Sisekaitseakadeemia
Sisejulgeoleku instituut

Saskia Kiisel

EESTI KÜBERJjulgeoleku TUGEVDAMISE VÕIMALUSED LÄBI KÜBERHEIDUTUSE: AMEERIKA ÜHENDRIIKIDE NÄITEL

Magistritöö

Juhendaja:
Lauri Luht, MA

Kaasjuhendaja:
Anne Valk, MBA

Tallinn 2018

ANNOTATSIOON

Sisejulgeoleku instituut	Kaitsmise kuu ja aasta: juuni 2018
Töö pealkiri eesti keeles: Eesti küberjulgeoleku tugevdamise võimalused läbi küberheidutuse: Ameerika Ühendriikide näitel. Töö pealkiri võõrkeeles: *Strenghtening Estonia's cyber security through cyber deterrence at the example of the United States of America*. Lühikokkuvõte: Magistritöö on kirjutatud eesti keeles, võõrkeelne resümee on inglise keeles. Töö koosneb 98 leheküljest, millest põhiosa moodustab 71 lehekülge. Töös on kasutatud 97 eesti ja ingliskeelset allikat. Töö sisaldab 8 joonist, 18 tabelit ja 3 lisa. Magistritöö eesmärk on välja selgitada, milliste küberheidutuse strateegiliste meetmetega oleks võimalik tugevdada Eesti küberjulgeolekut Ameerike Ühendriikide näitel. Töö eesmärgi saavutamiseks püstitati viis uurimisülesannet: selgitada välja Eesti ja Ameerika Ühendriikide küberjulgeoleku ohustajad; analüüsida heidutuse teooriat rahvusvahelise suhete tasandil, heidutuse definitsiooni, evolutsiooni, tingimusi ning heidutusstrateegiaid; selgitada välja Eesti ja Ameerika Ühendriikide küberjulgeolekuga seotud strateegiadokumentides kasutatud küberheidutuse meetmed; analüüsida Eesti julgeolekupoliitika kujundajate seisukohti; analüüsida dokumendianalüüsi ja eksperintervjuude tulemusi ning teha ettepanekuid Eesti küberjulgeoleku tugevdamiseks Ameerika Ühendriikide näitel. Magistritöö eesmärgi saavutamiseks ja uurimisülesannete täitmiseks kasutati uurimistrateegiana juhtumiuuringut. Magistritöö andmekogumise meetoditeks olid dokumendianalüüs, ankeetküsitlus ja poolstruktureeritud intervjuud. Kvalitatiivse sisuanalüüsi teostamiseks kasutati andmeanalüüsiprogrammi Nvivo for Mac ja NVivo 11 Pro. Magistritöö tulemusel selgusid Eesti küberjulgeoleku tugevdamise võimalused läbi küberheidutuse ning nende põhjal tegi magistritöö autor neli praktiliselt rakendatavat ettepanekut Eesti küberjulgeoleku tugevdamiseks.	
Lisad: Ei ole.	
Võtmesõnad: heidutus, julgeolekupoliitika, kaitsepoliitika, küberjulgeolek, riigikaitse, riiklik julgeolek, strateegia, küberheidutus	
Võõrkeelsed võtmesõnad: deterrence, security policy, defence policy, cyber security, national defence, strategy, national security, cyber deterrence	
Säilitamise koht: Sisekaitseakadeemia raamatukogu	
Töö autor: Saskia Kiisel 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: Lauri Luht Allkiri:	
Vastab lõputöö nõuetele Kaasjuhendaja: Anne Valk Allkiri:	
Kaitsmisele lubatud Rektor: Katri Raik Allkiri:	

SISUKORD

MÕISTETE JA LÜHENDITE LOETELU

demarš – riigi diplomaatiline väljaastumine teise vastu (surve avaldamiseks) noodi, memorandumi, protesti vms näol (Eesti Keele Instituut, 2018).

heidutus (*dēterrere*) – hirmutama ära või eemale (Bendiek & Metzger, 2015, pp. 4–5); ajendada oponenti loobuma oma kavatsus(te)st (vt käesolev töö, lk 11).

kerksus (*resilience*) – võime vastupidada ja taastuda kiirelt rünnakutest, õnnetusjuhtumitest jms sündmustest, mis takistab vaenlasel oma eesmärki saavutada (White House, 2015, pp. 5, 10, 13–14; White House, 2017, p. 13); osa tõrjuvast heidutusstrateegiast.

küberheidutus – käesoleva töö kontekstis lähtutakse laiemast tõlgendamisviisist: küberruumis leiduvad meetmeid, mis võivad vastasele mõjuda heidutavalt nii küberruumis sees kui ka teistes domeenides (vesi, maa, õhk, kosmos) ning samuti teistes domeenides leiduvad meetmed, mis võivad mõjuda heidutavalt küberdomeenis läbiviidavat või plaanitavat tegevust (vt käesolev töö, lk 17).

