasolevaid turvameetmeid ja protseduure suunata ründevektori tuvastamiseks (Shackleford, 2015; Dalziel, 2015; Friedman & Bouchard, 2015). Küberkaitse tugevdamise aspektist võimaldab küberolukorrateadlikkuse rakendamine organisatsioonidel saada rünnakute tõrjumiseks ja ennetamiseks õigel ajal õiget infot, mis omakorda aitab optimeerida küberkaitse kulutusi rünnakute avastamiseks ja nendele reageerimiseks (Dalziel, 2015; Cunningham, 2015). Küberolukorrateadlikkust defineeritakse kui küberohu teabe kogumise, teisendamise, analüüsimise, tõlgendamise või rikastamise teel saadud teadlikkust, mis pakub vajalikku konteksti otsuste tegemise protsessides (ECB, 2018; CPMI & IOSCO, 2016). Küberolukorrateadlikkuse loomiseks saab teavet hankida erinevatest allikatest- avalikud,

teenusepakkujad, koostööpartnerid, grupeeringud, katusorganisatsioonid jt. Igal organisatsioonil, kes rakendab küberolukorrateadlikkust oma otsustusprotsessides, tuleb enda jaoks leida küberolukorrateadlikkuse loomiseks õiged kanalid ja allikad, mis omakorda sõltuvad küberolukorrateadlikkuse rakendamise vajadustest. Strateegilisel-operatsioonilisel juhtimistasanditel (näiteks organisatsiooni juhid, turvajuhid, riskijuhid) vajatakse kõrgema taseme teadlikkust küberkaitse planeerimise, riskihindamise, turvameetmete väljatöötamise jt juhtimistaseme protsessides. Selleks võib olla teadlikkus küberohtudest, küberohutrendidest, aktuaalsetest ja potentsiaalsetest rünnakutest, mis võivad organisatsiooni äriprotsesse ohustada. Teadlikkuse sidumine organisatsiooni riskijuhtimise protsessiga võimaldab küberruumist tulenevaid rünnakute mõju palju täpsemalt hinnata. Riskipõhine lähenemine võimaldab kohaldada rakendatavaid meetmeid vastavalt organisatsiooni vajadusele ning kasutusele võtta tulemuslikumad ja kuluefektiivsemad kaitsemeetmed rünnakute tõrjumiseks (Department of Homeland Security, 2011). Taktikalisel-tehnilisel juhtimistasandil (näiteks süsteemi/turvalahenduste haldurid, intsidentide käitlemise üksus) vajatakse omakorda spetsiifilist küberolukorrateadlikkust küberrünnakute ennetamiseks, tuvastamiseks ja tõrjumiseks. Selleks võib olla teadlikkus ründaja poolt kasutatavast taktikast, tehnikast ja protseduuridest (TTP), teave organisatsiooni vastu suunatud ründest, kompromiteerimise identifikaatoritest (IoC) või muu teave, mis aitab küberintsidentide ennetamisele, tuvastamisele ja reageerimisele kaasa. Organisatsioonides, mis kasutavad küberolukorrateadlikkust võimalikult hästi ära, on küberkerksemad ja teadlikkumad organisatsiooni ohustavatest küberohtudest (Chismon & Ruks, 2015). Küberkerksus on organisatsiooni võime jätkata oma missiooni teostamist küberohtudest ja muudest keskkonna muutustest tulenevate mõjude ennetamise ning nendega kohanemise kaudu, seistes vastu, lahendades ja kiiresti taastudes küberintsidentidest (ECB, 2018). Küberolukorrateadlikkuse loomine ja selle rakendamine organisatsioonide erinevates otsustusprotsessides on kujunemisjärgus. Sellest lähtuvalt keskendutakse magistritöös finantssektori küberolukorrateadlikkuse loomise ja rakendamise uurimisele analüüsides, millised on küberolukorrateadlikkuse loomise ja rakendamise võimalused ning kuidas tõhustada küberolukorrateadlikkuse loomist ja rakendamist. Kuna Eesti finantssektoris tegutsevad organisatsioone on palju, siis fokuseerib töö elutähtsat makseteenust ja sularaharinglust pakkuvate ettevõtete hindamisele. Eesti Panga Presidendi 08.03.2019 jõustunud määruse makseteenuse ja sularaharingluse kirjeldus ja toimepidevuse nõuded §2

lõike 1 kohaselt on elutähtsa finantsteenuse osutajad AS SEB Pank, Swedbank AS, Luminor Bank AS ja AS LHV Pank (Eesti Panga President, 2019). Lisaks on fookuses Riigi Infosüsteemi Amet, kes küberturvalisuse seaduse §8 ja §12 lõike 2 ja 3 kohaselt omab riigiülest küberruumi olukorrapilti ja §12 lõike 3 kohaselt edastab küberintsidentide ennetamiseks ja lahendamiseks ohuteateid isikutele, olles seeläbi oluliseks partneriks elutähtsat teenust osutavatele ettevõtetele küberolukorrateadlikkuse kujundamisel (Küberturvalisuse seadus, 2018).

Küberkaitse arendamine on tänapäeval aina rohkem infotehnoloogiast sõltuvas maailmas olulise tähtsusega. 2014-2017 küberjulgeoleku strateegia kohaselt tulenevad peamised küberjulgeoleku ohud Eesti Riigi, majanduse ja elanikkonna ulatuslikust ning kasvavast sõltuvusest info- ja kommunikatsioonitehnoloogia taristust ja e-teenustest (Majandus- ja Kommunikatsiooniministeerium, 2014). Eesti küberturvalisust mõjutab paratamatult ka keerukas julgeolekuolukord nii siinses regioonis kui kogu maailmas. Küberoperatsioonide kasutamine riikide soovitud strateegilise eesmärgi või mõju saavutamiseks on viimastel aastatel muutunud sagedamaks ja tõsisemaks: mõjutatakse nii demokraatlikke protsesse (valimised ja referendumid ning nendega seotud kampaaniad) kui ka rünnatakse elutähtsat taristut eeskätt energia-, side- ja pangandussektorit (Majandus- ja Kommunikatsiooniministeerium, 2018). Küberohtudele operatiivselt reageerimise kaudu on võimalik rünnak õigeaegselt avastada ja kaitsemeetmed rakendada.

Magistritöö on **aktuaalne**, kuna finantssektor on küberkurjategijatele üks atraktiivsemaid rünnatavaid objekte kuritegelikul teel raha teenimise eesmärgil. Küberkurjategijate kõrvale on tekkinud riiklikult toetatud grupeeringud, kellel on piisavalt aega, vahendeid ja oskuseid, et mööda minna tavapärastest kaitsemeetmetest ja vältida rünnakute tuvastamist (Riigi Infosüsteemi Amet, 2018b, lk 34; Chen et al., 2016). Küberruumis on üha raskem vahet teha, kas küberkuritegevuse taga on kurjategija, kelle motiiviks on isikliku kasu saamine või töötab ta vaenuliku riigi eriteenistuse kasuks, valmistades ette järgmist rünnakut elutähtsate teenuste tõkestamiseks (Riigi Infosüsteemi Amet, 2015). Üks mitmest sellise mõjuga rünnakutest finantssektori vastu leidis aset 2016 aasta kevadel, mil Põhja-Korea häkkerirühmitus Lazarus ründas Bangladesh Keskpanga arveldussüsteeme, mille käigus varastati 81 miljon dollarit (Buck, et al., 2016). Rünnak oli põhjalikult planeeritud ja läbi viidud, mille käigus manipuleeriti panga arveldussüsteemidega, minnes mööda turvameetmetest ja lülitades välja süsteemi kontrollmeetmed ebaseaduslike ülekannete

tegemiseks. Sama rühmitust peetakse vastutavaks pikaajaliste kampaaniate eest 31 riigi pangandussektori sihtmärkide vastu. Euroopa Liidu piirides nakatati Poola finantsjärelevalveasutuse veebileht tundmatu pahavaraga, mille tulemusena nakatusid omakorda Poola kommertspangad pahavaraga läbi järelevalveasutuse veebilehe külastamise (Riigi Infosüsteemi Amet, 2018b, lk 34). 2016 aastal alguse saanud intsidentide tulemusena vaadatakse küberkaitse korraldust kogu sektoris üle. Näiteks üks suuremaid pankadevahelist arveldusteenust pakkuv ettevõte SWIFT on peale intsidenti kehtestanud hulga meetmeid arveldusteenuse täiendavaks kaitsmiseks nii enda kui ka klientide infosüsteemides. Ühe meetmena pakutakse klientidele küberolukorrateadlikkust, mille rakendamine erinevatel juhtimistasanditel võimaldab efektiivselt reageerida, ennetada ja tõrjuda järjest keerukamaid küberrünnakuid (SWIFT, 2017; ECB, 2018; ENISA, 2019; Skopik, 2018; Friedman & Bouchard, 2015).

Eesti andmebaaside otsingutest tuvastas autor varasemalt käsitletud uurimistöid küberolukorrateadlikkuse aspektist (Vahturov, 2018; Farár, 2016). Otsinguks kasutas autor Google Scholar, ESTER, Tallinna Tehnikaülikooli raamatukogu digikogu ja DSpace teadusallikate andmebaase. Organisatsiooni teadlikkuse loomine küberruumis valitsevatest ohtudest ei ole uudne teema, kuid selle loomine ja rakendamine proaktiivselt organisatsiooni erinevates otsustusprotsessides vastavalt pidevalt muutvale ohupildile on **uudne** teema, mille osas organisatsioonid alles otsivad võimalusi, et tagada organisatsiooni toetav küberkerksuse tase (ENISA, 2019, p. 8). Küberolukorrateadlikkuse teema kohta teostatud otsing andis teadusallikatest vähe informatsiooni. Inglisekeelsele terminile „cyber threat intelligence“ on eestikeelne vaste alles kujunemisel, mis sai kinnitust ekspertintervjuude käigus. Käesolevas töös kasutatakse termini eestikeelse vastena küberolukorrateadlikkust. Termini vastena pakuti intervjuudel veel küber- ohuluuret, ohuolukorrapilti, küberohuteadlikkust jt. Lisaks Eesti teadusallikate andmebaasi otsingule teostati otsing rahvusvahelistes teadusallikate andmebaasides, kasutades märksõnu „küberoht“, „küberohuteadlikkus“, „threat intelligence“, „cyber threat intelligence“, „situational awareness“. Otsingute tulemusena leidus rahvusvahelistest andmebaasidest teadusallikaid, mis käsitlevad küberolukorrateadlikkust ja selle erinevaid rakendamise käsitlusi (Cunningham, 2015; Boukhtouta, 2016; Ionita & Patriciu, 2016). Töid, mis uuriksid küberolukorrateadlikkuse loomist ja rakendamist Eesti finantssektori näitel, autor ei tuvastanud.

Käesoleva magistritöö **uurimisprobleem** on püstitatud küsimusega: kuidas tõhustada küberolukorrateadlikkuse loomist ja rakendamist elutähtsat finantsteenust pakkuvates organisatsioonides? Uurimisprobleemi täpsustamiseks esitatakse järgmised **uurimisküsimused:**

1. Milline on parim eestikeelne vaste inglisekeelsele terminile „cyber threat intelligence“?
2. Millised on küberolukorrateadlikkuse loomise ja rakendamise üldtunnustatud alused?
3. Milline on organisatsioonide küberolukorrateadlikkuse loomise ja rakendamise seis?
4. Millised on organisatsioonide küberolukorrateadlikkuse loomise ja rakendamise vajadused?
5. Kuidas tõhustada küberolukorrateadlikkuse loomist ja rakendamist?

Kavandatava magistritöö **eesmärgiks** välja selgitada küberolukorrateadlikkuse loomise ja rakendamise tõhustamise võimalused, sh leida inglisekeelsele terminile „cyber threat intelligence“ parim eestikeelne vaste, mis iseloomustaks kõige täpsemalt termini taga olevat kontseptsiooni. Eesmärgi saavutamiseks püstitatakse järgmised **uurimisülesanded**:

1. Tuvastada inglisekeelse termini „cyber threat intelligence“ parim eestikeelne vaste;
2. Analüüsida küberolukorrateadlikkuse loomise ja rakendamisega seotud dokumente;
3. Analüüsida organisatsioonide küberolukorrateadlikkuse loomist ja rakendamist ning selgitada välja organisatsioonide vajadused;
4. Analüüsida küberolukorrateadlikkuse teoreetilist käsitlust ning empiirilise uuringu tulemusi ja esitada ettepanekuid küberolukorrateadlikkuse parandamiseks.

Magistritöö on kvalitatiivne empiiriline uurimustöö, mille uurimisstrateegiaks on valitud juhtumiuuring (*case study*), mis on disainitud põimunud üksikjuhtumiuuringuna (*embedded single case design*) (Yin, 2014, pp. 49-56). Juhtumiuuringu läbiviimisel lähtutakse Robert K. Yin käsitlusest, mille kohaselt on juhtumiuuring meetod, õppimaks keerukast juhtumist, tuginedes antud juhtumi kõikehõlmavale mõistmisele, mis on saadud ulatuslikult kirjeldades ja analüüsides juhtumit tervikuna ja tema kontekstis (Yin, 2014, p.

16). Juhtumiuuringu uurimisobjektiks on küberolukorrateadlikkuse protsess. Juhtumiks on küberolukorrateadlikkuse loomine ja rakendamine. Uurimisobjektideks ja subjektideks on küberolukorrateadlikkuse teoreetilised allikad, üldtunnustatud küberkaitset korraldavad dokumendid, küberturvalisuse strateegiad, regulatsioon ning kriitilist finantsteenust pakkuvad ja seotud organisatsioonid.

Käesolevas töös kasutatakse andmekogumise meetodina dokumendianalüüsi ja poolstruktureeritud ekspertintervjuusid, mille valimid on eesmärgistatud *(purposive ssampling)* (Babbie, 2013, pp. 128-129). Dokumendianalüüsi eesmärgiks oli analüüsida küberolukorrateadlikkuse käsitlust küberkaitset käsitlevates dokumentides, regulatsioonis ja strateegiates. Kasutatud dokumentide nimekiri on toodud vastavalt tabelis 3. Poolstruktureeritud ekspertintervjuud viidi läbi kuue küberkaitse eksperdiga. Ühte intervjueeritavat küsitleti kirjalikult lisas 2 toodud küsitluse põhjal, mille tulem ei klassifitseeru kvalitatiivsete andmete kogumise klassi. Samas pidas autor oluliseks kasutada kirjalikku vastust intervjuude analüüsis. Täiendavate küsimuste esitamiseks lepiti kokku ja suheldi e-kirja vahendusel. Intervjueeritavate valim moodustus kriitilist finantsteenust osutavate pankade ja Riigi Infosüsteemi Ameti küberkaitse valdkonna ekspertidest.

Magistritöö koosneb kahest peatükist. **Esimene peatükk** käsitleb küberolukorrateadlikkuse loomise ja rakendamise teoreetilisi aluseid, milles tuvastatakse läbi küberohumaastiku kaardistamise võimalikud ohud ja nende trendid, mis on küberolukorrateadlikkuse loomise aluseks. Kirjeldatakse küberolukorrateadlikkuse loomise protsess ja tuuakse esile küberolukorrateadlikkuse rakendamise võimalused. **Teine peatükk** analüüsib küberolukorrateadlikkuse loomise ja rakendamisega seotud dokumente, organisatsioonide küberolukorrateadlikkuse loomist ja rakendamist, organisatsioonide vajadusi küberolukorrateadlikkuse loomiseks ja rakendamiseks ning analüüsitud-sünteesitud uurimistulemuste põhjal esitatakse ettepanekud küberolukorrateadlikkuse loomise ja rakendamise tõhustamiseks.

1. KÜBEROLUKORRATEADLIKKUSE TEOREETILISED ALUSED

Inglisekeelsele terminile „cyber threat intellience“ ei ole eestikeeles ühtset ja ühtselt mõistetavat vastet tekkinud. Eestikeelse termini vaste leidmiseks konsulteeriti erinevate küberkaitse valdkonna ekspertidega, teadlaste ja Kaitseministeeriumi terminoloogia komisjoni liikmega. Käesolevas töös käsitletakse eestikeelse terminina **küberolukorrateadlikkust**. Ekspertide poolt pakutud termini käsitlused on veel küberohuteadlikkus, küberohupilt, küber olukorrapilt ja küberohuluure. Töö koostamise etapis kasutati terminina „küberohu teadlikkus“, mida testiti ekspertintervjuudel ekspertide peal. Peale ekspertintervjuude läbiviimist ja tulemuste analüüsimist muudeti termini käsitlus küberolukorrateadlikkuseks, mis praeguste teadmiste juures kirjeldab kõige täpsemalt termini „cyber threat intelligence“ tähendust. Küberolukorrateadlikkust käsitletakse kui otsustamisprotsessis kasutatavat konteksti, mis on saadud küberohu teabe kogumise, teisendamise, analüüsimise, tõlgendamise või rikastamise teel moodustunud teadlikkusest.

Järgnevalt analüüsitakse küberolukorrateadlikkuse loomiseks kasutatavat teavet, küberolukorrateadlikkuse loomise protsessi ja rakendamise võimalusi.

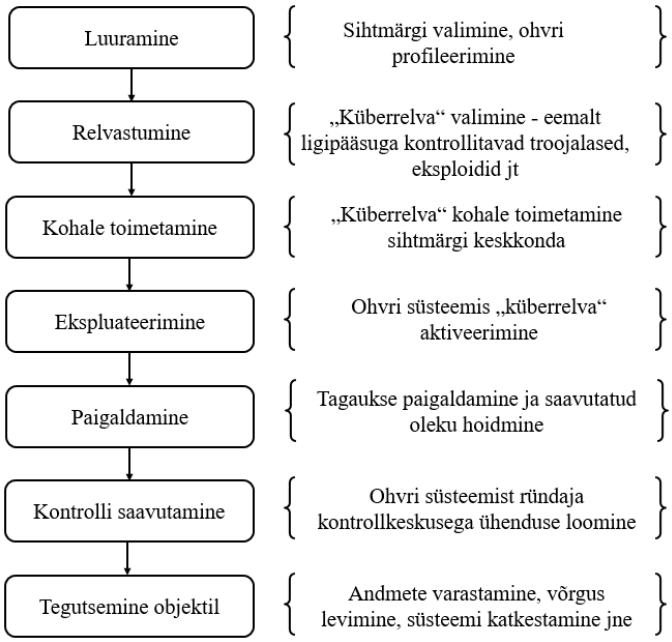
1.1. Küberolukorrateadlikkuse loomiseks kasutatav teave

Käesoleva peatüki eesmärk on analüüsida küberolukorrateadlikkuse loomiseks kasutatavat teavet. Teadlikkust on uuritud juba enne seda, kui küberruum oma arengu ja seal tekkinud ohtudega teiste teadlikkuse domeenide kõrvale lisandus. Sellest lähtuvalt enne, kui küberolukorrateadlikkuse analüüsiga süvitsi minnakse, vaadeldakse küberolukorrateadlikkust laiemas võtmes, et kaardistada see teadlikkuse maastikul. Inglisekeelsele terminile „intelligence“ on eesti keeles laialdaselt kasutatud luure kontekstis. Samuti sobib termini käsitlusena teadmus, kui teadmised millegi kohta kogumina (EKSS, 2019). Käesolevas töös käsitletakse eestikeelse terminina teadlikkust, olles sünonüümiks sõnadele teadmus ja luure.

Johnson jagab teadlikkuse tulenevalt andmeallikate päritolust kaheks – inimluure ehk HUMINT (*Human Intelligence*) ja tehniline luureteave ehk TECHINT (*Technical Intelligence*). Tehnilist luureteavet jagatakse omakorda väiksemateks kategooriateks, sõltuvalt andmete päritolust vastavalt signaaliluure ehk SIGINT (*Signal intelligence*), visuaalne luure ehk IMINT (*Image Intelligence*) ja avalike allikate luure ehk OSINT (*Open Source Intelligence*) (Johnson, 2007). Luuredomeenide kaardistuste seast otsiti küberolukorrateadlikkuse või küberohuluure käsitlust, mille kohta leiti teadusallikatest üks vaste, milles küberolukorrateadlikkus jaotati rakendatava teadlikkuse (*Actionable Intelligence*) kategooriasse (Planque, 2017). Tegemist on väga laia klassifitseerimisega, sest rakendatava teadlikkuse/luure kategooriasse saab klassifitseerida väga laia spektriga luureteavet (lisaks CTI-le IMINT, OSINT, SIGINT jt), mis on rakendatav erinevates otsustamise protsessides. Luure informatsiooni loomise eesmärgiks on pakkuda otsustajatele otsuse langetamiseks vajalikku teadlikkust, mis saadakse informatsiooni kogumise ja analüüsimise tulemusena (Juurvee, 2018). Proovides klassifitseerida küberolukorrateadlikkust Johnsoni jaotuses tehnilise või inimluure kategooriate vahel, siis see ei õnnestu, sest küberolukorrateadlikkuse loomiseks võib info pärineda erinevatest kategooriatest. Peamiselt kogutakse teavet tehniliste vahendite vahendusel (TECHINT, sh OSINT, SIGINT jt). Samas on tähtsal kohal ka inimestelt kogutud teabel (HUMINT), näiteks töötaja poolt tuvastatud anomaaliad ja/või suunatud ründed (kalasuts või õngitsemine). Küberolukorrateadlikkust (küberohuluuret) tuleks käsitleda pigem eraldi kategooriana (CTI), kui püüda seda klassifitseerida mõne olemasoleva luure kategooria alla.

Et küberolukorrateadlikkust paremini mõista, analüüsitakse järgnevalt teavet, mis on vajalik küberolukorrateadlikkuse loomiseks. Euroopa Liidu Võrgu- ja Infoturbeameti ENISA on koostatud küberohtude taksonoomia mudeli, milles jaotatakse ohud vastavalt nende tekkepõhjusele viie kategooria vahel – inimveast, süsteemi rikkest, loodusest ja sotsiaalsest nähtusest, kolmandast osapoolest ja pahavara tegevusest põhjustatud ohud (vt lisa 1) (ENISA, 2016b). Kuna küberolukorrateadlikkuse skoobis on saada teavet küberruumist tulenevate ohtude kohta, siis taksonoomia mudeli elementidest pakuvad huvi pahavara tegevustest põhjustatud ohud, mis omakorda jaotatakse – teenustõkestusrünnak (DDOS), pahavara IT varades, tarkvara nõrkuste ärakasutamine, ligipääsu ja õiguste väärkasutus (sh autentimisinformatsiooni murdmine), võrgu põhised ründed, suhtlusründed

(õngitsusründed jt), andmete ja tarkvara/riistvara rikkumine ja pahavarast tulenev füüsilise ründe oht (seiskub kriitiline taristu/teenus). Küberruumi ohtudest tuleneva mõju maandamiseks on oluline saada teadlikkust nimetatud rünnakute kohta, mis aitab otsustajaid otsuste tegemisel. Barnum võrdleb küberolukorrateadlikkust tavapärase kuritegevuse avastamise protsessiga, milles kogutakse teavet vastase võimekusest, tegevusest ja kavatsustest, mis kantakse üle kuritegevuse domeenist küberdomeeni (Barnum, 2014). Kogutud teave annab infoturbe või küberkaitse eest vastutavatele töötajatele teavet ründaja võimekusest, tegevusest ja kavatsustest, mille põhjal saab omakorda rakendada meetmeid rünnaku ennetamiseks, tuvastamiseks ja tõrjumiseks. Küberolukorrateadlikkuse aspektist koondatakse selline teave taktikaliste, tehniliste ja protseduuriliste (TTP) teabeliikide alla (Friedman & Bouchard, 2015, p. 26). Lisaks küberohtudele ja ründaja taktikatest, tehnikatest ja protseduuridest vajatakse kaitsmisel teavet ründevektori erinevate etappide kohta, et rünnakut tuvastada ja võimalikult kiiresti ning efektiivselt kahjutuks teha (Yadav & Mallari, 2016, Zimmerman, 2014). Ründevektor jaotatakse seitsmeks etapiks, milleks on: luuramine, relvastumine, kohale toimetamine, ekspluateerimine, paigaldamine, kontrolli saavutamine ja tegutsemine objektil. Protsessi ahelat nimetatakse küberkaitse aspektist kui „(küber) tapmisahel“ (*(cyber)kill-chain*), mille ahela igale etapile vastab komplekt meetmeid, mida rakendatakse kaitses ründevektori kahjutuks tegemisel (vt joonis 2). Küberolukorrateadlikkuse loomise ja rakendamise aspektist on oluline koguda ründevektori ahela osade lõikes teavet, mis aitavad ründevektorit ennetada, tuvastada ja kahjutuks teha (Yadav & Mallari, 2016, Barnum, 2014, Zimmerman, 2014). Sellise teabe käsitlust võib leida kompromiteerimise identfikaatorite *(IoC)* ja/või TTP teabeliikide alt. IoC-d pakuvad kaitsjatele indikaatoreid pahavara tuvastamiseks ja tõrjumiseks (Friedman & Bouchard, 2015, p. 2).



Joonis 1. Ründevektori etapid (autori koostatud)

Kuna küberohte on palju, mida omakorda kasutatakse erinevates ründevektorites, siis nende kaardistamiseks analüüsitakse ENISA küberohumaastiku 2012 – 2018 aastaraporteid. Raportites keskendutakse 15-le kõige aktuaalsemale küberohule, mida võrreldakse varasemal aastal läbi viidud analüüsi tulemustega. Aastaaruannete koostamiseks kogus ENISA avalikest allikatest kokku toimunud intsidendid ja jagas need vastavatesse küberohu kategooriatesse (ENISA, 2017, pp. 19-20). Küberohumaastiku kujunemisest ja trendidest ülevaatliku pildi saamiseks kõrvutatakse erinevate aastate raportite tulemid ühte tabelisse kokku (vt tabel 1). Tabelis esitatakse ohud esinemissageduse järjestuses, kus eespool on ohud, mis esinesid kogutud allikates kõige sagedamini. ENISA 2018 küberohumaastikku ohte kokkuvõttev raport tõi ohtude nimekirja juurde uue krüptokaevekaaperduse (*cryptojacking*) ohu, mis on tulenevalt plokiahela tehnoloogia kasutuselevõtu populaarsuse kasvuga kasvutrendis (ENISA, 2019). Krüptokaevekaaperdus on olemuselt veebisirvijate nõrkuseid ära kasutav oht eesmärgiga rakendada ohvri arvuti ressursse krüptoraha kaevandamiseks ja/või krüptoraha varguseks (ENISA, 2019; NCSC, 2018).

Tabel 1. ENISA küberohumaastiku aastaraportite põhjal koostatud ülevaade küberohtudest ja nende trendidest (autori koostatud).

Ohtude pingerida	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
1. Pahavara	↑	↑	↑	↑	↑	→	→
2. Veebipõhised rünnakud (pahavara alla laadimine, pahavaraga nakatunud url-id, veebisirvija põhised ründed)	-	-	↑	↑	↑	↑	↑
3. Rünnak veebirakendustele (koodi süstimised: SQL, XSS)	↑	↑	↑	↑	↑	↑	→
4. Teenustõkestamise rünnak *(Denial of Service- DOS)*	→	↑	↑	↑	↑	↑	↑
5. Robotvõrk *(Botnet)*	↑	→	↓	↓	↑	↑	↑
6. Kalastus/õngitsemine *(Phishing)*	→	↑	↑	→	→	↑	↑
7. Rämpspost *(Spam)*	↓	→	↓	↓	↓	↑	→
8. Lunavara	-	-	↓	↑	→	↑	↓
9. Sisemine oht *(Insider threat)*	-	-	→	↑	→	→	↓
10. Füüsiline manipuleerimine/rikkumine/ vargus/kaotus	↑	↑	↑	→	↑	→	→
11. Eksploidipakid	↑	↑	↓	↑	↑	↓	-
12. Andmete murdmine *(data breach)*	↑	↑	↑	→	↑	↑	↑
13. Identiteedivargused	↑	↑	↑	→	↓	↑	↑
14. Krüptokaevekaaperdus	-	-	-	-	-	-	↑uus
15. Informatsiooni lekkimine *(information leakage)*	↑	↑	↑	↑	↑	↑	↑
16. Küberspionaaž	-	-	↑	↑	↓	↑	↓

Trendide hinnangud: ↑ Tõusev → Stabiilne ↓ Langev - Ei hinnatud

Küberohutrendide analüüsist selgub, et küberohumaastikku juhivad pahavara seotud ohud, mida rakendatakse kõige enam erinevates ründevektorites. Teisel kohal on veebipõhised rünnakud, mis kasutavad ründe lõppstaadiumis pahavara. Veebipõhistes rünnakutes kasutatakse ära veebisirvijate, veebilehtede, veebiteenuste, veebilehe sisuhaldustarkvara nõrkuseid, manipuleeritakse veebiliiklusega jne. Näiteks 2018 aastal kasutati finantssektori suunas uut tüüpi veebipõhiseid pahavarasid nagu „Dridex“, „Emotet“, „BlackSwap“, „Zeus“ jt, mis nakatati eduka veebirakenduse koodisüstimise või ümbersuunamise teel eesmärgiga varastada veebirakendusse sisenemiseks kasutatavad identiteedi tõendamise andmed (kontoandmed – kasutajatunnus, parool, PIN jt) (ENISA, 2019, p. 33). Kolmandal

kohal on rünnak veebirakenduste, veebiteenuste ja mobiilirakenduste vastu. Kuigi veebirakendustele mõjuvad ka veebipõhised ründed, siis veebirakenduste puhul keskendutakse kitsamalt veebi rakendusliidesega (API- Application Program Interface) seotud küberohtudele. Ohtude all käsitletakse näiteks SQL süstimist, murdskriptimist (Cross-Site scripting), veebilehe sisuhaldustarkvara nõrkuseid jne. Teenustõkestusrünnaku korral on ründaja eesmärgiks üle koormata päringutega veebiteenused, mille peamiseks ohvriks on teenust pakkuvad era- ja avaliku sektori organisatsioonid. Finantssektori vaates on teenustõkestusründe oht suur e-panga teenuste vaates, millest märkimisväärseim rünnak Eesti finantssektori vastu leidis aset 2007 aasta „pronksiöö“ sündmuse tagajärjel (Geers, 2011). Teenustõkestusründe läbiviimiseks võib ründaja kasutada robotvõrku, mis koosneb zombidest ehk ründaja poolt nakatatud ja selle läbi kontrollitavatest internetiühendusega seadmetest (arvutid, mobiilseadmed, nutitelerid, ruuterid, robottolmuimejad jt). 2018 aasta seisuga toimuvad 97% rämpsposti saatmistest robotvõrkude „Necrus“ ja „Gamut“ vahendusel. Samuti kasutatakse robotvõrku teenustõkestusründes, krüptokaevandamisel, kasutajakonto lahtimurdmisel, pahavara levitamisel jt (ENISA, 2019). Kalastusründe korral kasutavad ründajad ohvri suhtes manipuleerimisvõtteid oma eesmärgi saavutamiseks. Üle 90% pahavaraga nakatumised ja 72% andme lekkimised viiakse ellu just kalastusrünnakute vahendusel (ENISA, 2019). Rämpsposti oht on e-posti teenuse kuritarvitamine, kus kasutatakse kirja saatmise tehnoloogiat e-posti serveri koormamiseks või ohvri postkasti ummistamiseks (spamming) (Riigi Infosüsteemi Amet, 2015). Viimase kümnendi jooksul on rämpskirja oht märkimisväärselt alanenud 85%-lt 39,2%-ni kirjade kogumahust filtreerimistehnoloogiate ja seadusandluse paranemise tulemusena. Lunavara rünnaku oht on püsinud juba kümnendiku, kus rahaliselt motiveeritud ründaja, saades ligipääsu ohvri andmetele, blokeerib neile ligipääsu, pakkudes raha eest andmete blokeeringu alt vabastamise. RIA aastaaruande põhjal tuleb sellisel juhul kindlasti vältida raha tasumist ründajale, et mitte toetada kuritegelikku tegevust (Riigi Infosüsteemi Amet, 2016). Andmete murdmise oht peegeldab endas edukat pahavara tegevust, mille tagajärjel on andmete kompromiteerimine, kaotamine või lekkimine. Tuginedes 2018 esimese poolaasta andme murdmise indeksile (*breach level index*), siis avalikustatakse iga päev 18,5 miljonit kompromiteeritud või kaitsmata kirjet (Gemalto, 2018). Sisemised ohud eksisteerivad igas organisatsioonis, mis võib väljenduda töötava või lahkunud töötaja või partneri kaudu, kes kuritarvitab tahtlikult või tahtmatult ligipääsu digitaalsele varale. Sisemisi ohte jaotatakse siseringi *(insider)* töötajate põhjal kolmeks- pahatahtlik, lohakas

ja kompromiteeritud. Füüsilise manipuleerimise oht ei tulene küberruumist, küll aga on oht seotud tulenevalt seadmetest, millele tekib pahatahtlikul ründajal ligipääs. Finantssektori vaates on sellisteks haavatavateks seadmeteks näiteks pangaautomaadid (ATM), mis on teenuse pakkumiseks kõigile ligipääsetav. Samuti on füüsilise manipulatsiooni ohust mõjutatud isikute või töötajate kaotatud või varastatud seadmed. Eksploidipakkide kasutamine võimaldab tuvastada ohvri süsteemi haavatavusi ja neid automaatselt pakis oleva pahavaraga ära kasutada. Sagedasti rünnatakse ekspliodipakkidega kasutajate veebisirvijaid (n veebisirvija Java, Adobe Flash lisasid) või veebiteenuseid (n Drupal, WordPress jt veebiteenuste haavatavused), mille nõrkuste korral need ekspluateeritakse. Vaatamata sellele, et eksploidipaki ohutrendid on taandumas, ohustab see jätkuvalt kaitsmata ja paikamata IT keskkondasid (NCSC, 2018). Andmete murdmise oht on seotud pahavara ohuga, mille vahendusel kaitstud andmed lahti murtakse ja organisatsioonilt varastatakse. Identiteedi oht seisneb identiteedivarguses, kus ohvri kohta kogutud teavet kasutatakse kas ohvri vastu või edasistes rünnakutes. Identiteedi oht on kasvavas trendis, kuna inimeste personaalsed andmed on digitaalsel kujul, need on kas avalikult kättesaadavad või kasutatakse andmete murdmist nendele ligipääsu saamiseks. Identiteedi või isikuandmetena käsitletakse näiteks pangakonto andmeid, kodust aadressi, maksekirjed, terviseandmed jt. Üks suuremaid isikuandmete lekkeid leidis aset 2017 aastal, kus andmete analüütika ja tehnoloogia ettevõttest Equifax lekkisid 145 miljoni inimese personaalsed andmed (Berghel, 2017; Moore, 2017).

Informatsiooni lekkimise oht katab laia spektriga kompromiteeritud informatsiooni, alates ettevõtetest kogutud personaalsest informatsioonist kuni äriinformatsioonini. Informatsiooni lekke oht realiseerub läbi teiste tabelis 1 käsitletud ohtude. Näiteks informatsiooni lekkimine andmete murdmise, organisatsiooni sisemistest ohtudest, pahavarast tingituna. Küberspionaaži oht on kasvanud seoses teatud riikide huviga spioneerida tööstussektorit, ülemaailmselt kriitilist ja strateegilist infrastruktuuri, sh valitsusasutusi, raudteid, telekommunikatsiooni teenuse pakkujaid, energia ettevõtteid, haiglaid ja pankasid (Black Hat USA, 2018). Küberspionaaž on ajendatud geopoliitilistest eesmärkidest, varastades riikide ja kaubanduse tundlikku ning salastatud teavet, strateegilise valdkonna intellektuaalse omandi- ja patendiõigusega seotud informatsiooni. ENISA pakutud küberohtude nimekiri ei ole ideaalne, sest mitmed ohud on kattuvad. Näiteks pahavara kõrval käsitletakse eraldi lunavara või eksploidipakke, mis on pahavara

erinevad variatsioonid. Samuti andmetega seotud murdmise ja lekkimise ohud, veebiteenuste põhiseid ja veebirakenduse, DDOS, robotvõrk konsolideerida vastavalt andmete ja veebipõhisteks ohtudeks. Samas annab tabel ohutüübi aspektist täpsema ülevaate küberohtu trendist. Finantssektori vaates tuleb välja tuua ka kinnisründeoht, mis ENISA käsitluses otseselt ei ole välja toodud. Lisaks kinnisründe ohule tuuakse finantssektori vaates esile pahavara, veebipõhised ründed, kalastamine, DDOS, robotvõrgud, füüsiline manipuleerimine ja lunavara seotud ohud. (ENISA, 2019; SANS, 2016). Küberohutrende vaadates (vt tabel 1)näitab langusetrende ainukesena lunavara, mida kompenseerib krüptokaevekaaperduse oht. Teised tabelis käsitletud finantssektori ohud hoiavad aastate lõikes kas stabiilset joont või on kasvavas trendis, mille põhjal nähtub, et finantssektori vaates on küberohutrendid pigem kasvutendentsis.

Lisaks ohtudele on küberolukorrateadlikkuse loomiseks oluline saada teavet ründajast või tegutsejatest. USA mõttekoda RAND jaotab oma uuringus tegutsejad (*actors*) kolme kategooriasse- riigid, kasumi saamise eesmärgiga kriminaalid ja häktivistid ning ekstremistid (Meaulen, et al., 2015, pp. 28-33). Finantssektori vaates tuleb küberkaitse tagamisel arvestada kõigi nimetatud kategooria tegutsejatega. Rahaliselt motiveeritud küberkurjategijate kõrval on aset leidnud väiksema osakaaluga, kuid suure mõjuga rünnakud finantssektori arveldussüsteemide vastu, mille taga on riiklikult toetatud gruperingud, kes omavad kinnisründeohu realiseerimise võimekust (SWIFT, 2017; RIA, 2018). Mõned paljudest sellise võimekusega grupeeringutest on Cobalt Group, Carbanak, FIN7 ja Lazarus (ENISA, 2019; RIA, 2018). RAND-i jaotuse viimases kategoorias käsitletakse häktiviste ning ekstremiste, kelle peamiseks motiiviks ei ole saada rahaline kasu, vaid tõkestada finantsteenuse osutamist näiteks teenustõkestusründe korraldamise vahendusel või tekitada organisatsioonile maineline kahju näotustades organisatsiooni veebileht ning postitades seal oma sõnumit (Richards & Wood, 2018). Küberolukorrateadlikkuse aspektist aitab teave ründajast või ründaja kategooriast (riik, küberkurjategijad, aktivistid ja häktivistid) ennustada tema tegutsemisviisi, mille põhjal saab kaitsemeetmeid täpsemalt fokusseerida ründe ennetamiseks, tuvastamiseks ja tõrjumiseks. Samas tulenevalt küberruumi anonüümsusest, on küllaltki keeruline tuvastada küberrünnaku läbiviija ja omakorda seostada küberrünnak läbiviijaga.

Peatükis käsitletud küberolukorrateadlikkuse loomiseks kasutatav teave ei ole lõplik, vaid see selgub iga organisatsiooni enda teadlikkuse rakendamise vajadustest.

Küberolukorrateadlikkus võib üldisemas käsitluses sisaldada teavet küberohtudest, ohutrendidest, ründajatest, kasutatavatest pahavaradest, haavatavustest ja muust teabest, mida saab rakendada küberohust tuleneva mõju maandamiseks. Peatükis käsitleti ka spetsiifilisemate küberolukorrateadlikkuse teabeliikidena IoC-d ja TTP-d, mis on suunatud pigem tehnilisele personalile küberrünnakute ennetamiseks, tuvastamiseks ja tõrjumiseks. IoC-d ja TTP-d käsitlevad täpsemalt teavet ründaja taktikast, tehnikast ja protseduuridest, ründevektorist, ründes kasutatavatest vahenditest, nende tuvastamise signatuuridest, võimalusel meetmed ründe kahjutuks tegemiseks jne.

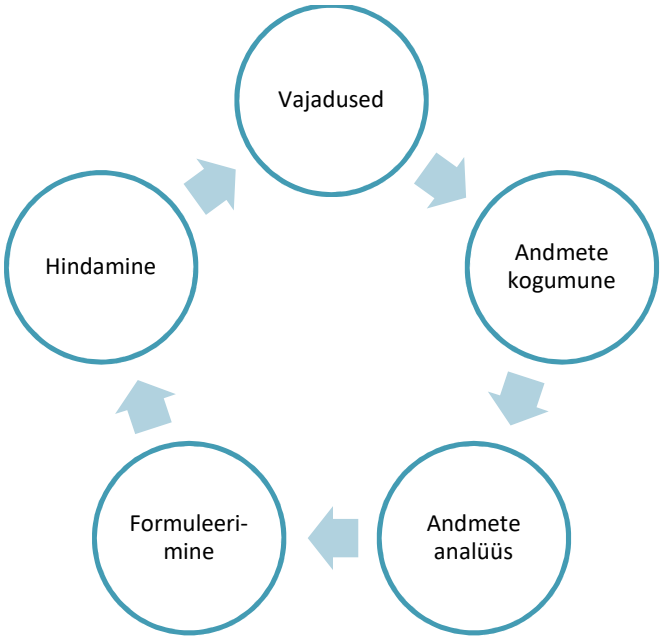
Kui käesolevas alampeatükis käsitleti laiemalt küberolukorrateadlikkuse loomiseks kasutatavat teavet, siis järgnevates peatükkides analüüsitakse täpsemalt küberolukorrateadlikkuse loomise protsessi ja selles valminud teadlikkuse rakendamise võimalusi.

1.2. Küberolukorrateadlikkuse loomise protsess

Eelmises alampeatükis kaardistati küberolukorrateadlikkuse loomise aluseks kasutatav teave ja toodi välja peamised küberohud ning nende trendid, mis on sisendiks küberolukorrateadlikkuse loomiseks.

Gill ja Phythian käsitlevad küberolukorrateadlikkust kui tsüklit või protsessi, mis koosneb neljast sammust- planeerimine, kogumine, töötlemine ja jagamine, mille eesmärk on säilitada või parandada suhtelist turvalisust, pakkudes eelhoiatust ohtudest või võimalikest ohu viisidest, mis võimaldavad ajaliselt õigeaegselt rakendada ennetavaid poliitikaid või strateegiaid, et tuvastada varjatud tegevusi (Gill & Pythian, 2006). Sarnaselt Gill ja Phythian käsitlusele, käsitlevad Chrismon ja Ruks küberolukorrateadlikkuse loomist kui tsüklit, mis koosneb viiest sammust – vajaduste/eesmärgi kaardistamine, andmete kogumine, kogutud andmete analüüsimine, loodud teadlikkuse formaliseerimine ja lõpptulemuse hindamine (vt joonis 2). Antud mudeli teadlikkuse loomise põhitegevus leiab aset andmete analüüsimise etapis, mille sisendiks on kogutud andmed ja lõpptulemiks tekkinud teadlikkus (Artner, et al., 2016). Ülejäänud protsessi tegevused on toetatavad, ehk vajaduste kaardistamine, andmete kogumine, tekkinud teadlikkuse formuleerimine ja selle hindamine. Vajaduste kaardistamise etapis selgitatakse välja, millistele kriteeriumitele

peab teadlikkus vastama, mis omakorda sõltub tellija vajadustest. Peale vajaduste kaardistamist kogutakse analüüsiks vajalikud andmeid, analüüsitakse ja analüüsi loodud teadlikkus formuleeritakse kokkulepitud formaadis. Viimase etapi sammuna hinnatakse formaliseeritud teadlikkuse vastavust protsessi alguses kokkulepitud vajadustele (Chismon & Ruks, 2015).



Joonis 2. Küberolukorrateadlikkuse loomise tsükkel (autori koostatud).

Protsessi tsükkel toimub samuti vajaduste põhiselt. Näiteks küberrünnaku all olles on teadlikkuse vajadus suurem, kus iga uus detail ründevektori kohta võib olla oluline küberründele reageerimisel. Sõltuvalt vajadusest võivad teadlikkuse loomise tsüklid olla perioodilised. Näiteks küberohtude kuuaruanne strateegilisel tasemel juhtidele, nädalane ülevaade IT personalile ja igapäevane üksusele (Zimmerman, 2014, p. 225).

Küberolukorrateadlikkuse loomise protsessis on olulisel kohal andmeeallikate kogumisel, mida kasutatakse teadlikkuse loomiseks. Allikate defineerimine tähendab organisatsioonile lahtimõtestamist, mis hulgal ja mis sagedusega teavet vajatakse, et rahuldada küberolukorrateadlikkuse loomise vajadusi (Bromiley, 2016). Üleliigse informatsiooni kogumine võib muutuda müraks, mille tulemusena võib vajalik informatsioon minna kaduma. Sama lugu on vähese informatsiooniga, mille tulemusena jääb oluline info saamata. Samuti on oluline hinnata allikatest pärineva info kvaliteeti, et need oleksid usaldusväärsed ja vastaks organisatsiooni seatud eesmärkidele. (Meaulen, et al., 2015, pp.

78-79). Küberolukorrateadlikkuse loomiseks tuleb allikaid koguda erinevatest kanalitest (Zimmerman, 2014, pp. 32-43). Tulenevalt vajadusest, varieeruvad ka analüüsis kasutavate allikate kanalid, mis võivad omakorda pärineda sisemistest või välistest kanalitest. Sisemisteks kanaliteks võivad olla organisatsiooni kogutud logid. Väliseid omakorda jaotuvad sõltuvalt nende omadustest või kättesaadavusest. Näiteks leiab internetist avalikest allikatest kogutud teadlikkust (*Open Source Intelligence - OSINT*) sisaldades interneti avarustest avalikult kokku kogutud teavet (Steele, 2007). Näiteid allikatest on toodud lisas 3. Sisemiste ja väliste allikate põhjal loodud teadlikkus võimaldab organisatsioonil saavutada olukorrateadlikkus, mille põhjal mõistab organisatsioon IT konfiguratsiooni, kehtestades vastavalt konfiguratsioonile turvakontrollid ning tuvastab ja reageerib efektiivsemalt intsidentidele (Barford, et al., 2010).

Küberolukorrateadlikkuse andmete haldamiseks ja jagamiseks pakutakse erineva formaadiga struktuure. Näiteks USA mittetulundusühing MITRE on välja töötanud väga mitmeid erinevaid küberolukorrateadlikkuse formaate, sõltuvalt küberolukorrateadlikkuse tarbimise eesmärgist. Mõned näited on STIX, TAXII ja CVE. Neist esimest STIX (*Structured Threat Information eXpression*) formaadis kirjeldatakse kui struktuurset küberohu väljendamise keelt, mis aitab vahendada küberohuteavet erinevate osapoolte vahel, olles oma struktuurilt võimalikult inimloetav. STIX käsitluses koosneb küberolukorrateadlikkus järgnevatest komponentidest:

– jälgitavad/tuvastatavad *(Observables)* kirjed (näiteks informatsioon faili nime, suuruse, räsi kohta, registrivõtme väärtused jne);

– indikaatorid, mille põhjal on rünnak tuvastatav (näiteks ründemustrid, aeg, mõju jt);

– intsidendid, mis ründega kaasnevad või ründe käigus tuvastatakse;

– taktikad, tehnikad ja protseduurid, mis kirjeldavad ründaja käitumismustrit;

– kampaaniate kirjeldused, millega ründajad rünnakut ellu viivad (näiteks NotPetya ja Wannacry kampaaniad (Riigi Infosüsteemi Amet, 2019)).

– Küberohustajad ehk kirjeldus ründajast, tema motiivist, ründemustrist;

– Ekspluateeritavad sihtmärgid ehk teave haavatavustest ja nõrkustest tarkvaras, süsteemides, võrgus või konfiguratsioonis;

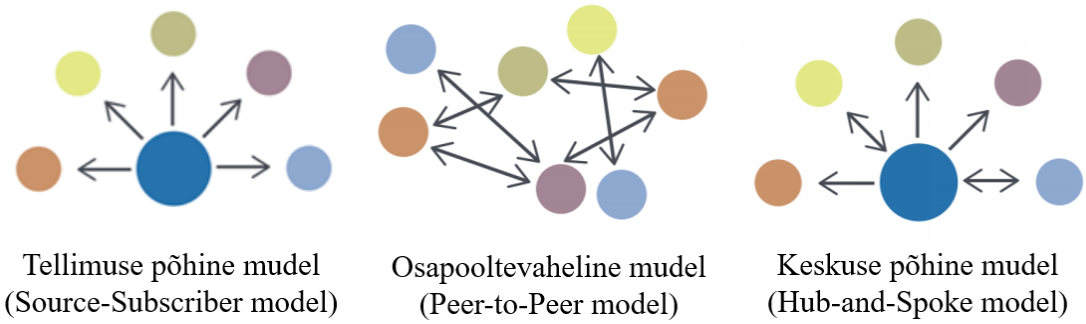
– Tegevussuunised ründe tõrjumiseks (Barnum, 2014).

STIX küberolukorrateadlikkuse struktuur toetab käesoleva töö eelmises alampeatükis käsitletud küberohuteadlikkuse komponente. Analüüsides TAXII (*Trusted Automated*

Exchange of Intelligence Information) formaadistandardi dokumentatsiooni järeldub, et tegemist on STIX formaadi analoogiga selle erisusega, et sinna on lisatud automatiseeritud töötlussüsteemi andmetöötlust toetavad funktsionaalsused (Davidson & Schmidt, 2014). CVE *(Common Vulnerabilities and Exposures)* formaat on mõeldud tuvastatud haavatavuste kaardistamiseks, mille alusel määratakse igale uuele tuvastatud haavatavusele unikaalne identifikaator koos selle kirjeldusega (MITRE, 2018). CVE puhul on tegemist kitsama küberolukorrateadlikkuse käsitlusega, milles kirjeldatakse tarkvara nõrkuseid ja/või haavatavusi, käsitledes STIX formaadi ühte komponenti ehk ekspluateeritavad sihtmärgid. Sellest tulenevalt on põhjalikuma küberolukorrateadlikkuse saavutamiseks soovitav lähtuda STIX formaadist, kus CVE-d saab kasutada täiendava allikana. Formaatide paljususe tõttu toob Dulaunoy esile vajaduse raamistike ühtlustamiseks, mis toetaks organisatsioonide vahelist küberolukorrateadlikkuse jagamise arengut ja selle integreerimist organisatsioonide erinevates juhtimistasandites (Dulaunoy, 2017, Athias, 2015, Ginn & Lingris, 2017).

Küberolukorrateadlikkuse saamise ja/või jagamise aspektist soovitatakse organisatsioonidel liituda vastavate gruppidega, milles jagatakse teiste poolt koostatud teadlikkust. Näiteks soovitatakse liituda küberintsidentide lahendamise üksuste (CERT jt) või valdkonna põhiste kanalitega (FinTech, Banking Security jt) (Skopik, 2018, ENISA, 2018; Johnson et al., 2016). Mõned näited sellistest organisatsioonidest on toodud käesoleva töö lisas 3. Eelnevas lõigus tuvastati, et teadlikkus võib olla erineva struktuuriga ja samuti teadlikkuse loomise protsessi analüüsis selgus, et loodav teadlikkuse võib olla sõltuvalt püstitatud eesmärgist erinev. Sellest tulenevalt soovitatakse jagamisgruppidel fikseerida teadlikkuse jagamise tingimused koostöödokumendis (*n membership conditions*), millega reguleeritakse grupis jagatav teadlikkus. (Skopik, 2018). Näiteks võib mõne grupi skoop olla jagada ainult kompromiteerimise indikaatoreid (*Indicators of Compromise – IoC*), teistel soov jagada laiema spektriga teadlikkust. Teabe saamise ja jagamise koostöömudeleid jagatakse tellimismudeliks (*source –subscriber model*), osapoolte vaheliseks mudeliks (*peer-to-peer model*) ja keskuse põhiseks mudeliks (*hub-and-spoke model*). Viimane neist on sarnane „peer-to-peer“ mudelile, kuid teabe saamine ja jagamine läbib keskset üksust (vt joonis 3) (Ionita & Patriciu, 2016). Esimene mudelitüüp iseloomustab teadlikkuse tellimist teenusepakkujalt, millele ligipääsuks tuleb liituda teenusega. Teine tüüp iseloomustab teadlikkuse jagamist osapoolte vahel, kus käesoleva

töö skoobis on osapoolteks pangad. Tegemist on omavahelistel suhetel põhineval teadlikkuse jagamisel, mille puhul võib, kuid ei pea olema sõlmitud osapoolte vaheline koostöökokkulepe. Viimane mudel iseloomustab näiteks riigiülese CERT vahendusel jagatavat teadlikkust, kellega kõik abonendid suhtlevad ja kes keskselt teadlikkust jagab. Samaselt eelneva mudeliga võib, kuid ei pea sõlmima osapoolte vahel koostöökokkulepet.

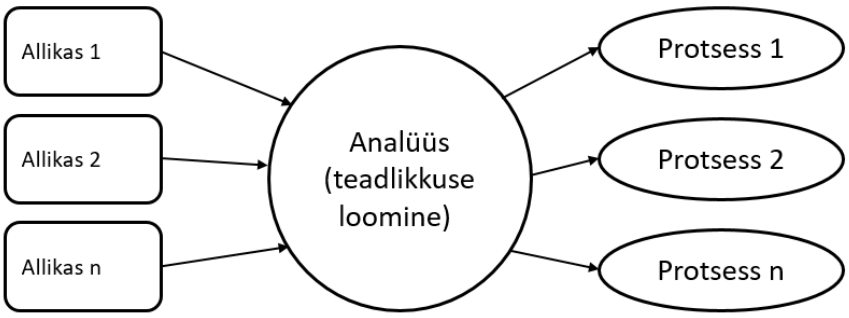


Tellimuse põhine mudel (Source-Subscriber model) | Osapooltevaheline mudel (Peer-to-Peer model) | Keskuse põhine mudel (Hub-and-Spoke model)

Joonis 3. Teadlikkuse jagamise koostöömudelid (Ionita & Patriciu, 2016)

Küberolukorrateadlikkuse jagamise aspektist rõhutavad Kourmaier ja Jaouen teadlikkuse jagamise vajadust kriitilist infrastruktuuri omavate era ja avaliku sektori organisatsioonide vahel (Kornmaier & Jaonen, 2014). Sellest järeldub, et kriitilist finantsteenust pakkuvad ettevõtted peaksid tegema teadlikkuse jagamisel koostööd. Küberintsidentide lahendamise üksuste (CERT-de) koostöös on loodud küberolukorrateadlikkuse haldamist ja jagamist toetav infosüsteem *(malware information system platform – MISP)*, mis soodustab küberolukorrateadlikkuse vahendamist ja jagamist osapoolte vahel. Infosüsteemi näol on tegemist avatud lähtekoodil põhineva tarkvaraga, mis toetab infosüsteemi laialdasemat kasutuselevõttu, mida soovitatakse organisatsioonidel rakendada küberolukorrateadlikkuse protsessi automatiseerimiseks (Wagner, et al., 2016, Sauerwein, et al., 2017).

Teooria käsitluse põhjal pakutakse järgnevalt küberolukorrateadlikkuse loomist ja rakendamist kirjeldav lihtsustatud mudel (vt joonis 4), mille keskmes on teadlikkuse loomine. Teadlikkuse loomiseks kasutatakse sisendiks allikaid ja loodud teadlikkus suunatakse seda tarbivasse protsessi (n riskijuhtimine, andurite seadistamine, kaitsemeetmete kujundamine jt).



Joonis 4. Küberolukorrateadlikkuse loomise ja rakendamise mudel (autori koostatud).

Peamised küberolukorrateadlikkuse loojad ja ka tarbijad on küberkaitse/küberintsidentide lahendamise üksused/keskused (SOC, CERT jt). Üksuste peamiseks ülesandeks on juhitud tuvastamine (tuvastus ei toimu kaootiliselt) ja tuvastatud sündmustele reageerimine. Eesmärki aitavad saavutada toetavad funktsioonid, milleks on küberolukorrateadlikkuse loojad (väliste ohtude kaardistamine), üksuse analüütik(ud) (sisemiste allikate ja küberolukorrateadlikkuse kasutamine), mille põhjal toimub juhitud tuvastamine, mis omakorda jaotatakse pahavara jahtimiseks (*malware hunt*), intsidentidele reageerimiseks, ekspertiisiks (*forensics analysts*) ja „Punase üksuse“ (kui ründamist simuleeriva üksuse) poolt haavatavuste tuvastamiseks. Küberolukorrateadlikkuse loojatel on tähtis roll üksuses, sest nende loodud teadlikkus on oluliseks sisendiks kõikidele teistele protsessidele (Akinrolabu, et al., 2017, Zimmerman, 2014). Välised allikad võivad pärineda omakorda avalikest allikatest, vastavalt koostöömudelile koostööpartneritelt, foorumitest, sotsiaalmeediast (n Twitter, Facebook), teenusepakkujatelt (*Cyber Threat Intelligence feed*) või muudest kanalitest. Allikate osas on oluline analüüsida nende usaldusväärsus, et valede andmete põhjal ei tekiks kallutatud küberolukorrateadlikkuse pilt (Barnum, 2014).

Küberintsidentide üksuse põhjal toodud näide on üks mitmest võimalusest küberolukorrateadlikkuse loomiseks ja rakendamiseks. Peatüki käsitlusest selgus, et küberolukorrateadlikkuse loomine on protsess, milles teadlikkus luuakse andmete analüüsimise tulemusena, mis omakorda hinnatakse ja esitatakse kokkulepitud formaadis tarbijale. Samuti selgus, et teadlikkuse loomise protsessis on olulisel kohal teabe jagamise ja saamise koostööl. Viimaseks loomiseprotsessi oluliseks sisendiks on selle rakendamise vajadused, mida käsitletakse põhjalikumalt järgnevas peatükis.

1.3. Küberolukorrateadlikkuse rakendamise võimalused

Eelnevas alapeatükis selgus, et küberolukorrateadlikkus luuakse selle rakendamise vajadustest lähtuvalt. Küberolukorrateadlikkuse rakendamine aitab rünnaku indikaatorid ära tunda, mille tulemusena saab suunata olemasolevaid või võtta kasutusele uusi kaitsemeetmeid rünnakute tõrjumiseks (Shackleford, 2015). Küberolukorrateadlikkuse rakendamine otsustusprotsessides võimaldab tegutseda õigeaegselt, et ära hoida ohu poolt tehtav kahju. (Zimmerman, 2014). Selline lähenemine võimaldab organisatsioonil oluliselt kiiremini tuvastada ründevektor ja võtta kasutusele meetmed ründe tõkestamiseks (ENISA, 2017). Küberolukorrateadlikkust soovitatakse rakendada kolmel-neljal juhtimistasandil: strateegiline, operatsiooniline ja tehniline-taktikaline (Chismon & Ruks, 2015). Kuna küberolukorrateadlikkuse rakendamine on erinevatel juhtimistasanditel läbipõimunud, vaadatakse järgnevalt küberolukorrateadlikkuse rakendamist strateegilisel-operatsioonilisel ja taktikalisel-tehnilisel tasanditel. Lisaks juhtimistasanditele, vaadatakse küberolukorrateadlikkuse rakendamist küberkerksuse ja selle küpsusmudeli rakendamise kaudu.

1.3.1. Küberolukorrateadlikkuse rakendamine strateegilisel-operatsioonilisel tasandil

Küberolukorrateadlikkust rakendatakse organisatsiooni ohustavate rünnakute tõrjumiseks. Strateegilisel tasandil tuleb küberolukorrateadlikkus viia organisatsiooni juhatuse/otsustajate tasemele, millega kaasatakse otsustajad küberkaitse planeerimise protsessi. Tavaliselt on strateegilise taseme küberolukorrateadlikkuse näol tegemist kõrge taseme informatsiooniga, milles puudub tehniline-taktikaline taseme sisu, mida kasutavad peamiselt tehnilise taustaga eksperdid teadlikkuse proaktiivseks rakendamiseks kaitsemeetmetes. Operatsioonilisel tasemel rakendatakse küberolukorrateadlikkust organisatsiooni kaitsemeetmete konfigureerimisel ja uute väljatöötamisel (Zimmerman, 2014). Operatsioonilise taseme ohuteadlikkuse tarbijatena käsitletakse infoturbe või küberkaitse eksperte, kes vajavad ohuteavet kaitsemeetmete kujundamiseks (Chismon & Ruks, 2015). RIA soovitab tippjuhile küberturvalisuse tagamisel toetada infoturbejuhi tööd, lähtuda infoturbe korraldamisel standardist või parimatest praktikatest, planeerida vahendeid infoturbe tagamiseks, tagama süsteemide regulaarse turvalisuse testimise, tagama töötajate turvateadlikkust läbi küberhügieeni parandamise, investeerima seiresse ja

võrgu kaitsesse, toetama krüpteerimislahenduste kasutuselevõttu, nõudma CERT.EE teavitamist turvanõrkustest ja intsidentidest ja nõudma kriitiliste logide pidamist (RIA, 2018). Kuna infoturbe/küberkaitse standardeid ja parimaid praktikaid on palju, saab infoturbejuht suunata organisatsiooni rakendama organisatsioonile sobilikku standardit või parimat praktikat. Standardite ja parimate praktikate küberolukorrateadlikkuse käsitlust käsitletakse lähemalt käesoleva töö dokumendianalüüsis.

SANS uuringus, mis keskendus küberolukorrateadlikkuse rakendamise uurimisele operatsioonilisel tasandil, vastas osalejatest 53%, et küberolukorrateadlikkus on rakendatud organisatsiooni sisestes küberoperatsioonide keskustes (SOC), 32% on rakendanud organisatsiooni infoturbe/küberkaitse üksustes ja 32% on rakendatud intsidentide lahendamise üksustes. Küberoperatsioonide keskuse ja intsidentide lahendamise üksuste näol on tegemist küberolukorrateadlikkuse rakendamisega tehnilisel-taktikalisel tasandil. Uuring ei too kahjuks välja, kui palju rakendatakse teadlikkusest teistel juhtimistasanditel. Chismon ja Ruks kirjelduse kohaselt vajavad operatiivne ja strateegiline taseme juhid kõrgema taseme teadlikkust, milles eemaldatakse tehnilisele-taktikalisele tasemele mõeldud teave. Sellest tulenevalt võib organisatsioonis olla küberolukorrateadlikkuse rakendajateks tehnilise-taktikalise tasandi eksperdid, kes serveerivad kõrgemale tasemele sobilikku teavet (Chismon & Ruks, 2015). Seda saab korraldada näiteks regulaarsete raportite näol, milles tehakse otsustajatele ülevaade ohutrendidest ja organisatsioonis tuvastatud ning tõrjutud rünnakutest.

1.3.2. Küberolukorrateadlikkuse rakendamine tehnilisel-taktikalisel tasandil

Tehnilisel või taktikalisel tasemel on peamisteks küberolukorrateadlikkuse rakendajateks tehnilise taseme eksperdid. Tehnilisel tasemel küberolukorrateadlikkuse rakendamine sõltub paljuski selles rakendamise vajadustest (Chismon & Ruks, 2015). Näiteks vajavad intsidentidele reageerimise üksused ja küberkaitse operatsioonide keskused (SOC) otsuste tegemiseks rakendatavat küberolukorrateadlikkust, mis aitab kaitsjatel või intsidentide lahendajatel kiiremini orienteeruda ja teha õigeid otsuseid ohust põhjustatud mõju maandamiseks. Kiirete otsuste tegemiseks on vaja määrata teadlikkusele kriteeriumid, näiteks kas tegemist on aegkriitilise teadlikkusega, mis rakendada teatud aja jooksul (Zimmerman, 2014). Taktikaline ohuteadlikkus käsitleb taktikaid, tehnikaid ja protseduure, mille tarbijateks on tehniline personal (Chismon & Ruks, 2015). Mittetulundusühing

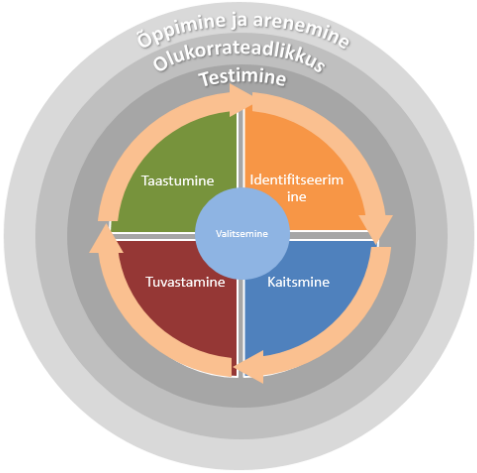
MITRE on koostanud tehnilisele ja taktikalisele taseme ekspertidele küberohtude tuvastamiseks raamistiku, milles kirjeldatakse enamlevinud rünnakute analüütikat, aidates selle läbi tuvastada organisatsiooni ohustavaid küberohte. Ründajad arenevad pidevalt süsteemi kompromiteerimise meetodeid, vältides tavapäraseid kaitsemeetmeid. Selleks on oluline, et tehniline personal mõistaks ja tuvastaks tema vastutusalas olevas võrgus olevaid küberohte. MITRE pakub rünnete tuvastamiseks käitumispõhist ohtude tuvastamise mudelit *(behavioral-based threat model)*, mis võimaldab tehnikutel tuvastada ja seadistada kaitsesensoreid vastavalt küberohu käitumisele. Tuvastusmeetmete vastavuse hindamiseks soovitatakse simuleerida küberrünnakuid lähtuvalt nende käitumismustrist (Storm, et al., 2017). Käitumispõhine analüütiline mudel kasutab sisendina olukorrateadlikkust, võimaldades tehnikutel välja töötada ja rakendada käitumispõhist analüütikat küberrünnakute tuvastamiseks ja tõkestamiseks. Sensoreid soovitatakse paigutada vähemalt kõikidesse lõppseadmetesse *(endpoint)*, et tehnik saaks kontrollida hallatavat võrku ja rakendada analüütikat. Näiteks kasutavad ründajad ründevektoris eemalt kontrollitavaid troojalasi *(Remote Access Trojan – RAT)*, mis peidetakse ohvri süsteemi protsessidesse selliselt, et tava vaatlusega ei oleks võimalik rünnet tuvastada (İlker & Aydos, 2019). Ohtude käitumispõhise analüütika rakendajad on peamiselt küberoperatsioonide keskuste analüütikud, kes igapäevaselt vastavalt muutuvale küberruumi ohtude dünaamikale häälestavad haldusala andureid. Sellise tehnika kasutamine on oluline kinnisründeohu tuvastamiseks, mida kasutavad finantsiliselt või poliitiliselt motiveeritud koordineeritud grupid avalikku- ja erasektori organisatsioonide ründamisel. RIA 2018 aastaraamatu kohaselt teeb ekspertidele muret Põhja-Korea kasvav küberründevõimekus, millest näiteks Lazarus grupeeringu fookuses on pangad, hasartmänguplatvormid, finantstarkvara tootjad ja krüptorahaäris osalejad. Pankade aspektist püütakse manipuleerida SWIFT sõnumiteenust, manipuleerida arvelduste kontrollimehhanisme või kasutatakse spetsiaalselt sihtmärgile kohandatud pahavara oma eesmärgi elluviimiseks (RIA, 2018). APT ründe teostamisel võib ründaja kombineerida erinevaid pahavarasid, näiteks kasutades ohvri arvuti ekspluateerimiseks eelnevalt nimetatud RAT ründevektorit, millega saavutab ründaja kontrolli ohvri seadme ühe ja mis jääb tavapärasele viirusetõrjeprogrammile nähtamatuks (Borrello, et al., 2019). Keerukate ründevektorite tuvastamiseks soovitatakse luua selle tuvastamisele spetsialiseerunud üksus, näiteks küberkaitse operatsioonide keskus (SOC) või eraldi üksus intsidentidele reageerimise meeskonnas. Nende töövahenditeks on tulemüüri, sissetungi ennetus ja

tuvastussüsteemi (IDS/IPS), proksi serveri, rakenduste serverite, domeeni nimeserveri (DNS) jt seadmete võrgulogid. Tekkinud suuremahuliste võrgulogide ja seal korreleeruvate sünduste tuvastamiseks soovitatakse kasutada turvaintsidentide haldamise süsteemi (SIEM) jt. Ehk tehnilisele ja taktikale taseme personali töövahendid moodustavad võrgulogid koos analüütikat võimaldava vahendiga, mis võimaldab tuvastada ründevektorit (Zimmerman, 2014). Tuvastamise sisendiks kasutatakse küberolukorrateadlikkust, millega seoses on tehnilise ja taktikalise taseme eksperdid ka kõige suurema küberolukorrateadlikkuse vajadusega tarbijad. Vastava üksuse igapäevasteks ülesanneteks on küberolukorrateadlikkuse loomine, pahavara jälgede tuvastamine (hunt), intsidentidele reageerimine, ohtude analüüsimine ja sündmuste seire (Akinrolabu, et al., 2017).

1.3.3. Küberkerksuse ja küpsusmudeli rakendamine küberolukorrateadlikkuse tagamiseks

Küberolukorrateadlikkuse rakendamise võimaluste analüüsimise käigus selgub, et küberolukorrateadlikkust käsitletakse ühe komponendina küberkerksuse raamistikus. Küberohtudest tulenevalt on kriitilist teenust pakkuvad organisatsioonid rakendamas strateegilise planeerimise ja riskijuhtimise protsessides küberkerksuse raamistikku (Roege, et al., 2017, Kopp, et al., 2017, Gallagher, et al., 2014, pp. 47-53). Küberkerksust defineeritakse kui organisatsiooni võimet pakkuda teenuseid ka siis, kui ollakse küberrünnaku olukorras (Björck, et al., 2015, pp. 311-316). Küberkerksuse raamistikku analüüsides, integreeritakse küberkerksus laiemalt teenuse osutamise ja tagamise protsessi ja seda kõikidel juhtimistasanditel. Kui analüüsida küberkerksuse rakendamist operatsioonilisel tasandil, siis tagab küberkerksuse rakendamine läbi küberkaitse koordineerimise ka küberolukorrateadlikkuse rakendamise. USA näitel kirjeldatakse küberkerksuse rakendamist rahvusvahelise standardi ja tehnoloogia instituudi NIST koostatud küberkaitse raamistiku põhjal. Küberkerksuse saavutamiseks vaadeldakse lähemalt identifitseerimise, kaitsmise, tuvastamise, vastamise ja taastamise protsessidest, milles olukorrateadlikkus toetab kõikide protsesside eesmärkide saavutamist (NIST, 2018, Homeland Security, 2016). Olukorrateadlikkus küberkaitse aspektist tähendab olla teadlik oma praegusest olukorrast, ründe mõjust, olukorra kulgemisest, tegutsejate (ründaja) käitumisest, olukorra tekkest ja selle võimalikust edasiarengust. Samuti tuleb veenduda

oma olukorrateadlikkuse usaldusväärsuses, et mitte teha valesid otsuseid (Barford, et al., 2010). Olukorrateadlikkuse loomiseks kogutakse ohtude ja haavatavuste kohta teavet informatsiooni sisemistest (varad, tuvastatud nõrkused jt) ja välistest allikatest (ohuteavet jagavad foorumid jt allikad). Loodav olukorrateadlikkus dokumenteeritakse, mis jagatakse ja rakendatakse organisatsiooni erinevates protsessides – NIST näitel küberkaitse korraldamise protsessides, milleks on oma varade tuvastamine, varade kaitseks kaitsemeetmete rakendamine, kahtluste tuvastamine, nendele reageerimine ja teenuse taastamine. Kui otsida küberkerksuse rakendamist finantssektori skoobis, leiab Rahvusvaheliste Arvelduste Panga ja Euroopa Keskpanga poolt koostatud vastavad juhendid. Finantssektori dokumentides kirjeldatud küberkerksuse mudel sisaldab USA näites kirjeldatult identseid komponente – identifitseerimine, kaitsmine, tuvastamine ja taastumine (vt joonis 5). Joonisel tuuakse välja ka küberkerksuse valitsemine (strateegiline tase), testimine, olukorrateadlikkus, õppimine ja arenemine (BIS & IOSCO, 2016; ECB 2018). Samaselt USA käsitlusele, rakendatakse olukorrateadlikkust toetava protsessina kõikides teistes küberkerksuse mudeli komponentides. Finantssektori dokumendid põhjendavad olukorrateadlikkust kui küberohumaastiku mõistmist, milles ta opereerib, sh teadlikkus küberohtude mõjust ja küberriskide maandamise meetmete vastavusest. Küberolukorrateadlikkust käsitletakse osana olukorrateadlikkusest, mis pakub lisaks ohtudele ka ärispetsiifilist konteksti, võimaldades rakendada teadlikkust otsuste tegemisel, andes teadmisi küberründaja võimekusest, kavatsusest ja tegutsemisviisist (modus operandi) (Kott, et al., 2015, Franke & Brynielsson, 2014, BIS & IOSCO, 2016).



Joonis 5. Küberkerksuse raamistiku komponendid (CPMI & IOSCO, 2016)

Küberkerksuse rakendamise ulatuse hindamiseks on Euroopa Keskpank lisanud küpsusmudeli vastavate tasemetega arenev, edasijõudnud ja innovaatiline, milles iga tase sisaldab komplekti meetmeid, mis rakendamisel tõstavad organisatsioonide küberkerksust (BIS & IOSCO, 2016, ECB, 2018). Sellest tulenevalt pakutakse igast küpsustasemest tulenevalt ka küberkerksuse rakendamiseks kolme komplekti meetmeid. Arenev tase saavutatakse, kui organisatsioon on loonud küberolukorrateadlikkuse loomise võimekuse. Edasijõudnud taseme saavutamiseks tuleb valitsemisel rakendada teadlikkust organisatsiooni toetava küberkerksuse strateegia ja raamistiku kujundamisel, sh organisatsiooni kehtestatud poliitikate, protseduuride ja kontrollide kujundamisel. Tuvastamisel kasutama sisendina küberolukorrateadlikkust, mis võimaldab õigel ajal reageerida küberohtudele või haavatavustele ja uurida anomaalseid tegevusi. Rakendama teadlikkust testiprogrammi kujundamisel, millega veendutakse, et testiprogramm on vastavuses viimaste küberohu trendidega, ründaja käitumismustri ja haavatavustega. Organisatsioonil tuleb läbi viia „punase tiimi“ testimine, mis kasutab ründestsenaariumi väljatöötamisel küberolukorrateadlikkusest. Kui areneva taseme saavutamiseks tuli luua küberolukorrateadlikkuse loomise võimekus, siis edasijõudnud taseme saavutamiseks tuleb küberolukorrateadlikkus integreerida riskide raporteerimise protsessi, pakkudes teadlikkust organisatsiooni kõige tõenäolisematest ründajatest, ründaja poolt kasutatud TTP-st, milliseid haavatavusi kasutatakse ründes, ründe läbiviimise tõenäosus ja mõju terviklikkusele, käideldavusele, konfidentsiaalsusele ning võimalikud riski maandamise meetmed. Organisatsioonil tuleb aktiivselt osaleda küberolukorrateadlikkuse jagamise gruppides. Innovaatilise taseme saavutamiseks tuleb lisaks eelnevale rakendada küberolukorrateadlikkust proaktiivselt küberrünnetele reageerimisel ja talitluspidevuse planeerimisel. Küberolukorrateadlikkuse loomiseks tuleb lisaks koguda teavet sektori teistelt partneritelt, võimaldades kujundada sektoripõhist ja sektorite vahelist küberolukorrateadlikkust. Küberolukorrateadlikkuse protsess tuleb integreerida küberkaitse operatsioonide keskusesse (SOC). Organisatsioonil peab olema võimekus hankida küberolukorrateadlikkust mitmest allikast, sh geopoliitilisi sündmuseid, et paremini mõista küberohumaastiku arengut võimaldades rakendada ennetavaid meetmeid (BIS & IOSCO, 2016, ECB, 2018). Skopik lähtub küberkaitse küpsustasemete määratlemisel sarnaselt Euroopa Keskpanga käsitlusele, jaotades küpsustasemed nelja kategooriasse. Esimesel tasemel käsitletakse tavapäraseid kaitsemeetmeid (nt tulemüür, antiviirustarkvara jt), kuid siin ei eeldata küberolukorrateadlikkuse loomist ja rakendamist.

Teisel tasemel eeldatakse, et organisatsioon on rakendanud seire ja reageerimise võimekuse, et tuvastada potentsiaalne rünnak ja vähendada kahju. Kolmandal taseme meetmena käsitletakse küberolukorrateadlikkuse rakendamist, mis võimaldab juhtida eelnevates tasemetes käsitletud meetmete rakendamist. Neljandal tasemel eeldatakse automatiseeritud küberolukorrateadlikkuse rakendamist, milles kaitsemeetmed kohandatakse automaatselt ilma inimese sekkumiseta vastavalt muutuvale küberohumaastikule (Skopik, 2018). Käsitletud küpsusmudeleid saab kasutada organisatsiooni küberolukorrateadlikkuse rakendamise hindamiseks, võimaldades erinevatel organisatsioonidel võrrelda omavahel küpsustaset.

Käesolevas peatükis tuvastati, et küberolukorrateadlikkust võib rakendada kõikides peatükis käsitletud juhtimistasandite otsustusprotsessides- strateegiline, operatiivne, tehniline, taktikaline. Küberolukorrateadlikkust tuleks rakendada kõikides protsessides/teenustes, mis vajavad suuremal või vähemal määral sisendina teadlikkust küberruumist tulenevatest ohtudest. Samuti selgus, et küberolukorrateadlikkusel on oluline seos küberkerksuse raamistiku rakendamisel. Küberolukorrateadlikkust saab rakendada küberkerksuse raamistiku komponentide valitsemine, kaitsmine, tuvastamine, taastumine, testimine, olukorrateadlikkus ja õppimine ning arenemine otsustusprotsessides.

2. KÜBEROLUKORRATEADLIKKUS JA SELLE TÕHUSTAMISE VÕIMALUSED

Käesolev peatükk käsitleb esmalt magistritöös kasutatud uurimuse strateegiat, kirjeldab valimi ja küsimustiku moodustamist ning andmeanalüüsi metoodikat. Magistritöös käsitletakse uurimisobjektina küberolukorrateadlikkuse rakendamise võimalusi finantssektoris. Siinkohal täpsustan, et teadlikkuse all ei käsitleta magistritöös kasutajate teadlikkust *(awareness)* küberohtudest, vaid küberkaitse eest vastutava personali või üksuse (infoturbe-, küberkaitse juhid, operatsioonilise turvalisuse eest vastutav personal, infosüsteemi haldurid jt) küberolukorrateadlikkust *(cyber threat intelligence)*, mis on rakendatav kaitse taktikate, tehnikaate ja protseduuride kujundamisel, et tuvastada, tõrjuda ja ennetada organisatsiooni vastu suunatud küberrünnakuid. Teises ja kolmandas alampeatükis viiakse läbi analüüs ja tehakse järeldused dokumendianalüüsi, intervjuude ja e-kirja vahetuse põhjal. Neljandas peatükis tehakse ettepanekud küberolukorrateadlikkuse tõhustamiseks finantssektoris.

2.1. Uurimuse metoodika ja valim

Magistritöö on **kvalitatiivne empiiriline uurimustöö**, mille uurimisstrateegia valikuks on juhtumiuuring (*case study*). Uurimisstrateegia teoreetilise alusena tugines magistritöö autor Robert K. Yin käsitlusest „Case Study Research: Design and Methods“, mille kohaselt on juhtumiuuring meetod, õppimaks keerukast juhtumist, tuginedes antud juhtumi kõikehõlmavale mõistmisele, mis on saadud ulatuslikult kirjeldades ja analüüsides juhtumit tervikuna ja tema kontekstis (Yin, 2014, p.16). Juhtumiuuringu üheks kriteeriumiks on, et see sisaldab mitmeid erinevaid andmete kogumise meetodeid, mis sõltuvad konkreetse olukorra arusaamadest ja uuritava nähtuse spetsiifilisest kontekstist (Laherand, 2008, lk 83; Ritchie, et al., 2014, p. 76). Juhtumiuuringu kontekstis on küberolukorrateadlikkus, juhtumiks küberolukorrateadlikkuse loomine ja rakendamine, uurimisobjektideks ja subjektideks on küberolukorrateadlikkuse teoreetilised allikad, küberkaitse dokumentatsioon, küberjulgeoleku strateegiad, finantssektori ja avaliku sektori küberkaitsega valdkonna eksperdid. Magistritöö eesmärgi saavutamiseks rakendati

andmekogumise meetodina dokumendianalüüsi (Flick, 2009, pp. 255-262) ja ekspertintervjuud (Flick, 2009, pp.165-169), mille valiku alused on toodud tabelis 2. Dokumendianalüüsi ja ekspertintervjuude valim on toodud tabelites 3 ja 4.

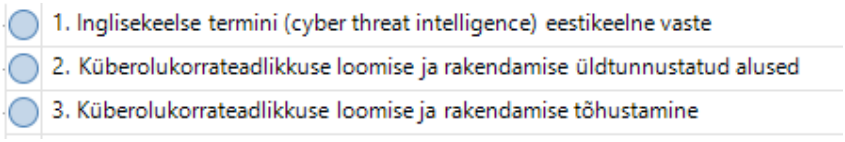
Tabel 2. Uurimisküsimuste seosed andmekogumise meetodiga (autori koostatud)

Uurimisküsimus	**Andmekogumise meetod**
Milline on parim eestikeelne vaste inglisekeelsele terminile „cyber threat intelligence“?	Teoorial põhinev vastus Dokumendianalüüs Intervjuud
Millised on küberolukorrateadlikkuse loomise ja rakendamise üldtunnustatud alused?	Teoorial põhinev vastus Dokumendianalüüs Ekspertintervjuud
Milline on organisatsioonide küberolukorrateadlikkuse loomise ja rakendamise seis?	Ekspertintervjuud Dokumendianalüüs
Millised on organisatsioonide küberolukorrateadlikkuse loomise ja rakendamise vajadused?	Dokumendianalüüs Ekspertintervjuud
Kuidas tõhustada küberolukorrateadlikkuse loomist ja rakendamist?	Teoorial põhinev vastus Dokumendianalüüs Ekspertintervjuud

Dokumendianalüüsi ja **ekspertintervjuude** valimiteks olid eesmärgistatud valimid (purposive sampling) (Teddie ja Yu, 2007, p.80; Neuman, 2011, pp 267-268; Babbie, 2013, pp. 128-129). Eesmärgistatud valim tähendab valimi koostamist kindlal eesmärgil, kus uuritavad nähtused valitakse valimisse kindla sisulise kriteeriumi alusel (Flick, 2009, pp. 122-125). Käesoleva magistritöö raames on küsitluse valimiks Eestis kriitilist finantsteenust pakkuvad ettevõtted ja küberkaitse valdkonda koordineeriva ning küberintsidente teavet koguva ning küberohtudest teavitava asutusena Riigi Infosüsteemi Ameti teenistujad.

Magistritöö andmeanalüüsi meetodiks oli kvalitatiivne sisuanalüüs (*qualitative content analysis*) (Laherand, 2008, lk 289-299; Flick, 2009, pp. 323-327), mis kontrollitavuse ja

korratavuse tagamiseks teostati, kasutades analüüsitarkvara NVivo 12 Pro. Tekstide kodeerimiseks kasutati magistritöös suunatud kodeerimist (*thematic coding*) tähenduses, et kodeerimine toimus vastavalt uurimisküsimustele (Flick, 2009, pp. 318-320; Kalmus, et al., 2015). Kõigi kasutatavate andmekogumise meetoditega kogutud andmete kodeerimiseks kasutati ühte ja sama koodipuud ning põhikategooriaid vastavalt joonisel 6 toodule.



Joonis 6. Analüüsitarkvaras NVivo 12 Pro loodud koodipuud (autori koostatud)

Dokumendianalüüs on süsteemne protseduur dokumentide sisu läbivaatamiseks ja hindamiseks (Brown, 2009, pp. 27-40). Dokumendianalüüs kui uurimismeetod on eriti sobilik kvalitatiivsetes uurimistöödes pakkudes intensiivse uuringuna rikkalikku kirjeldust üksikust nähtusest, sündmusest, organisatsioonist või programmist (Yin, 1994).

Dokumendianalüüs võimaldab kasutatud allikate juurde korduvalt tagasi tulla, kontrollida tehtud järeldusi, fakte, analüüse. Dokumendianalüüsis kasutatavad dokumendid võivad olla kas vabalt ligipääsetavad või ligipääsu piiranguga. Dokumentide juurdepääsu piiramine on ka üheks miinuseks dokumendianalüüsi läbiviimisel. Ligipääsu piirangud dokumentidele võib jagada info tundlikkuse, teadmisvajaduse, autoritasu aspektist lähtuvalt. Magistritöös kasutatud materjalid põhinevad enamuses avalikel ligipääsupiiranguta allikatel, kuid esineb ka dokumente, millele ligipääsu eelduseks on autoritasu maksmine. Dokumente, millele ligipääs on piiratud muudel põhjustel (salastatus, tundlikus, teadmisvajadus jt), magistritöös ei kasutata.

Dokumendianalüüsi valim on **eesmärgistatud** *(purposive sampling)*, mille põhjal moodustatakse valim dokumentide teatud ühiste omaduste põhjal, mis aitavad anda vastust uurimusküsimustele (Ritchie, et al., 2014). Finantssektor on hästi kontrollitud valdkond läbi erinevate järelevalve ja järelevaatamise mehhanismide. Eestis teostavad finantssektori järelevalvet ja järelevaatamist Finantsinspektsioon ja Eesti Pank. Küberturvalisuse nõuete

täitmise riiklikku ja haldusjärelevalvet teostab küberturvalisuse seaduse §14 kohaselt Riigi Infosüsteemi Amet (Küberturvalisuse seadus, 2018). Euroopa Liidu direktiivi 2016/1148 lg 13 kohaselt on panganduse ja finantsturutaristute sektori puhul järgimise ja järelevalve oluliseks osaks operatsioonirisk. See hõlmab kõiki operatsioone, sealhulgas võrgu- ja infosüsteemide turvalisust, terviklikkust ja vastupidavust (Euroopa Parlament ja Nõukogu, 2016a). Seda kinnitavad ka Euroopa Pangandusjärelevalve (EBA) poolt direktiivi (EL) 2015/2366 (PSD2) alusel välja töötatud suunised makseteenuste operatsiooni- ja turvariskide jaoks kasutatavate turvameetmete kohta, mida peavad järgima Euroopa Liidu majandusruumis tegutsevad makseteenuse pakkujad (EBA, 2018). Soovituslikest juhenditest kaasati valimisse Finantsinspektsiooni koostatud nõuded finantsjärelevalve subjekti infotehnoloogia ja infoturbe korraldusele, mis Finantsinspektsiooni seaduse § 57 lõigete 1 ja 3 kohaselt on koostatud finantssektori tegevust reguleerivate õigusaktide selgitamiseks või finantsjärelevalve subjektide suunamiseks (Finantsinspektsiooni seadus, 2019; Finantsinspektsioon, 2017). Finantsturu infrastruktuuride (FMI) kaitseks on Rahvusvaheliste Arvelduste Panga maksete ja turuinfrastruktuuride komitee (CPMI) ja Rahvusvaheline Väärtpaberijärelevalvete Organisatsioon (IOSCO) koostanud soovitusliku juhendi, mis annab täiendavaid juhiseid finantsturgude taristutele kehtivate põhimõtete täitmiseks, millest omakorda lähtutakse makse- ja arveldussüsteemide järelevaatamise teostamisel (Eesti Pank, 2019; CPMI&IOSCO, 2016; Euroopa Keskpank, 2014). Euroopa Keskpank, kes vastutab Euroalas opereerivate süsteemselt tähtsate maksesüsteemide järelevaatamise eest, on koostanud küberkerksuse järelevaatamise ootuste juhendi subjektidele (ECB, 2019; ECB, 2018). Lisaks regulatsioonile kaasati dokumendi valimisse Eesti ja Euroopa Liidu küberkaitse strateegiad. Küberkaitse ja infoturbe meetmete kogumikena kaastati valimisse ISO/IEC 27000 perekonna standardid ja infosüsteemide kolmeastmeline etalonturbesüsteem ISKE. ISO 27000 perekonna standardid toetavad operatsiooniriskide põhist meetmete rakendamist, mille tulemusena on see üks laiemalt kasutatav standard finantssektoris (Carter & Zheng, 2015, p. 7). ISKE rakendamine on kohustuslik kõigile riigi ja kohaliku omavalitsuse andmekogude pidamisel kasutatavate infosüsteemide ja nendega seotud infovaradele turvalisuse tagamiseks (Avaliku teabe seadus, 2019). ISKE kaasati valimisse, kuna küberkaitse tagamisel teeb finantssektor koostööd avaliku sektoriga. Strateegiad ja küberkaitset käsitlev standard ning ISKE raamistik kaasati valimisse, et hinnata ja analüüsida nendes küberolukorrateadlikkuse käsitlust. Nimekiri dokumentidest on toodud tabelis 3.

Tabel 3. Dokumendianalüüsis kasutatud dokumentide loetelu (autori koostatud)

Jrk	Aasta	Asutus	Dokumendi pealkiri
1. Küberkaitset juhendavad ja reguleerivad dokumendid			
1	2017	Finantsinspektsioon	Nõuded finantsjärelevalve subjekti infotehnoloogia ja infoturbe korraldusele (Finantsinspektsioon, 2017)
2	2016	Rahvusvaheliste Arvelduste Panga maksete ja turuinfrastruktuuride komitee (CPMI) ja Rahvusvaheline Väärtpaberijärelevalvete Organisatsioon (IOSCO)	Guidance on cyber resilience for financial market infrastructures (CPMI & IOSCO, 2016)
3	2018	Euroopa Keskpank	Cyber resilience oversight expectations for financial market infrastructures (ECB, 2018)
4	2018	Riigikogu	Küberturvalisuse seadus (Küberturvalisuse seadus, 2018)
5	2016	Euroopa Parlament ja Nõukogu	Direktiiv (EL) 2016/1148, meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (Euroopa Parlament ja Nõukogu, 2016a)
6	2018	Euroopa Pangandusjärelevalve (EBA)	Suunised direktiivi (EL) 2015/2366 (PSD2) alusel makseteenuste operatsiooni- ja turvariskide jaoks kasutatavate turvameetmete kohta (EBA, 2018)
2. Küberjulgeoleku/küberkaitse strateegiad			
7	2013	Euroopa Komisjon	Euroopa Liidu küberjulgeoleku strateegia: avatud, ohutu ja turvaline küberruum (Euroopa Komisjon, 2013)
8	2018	Majandus- ja Kommunikatsiooniministeerium	Küberturvalisuse strateegia 2019-2022 (Majandus- ja Kommunikatsiooniministeerium, 2018)
3. Küberkaitsemeetmete standardid ja kataloog			
9.	2017	Rahvusvaheline Standardimisorganisatsioon ja Rahvusvaheline Elektrotehnikakomisjoni tehniline komitee (ISO/IEC)	27002:2017 – Infotehnoloogia – Turbemeetodid – Infoturbemeetodite turvakoodeks (Eesti Standardikeskus, 2017)
10.	2018	Rahvusvaheline Standardimisorganisatsioon ja Rahvusvaheline Elektrotehnikakomisjoni tehniline komitee (ISO/IEC)	27032:2018 – Infotehnoloogia – Turbemeetodid – Küberturbe juhised (Eesti Standardikeskus, 2018)

11.	2018	Riigi Infosüsteemi Amet	Infosüsteemide kolmeastmeline etalonturbesüsteem (ISKE) rakendusjuhendi lisa 1: Kataloogid B, M ja H (Riigi Infosüsteemi Amet, 2018a)

Ekspertintervjuude valim on **eesmärgistatud**. Käesolev töö uurib küberolukorrateadlikkuse loomise ja rakendamise tõhustamise võimalusi finantssektoris, millest lähtuvalt on esimeseks valimi kriteeriumiks finantssektori küberkaitse eksperdid. Kuna käesoleva töö skoobis on tuvastada küberolukorrateadlikkuse tõhustamise võimalused kriitilist finantsteenust pakkuvate ettevõtete näitel, siis moodustatakse valim AS SEB Pank, Swedbank AS, Luminor Bank AS ja AS LHV Pank küberkaitse ekspertidest. Finantssektori väliselt kaasati intervjueeritavate valimisse Riigi Infosüsteemi Ameti eksperte, kes on finantssektorile oluliseks partneriks küberturvalisuse tagamisel. Nimekiri intervjueeritavatest on toodud tabelis 4.

Tabel 4. Intervjueeritavad eksperdid

Jrk	**Nimi**	**Amet**	**Intervjuu keel**	**Kestus**
1	Tiit Hallas	LHV Panga infoturbejuht	Eesti keel	30 min 59s
2	Toomas Vaks	Swedbank AS küberriskide juht (aastatel 2011-2017 Riigi Infosüsteemi Ameti peadirektori asetäitja küberturvalisuse alal)	Eesti keel	30 min 07s
3	Kadri Kaska	NATO Küberkaitsekoostöö Keskuse teadur (2017-2018 Riigi Infosüsteemi Ameti juhtivanalüütik)	Eesti keel	46 min 52s
4	Olegas Budnik	Luminor Group IT Security Manager	Inglise keel	33 min 08s
5	Heigo Tark	SEB Balti e-kanalite infoturbe juht	Eesti keel	Kirjalikult *
6	Tõnu Tammer	Riigi Infosüsteemi Ameti intsidentide käsitlemise osakonna juhataja	Eesti keel	32 min 17s

Ekspertidega lepiti eelnevalt intervjuu läbiviimise aeg ja koht e-kirja teel kokku. Eelistatult intervjueeritavaga kohtuti ja viidi intervjuud vahetult läbi. Osade intervjueeritavatega ei olnud võimalik vahetult kohtuda, millest tulenevalt viidi intervjuu läbi telefoni, Skype kõne vahendusel. Ühe eksperdiga viidi läbi küsitlus läbi kirjalikult e-posti vahendusel, mis ei kvalifitseeru kvalitatiivsete andmekogumismeetodite hulka. Samas peab autor vajalikuks arvestada kirjalikku sisendit antud teema uurimisel. Ekspertintervjuude kestus jäi 30 – 60 minuti vahele. Intervjuud salvestati kasutades selleks diktofoni või mobiiltelefoni helisalvestamise funktsionaalsust. Inglisekeeles läbiviidud intervjuud tõlgiti Eesti keelde. Helisalvestised transkribeeriti, mida analüüsiti sisuanalüüsitarkvaraga NVivo 12 Pro.

Dokumendianalüüsi ja transkribeeritud intervjuude andmete analüüsimisel kasutatakse **kvalitatiivset suunatud sisuanalüüsi** ehk **kontentanalüüsi**. Kvalitatiivse sisuanalüüsi käigus püütakse enamasti saada ülevaade uuritavast tekstist kui tervikust, näha teksti ja/või autori mõtteavalduste terviklikku mustrit või struktuuri. Erinevalt standardiseeritud kontentanalüüsist ei ole kvalitatiivse sisuanalüüsi eesmärgiks uuritavat teksti analüüsiühikute kaupa kodeerida ega koodide esinemissagedust määrata. Kvalitatiivse sisuanalüüsi nõrgad küljed on omakorda vastandid mõnedele standardiseeritud kontentanalüüsi tugevatele külgedele. Kvalitatiivne analüüs ei võimalda erinevaid tekste täpsetel alustel võrrelda. Tööjaotus uurijate vahel on raskendatud, mistõttu on keeruline läbi töötada suuri valimeid, mis omakorda tingib vähese üldistatavuse (Kalmus, et al., 2015).

2.2. Küberolukorrateadlikkuse loomise ja rakendamise dokumentide analüüs

Dokumendianalüüsiks vajalikud alusdokumendid hangiti avalikest allikatest. Dokumendianalüüsi eesmärk on analüüsi tulemusena tuvastada küberolukorrateadlikkuse loomise ja rakendamise tõhustamise võimalused finantssektorile suunatud küberkaitse korralduslikest juhendavatest, regulatsioonist ja strateegilistest dokumentidest. Analüüsi

tulemusi võrreldakse intervjuu tulemustega, mille põhjal saab tehakse järeldusi küberolukorrateadlikkuse tõhustamiseks. Uurimisel lähtuti joonise 6 toodud koodipuust, mida täiendati uurimisküsimustega.

2.2.1. Küberolukorrateadlikkuse loomise ja rakendamise dokumendianalüüsi tulemused

Tulemuste analüüsimiseks kasutati kvalitatiivset sisuanalüüsi, mida kasutatakse tekstide sisu ja kontekstilise tähenduse uurimiseks (Laherand, 2008, lk 289-299); Flick, 2009, lk 323-327). Tekstide analüüsimiseks kasutati magistritöös **suunatud kodeerimist** tähenduses, et kõigepealt loodi teooria põhjal mõned koodid. Edasises etapis otsitakse andmetest koodile vastavaid tekstilõike. Samade tunnustega koodid jaotati vastavatesse koodide kategooriatesse (Flick, 2009, pp. 318-320 Kalmus, et al., 2015). Suunatud kodeerimise puhul toimub kodeerimine vastavalt uurimisküsimustele ning muud teemad jäetakse tekstides kõrvale. Kodeerimiseks teemakohase teksti leidmiseks teostati valimisse kuulunud dokumentides vastavad otsingud, kasutades inglise- ja eestikeelseid märksõnu „küberolukorrateadlikkus“, „küberohu teadlikkus“, „olukorrateadlikkus“, „teadlikkus“, „olukorrapilt“ „cyber threat intelligence“, „threat intelligence“, „situational awareness“. Selle tulemusena eristusid dokumentides 97 analüüsiüksust, mis jaotati loodud alamkategooriate alla moodustunud 42 koodi vahel. Analüüsitehnikana kasutati juhtumiülest analüüsi *(cross-case analysis)* tähenduses, et erinevates dokumentides koguti kokku kõik konkreetsete alamkategooriate kohta käivad tekstilõigud ja võrreldi nende käsitlemist kõigi kogutud dokumentide lõikes (Babbie, 2013, p. 391; Kalmus, et al., 2015).

Joonis 7. Analüüsitarkvaras NVivo 12 Pro loodud dokumendianalüüsi koodipuu alamkategooriad (autori koostatud)

Esimese peakategoorias otsiti eestikeelsetest valimi dokumentides inglisekeelsele terminile „cyber threat intelligence“ eestikeelset vastet, kasutati märksõnu „küberolukorrateadlikkus“, „küberohu teadlikkus“, „olukorrapilt“, „luure*“, „ohuluure*“, „teadmus*“, „ohuteade“. Käesoleva töö käsitluses tuvastati terminile vastetena olukorrapilt ja ohuluureteave (Majandus- ja Kommunikatsiooniministeerium, 2018; EBA, 2018, lk 12). Luure termini käsitlust toetab ka teooria, mille põhjal klassifitseeruks käesolev termin teiste luurekäsitluse domeenidega (käesoleva töö lk 13-14). Samas käsitletakse luuret kui informatsiooni varjatud kogumise ja selle analüüsimisena, mida rakendatakse otsustusprotsessides (Juurvee, 2018). Varjatud tegevused seostuvad pigem luure ja vastuluurega tegelevate asutustega, mis ei haaku finantssektori organisatsioonide visiooni ja missiooniga.

Alamkategoorias 2.1. „Küberolukorrateadlikkuse loomiseks kogutavad andmed“ kodeerimiseks teostati dokumentides märksõnade otsingud, milles tulemusena tuvastati 18 erinevat koodi. Kõige enam esines kood, mille põhjal kogutakse küberolukorrateadlikkuse loomiseks andeid küberohumaastiku ja selle trendide kohta. Järgnevalt toon välja koodid, mis leidsid mitmel korral kajastust: avalikult teada ja teadmata teave haavatavustest, teave ründajast, ründaja võimetest, kavatsustest, tegutsemisviisist (modus operandi), TTP-st ja teave olulisest mõjust tulenevatest intsidentidest. Küberolukorrateadlikkuse loomise ja rakendamise formaatide käsitleti alamkategoorias 2.2. „Küberolukorrateadlikkuse loomise

formaat“ sõltub loodava teadlikkuse formaat selle rakendajatest ja nende vajadustest. Näiteks juhtidele soovitatakse pakkuda küberolukorrateadlikkust raportite näol, mis sisaldab perioodil toimunud intsidente, küberohuteadlikkus trendide kohta, tuvastatud kahtlased ja anomaalsed küberkaitse sündmused. Teadlikkuse jagamise ja hankimise aspektist käsitleti formaatidena e-posti, teenusepakkuja portaali, intranetti ehk asutuse sisevõrku, küberriskide näidikute paneeli (dashboard).

Küberolukorrateadlikkuse loomise ja rakendamise eesmärgid kaardistati alamkategoorias 2.3. „Küberolukorrateadlikkuse loomise ja rakendamise eesmärgid“, millest enim mainimist leidis kood „küberolukorrateadlikkuse rakendamise vajadus otsustusprotsessides“. Otsustusprotsesside tasemetena käsitleti strateegilist, operatsioonilisel ja taktikalist tasandit. Strateegilisel tasemel vajatakse küberolukorrateadlikkust strateegiliste eesmärkide seadmisel, algatuste koordineerimisel, küberkaitse tegevuste toetamiseks, plaanide väljatöötamisel, riskipõhiste otsuste tegemiseks. Operatiivsel tasandil vajatakse teadlikkust küberkaitse meetmete juurutamisel ja disainimisel, olemasolevate ja uute nõuete kujundamisel, talitluspidevuse plaanide testimisel, operatsiooniliste riskide haldamisel. Taktikalisel tasandil intsidentide/ründe tegevuste tuvastamises, võrgu, infrastruktuuri ja infosüsteemide seires. Osad nimetatud operatsioonid on organisatsiooni ülesed, mis on aktuaalsed kõikidel juhtimistasanditel, nagu operatsiooniline riskijuhtimine ja küberkerksuse võimete tõhustamine. Küberkerksuse tõhustamiseks vajatakse teadlikkust selle kõikide küberkerksuse raamistiku komponentide eesmärgi saavutamise toetamiseks (vt joonis 5). Euroopa Pangandusjärelevalve koostatud ja direktiivi (EL) 2015/2366 (PSD2) alusel makseteenuste operatsiooni- ja turvariskide jaoks kasutatavate turvameetmete kohta tuleb makseteenuste pakkujal suunise 6.7 kohaselt vähemalt kord aastas talitluspidevuse plaane ajakohastada testitulemuste, ajakohase ohuluureteabe, jagatud teabe ja eelmistest juhtumitest saadud kogemuste alusel, samuti arvestades taastamiseesmärkide muutumist ning (kui asjakohane) pärast süsteemide ja protsesside muudatusi (EBA, 2018, lk 12).

Alamkategoorias 2.4. „Küberolukorrateadlikkuse loomiseks kasutatavad allikad“ märgiti ära nii sisemiste kui ka väliste allikate kasutamist. Ülekaalukalt käsitleti väliseid allikaid, mis pärinesid teistelt finantssektori partneritelt ja usaldusväärsetelt küberolukorrateadlikkuse teenusepakkujatelt. Alamkategoorias 2.5. „Küberolukorrateadlikkuse loomise protsessi osalised“ märgiti küberolukorrateadlikkuse

teenusepakkujaid ja küberkaitse operatsioonide keskust (SOC). Viimast tuuakse esile kui keskust, kuhu tuleks integreerida küberolukorrateadlikkuse loomise protsess.

Alamkategoorias 2.6. „Küberolukorrateadlikkuse jagamine ja selle osalejad“ tuvastati lisaks sisemistele osapooltele, keda käsitleti eelnevalt alamkategoorias 2.3., väliste partneritena avaliku sektori asutustest Riigi Infosüsteemi Amet, Kaitseministeerium, Kaitseliit, Välisluureamet, Siseministeerium, Politsei- ja Piirivalveamet, Kaitsepolitseiamet, Siseministeeriumi Infotehnoloogia- ja Arenduskeskus. Nimetatud avaliku sektori asutuste ühise omadusena on osaleda ja panustada ühtse olukorrapildi loomisse. Teenusepakkuja intsidentidest teavitamisel käsitletakse mitmeid osapooli – Riigi Infosüsteemi Amet, Finantsinspektsioon, Euroopa Pangandusjärelevalve jt. Üldisemal tasemel on märgitud teadlikkuse jagamine partnerite, teenusepakkujate, teadlikkuse jagamise gruppidega, kolmandate osapooltega jt, ehk teadlikkust soovitatakse jagada kõikide seotud osapooltega, võimaldades teistel ohust tuleva mõju maandamiseks meetmed kasutusele võtta.

2.7. „Küberolukorrateadlikkuse jagamise tingimused“ eeldatakse, et osapooled fikseerivad jagamise tingimused kokkulepetes. Kokkulepe võib olla sõltuvalt jagamise viisist bilateraalne või multilateraalne. Teabe raporteerimise nõuded tuleb fikseerida kokkuleppes. Sektori üleselt soovitatakse jagada vähemalt teavet intsidentidest. Alamkategoorias 2.8. „Küberolukorrateadlikkuse loomise ja jagamise tehnilised lahendused“ tuvastati kolm koodi- e-posti, küberolukorrateadlikkusel põhinevat riskide näidikutepaneeli (dashboard) ja intranet. Valimis on tegemist kõrgema taseme dokumentidega, mis ei lähe tehniliste lahenduste aspektist detailidesse.

Peakategoorias 3. „Küberolukorrateadlikkuse loomise ja rakendamise tõhustamine“ alamkategooria 3.1. „Küberolukorrateadlikkuse loomise ja rakendamise võimalused dokumendianalüüsi põhjal“ alla koondati dokumendianalüüsis tuvastatud tõhustamise võimalused, milleks on järgmised leiud:

- Küberolukorrateadlikkuse saamiseks/loomiseks koguda välistest allikatest küberolukorrateadlikkust/küberohuteavet, liitudes/osaledes seda jagavates gruppides, teenusepaakuja ja või koostööpartneritega;

- Regulaarselt küberolukorrateadlikkuse loomisprotsessi (sh hangitava teabe) ülevaatamine veendumaks, et loomisprotsess ja selle tulem vastab vajadustele;
- Küberolukorrateadlikkuse rakendamine erinevate juhtimistasandite otsustusprotsessides, mis vajavad teadlikkust küberruumi ohtudest tuleneva mõju maandamiseks;
- Küberolukorrateadlikkuse loomist ja jagamist toetavate tehnoloogiliste lahenduste kasutamine;
- Teadlikkuse jagamine teiste partnerite/osapooltega küberohtudest tuleneva mõju maandamiseks;
- Küberolukorrateadlikkuse jagamisel leppida osapooltega kokku jagatava teabe skoop, jagamise reeglid ja tingimused, fikseerides need kirjalikult näiteks teabe jagamise koostöökokkuleppes;
- Küberolukorrateadlikkuse rakendamine küberkerksuse tagamisel (küberkerksuse strateegia kujundamine, teadlikkuse tõstmine, testimine, olukorrateadlikkuse kujundamine, kaitse/tuvastus meetmete loomine ja olemasolevate kujundamine, tuvastatud intsidentidele reageerimine, talitluspidevuse planeerimine);
- Testida organisatsioonide küberolukorrateadlikkuse loomise ja rakendamise efektiivsust küberõppuse vahendusel. Õppuse stsenaariumi koostamisel lähtuda küberolukorrateadlikkust.
- Küberolukorrateadlikkuse loomise ja rakendamise tõhustamiseks regulatsiooni täiendamine.

2.2.2. Küberolukorrateadlikkuse loomise ja rakendamise dokumendianalüüsi järeldused

Esimese järeldus põhineb küberolukorrateadlikkuse teooria ja dokumendianalüüsile tuginedes, milles selgus, et traditsioonilised küberkaitse meetmete kogumikud (ISO 27000 perekond ja ISKE) ei käsitle küberolukorrateadlikkust. Samas on nendes dokumentides suuremal ja vähemal määral elemente, mis soodustavad küberolukorrateadlikkuse rakendamist. Näiteks intsidentide haldus ja nendest teavitamine, mis suunavad organisatsioone jagama intsidentide kohta käivat informatsiooni teiste osapooltega, keda intsident võib mõjutada. Valimis olevatest klassikalistest turvanõuete dokumentidest

kirjeldab ja käsitleb kõige lähemalt küberolukorrateadlikkust ISO 27032:2018 küberturbe juhis, mille teabe jagamise ja koordineerimise karkassi (*framework for information sharing*) peatükis kirjeldatakse poliitikad, meetodid ja protsessid, inimesed ja organisatsioonid ning tehnilised meetmed (Eesti Standardikeskus, 2018). Klassikalisi turvanõudeid koondavaid dokumente uuendatakse regulaarselt, millest tulenevalt võivad uuemad versioonid käsitleda endas juba täpsemalt endas küberolukorrateadlikkust, selle loomist ja rakendamist. Käesoleva töö küberolukorrateadlikkuse loomise ja rakendamise alused kaardistati peamiselt küberkerksuse raamistikel põhinevate dokumentide põhjal. Teadlikkuse loomiseks hangitakse teavet küberohtudest, küberohutrendidest, ründajast, ründaja võimekusest, tegutsemisviisist, taktikad, tehnikad ja protseduurid ründe tõrjumiseks ja muu teave (kokku kaardistati 18 eriliiki teavet), mis aitavad küberruumist tulenevaid ohuriske maandada.

Küberolukorrateadlikkuse loomise formaadi osas käsitlesid dokumendid peamiselt selle kasutamist kõrgema taseme otsuste tegemisel. Näiteks soovitatakse küberolukorrateadlikkus dokumenteerida ja esitleda viisil (näiteks raportid), mida saab koosolekutel ja juhatuse istungitel rakendada otsuste tegemiseks.

Küberolukorrateadlikkuse loomise ja rakendamise eesmärke käsitleti alamkategoorias 2.3, mille peamiseks eesmärgiks on küberolukorrateadlikkuse kasutamine strateegilise, operatsioonilise ja taktikalise taseme otsustusprotsessides. Näiteks strateegilisel tasemel rakendatakse küberolukorrateadlikkust küberkaitse strateegia kujundamisel, planeerimisel, eelarvestamisel. Operatsioonilisel tasemel kontrollmeetmete juurutamisel ja disainimisel, nõuete, poliitikate väljatöötamisel, töötajate teadlikkuse tõstmisel. Taktikalisel tasemel ründe tuvastamise võimekuse arendamisel, võrgu ja infrastruktuuri kaitsmisel, intsidentide haldamisel, infosüsteemi/infrastruktuuri seirel, võimalike küberintsidentide tuvastamisel jt eesmärkidel. Intsidentide käitlemist käsitlesid kõik valimi dokumendid tuvastamise, reageerimise ja teavitamise aspektist. Küberturvalisuse seadus defineerib küberintsidenti kui süsteemis toimuvat sündmust, mis ohustab või kahjustab süsteemi turvalisust (Küberturvalisuse seadus, 2018). ISO standard käsitleb intsidenti kui soovimatut või ootamatut infoturvasündmustikku, mis võib kahjustada organisatsiooni tegevust või ähvardada teabe turvalisust (Eesti Standardikeskus, 2018). Välismõjuga turvaintsidente saab kasutada sisendina küberolukorrateadlikkuse loomiseks. Finantsinspektsiooni juhendi põhjal tuleb organisatsil teavitada Finantsinspektsiooni intsidendist, mis sisaldab

järgmiseid andmeid: intsidendi tüüp (käideldavus, terviklikkus, konfidentsiaalsus), toimumise aeg, ulatus ja mõju, kirjeldus, põhjus, lahendus ja meetmed, mida kavatsetakse rakendada tulevikus sarnaste juhtumite ärahoidmiseks (Finantsinspektsioon, 2017). Sellise detailsusega intsidenditeavet, mis võib sisaldada küberolukorrateadlikkuse komponente nagu TTP, IOC jt, oodatakse hiljemalt kolme päeva möödumisel pärast olulise intsidendi lahendamist. Intsidendi hetkel tuleb edastada intsidendi osas niipalju infot, kui teavitamise hetkel on võimalik.

Vahetust intsidendist teavitamisel on kindlasti kasu teistel osapooltel, aidates kasutusele võtta meetmeid intsidendi ärahoidmiseks. Küberolukorrateadlikkuse loomisel on olulisel kohal saada teavet teistes organisatsioonides tuvastatud küberintsidentidest. Euroopa Liidu direktiivi (EL) 2016/1148, meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus kohaselt tuleb küberintsidentide teateid edastada ühtsele kontaktpunktile (CSIRT), milleks küberturvalisuse seaduse §5 kohaselt on Riigi Infosüsteemi Ametis tegutsev küberintsidentide käsitlemise üksus CERT-EE. Alamkategoorias 3.1. kaardistati küberolukorrateadlikkuse loomise ja rakendamise tõhustamise võimalusena osapooltega kokku leppida teabe jagamise skoop ning alamkategoorias 2.7. küberolukorrateadlikkuse jagamise tingimused. Küberturvalisuse seadus seab teenuse osutajale kohustuseks teavitada CERT-EE-d viivitamata, kuid hiljemalt 24 tundi pärast teada saamist küberintsidendist, millel on süsteemi turvalisusele või teenuse toimepidevusele oluline mõju ja/või mille oluline mõju süsteemi turvalisusele või teenuse osutamisele ei ole ilmne, kuid seda võib mõistlikult eeldada. Samuti tuleb teenuse osutajal teavitada mõistliku aja jooksul isikut, keda olulise mõjuga küberintsident võib mõjutada, või avalikkust, kui mõjutatud isikuid ei ole võimalik eraldi teavitada. Seadusega reguleeritakse teavitamise kanalid ja tingimused, mille kohaselt on elutähtsa teenuse osutajad (sh elutähtsad finantsteenuse osutajad) kohustatud teavitama CERT-EE-d, isikut või avalikkust, olulise mõjuga küberintsidendist. Reguleeritud intsidentidest teavitamisest on palju abi küberolukorrateadlikkuse jagamisel, sest selleks saab kasutada samasid reguleeritud teavitamise kanaleid. Teavitamiseks tuleb teenuse osutajal edastada Riigi Infosüsteemi Ametile raport, mis sisaldab informatsiooni küberintsidendi tekkepõhjusest, selle lahendamiseks kulunud aja ja rakendatud abinõude ning küberintsidendi mõju kohta, millega on reguleeritud intsidendi jagamise skoop. Samas öeldakse ka seaduses, et teenuse osutaja võib CERT-EE-d teavitada seaduses sätestatud

mitteolulisest küberintsidendist. Ehk kõik eeldused küberolukorrateadlikkuse jagamiseks on olemas. Teenuse osutajad saavad edastada küberolukorrateadlikkust CERT-EE-le, kes vastavalt vajadusele saab intsidendi ennetamiseks ja lahendamiseks edastada ohuteateid mõjutatud isikutele. Lisaks on CERT-EE teavitamine kirjeldatud infosüsteemide kolmeastmelises etalonturbesüsteemis ISKE järgnevalt:

/Sündmus, millega kaasneb andmete või muude infovarade käideldavuse, tervikluse või konfidentsiaalsuse kadu või tekib oht nende kadumiseks, siis tuleb lisaks asjassepuutuvate isikute turvaintsidendist teavitamise nõuetele sellest teavitada ka Eesti riigi rahvuslikku CERT'i vastavalt Riigi Infosüsteemi Ameti (RIA) poolt antud juhisetele. Oluline turvaintsident võib lisaks oma infosüsteemile mõjutada teiste asutuste teenuste osutamiseks vajalike infosüsteemide toimimist./ (Riigi Infosüsteemi Amet, 2018a).

Makseteenuse direktiivi kohaselt tuleb kõikidel makseteenuse osutajatel teavitada olulistest intsidentidest Finantsinspektsiooni, kes teostab riiklikku finantsjärelevalvet. Euroopa Pangandusjärelevalve poolt koostatud olulistest intsidentidest teatamise suunistele tuginedes edastab Finantsinspektsioon saadud olulise intsidendi raportid Euroopa Pangandusjärelevalvele ja Euroopa Keskpangale. Sellest tulenevalt võib finantssektori vaates kokku leppida ja jagada küberolukorrateadlikkust Finantsinspektsiooni vahendusel. Samas teostab Finantsinspektsioon järelevalvet ühe sektori lõikes, mille põhjal on CERT-EE teadlikkuse saamise jagamise keskusena parem kontaktpunkt, võimaldades sektoriülest küberolukorrateadlikkuse jagamist.

Alamkategoorias 3.1. tuvastati küberolukorrateadlikkuse loomise ja rakendamise võimaluste seas tehnilise lahendustena riigi automaatseire laheduse laiendamine erasektori võrkudele, pakkudes osapooltele terviklikku küberruumi olukorrapilti. Automaatseire laiendamine finantssektorile aitaks kaasa riigiülese küberruumi olukorrapildi loomisele. Samuti saaksid finantssektori organisatsioonid kasutada riigiülest olukorrapilti küberolukorrateadlikkuse loomiseks. Küberolukorrateadlikkuse loomise ja rakendamise aspektist tuleks kaaluda tegevust soodustava ja toetava infosüsteemi rakendamist. Küberolukorrateadlikkuse integreerimine küberruumi olukorrapilti oleks üheks võimaluseks, mis annaks pikema ja põhjalikuma ülevaate küberruumi ohtudest, võimaldades organisatsioonidel ennetada ja proaktiivselt rakendada teadlikkust küberruumist tulenevate ohuriskide maandamiseks.

Alamkategoorias 3.1. tuvastati küberolukorrateadlikkuse loomise ja rakendamise võimalusena selle rakendamine küberkerksuse raamistiku elluviimisel. Küberkerksuse raamistik on jaotatud kaheksaks komponendiks, millest igas komponendis saab rakendada küberolukorrateadlikkust eesmärgi saavutamiseks. Küberkerksuse komponendid on valitsemine, identifitseerimine, kaitsmine, tuvastamine, taastumine, testimine, olukorrateadlikkus ja õppimine ning arenemine (vt joonis 5), mida analüüsin küberolukorrateadlikkuse aspektist lähemalt. Küberkerksuse valitsemise komponendis käsitletakse küberriskide haldust. Efektiivse valitsemise aluseks on selge ja kõikehõlmav küberkerksuse raamistik, milles prioriseeritakse küberkaitse eesmärgid ja tase, mida soovitakse hoida või saavutada. Selleks käsitletakse valitsemises erinevaid otsustusprotsesse (n strateegilised, riskipõhised otsused), mille sisendina rakendatakse küberolukorrateadlikkust, võimaldades teha valitsemise otsuseid tulenevalt muutuvast küberruumi olukorrast. Identifitseerimise komponendis käsitletakse organisatsiooni kohustust identifitseerida operatsioone ja nende elluviimiseks kasutatavaid infovarasid, mis vajavad kompromiteerimise eest kaitset. Küberolukorrateadlikkus võib anda teavet, milliseid operatsioone ja varasid konkreetses ründes ära kasutatakse, mis aitab organisatsioonil fokusseerida oma kaitsemeetmed rünnatavate operatsioonide ja varade kaitseks. Kaitsmise komponendis käsitletakse kontrollmeetmeid, mis on olulised küberkerksuse saavutamiseks läbi varade ja teenuste konfidentsiaalsuse, terviklikkuse ja käideldavuse tagamise. Meetmed peavad olema proportsionaalselt vastavuses küberruumi ohumaastikuga, toetama finantssüsteemi rolli täitmist ja olema kooskõlas riski taluvusega. Küberolukorrateadlikkuse võib anda ründe kohta teavet, mille põhjal saab näiteks hinnata rakendatud kaitsemeetmete piisavuses, mis võimaldab organisatsioonil kasutusele võtta vastavad ja efektiivsed kaitsemeetmed. Küberkerksuse raamistiku tuvastamise komponent keskendub tegelikule organisatsiooni vastu suunatud rünnaku tuvastamisele. Rünnaku varajane avastamine annab organisatsioonile väärtuslikku aega, et rakendada rünnaku tõrjumiseks vastumeetmed. Küberolukorrateadlikkuse rakendamise kaudu võib organisatsioon teada saada ja tuvastada tema vastu suunatud rünnakust, võimaldades organisatsioonil õigeaegselt (varajases staadiumis) tuvastada rünnak. Küberkerksuse raamistiku vastamise ja taastumise komponendis keskendutakse tuvastatud rünnaku tõrjumisele ja rünnaku tulemustel tehtud kahjude kõrvaldamise ja taastumisega. Küberolukorrateadlikkus pakub väärtuslikku informatsiooni ründaja kohta, tema tegutsemisviisist (modus operandi), ründes kasutatavate vahendite ja muu teave, mis aitab

rünnakut tõrjuda. Taastumise aspektist annab küberolukorrateadlikkus sisendit talitluspidevuse/toimepidevuse paneerimisse, võimaldades välja töötada adekvaatsed ja efektiivsed plaanid süsteemide ning teenuste taastamiseks. Küberkerksuse raamistiku komponent testimine keskendub organisatsioonis rakendatud küberkerksuse efektiivsuse tuvastamisele ja hindamisele. Küberolukorrateadlikkus annab sisendit aktuaalsetest küberohtudest testimise planeerimisprotsessi ja tõenäolise testistsenaariumi väljatöötamiseks. Ründestsenaariumi läbimängimine võib esile tuua organisatsiooni nõrkused rakendatud kaitsemeetmetes, tuvastamisel, tõrjumisel, taastumisel, talitluspidevuse plaanimisel, riskijuhtimisel, küberolukorrateadlikkuse loomisel ja rakendamisel jt protsessides. Küberkerksuse raamistiku komponendis olukorrateadlikkus käsitletakse organisatsiooni mõistmist ohumaastikust, milles ta tegutseb ja mõistmist mõjudest, mis kaasnevad selles keskkonnas tegutsemisega. Samuti sisaldab olukorrateadlikkus infot organisatsiooni kaitstavatest varadest, protsessidest, kaitsemeetmetest, tuvastamise, reageerimise ja taastumise võimekusest. Olukorrateadlikkus käsitleb ka teadlikkust organisatsiooni hetkeolukorrast küberrünnete aspektist. Küberolukorrateadlikkus annab teavet küberohtudest, ohutrendidest, võimalikest tarkvara nõrkustest, ründajast, ründaja tegutsemise viisist jm teave, mis aitab kaasa organisatsiooni olukorrateadlikkuse tekkimiseks, võimaldades ennetada või tuvastada õigeaegselt organisatsiooni ohustavad rünnakud. Näiteks teave ohumaastikust võimaldab organisatsioonil paremini mõista oma kriitiliste funktsioonide haavatavusi, hõlbustades asjakohaste riske maandavate tegevuste kasutusele võtmist. Tegevusteks võivad olla näiteks strateegilise suuna kehtestamine, ressursi ümberkorraldamine, protsesside, protseduuride ja kontrollide kujundamine piisava küberkerksuse saavutamiseks. Olukorrateadlikkuse tekkimiseks on võtmetähtsusega küberolukorrateadlikkuse alase teabe jagamisel usaldusväärsete partneritega nii sektori siseselt kui väliselt. Küberkerksuse raamistiku õppimise ja arenemise komponent keskendub muutuva küberohu maastiku õppimisele ja vastavalt sellele pidevale arenemisele, et saavutada või hoida organisatsiooni soovitud küberkerksuse taset. Küberolukorrateadlikkus näitab ohumaastiku kujunemise trende. Näiteks on ENISA raporti põhjal uue trendina esile kerkinud oht krüptovaluuta ja selle kuritegelikul teel kaevandamine, mille osas tuleb organisatsioonil tundma õppida uusi trende, hinnata nende mõju organisatsioonile ja siit edasi arendada kaitsemeetmeid, tuvastamist, reageerimist ja taastumist oma varade kaitsmiseks (ENISA, 2019).

Euroopa Liidu küberjulgeoleku strateegia toob ühena viiest peamisest strateegilisest prioriteedist esile küberkerksuse saavutamise küberturvalisuse tagamisel (Euroopa Komisjon, 2013). Dokumendianalüüsist selgub, et finantssektori aspektist on järelevalve dokumentide põhjal küberkerksuse rakendamine reguleeritud arveldusteenuste tagamiseks. Samas ei tuvastatud regulatsiooni osas seost Eesti küberturvalisuse seaduse ja küberkerksuse saavutamise vahel. Ühe võimalusena saavad kõik elutähtsat teenust osutavad ja korraldavad organisatsioonid reguleerida küberkerksuse tagamist sektori põhiselt, kuid killustatuse vähendamiseks ja sektorite ülese küberkerksuse rakendamise tagamiseks aitaks kaasa selle keskne reguleerimine.. Sektorite ülese küberkerksuse tagamine aitaks kaasa ka küberolukorrateadlikkuse laiemale rakendamisele, sest eelneva lõigu põhjal on küberolukorrateadlikkusel oluline roll küberkerksuse raamistikus selle eesmärkide elluviimisel.

Küberolukorrateadlikkuse ühe tõhustamise võimalusena toon välja selle rakendamine „punase meeskonna“ testide tegemisel. „Punase meeskonna“ puhul on tegemist testijatega, kes imiteerivad ründajaid. Küberolukorrateadlikkus aitab välja töötada tõenäolist ründestsenaariumit, mida läbi „punase meeskonna“ ründetestide saavad organisatsiooni kaitsemeeskonnad testida oma kaitse, tuvastamise, reageerimise ja taastamise võimekust.

2.3. Küberolukorrateadlikkuse ekspertintervjuud

2.3.1. Küberolukorrateadlikkuse ekspertintervjuude tulemused

Ekspertintervjuude valim on eesmärgistatud. Valim moodustati riigi ja finantssektori küberkaitse ekspertidest (vt tabel 4), kellelt koguti teadmisi küberolukorrateadlikkuse loomisest ja rakendamisest (Kolb, 2008, p. 142). Tulemuste analüüsimiseks kasutati **kvalitatiivset sisuanalüüsi** (Flick, 2009, pp. 323-327). Transkriptsioonid kodeeriti kasutades **suunatud kodeerimist** (Flick, 2009, pp. 305-332 Kalmus, et al., 2015). Kodeerimisel lähtuti joonisel 6 toodud koodipuust, mille peakategooriat 3. “Küberolukorrateadlikkuse liimise ja rakendamise tõhustamine“ alamkategooriat 3.2. „Küberolukorrateadlikkuse loomise ja rakendamise võimalused ning vajadused intervjuude tulemusel“ täiendati joonisel 8 toodud alamkategooriatega.

Joonis 8. Analüüsitarkvaras NVivo 12 Pro loodud intervjuude koodipuu (autori koostatud)

Analüüsitehnikana kasutati juhtumiülest analüüsi *(cross-case analysis)* tähenduses, et erinevate intervjuude transkriptsioonidest koguti kokku kõik konkreetsete alamkategooriate kohta tekstiosad ja võrreldi nende käsitlemist kõigi transkriptsioonide lõikes (Babbie, 2013, p. 391; Kalmus et al., 2015).

Intervjuu läbiviimiseks võeti ekspertidega e-kirja teel ühendust, mille vahendusel lepiti kokku intervjuu läbiviimise aeg ja koht. Eelistatult viidi intervjuud läbi vahetult. Eksperdid, kellega ei õnnestunud kohtuda, viidi intervjuu läbi telefoni või Skype vahendusel. Ühte eksperti küsitleti kirjaliku küsitluse põhjal, mis ei klassifitseeru kvalitatiivse andmete kogumismeetodite alla. Paraku oli see ainuke viis vastuse saamiseks. Autor pidas oluliseks arvestada kirjalikult saadud vastuseid analüüsi järelduste tegemiseks. Nimekiri intervjueeritavatest on toodud tabelis 4.

Ekspertintervjuude küsimused jaotusid kolme grupi küsimuste vahel – sissejuhatavad küsimused, küberolukorrateadlikkuse kujunemine ja küberolukorrateadlikkuse rakendamine. Sissejuhatavate küsimuste käigus uuriti eesti keelt kõnelevatelt intervjueeritavatelt inglisekeelse termini „cyber threat intelligence“ eestikeelse termini käsitlust. Ekspertintervjuude käigus pakkus autor esialgse eestikeelse terminina „küberohu teadlikkust“, mida eksperdid kategoriseerisid üldisesse küberhügieeni või kasutajate teadlikkuse tõstmise valdkonda. Ühe eksperdi soovitus oli „küberohu teadlikkus“ kokku

kirjutada, mis aitaks terminit eristada üldisest küberhügieeni käsitlusest. Esialgu pakutud termini „küberohu teadlikkus“ käsitluses jaotus intervjueeritavate käsitluses kolmeks – ebaselge termini käsitlus, üldine kasutajate teadlikkuse tõstmine ohtudest ja viimasena vastav „cyber threat intelligence“ käsitlusele.

Näide eksitavast või ebaselgest „küberohu teadlikkuse“ termini tõlgendusest:

/Tegelikult minu jaoks see küberohumõiste on selles mõttes natukene segane, et vähemalt terminina, et ta sõltub paljuski kontekstist, kui me räägime tädi Maaliga, siis küberoht ikkagi me peame rääkima väga suuresti küberhügieeni võtmes, ja sellised lihtsad asjad mis tavainimest võivad puudutada. Kui me räägime nüüd natuke laiemalt on see siis sektori või riigi põhiselt ohuolukorra pildist, siis seal see mõiste omistab natuke teise tähenduse./ .. /selle termini taga minu jaoks on eelkõige teadmine või selline teadmusbaas mis toimub laiemalt kas riigis, regioonis või terves maailmas, et millised on trendid, millised on sellised levinud vektorid, niisama mis lihtsalt toimub, et kasulik hoida silmad lahti./ (E1)

Teiseks käsitleti terminit „küberohu teadlikkus“ kasutajate teadlikkuse tõstmisena:

/Esmajoones seostub selle terminiga kasutajate teadlikkus ja informeerimine erinevate kübermaailma ohtude kohta. Arvestades keskmist töötajat, siis täpsema definitsiooni osas keskenduksin pigem üldistele teemadele./ (E3)

Kolmandaks käsitleti terminit „küberohu teadlikkus“ käsitlusele vastavalt:

/.. see on ennekõike see, et me teame millistes piirides oht tekkida võib, kus kohas ta võib tekkida, ehk ohu allikad, ja sellised asjaolud, millest oht tekkida võib, ja samuti see, et millistes piirides kogu oht meid mõjutab/ (E2).

/Küberohu teadlikkus, mitu aspekti, et minu enda jaoks on see et ma tahan teada või mul on oluline et ma teaksin mis on need potentsiaalsed ohud või ründevektorid, mida tänapäeval kasutatakse või mis on need asjad, mis võivad kas mulle või minu vastutusalale kurja teha ja nendest tulenevalt siis adekvaatselt nendesse suhtuda…/ (E5).

Eestikeelne termin „küberohu teadlikkus“ oli suures osas kas segadust tekitav või tõlgendati seda pigem üldise kasutajate teadlikkuse tõstmisena. Intervjuudel paluti ekspertidel anda oma eestikeelne vaste inglisekeelsele terminile „cyber threat intelligence“, mille tulemusena pakuti vastena „küberohuluuret“, „küberolukorrapilt“, „küberruumi olukorrapilt“, „küberolukorrateadlikkus“. Intervjuude käigus selget ja ühest inglisekeelse termini „cyber threat intelligence“ eestikeelset vastet ei selgunud. Intervjuude tulemusena selgus, et autori poolt pakutud esialgne termini tõlgendus „küberohu teadlikkus“ on mõistetav pigem üldise kasutajate küberohtude teadlikkuse tõstmisega, millest tulenevalt tuleb leida parem termini eestikeelne vaste.

Põhikategooria 3. „Küberolukorrateadlikkuse loomise ja rakendamise tõhustamise“ alamkategoorias 3.2. Küberolukorrateadlikkuse loomise ja rakendamise võimalused ning vajadused intervjuude tulemusel“ tõid eksperdid esile selle rakendamise võimalustena kõikides valdkondades, kus on IT rakendatud. Näiteks küberolukorrateadlikkuse kasutamine operatsioonilisel ja poliitilisel tasemel, riskijuhtimise protsessis, tehnilisel tasemel küberkaitse otsuste tegemisel, võimaldades proaktiivselt reageerida ohtudele.

/..*Strateegilisel tasemel on seotud riskijuhtimisega, aga see on juba nii pikk vaade, et seal selline vahetu trendide ja sündmuste nägemine mõjutab vähem, seal mõjutab see ots et kes on toimijad, mis on nende võimekused, nende motiivid, millised on nende ressursid ja pikaajalised eesmärgid..*/ E6

Lisaks dokumendianalüüsis kaardistatule lisandus küberolukorrateadlikkuse rakendamine poliitilisel tasandil, mille skoobis võib olla nii üksik organisatsioon, finantssektor või sektorite ülene küberkaitse poliitika kujundamine. Siit tulenevalt võivad poliitika kujundajateks ja ka küberolukorrateadlikkuse rakendajaks olla finantssektori organisatsioon(id), finantssektorit korraldav ja/või järelevaadatav organisatsioon ja sektori üleselt riigi asutused.

Küberolukorrateadlikkuse loomise ja rakendamise vajadustena tõid intervjueeritavad esile selle jagamise tähtsust. Teadlikkuse jagamisena nimetati Finantsinspektsiooni, CERT-EE-d, Eesti Panka ja Pangaliitu kui keskset kontaktpunkti, mille vahendusel jagatakse kõikidele Eesti finantssektori osapoolte poolt tuvastatud küberintsidendid teiste osapooltega. Jagamise osas eelistatakse keskset kontaktpunkti, kes intsidendi alase teabe teistele edastab.

Omavahelisest konkurentsist tulenevalt ei soovita ennast teiste konkurentide ees haavatavana näidata, mille tulemusena saab keskne kontaktpunkt küberolukorrateadlikkuse teistele edastamisel sellteabe päritolu anonüümseks muuta. Osad eksperdid tõid esile ka jagatava informatsiooni tundlikkuse, mille tulemusena on selle jagamine ilma otsese aluseta kolmandate osapooltega keeruline.

/..Piiravaks siinkohal saaks kindlasti pankade poolt sisendi andmine, kuna üldjuhul on igasugune info konfidentsiaalne, mistõttu peaks peamine info tulema just riikliku organisatsiooni poolt/ E3

Küberolukorrateadlikkuse jagamise aspektist uuriti osapooltelt, millised koostööformaadid on kasutusel ja millist teavet peamiselt jagatakse. Tulenevalt regulatsioonist jagatakse küberintsidendi teavet CERT ja teiste osapoolte vahel (n Finantsinspektsioon). Koostöökokkulepetena mainiti ka „peer-to-peer" koostöö tegemise formaati ja lepingulisi suhteid küberolukorrateadlikkuse teenusepakkujatega. Kõik teoorias käsitletud koostöö mudelid on pankades suuremal ja vähemal määral kasutuses (vt joonis 3). Küberolukorrateadlikkuse jagamise osas uuriti ka Eesti keskselt reguleerimise või koostöökokkuleppe vajadust. Üldine arvamus oli, et läbi intsidentidest teavitamise on valdkond juba piisavalt reguleeritud nii finantssektori kui ka riigi tasandil. Ekspertidelt küsiti ka Eesti finantssektori ülese küberolukorrateadlikkuse keskuse loomise vajadust, mida võiks Pangaliit, Eesti Pank, Finantsinspektsioon hallata. Suurem osa vastanutest on arvamusel, et CERT-EE teavitamise kõrvale Eesti siseselt konkureeriva kanali loomine ei ole otstarbekas. Lisaks toodi esile, et Euroopas ja ülemaailmselt on erinevaid küberolukorrateadlikkuse teenuse pakkujaid, kellelt vajadusel teadlikkust hankida. Kõik vastanutest juba hangivad erinevatest kanalitest teavet küberolukorrateadlikkuse loomiseks. Hangitakse küberolukorrateadlikkust teenusepakkujatelt, partnerorganisatsioonidest, välistest vabalt kättesaadavatest allikatest (OSINT- open source intelligence), CERT teavitused ja arvamusliidritelt. Kõige rohkem mainiti erinevate riikide CERT-e, kellelt saadakse teadlikkust küberohtudest. Osad intervjueeritavad mainisid ka CERT-EE igapäevaseid avalike allikate kokkuvõtete kasutamist. CERT-EE teadete osas toodi välja, et need peegeldavad eelmise päeva avalikest kanalitest kajastatud teavet, mille tulemusena on teave üldjuhul juba eelnevalt olemas. Samas võib CERT-EE kokkuvõte esile tuua midagi uut või enda poolt kogutud teabe osas midagi märkamatuks jäävat. CERT-EE teated on abiks, kui ise avalikke allikaid läbi ei jõua töödelda.

Küberolukorrateadlikkuse peamise rakendamise vajadusena toodi esile küberruumist tulenevate riskide maandamine, mis aitab teha õigeaegselt otsuseid küberintsidentide ennetamiseks, tuvastamiseks, intsidendile reageerimiseks ja taastumiseks. Teabe vajaduste osas toodi esile finantsteenuseid või finantstehnoloogiat puudutava ohuteabe järele, mis aitab kahtlustele ja intsidentidele reageerida. Näiteks Eestis ühe panga poolt tuvastatud pangaautomaatide vastase ründe alase teabe jagamine teiste osapooltega, mille osas saavad teised kontrollida ja kasutusele võtta vastumeetmed riski maandamiseks. Kõige rohkem käsitleti küberolukorrateadlikkuse rakendamist riskijuhtimise

Teabe spektri osas soovitakse hoida seda võimalikult laiahaardelisena, mille hulgast võib leida enda jaoks olulise infokillu. Samuti annab see laiema pildi ümbritsevast, näiteks milliseid tehnikaid rünnakutes kasutatakse, millist tehnoloogiat rünnatakse, millised on käimasolevad ründekampaaniad jne. Küberolukorrateadlikkuse tähtsuse osas toodi esile IoC ja TTP, mis võimaldavad proaktiivselt reageerida sealt saadud teadlikkusele. Esimene neist annab teadlikkust kompromiteerimise kohta. Teine jällegi teadlikkust taktikatest, tehnikatest ja protseduuridest ründevektori ennetamiseks, tuvastamiseks ja tõrjumiseks. Mõlema puhul on tegemist rakendatava (actionable) teadlikkusega, mille põhjal saab ennetada, kontrollida ja tuvastamisel reageerida ründe tõrjumisel ning süsteemi.

/Kõige tähtsam on tehnoloogiline osa, üldine teadmine et krüptoviirused levivad ei ole huvitav, aga saada teada selle kohta, et seda organisatsiooni häkiti ja kasutati sellist tehnoloogiat ja sellises versioonis, ja ründevektor oli SMB jne, see võimaldab sul aru saada, kas rünnak võib mõjutada sinu organisatsiooni../ /..häkkimisi juhtub kogu aeg, mis suuremal või väiksemal määral ei oma tähtsust, mis omab tähtsust on see, mis mustrit see ründes kasutab/ E6.

Uuriti ka küberolukorrateadlikkuse formaatide (STIX, TAXII jt), teadlikkuse haldamise ja jagamist toetavate infosüsteemide kasutamise kohta (n MISP), kuid nende kasutamist kinnitasid üksikud. Pankade poolt teavitatakse peamiselt küberintsidentidest, milleks kasutatakse kokkulepitud kanalitena e-posti teenust või intsidentidest teavitamise portaali. Finantsinspektsioonile intsidendist teatamisel lähtutakse Euroopa Pangandusjärelevalve suunises olulistest intsidentidest direktiivi (EL) 2015/2366 kohaselt teatamise kohta toodud vormist. CERT-EE teavitamisel lähtutakse Euroopa Pangandusjärelevalve kehtestatud vormist või Küberturvalisuse seaduse §8 kohaselt. Intsidendist teatamise puhul koostatakse

raport manuaalselt, mis toob kaasa teatud hilinemisi teavitamisel. Intsidendi raportid edastatakse kas e-posti või vastava portaali vahendusel.

2.3.2. Küberolukorrateadlikkuse ekspertintervjuude järeldused

Esimesele uurimisküsimus, milline on parim eestikeelne vaste inglisekeelsele terminile „cyber threat intelligence“, pakuti eestikeelsete vastetena „(küber)ohuluure“, „küberohuteadlikkus“, „küberolukorrateadlikkus“, „küberolukorrapilt“. Autori poolt esialgu pakutud termini vastet „küberohu teadlikkus“ tõlgendati pigem üldise kasutajate küberohuteadlikkuse tõstmisena, millest tulenevalt oli soovitus leida terminile täpsem vaste. Intervjuude põhjal ei selgunud üheselt käsitlevat eestikeelset termini vastet.

Alampeatükis 3.2.1. „Küberolukorrateadlikkuse loomiseks kogutavad andmed“ kasutatakse küberolukorrateadlikkuse loomiseks võimalikult laia spektriga andmeid. Alampeatükis 3.2.2. „Küberolukorrateadlikkuse loomise formaat“ kasutatakse intsidentidest teavitamisel regulatsiooniga ette antud raporteid ja vorme. Küberolukorrateadlikkuse jagamiseks eraldi formaati kokku lepitud ei ole. Organisatsiooni siseselt jagatakse teadlikkust erinevas vormingus (raportid, e-mail, teadlikkuse tõstmise koolitused jt). Alampeatükis 3.2.3. „Küberolukorrateadlikkuse loomise ja rakendamise eesmärgid“ nimetati kõige rohkem küberolukorrateadlikkuse rakendamist küberohtude tuvastamisel ja tõrjumisel, riskide hindamisel, otsuste tegemisel. Alampeatükis 3.2.4. „Küberolukorrateadlikkuse loomiseks kasutatavad allikad“ nimetati kõige rohkem avalikke allikaid. Nende kõrval CERT poolt pakutavat avalike allikate põhjal tehtud kokkuvõtteid, finantssektori põhistes gruppides jagatavat küberolukorrateadlikkust jt. Kõik intervjueeritavad kasutavad rohkem kui ühte allikat küberolukorrateadlikkuse loomiseks. Alampeatükis 3.2.5. „Küberolukorrateadlikkuse loomise protsessi osalised“ nimetati organisatsiooni väliseid partnereid, kellelt saadakse jagatavat teadlikkust (CERT, teenusepakkujad jt). Organisatsiooni siseselt vastutavad küberolukorrateadlikkuse loomise eest küberkaitse valdkonna eest vastutavad töötajad. Alampeatükis 3.2.6. „Küberolukorrateadlikkuse jagamine ja selle osalised“, nimetati mitmeid koostööpartnereid – Pangaliit, RIA (CERT-EE), teiste riikide CERT-e jt. Osad tõid

probleemina välja küberintsidentide alase teabe mittejagamist konkureerivate partnerite vahel. Põhjuseks on esiteks küberintsidendi alase teabe tundlikkus ja teiseks soov konkurendile oma nõrkuseid mitte avalikustada. Probleemi aitab vältida ühtse konkurentidest sõltumatu kontaktpunkti kasutamine, kes vajadusel saadud teadlikkuse või küberintsidendi raporti edastab anonüümseks muudetuna teistele osapooltele. Alampeatükis 3.2.7. „Küberolukorrateadlikkuse jagamise tingimused“ käsitleti finantssektori vaates juba reguleeritud küberintsidentidest teavitamist. Täpsemad küberolukorrateadlikkuse saamise ja jagamise tingimused on fikseeritud teenusepakkujatega sõlmitud koostöökokkulepetes. Teiste osapooltega ei ole eraldi küberolukorrateadlikkuse jagamise tingimusi kokku lepitud. Jagatakse küberintsidentide alast teavet, mis on juba regulatsiooniga reguleeritud. Intervjueeritavatelt uuriti nende hinnangut küberolukorrateadlikkuse jagamise tingimuste fikseerimise osas, kuid täiendavat fikseerimise vajadust ei nähtud. Peamise põhjusena toodi esiteks soov jagamist mitte üle reguleerida ja teiseks soov saada laia spektriga teavet ja mitte piiritleda seda ainult finantssektoriga.

Alampeatükis 3.2.8. „Küberolukorrateadlikkuse loomise ja rakendamise tehnilised lahendused“ jätsid osad küsimusele vastamata, tuues põhjuseks teabe tundlikkuse, mida ei soovita avalikustada. Küsimusele vastanute seas, jagunesid vastused vastavalt tehniliste lahenduste (infosüsteemide) kasutamise ja mittekasutamise vahel. Küberolukorrateadlikkuse haldamiseks kasutatavate infosüsteemide osas nimetati nii organisatsiooni siseselt kasutatavaid süsteeme kui ka teenusepakkuja poolt pakutud lahendusi. Vastajad, kes ei kasuta küberolukorrateadlikkuse haldamiseks infotehnoloogilist lahendust, haldavad seda manuaalselt. Näiteks kogutakse manuaalselt andmed allikatest kokku, mille põhjal kujundatakse teadlikkus. Küberolukorrateadlikkuse haldamiseks kasutatav infosüsteem võimaldab automatiseerida küberolukorrateadlikkuse loomise ja rakendamise protsesse. Näiteks võimaldab infosüsteem allikatest automaatselt küberolukorrateadlikkuse loomiseks andmed kokku koguda. Analüüsi hõlbustamiseks võib infosüsteem pakkuda andmete filtreerimise ja konsolideerimise võimekust, mis tõstab küberolukorrateadlikkuse loomise ja rakendamise efektiivsust. Infosüsteem võib pakkuda ka teabe või teadlikkuse prioriseerimist, mis võimaldab olulisema või kriitilisema teabe esile tõsta. Teadlikkuse jagamise automatiseerimise näiteks STIX vormingut kasutades

võimaldaks efektiivsemat teadlikkuse jagamist, vähendades ajakadusid ja inimvigu, mis kaasneksid manuaalse küberolukorrateadlikkuse haldamisega.

Viimase kokkuvõtva alampeatüki 3.2.9. „Küberolukorrateadlikkuse loomise ja rakendamise tõhustamise võimalused“ saab intervjuude põhjal järeldada, et küberolukorrateadlikkuse loomise ja rakendamise olukord organisatsioonides on hea. Küberolukorrateadlikkuse loomiseks hangitakse andmeid vähemalt ühest välisest allikast (avalikke allikaid nimetasid kõik intervjueeritavad). Küberolukorrateadlikkust rakendatakse erinevates otsustusprotsessides, mis on seotud küberohtudest tulenevate riskide maandamisega. Küberolukorrateadlikkuse jagamise osas on tänu intsidentidest teavitamise reguleerimisega kontaktpunktid loodud, mida saab kasutada ka küberolukorrateadlikkuse jagamiseks. Ühe tõhustamise võimalusena on soovitav küberolukorrateadlikkuse loomiseks ja rakendamiseks kasutusele võtta selle loomist, rakendamist ja haldamist toetav infosüsteem, mis tõstab küberolukorrateadlikkuse loomise ja rakendamise efektiivsust. Infosüsteem võimaldab paremini hallata kogutud andmeid, andes vahetut ja ilma võimalikult väheste hilinemistega ülevaadet küberohtudest, nende trende jm teabest, mis aitab tõhustada küberohtudest tulenevate riskide ennetamist, tuvastamist ja tõrjumist.

2.4. Järeldused ja ettepanekud küberolukorrateadlikkuse loomise ja rakendamise tõhustamiseks

Magistritöö esimeses, teoreetilises peatükis selgitati küberolukorrateadlikkuse loomise ja rakendamise teoreetilisi aluseid, mille tulemuste põhjal disainiti uurimisinstrumente uurimustulemuste analüüsimiseks. Magistritöö teises, empiirilises peatükis analüüsiti valdkonna dokumente (regulatsioon ja sellest tulenevad küberkaitset korraldavad dokumendid, strateegiad ja küberkaitse meetmeid käsitlevad dokumendid) ja ekspertintervjuude tulemusi, et välja selgitada küberolukorrateadlikkuse loomise ja rakendamise üldtunnustatud aluseid, organisatsioonide küberolukorrateadlikkuse loomise ja rakendamise seis, vajadused ja küberolukorrateadlikkuse loomise ning rakendamise tõhustamise võimalused. Tulenevalt inglisekeelsele termini „cyber threat intelligence“

eestikeelse ühtse vaste puudumisega, analüüsiti termini võimalikke eestikeelseid tõlgendusi, et leida inglisekeelsele terminile parim eestikeelne vaste.

Termini käsitlusest tulenevalt on püstitatud ka **esimene uurimisküsimus**, milline on parim eestikeelne vaste inglisekeelsele terminile „cyber threat intelligence“, millele vastuse saamiseks konsulteeriti kõigepealt akadeemikute ja Kaitseministeeriumi terminoloogia komisjoni liikmega. Selle tulemusena kasutati esilagu eestikeelse terminina „küberohu teadlikkus“, mis otsetõlkes oleks olnud kõige lähem tõlgendus inglisekeelsele terminile. Terminit testiti küberkaitse ekspertide peal intervjuude käigus (käesolev töö lk 53-54), mille käigus selgus, et terminit „küberohu teadlikkus“ tõlgendati pigem küberhügieeni või üldises teadlikkuse tõstmise võtmes. Ekspertide seas pakuti erinevaid termini käsitlusi, näiteks „(küber)ohuluure“, „küberolukorrapilt“, „küberolukorrateadlikkus“. Küberolukorrapildi kasutamine viitab pigem valminud küberolukorrateadlikkuse serveerimise formaadile, ehk pildi näol kuvamine. Pakutud eestikeelsetest terminitest on kõige täpsemad vasted „(küber)ohuluure teave“ ja „küberolukorrateadlikkus“. Luure terminit toetab teoorias käsitletud erinevad luure käsitlused (OSINT, SIGINT, TECHINT jt), millest küberohuluure oleks üks domeenidest. Ohuluureteabe termini käsitlust tuvastati dokumendianalüüsi käigus Euroopa Pangandusjärelevalve suuniste inglisekeelsest teksti tõlke eestikeelses dokumendis (EBA, 2018. lk 12). Luuret käsitletakse pigem varjatud informatsiooni kogumise ja selle analüüsimisena, ehk termini kasutamise vastu räägib varjatud tegevus, millega tegelevad eelkõige luurega tegelevad asutused (Juurvee, 2018). Küberolukorrateadlikkuse termini käsitlust toetab teoorias ja dokumendianalüüsis põhjal tuvastatud termini tõlgendus, mille põhjal moodustub teadlikkus küberohuteabe koondamise, transformeerimise, analüüsimise, tõlgendamise või täiustamise tulemusena, et pakkuda otsustusprotsessidele vajalikku konteksti. Küberolukorrateadlikkus on osa olukorrateadlikkusest, mida tõlgendatakse kui võimet läbi küberolukorrateadlikkuse protsessi tuvastada ja mõista potentsiaalseid kahjulikke sündmuseid ning kasutusele võtta meetmeid riski leevendamiseks. Käesolevas töös otsustati termini „küberolukorrateadlikkuse“ kasuks.

Teisele uurimisküsimusele, milleks on saada vastus küberolukorrateadlikkuse üldtunnustatud alustele, leiti vastused küberolukorrateadlikkuse teoreetilise, dokumendianalüüsi ja intervjuude põhjal. Küberohuteadlikkust tõlgendatakse kui otsustamisprotsessi kasutatavat konteksti, mis on saadud küberohuteabe koondamise,

transformeerimise, analüüsimise, tõlgendamise või täiustamise tulemusena. Küberolukorrateadlikkus on osa olukorrateadlikkusest, mida tõlgendatakse kui võimet läbi küberolukorrateadlikkuse protsessi tuvastada ja mõista potentsiaalseid kahjulikke sündmuseid ning kasutusele võtta meetmeid riski leevendamiseks (CPMI & IOSCO, 2016; ECB, 2018). Küberolukorrateadlikkuse konteksti loomiseks analüüsiti teoreetilises käsitluses, dokumendianalüüsis ja intervjuudes teavet, mis on sisendiks küberolukorrateadlikkuse loomisele ja rakendamisele. Teooria, dokumendianalüüsi ja intervjuude põhjal analüüsiti küberolukorrateadlikkuse loomise protsessi ja rakendamise võimalusi. Küberolukorrateadlikkuse loomiseks kasutatav teave sisaldab endas peamiselt informatsiooni küberruumi ohtudest, ohu trendidest, ründajast, ründaja võimekusest, ründes kasutatavatest vahenditest, taktikaid, tehnikaid ja protseduure, kompromiteerimise indikaatoreid jm informatsioon, mis aitab ennetada, tuvastada ja tõrjuda küberruumist tulenevaid ohte. Intervjuude põhjal kinnitasid eksperdid, et küberohtudes tulenevate riskide maandamiseks soovitakse Küberohutrendide kaardistamiseks kõrvutati ENISA küberohtu trendide aastaraportite tulemused, mille tulemusena kaardistati 16 küberohtu koos nende trendide dünaamikaga aastate lõikes (vt käesolev töö lk 17 tabel 1). Küberolukorrateadlikkuse loomise protsessi analüüsi põhjal moodustati küberolukorrateadlikkuse loomist ja rakendamist kirjeldav lihtsustatud mudel (vt käesolev töö lk 25 joonis 4). Küberolukorrateadlikkuse teoreetilises käsitluses ja dokumendianalüüsis tuvastati, et küberolukorrateadlikkus on osa olukorrateadlikkusest, mida tõlgendatakse kui võimet läbi küberolukorrateadlikkuse protsessi tuvastada ja mõista potentsiaalseid kahjulikke sündmuseid ning kasutusele võtta meetmeid riski leevendamiseks (käesolev töö lk 30-33, 48-50). Küberkerksuse raamistiku komponente eraldi analüüsides, aitab küberolukorrateadlikkuse rakendamine komponentide otsustusprotsessides efektiivsemalt ennetada, tuvastada, tõrjuda ning taastuda küberruumist tulenevatest ohtudest (käesolev töö lk 48-50).

Kolmandale uurimisküsimusele, milline on organisatsioonide küberolukorrateadlikkuse loomise ja rakendamise seis, saadi vastus intervjuude ja dokumendianalüüsi tulemusena. Intervjueeritavatelt koguti andmeid organisatsioonis küberolukorrateadlikkuse loomiseks kasutatavatest andmetest, küberolukorrateadlikkuse loomise formaadist, eesmärgid, allikad, loomise protsessis osalejad, küberolukorrateadlikkuse jagamine ja selle osalised, jagamise tingimused, küberolukorrateadlikkuse loomise ja rakendamise tehnilised

lahendused. Kogutud andmete põhjal järeldus, et elutähtsat makse- ja sularaharingluse teenust pakkuvate ettevõtete ja Riigi Infosüsteemi Ameti küberolukorrateadlikkuse loomise ja rakendamise seis on hea. Kõik osapooled koguvad andmeid vähemalt ühest allikast, mida kasutatakse küberolukorrateadlikkuse loomiseks. Formaadina esitatakse küberolukorrateadlikkust peamiselt raportitena, mis luuakse käsitsi (manuaalselt), tehnilisi lahendusi kasutades või juba valmis kujul saaduna. Küberolukorrateadlikkuse jagamise osas kasutatakse samu kontakte, mis on regulatsiooni põhjal intsidentidest teavitamiseks kokku lepitud. Dokumendianalüüsist selgus, et Euroopa Pangandusjärelevalve, Euroopa Keskpanga, Rahvusvaheliste Arvelduste Panga ja Rahvusvahelise Väärtpaberiarvelduste Organisatsiooni poolt on koostatud mitmed nõuded ja soovituslikud juhendid finantssektorile, mis soodustavad küberolukorrateadlikkuse rakendamist (näiteks läbi küberkerksuse raamistiku rakendamise). Tuginedes eelnevale ja Euroopa Liidu küberjulgeoleku strateegiale, on ettepanek võtta üle küberkerksuse raamistik ka Eesti küberturvalisuse seaduse küberturvalisuse tagamise turvameetmete ja riskianalüüsi protsessides.

Neljandale uurimisküsimusele, millised on organisatsioonide küberolukorrateadlikkuse loomise ja rakendamise vajadused, leiti vastus küsimusele ekspertintervjuude ja dokumendianalüüsi käigus. Küberolukorrateadlikkuse peamise rakendamise vajadusena toodi esile küberruumist tulenevate riskide maandamine, mis aitab teha õigeaegselt otsuseid küberohust tuleneva mõju ennetamiseks, tuvastamiseks, reageerimiseks ja taastumiseks. Näiteks nimetati teavet kompromiteerimise identifikaatoritest, ründe taktikatest, tehnikatest ja protseduuridest, mis võimaldab proaktiivselt reageerida küberohutele. Teabe spektri osas soovitakse hoida seda võimalikult laiahaardelisena, mille hulgast võib leida enda jaoks olulise infokillu. Samuti annab see laiema pildi ümbritsevast, näiteks milliseid tehnikaid rünnakutes kasutatakse, millist tehnoloogiat rünnatakse, millised on käimasolevad ründekampaaniad jne. (käesolev töö lk 55-56). Teadlikkuse jagamise osas toodi probleemina välja küberintsidentide alase teabe mittejagamist konkureerivate partnerite vahel. Põhjuseks on esiteks küberintsidendi alase teabe tundlikkus ja teiseks soov konkurendile oma nõrkuseid mitte avalikustada. Probleemi aitab vältida ühtse konkurentidest sõltumatu kontaktpunkti kasutamine, kes vajadusel saadud teadlikkuse või küberintsidendi raporti edastab anonüümseks muudetuna teistele osapooltele (näiteks CERT-EE vahendusel). Teiste partneritena nimetati ka Pangaliitu ja

teiste riikide CERT-e, kuid täiendava teavitamise kanali kokkuleppimine ei ole leidnud põhjendamist. Küberolukorrateadlikkuse jagamise ja haldamise tõhustamiseks on ettepanek kasutusele võtta küberolukorrateadlikkuse loomist, haldamist ja jagamist toetav infosüsteem (käesolev töö lk 56). Dokumendianalüüsist tulenesid mitmed küberolukorrateadlikkuse loomise ja rakendamise tõhustamise võimalused (vt käesoleva töö lk 43). Nimekirjast võimaldab küberründe stsenaariumi põhine testimine kõige täpsemalt tuvastada organisatsiooni nõrkuseid ja tõhustamise vajadusi. Sellest lähtuvalt on kolmas ettepanek elutähtsat makseteenust ja sularaharingluse pakkuvatel organisatsioonidel viia läbi küberründe stsenaariumi põhine test, millega tuvastatakse .

Viiendale uurimisküsimusele, kuidas tõhustada küberolukorrateadlikkuse loomist ja rakendamist, toetub magistritöö autor teisele, kolmandale ja neljandale uurimisküsimuste järeldustele ja ettepanekutele. Kõik ettepanekud koondati tabelisse 5, mis on suunatud küberolukorrateadlikkuse tõhustamiseks Majandus- ja Kommunikatsiooniministeeriumile, CERT-EE-le ning elutähtsat makseteenust ja sularaharinglust pakkuvatele ettevõtetele rakendamiseks.

Tabel 5. Ettepanekud küberolukorrateadlikkuse tõhustamiseks (autori koostatud)

Nr	Ettepanek
1.	Täienda õiguslikku raamistikku selliselt, et see tagaks küberkerksuse raamistiku rakendamist elutähtsat makseteenust ja sularaharinglust pakkuvates ettevõtetes.
2.	Tõhustada elutähtsat makseteenust ja sularaharinglust pakkuvate ettevõtete vahelist teadlikkuse jagamist, võttes kas lokaalselt või tsentraalselt kasutusele küberolukorrateadlikkuse loomist, haldamist ja jagamist toetav infosüsteem.
3.	Viia läbi küberründe stsenaariumi põhiseid teste elutähtsat makseteenust ja sularaharinglust pakkuvate ettevõtete küberkaitse (sh küberolukorrateadlikkuse) efektiivsuse hindamiseks.

KOKKUVÕTE

Tulenevat sellest, et finantssektor on küberkurjategijate peamiseid sihtmärke, mille taga ei ole ainult motiveeritud ja hästi ettevalmistunud ründajad, vaid ka riiklikult toetatud, uudsete ründevahendite ja oskustega varustatud rühmitused, otsiti magistritöös vastust **uurimisprobleemile**: kuidas tõhustada küberolukorrateadlikkuse loomist ja rakendamist kriitilist finantsteenust pakkuvates organisatsioonides. Magistritöö **aktuaalsus** tuleneb muutunud küberruumi olukorrapildist, kus finantssektori vastu on sagenenud kõrgetasemelised ründed, millega tekitatakse finantssektorile ja selle läbi majandusele olulist kahju.

Uurimisprobleemi aitavad lahendada käesolevas töös püstitatud **viis uurimisküsimust**, millele vastamist toetavad teooria sünteesist, dokumendianalüüsist ja ekspertintervjuude tulenevad järeldused. Magistritöö **eesmärgiks** on välja selgitada küberolukorrateadlikkuse loomise ja rakendamise tõhustamise võimalused, sh inglisekeelse termini „cyber threat intelligence“ parim eestikeelne vaste, mis iseloomustaks kõige täpsemalt termini taga olevat kontseptsiooni. Eesmärgi saavutamist toetasid käesolevas töös püstitatud neli uurimisülesannet. Töös püstitatud eesmärgi saavutamiseks vastati uurimisprobleemile ja seda toetavatele uurimisküsimustele ning lahendati uurimisülesanded.

Esimene uurimisülesanne seisnes inglisekeelse termini „cyber threat intelligence“ parima eestikeelse vaste leidmises, milleks praeguste teadmiste juures kujunesid kaks konkureerivat terminit- „küberolukorrateadlikkus“ ja „(küber)ohuluure teave“. Käesolevas töös otsustati kasutada eestikeelse terminina „küberolukorrateadlikkust“.

Teine uurimisülesanne seisnes küberolukorrateadlikkuse loomise ja rakendamisega seotud dokumentide analüüsimisel. Dokumentide valimi moodustasid finantssektori küberkaitset reguleerivad ja juhendavad dokumendid, Eesti ja Euroopa Liidu strateegiad, küberkaitsemeetmeid käsitlevad standardid ja kataloog. Valimisse kuulunud dokumentide analüüsimise kaudu leidis autor vastused kõikidele viiele uurimisküsimustele.

Kolmas uurimisülesanne seisnes organisatsioonide küberolukorrateadlikkuse loomise ja rakendamise analüüsimisel ja organisatsioonide küberolukorrateadlikkuse loomise ja rakendamise vajaduste väljaselgitamisel. Ekspertintervjuude põhjal selgus, et küberolukorrateadlikkuse loomise ja rakendamise seis elutähtsat makseteenust ja

sularaharinglust ettevõtetes ning Riigi Infosüsteemi Ametis on hea. Kõik osapooled koguvad küberolukorrateadlikkuse loomiseks ja rakendamiseks andmeid vähemalt ühest kanalist (kõik osapooled nimetasid avalike allikate kasutamist). Loodud küberolukorrateadlikkust rakendatakse erinevate juhtimistasandite otsuste tegemises. Peamiste küberolukorrateadlikkuse loomise ja rakendamis vajadustena toodi esile küberruumist tulenevate riskide maandamine, mis aitab teha õigeaegselt otsuseid küberohust tuleneva mõju ennetamiseks, tuvastamiseks, reageerimiseks ja taastumiseks. Küberolukorrateadlikkuse saamise ja jagamise osas nimetati kompromiteerimise identifikaatorite ja ründe taktikate, tehnikate ning protseduuride kohta käva teabe tähtsust, mida saab rakendada küberohtudest tulenevate riskide maandamiseks. Organisatsioonid tõid esile küberolukorrateadlikkuse jagamise vajaduse. Peamise aspektina toodi välja CERT ja osapoolte vahelise küberolukorrateadlikkuse saamise ja jagamise vajadused. Ekspertidelt uuriti ka finantssektori spetsiifilise küberolukorrateadlikkuse jagamise võrgustiku loomist, kuid enamus ei pidanud seda oluliseks põhjendusega, et neid koostöövorme on juba praegu palju (n Pangaliit, CERT vahendusel, teenuse pakkujad, finantssektori skoobiga grupid jt).

Neljas uurimisülesanne seisnes küberolukorrateadlikkuse teoreetilise käsitluse ja empiirilise uuringu tulemuste analüüsis, mille põhjal esitati dokumendianalüüsis tuvastatud 9-st tõhustamise võimalusest 3 ettepanekut küberolukorrateadlikkuse loomise ja rakendamise tõhustamiseks, mis on suunatud elutähtsat makseteenust ja sularaharinglust pakkuvatele ettevõtetele, Majandus- ja Kommunikatsiooniministeeriumile rakendamiseks. Riigi Infosüsteemi Ameti küberintsidentide käsitlemise üksusel CERT-EE soovitan kaaluda tsentraalse vajalike osapooltega jagatava küberolukorrateadlikkuse infosüsteemi rakendamist.

Magistritöö tulemusi on võimalik laiemalt rakendada Eesti makseteenuse pakkujatele (Pangaliidu kohaselt lisaks neljale elutähtsa makseteenuse ja sularaharingluse teenusepakkujale veel kaheksale makseteenuse pakkujale). Magistritöö teemat tuleks küberolukorrateadlikkuse loomise ja rakendamise osas **edasi uurida,** et välja selgitada teiste elutähtsate teenusepakkujate küberolukorrateadlikkuse vajadusi.

SUMMARY

The title of the Master's thesis is „Cyber threat intelligence and it's strengthen possibilities at the example of critical financial service providers". The objective of the thesis was to determine the directions for improving cyber threat intelligence in and between critical financial service providers.

Four-research task were set for achieving the objective of the thesis:

1. To determine term „cyber threat intelligence" equivalent in Estonian language.
2. To analyze the documents of cyber threat intelligence creation and implementation.
3. To analyze organizations needs for cyber threat intelligence creation and implementation.
4. To analyze theory and the outcomes of empirical research and present implementable improvements proposal for cyber threat intelligence in financial sector.

The thesis was designed within the framework of case study research strategy and consists of two chapters. First, theoretical chapter analyzed theoretical aspect for cyber threat intelligence creation and implementation. The conclusions made in the first chapter were used for designing the empirical research. In the second, document analysis, and semi-structured interviews were used as methods for data collection. The content of eleven documents and six semi-structured interviews were analyzed by the author for reaching the objective of the thesis. The method of analysis used was qualitative content analysis and it was conducted using qualitative data analysis software NVivo 12 Pro.

Based on the results of the research the author achieved the goal and proposed three recommendation on how to strengthen cyber threat intelligence creation and implementation based on Estonian critical financial service providers. The set research tasks were accomplished and the objective of the thesis was achieved.

KASUTATUD ALLIKATE LOETELU

Akinrolabu, O., Agrafiotis, I. & Erola, A., 2017. *The challenge of detecting sophisticated attacks:Insights from SOC Analysts.* Washington DC: Conference'17.

Ask, M. et al., 2014. *Advanced persistent threat (APT) beyond the hype,* GjoviN : Project Report in IMT4582 Network Security at GjoviN University College.

Athias, J., 2015. *Cyber Threat Intelligence Sharing Standards,* Abu Dhabi: RSA Conference 2015.

Avaliku teabe seadus (2019) RT I, 15.03.2019, 11.

Babbie, E., 2013. *The Practice of Social Research.* 13th ed. Canada: Wadsworth Cengage Learning.

Barford, P. et al., 2010. *Cyber SA: Situational Awareness for Cyber Defense. Cyber Situational Awareness.* s.l.:s.n.

Barnum, S., 2014. *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™).* Bedford: MITRE Corporation.

Berghel, H., 2017. *Equifax and the Latest Round of Identity Theft Roulette. Computer,* 50(12), pp. 72-76.

Björck, F., Henkel, M., Stirna, J. & Zdravkovic, J., 2015. *Cyber Resilience – fundamentals for a definition.* Stocholm: Springer.

Black Hat USA, 2018. *Where Cybersecurity Stands.* [Võrgumaterjal] Leitav: https://www.blackhat.com/docs/us-18/black-hat-intel-where-cybersecurity-stands.pdf
[Kasutatud 3. 02. 2019].

Borrello, P., Coppa, E., Cono D'Eli, D. & Demetrescu, C., 2019. *The ROP Needle: Hiding Trigger-based Injection Vectors via Code Reuse,* Rome: Sapienza University of Rome.

Boukhtouta, A., 2016. *On the Generation of Cyber Threat Intelligence: Malware and Network Traffic Analyses.* Montréal: Concordia University.

Bromiley, M., 2016. *Threat Intelligence: What It Is, and How to Use It Effectively.* [Võrgumaterjal]
Leitav: https://www.sans.org/reading-room/whitepapers/analyst/threat-intelligence-is-effectively-37282
[Kasutatud 19. 09. 2017].

Brown, G. A., 2009. *Document Analysis as a Qualitative Research Method.* vol 9 no 2. s.l.:Qualitative Research Journal.

Buck, P., Disso, D. J. P. & Densham, B., 2016. *Threat Advisory SWIFT Banking.* s.l.:Nettitude.

Carter, W.A. and Zheng, D.E., 2015. *The Evolution of Cybersecurity Requirements for the US Financial Industry.* Center for Strategic and International Studies.

CEPS-ECRI, 2018. *Cybersecurity in Finance, Getting the policy mix right.* Brüssel: CEPS.

Chen, P., Desmet, L. & Huygens, C., 2014. A Study on Advanced Persistent Threats. Rmt: *IFIP International Conference on Communications and Multimedia Security.* Berlin: Springer, pp. 63-72.

Chismon, D. & Ruks, M., 2015. *Threat Intelligence: Collecting, Analysing, Evaluating.* London: MWR InfoSecurity.

Cole, D. E., 2013. *Advanced Persistent Threat, Undrestanding the Danger and How to Protect Your Organisation.* USA, Waltham: Syngress.

CPMI & IOSCO, 2016. *Guidance on cyber resilience for financial market infrastructures.* [Võrgumaterjal]
Leitav: https://www.bis.org/cpmi/publ/d146.pdf
[Kasutatud 19. 04. 2017].

Cunningham, T., 2015. *A Cyber-Threat Intelligence Program-How to develop one and why it matters.* Luleå: Luleå University of Technology.

Cybernetica, 2019a. Fotoluure. *Andmekaitse ja infoturbe leksikon.* [Võrgumaterjal]
Leitav: https://akit.cyber.ee/term/1679
[Kasutatud 19. 04. 2019].

Cybernetica, 2019b. Inimluure. *Andmekaitse ja infoturbe leksikon.* [Võrgumaterjal]
Leitav: https://akit.cyber.ee/term/1685
[Kasutatud 19. 04. 2019].

Cybernetica, 2019c. Leheluure. *Andmekaitse ja infoturbe leksikon.* [Võrgumaterjal]
Leitav: https://akit.cyber.ee/term/1145
[Kasutatud 19. 04. 2019].

Cybernetica, 2019d. Küberruum. *Andmekaitse ja infoturbe leksikon.* [Võrgumaterjal]
Leitav: https://akit.cyber.ee/term/568-kuberruum
[Kasutatud 09. 04. 2019].

Cybernetica, 2019f. Signaaliluure. *Andmekaitse ja infoturbe leksikon.* [Võrgumaterjal]
Leitav: https://akit.cyber.ee/term/1664
[Kasutatud 19. 04. 2019].

Cybernetica, 2019g. SQL süst. *Andmekaitse ja infoturbe leksikon.* [Võrgumaterjal]
Leitav: https://akit.cyber.ee/term/1407-sql-injection
[Kasutatud 19. 04. 2019].

Cybernetica, 2019h. Tehniline luureteave. *Andmekaitse ja infoturbe leksikon.*
[Võrgumaterjal]
Leitav: https://akit.cyber.ee/term/1702
[Kasutatud 19. 04. 2019].

Dalziel, H., 2015. *How to Define and Build an Effective Cyber Threat Intelligence Capability.* s.l.:s.n.

Davidson, M. & Schmidt, C., 2014. *TAXII Overview.* 1.1 toim. Virginia: MITRE.

Department of Homeland Security, U., 2011. *Blueprint for a Secure Cyber Future.* Washington DC:Homeland Security.

Dulaunoy, A., 2017. *CTI and Automation,* Athena: ENISA.

EBA, 2018. *Suunised direktiivi (EL) 2015/2366 (PSD2) alusel makseteenuste operatsiooni- ja turvariskide jaoks kasutatavate turvameetmete kohta*. [Võrgumaterjal] Leitav: https://eba.europa.eu/documents/10180/2081899/Guidelines+on+the+security+measures+under+PSD2+%28EBA-GL-2017-17%29_ET.pdf/4a7ba8d0-f0b3-4a7f-aca4-5652e46f711a [Kasutatud 24. 04. 2019].

ECB, 2018. *Cyber resilience oversight expectations for financial market infrastructures.* Frankfurt: European Central Bank.

ECB, 2019. *Cyber resilience and financial market infrastructures.* [Võrgumaterjal] Leitav: https://www.ecb.europa.eu/paym/cyber-resilience/fmi/html/index.en.html [Kasutatud 18. 02. 2019].

Eesti Panga President, 2019. *Makseteenuse ja sularaharingluse kirjeldus ja toimepidevuse nõuded. Määrus. RT I, 05.03.2019, 21.*

Eesti Pank, 2019. *Järelevaadatavad süsteemid.* [Võrgumaterjal] Leitav: https://www.eestipank.ee/maksed-arveldused/jarelevaadatavad-susteemid [Kasutatud 24. 04. 2019].

Eesti Standardikeskus, 2017. *Infotehnoloogia – Turbemeetodid – Infoturbemeetodite turvakoodeks. EVS-ISO/IEC 27002:2017,* Tallinn:Eesti Standardikeskus.

Eesti Standardikeskus, 2018. *Infotehnoloogia – Turbemeetodid – Küberturbe juhised. EVS-ISO/IEC 27032:2018,* Tallinn:Eesti Standardikeskus.

EKSS, 2019. Teadmus. *Eesti keele seletav sõnaraamat* [Võrgumaterjal] Leitav: http://eki.ee/dict/ekss/index.cgi?Q=teadmus [Kasutatud 19. 04. 2019].

ENISA, 2016a. *ENISA Threat Landscape 2015.* Athena: ENISA.

ENISA, 2016b. *Threat taxonomy.* [Võrgumaterjal] Leitav: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-

trends/enisa-threat-landscape/threat-taxonomy/at_download/file
[Kasutatud 12. 02. 2018].

ENISA, 2017. *ENISA Threat Landscape Report 2016.* [Võrgumaterjal] Leitav: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016 [Kasutatud 18. 09. 2017].

ENISA, 2018. *ENISA Threat Landscape Report 2017.* 1 toim. Athena: ENISA.

ENISA, 2019. *ENISA Threat Landscape Report 2018, Top Cyberthreats and Trends.* Athena: ENISA.

Euroopa Keskpank, 2014. *Määrus süsteemselt oluliste maksesüsteemide järelevaatamise kohta.(EL) nr 795/2014.*

Euroopa Komisjon, 2013. *Euroopa Liidu küberjulgeoleku strateegia: avatud, ohutu ja turvaline küberruum.* Brüssel: Euroopa Komisjon.

Euroopa Parlament ja Nõukogu, 2016a. *Meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus. Direktiiv (EL) 2016/1148.*

Euroopa Parlament ja Nõukogu, 2016b. *Füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). Määrus (EL) 2016/679.*

Farár. A. E., 2016. *Pettesüsteemi meetodi kasutamine keerukate küberrünnakute varajasel tuvastamisel.* Tallinn:Tallinna Tehnikaülikool.

Finantsinspektsioon, 2017. *Nõuded finantsjärelevalve subjekti infotehnoloogia ja infoturbe korraldusele.* Tallinn: Finantsinspektsioon.

Finantsinspektsiooni seadus (2019) RT I, 13.03.2019, 51.

Fireeye, 2014. *APT28: A Window Into Russia's Cyber Espionage Operations?,* Milpitas: Fireeye.

Flick, U., 2009. *An Introduction to Qualitative Research*. 4th ed. London: SAGE Publications.

Franke, U. & Brynielsson, J., 2014. Cyber situational awareness - A systematic review of the literature. *Computers & Security,* lk. 18-31.

Friedman, J. & Bouchard, M., 2015. *Definitive Guide to Cyber Threat Intelligence.* Annapolis: CyberEdge Group, LLC.

Gallagher, H., McMahon, W. & Morrow, R., 2014. Cyber Security: Protecting the Resilience of Canada's Financial System. *Bank of Canada Financial System Review.*

Geers, K., 2011. *Strategic Cyber Security.* Tallinn: CCD COE Publication.

Gemalto, 2018. *Breach Level Index H1 2018 Infographic.* [Võrgumaterjal] Leitav: https://safenet.gemalto.com/resources/data-protection/breach-level-index-2018-h1/
[Kasutatud 2. 02. 2019].

Gill, P. & Pythian, M., 2006. *Intelligence in an Insecure World.* Combridge: Polity Press.

Ginn, J. & Lingris, S., 2017. *CTI Information Sharing,* Roma: ENISA.

Homeland Security, 2016. *Cyber Resilience Review (CRR): NIST Cybersecurity Framework Crosswalks.* [Võrgumaterjal] Leitav: https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-nist-framework-crosswalk.pdf
[Kasutatud 2. 02. 2019].

İlker, K. & Aydos, M., 2019. The Ghost In The System: Technical Aanalysis of Remote Access Trojan. *International Journal on Information Technologies & Security,* pp. 73-84.

Ionita, M.-G. & Patriciu, V.-V., 2016. Secure Threat Information Exchange across the Internet of Things for Cyber Defense in a Fog Computing Environment. *Informatica Economică,* 20(3).

Isikuandmete kaitse seadus (2019) RT I, 04.01.2019, 11.

Johnson, C. et al., 2016. *Guide to Cyber Threat Information Sharing.* Gaithersburg: NIST.

Johnson, L. K., 2007. *Handbook of Intelligence Studies.* New York: Routledge.

Juurvee, I., 2018. *100 aastat luuret ja vastuluuret Eestis.* Tallinn: Post Factum.

Kalmus, V., Masso, A. & Linno, M., 2015. *Kvalitatiivne sisuanalüüs.* [Võrgumaterjal] Leitav: http://samm.ut.ee/kvalitatiivne-sisuanalyys [Kasutatud 21. 01. 2019].

Kopp, E., Kaffenberger, L. & Wilson, C., 2017. *Cyber Risk, Market Failures, and Financial Stability.* s.l.:International Monetary Fund.

Kornmaier, A. & Jaonen, F., 2014. Beyond technical data - a more comprehencive Situational Awareness fed by available Intelligence information. Rmt: *2014 6th International Conference on Cyber Conflict.* Tallinn: CCDCOE, pp. 139-156.

Kott, A., Wang, C. & Erbacher, R., 2015. *Cyber defense and situational awareness.* s.l.:Springer.

Küberturvalisuse seadus (2018) RT I, 22.05.2018, 1.

Laherand, M., 2008. *Kvalitatiivne uurimisviis.* Tallinn: Infotrükk.

Majandus- ja Kommunikatsiooniministeerium, 2014. *2014-2017 Küberjulgeoleku strateegia*. [Võrgumaterjal] Leitav: https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf [Kasutatud 15. 09. 2017].

Majandus- ja Kommunikatsiooniministeerium, 2018. *Küberturvalisuse strateegia 2019-2022*. [Võrgumaterjal] Leitav: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf [Kasutatud 14. 04. 2019].

Meaulen, D. et al., 2015. *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses.* [Võrgumaterjal] Leitav: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf [Kasutatud 15. 09. 2017].

MITRE, 2018. *Common Vulnerabilities and Exposures (CVE).* Virginia: MITRE.

Moore, T., 2017. On the harms arising from the Equifax data breach of 2017. *International Journal of Critical Infrastructure Protection,* pp. 47-48.

NCSC, 2018. *Cyber Security Assessment Netherlands.* Haag: The National Coordinator for Security and Counterterrorism.

Neuman, W. L., 2011. *Social Research Methods*. 7th ed. Boston: Pearson.

NIST, 2018. *Framework for Improving Critical Infrastructure Cybersecurity.* [Võrgumaterjal]
Leitav: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
[Kasutatud 20. 04. 2019].

Planque, D., 2017. *Cyber Threat Intelligence - From confusion to clarity; An investigation into Cyber Threat Intelligence.* The Hague: Cyber Security Academy.

Richards, I. & Wood, M., 2018. Hacktivists against terrorism: a cultural criminological analysis of anonymous' anti-IS campaigns. *International journal of cyber criminology*, vol. 12, no. 1, January-June, pp. 187-205.

Riigi Infosüsteemi Amet, 2018a. I*nfosüsteemide kolmeastmeline etalontubesüsteem ISKE rakendusjuhendi lisa 1: Kataloogid B,M ja H*[Võrgumaterjal] Leitav: https://iske.ria.ee/iske_portal_static/ISKE_kataloogid_8_06.pdf [Kasutatud 04. 03. 2019].

Riigi Infosüsteemi Amet, 2018b. *Küberturvalisus 2018.* Tallinn: Riigi Infosüsteemi Amet.

Riigi Infosüsteemi Amet, 2015. *Riigi Infosüsteemi ameti küberturvalisuse teenistuse 2015 aasta kokkuvõte.* Tallinn: RIA.

Riigi Infosüsteemi Amet, 2016. *Riigi Infosüsteemi Ameti küberturvalisuse teenistuse 2016. aasta kokkuvõte.* Tallinn: Riigi Infosüsteemi Amet.

Ritchie, J., Lewis, J., Nichollos, C. M. & Ormson, R., 2014. *Qualitative Research Practice.* Los Angeles, London, New Delhi, Singapore, Washington DC: Sage Publications Ltd.

Roege, P. E. et al., 2017. Bridging the gap from cyber security to resilience.. rmt:: *Resilience and Risk.* Dordrecht: Springer, pp. 383-414.

SANS, 2016. *SANS 2016 Survey on Security and Risk in the Financial Sector.* s.l.:SANS Institute.

Sauerwein, C., Sillaber, C., Mussmann, A. & Breu, R., 2017. *Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives.*. Innsbruck: University of Innsbruck, Department of Computer Science, Innsbruck, Austria.

Shackleford, D., 2015. *Who's Using Cyberthreat Intelligence and How?,* s.l.: SANS Institute.

Skopik, F., 2018. *Collaborative Cyber Threat Intelligence: detecting and responding to advanced cyber attacks at national level.* New York: CRC Press.

Steele, R. D., 2007. Open Source Intelligence. Rmt: *Handbook of Intelligence Studies.* New York: Routledge, pp. 130-147.

Storm, B. E. et al., 2017. *Finding Cyber Threats with ATT&CK™-Based Analytics.* s.l.:MITRE.

SWIFT, 2017. *Customer Security Program (CSP).* [Võrgumaterjal] Leitav: https://www.swift.com/myswift/customer-security-programme-csp#topic-tabs-menu
[Kasutatud 22. 11. 2017].

Zimmerman, C., 2014. *Ten Strategies of a World-Class - Cybersecurity Operations Center.* Bedford:The MITRE Corporation.

Vahturov, K., 2018. *Kompromiteerimise indikaatorite kasutamine küberintsidentide triaaži automatiseerimiseks. Kontseptsiooni tõendus.* Tallinn:Tallinna Tehnikaülikool.

Wagner, C., Dulaunoy, A., Wagener, G. & Iklody, A., 2016. *MISP - The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform..* s.l.:ACM.

Wang, C., Somesh Jha, M. C., Maughan, D. & Song, D., 2007. *Malware Detection.* s.l.:Springer.

Weedon, J., 2015. *Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine.* Tallinn 2015:NATO CCD COE Publications.

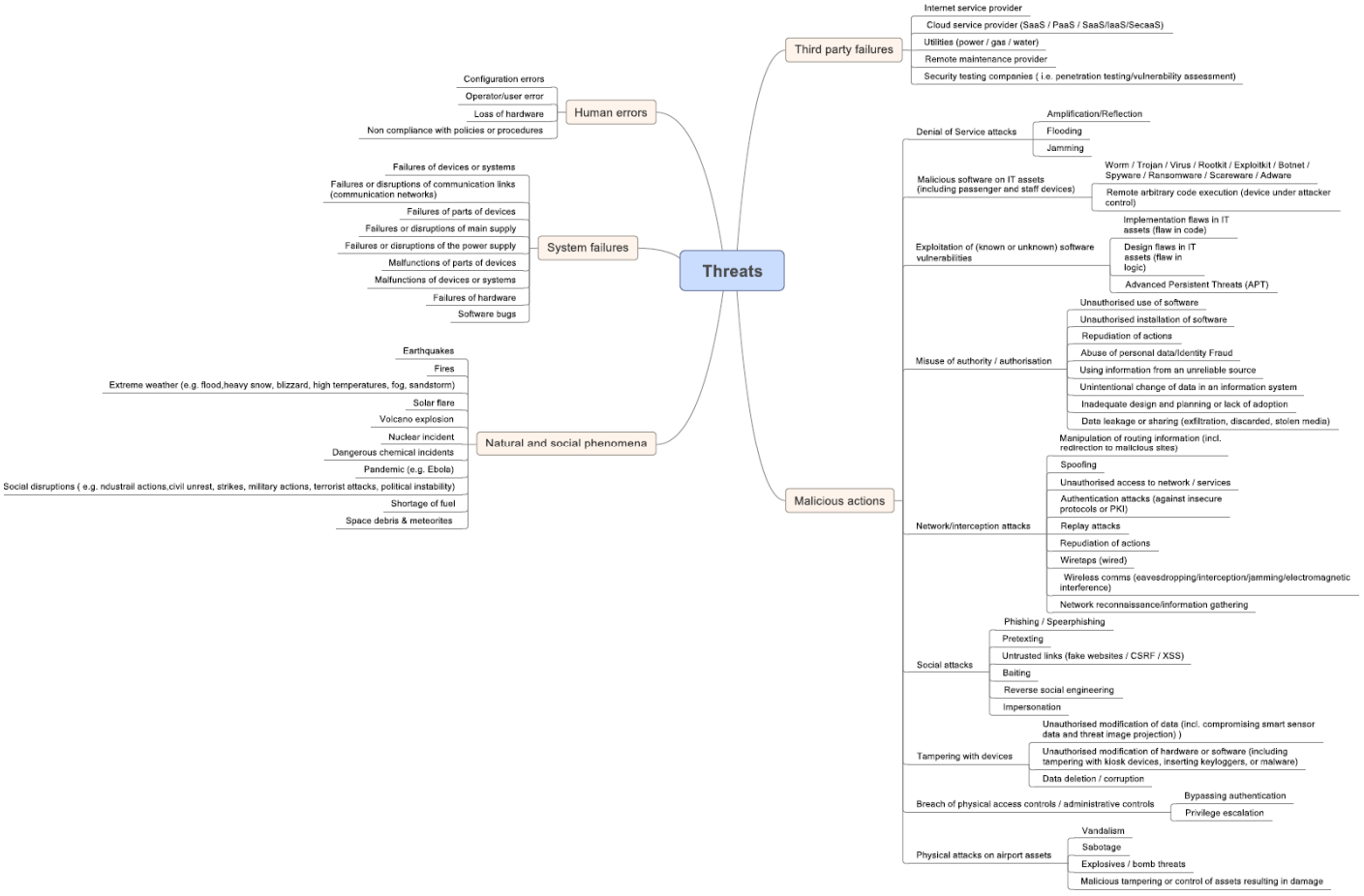
Yadav, T. & Mallari, R. A., 2016. *Technical Aspects of Cyber Kill Chain.* s.l.:Cornell University.

Yin, R. K., 2014. *Case Study Research. Design and Methods.* 5th ed. Thousand Oaks:SAGE Publications.

TABELITE JA JOONISTE LOETELU

LISAD

Lisa 1. ENISA ohtude taksonoomia mudel



Lisa 2. Ekspertintervjuude küsimused

Sissejuhatavad küsimused

1. Palun selgitage oma käsitlust terminist küberolukorrateadlikkus *(cyber threat intelligence)*?
2. Milliseid võimalusi näete küberolukorrateadlikkuse rakendamisel organisatsioonis?

Küberolukorrateadlikkuse loomine

3. Kuidas tekib küberolukorrateadlikkus organisatsioonis?
4. Milliseid allikaid kasutate küberolukorrateadlikkuse loomiseks?
5. Kuidas te hindate loodud küberolukorrateadlikkuse kvaliteeti? (detailsus, õigeaegsus, müra, muu)

Küberolukorrateadlikkuse rakendamine

6. Millistele kriteeriumitele peab küberolukorrateadlikkus vastama?
7. Milliseid ressursse ja platvorme kasutate küberolukorrateadlikkuse haldamiseks? (Inimressurss – analüütik, SOC, muu, tehnoloogiline ressurss – MISP (Malware information system platform) platvorm või teised)
8. Kuidas rakendatakse küberolukorrateadlikkust?
9. Kas teete mõne teise organisatsiooniga koostööd küberolukorrateadlikkuse saamise/jagamise osas, põhjendage?
10. Kas osapoolte vahel on kokku lepitud andmete vahetamise formaat (STIX, TAXII, Mitre At&&CK, IODEF jt)?
11. Kuidas tuleks teie hinnangul parandada finantssektori küberolukorrateadlikkuse kogumist ja jagamist?

Kas Teil on intervjuu või teemade osas täiendavaid küsimusi?

Tänan intervjuu eest!

Lisa 3. Näited küberolukorrateadlikkuse allikatest ja platvormitest

Allikas	Allika pakkuja	Kirjeldus
https://cert.europa.eu	CERT-EU	Veebilehel serveeritakse avalikest allikatest (uudistevoogudest) kogutud küberohtude teavet. Küberolukorrateadlikkuse raporteid veebilehel ei pakuta.
https://www.dni.gov/index.php/ctiic-home	Cyber Threat Intelligence Integration Center	USA küberolukorrateadlikkuse keskus,
@Bank_Security	Twitter	Finantssektorit puudutavad ohud
@CERT_EE	Twitter	CERT-EE teavitused

Küberolukorrateadlikkuse platvormid ja teenusepakkujad

Toode	Tootja	Kirjeldus
Open Threat Exchange - OTX	AlienVault	Avalik küberolukorrateadlikkuse kogukond, kus jagatakse informatsiooni käimasolevatest küberrünnetest ja ohtudest.
FireEye iSIGHT Threat Intelligence	FireEye	Portaal, milles pakutakse tellimuse põhiselt rakendatavat küberolukorrateadlikkust (Haavatavused, operatsiooniline, C-taseme teadlikkus – turvajuhtidele, globaalne olukorrateadlikkus jt)
Malware Information Sharing Platworm (MISP)	Vabavara (open source)	Vabavaraline platvorm küberolukorrateadlikkuse kogumiseks ja jagamiseks.
Cyber_reveal	BAE Systems	Platvorm, kus jagatakse küberolukorrateadlikkust, aidates suurendada ohtude tuvastust ja prioriseerida intsidentide uurimist
IBM X-Force Threat Intellience	IBM	Pilvepõhine küberolukorrateadlikkuse jagamise platvorm, aidates läbi turvasündmustele konteksti lisamise põhjuseid tuvastada,
ThreatConnect	ThreatConnect	Vaba küberolukorrateadlikkuse platvorm koos küberolukorrateadlikkuse jagamise võimalustega