küberjulgeolek – käesolevas töös mõistetakse küberjulgeolekut riigis kehtiva korra, valitsemisviisi või riikliku terviklikkuse tagamist küberruumis (Majandus- ja Kommunikatsiooniministeerium, 2014b, lk 7).

küberruum – infokeskkonna globaalne piirkond, mille moodustab infosüsteemide üksteisest sõltuvate taristute võrk, millesse kuuluvad Internet, sidevõrgud, arvutisüsteemid ning sisseehitatud protsessorid ja kontrollerid (Cybernetica, 2017).

küberrünne – küberruumi kaudu sooritatav rünne, mis on suunatud küberruumi kasutamisele organisatsioonis ning püüab häirida, pärssida, hävitada või kahjustavalt valitseda andmetöötluse keskkonda või taristut, rikkuda andmete terviklust või varastada reguleeritud teavet (Cybernetica, 2018b).

küberturvalisus – ühiskonna seisund, mida iseloomustab võrgu- ja infosüsteemi kaudu avalikku korda, isikute tervist, vara ja keskkonda mõjutavate ohtude realiseerumise madal tõenäosus, võimekus ohtudele reageerida ja leevendada ohtude realiseerumisel tekitatud kahjulikku mõju ning mis tagatakse füüsiliste, organisatsiooniliste ja infotehniliste abinõude rakendamisega (Vabariigi Valitsus, 2018, lk 4).

sanktsioon – välispoliitika meede, mille eesmärk on rahu säilitamine või taastamine, konfliktide ära hoidmine, rahvusvahelise julgeoleku tugevdamine, demokraatia, õigusriigi põhimõtete ja inimõiguste toetamine ja tugevdamine või terrorismi vastu võitlemine. Rahvusvahelise sanktsiooni kehtestamise eesmärk kitsamalt on suunata kolmandaid riike või sanktsioneeritud isikuid järgima rahvusvahelise õiguse norme ja põhimõtteid, muuta sanktsioneeritud tegevuse jätkamine võimalikult kulukaks ja ebamugavaks või tõkestada sanktsioonide adressaadi vastuvõetamatut tegevust. (Välisministeerium, 2017)

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

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

SOP (*Standard Operating Procedure*) – püsitoimingud ehk juhiste kogum, mis hõlmab operatsioonide neid tunnusjooni, mille suhtes on võimalik kohaldada kindlaid või standardseid toiminguid ilma, et nende tõhusus selle all kannataks (Eesti Keele Instituut, 2017).

TTP (*Tactics, Techniques and Procedures*) – taktika, tehnika ja protseduur.

SISSEJUHATUS

Heidutus ehk vaenlase ajendamine oma kavatsustest loobuma, on iidne kontseptsioon, mille sarnaseid põhimõtteid on kasutatud riigivalitsemises pragmaatilisest tarkusest, elukogemusest ja intuitsioonist lähtuvalt. Heidutuse olemus, struktuur ja funktsioon on tänapäeval jäänud samaks, kuid selle rakendamine on pidevas muutumises. (Gray, 2000, p. 255) 21. sajandi hakul, mil riikidevahelised suhted on taas pingestunud, (Lowther, 2013, p. 4) on järjekordselt päevakajaline otsida lahendusi, millega heidutada riigi julgeoleku ohustajaid ehk teisisõnu vältida konflikte. Veelgi keerulisemaks teeb olukorra küberruum, mille ebaselget regulatsiooni lubatu ja keelatu vahel kasutavad riigid üha enam ära oma poliitilise agenda täitmisel. Näiteks arvatakse, et Põhja-Korea kasutas küberründeid raha teenimise eesmärgil, kui rahvusvahelised sanktsioonid olid surunud riigi kitsikusse (Greenberg, 2017). Samuti on märgata küberruumis Venemaa üha vaenulikumat poliitikat Lääne demokraatlikke riikide vastu – 2016. aastal kasvasid Venemaa küberründed NATO sihtmärkide vastu 60% ja Euroopa Liidu institutsioonide vastu 20%. Venemaa on sekkunud teadaolevalt nii USA, Saksamaa, Prantsusmaa kui Hollandi valmistesse. (Singer, 2017, p. 1) 2018. aastal süüdistasid Suurbritannia, USA, Austraalia ja Eesti valitsused Venemaad 2017. aastal pahavarakampaania NotPetya korraldamises Ukraina valitsuse ning finants- ja energiasektori vastu, (Riigi Infosüsteemi Amet, 2018b) mida võib pidada osaks käimasolevast Ukraina hübriidsõjast. Spekuleeritakse, et 2011. aastal Iraani tuumajaamast avastatud küberrelva Stuxnet korraldamise taga olid USA ja Iisrael, mille eesmärgiks oli kahjustada Iraani tuumaprogrammi (Singer, 2012). Üha enam küberruumis aset leidvate võimumängude tõttu on hakatud uurima, kas küberheidutus võiks pakkuda võimalusi selliste ohtudega võitlemiseks.

Ameerika Ühendriigid, riik, kus loodi ja arendati välja nii heidutuse teooria (Gray, 2003, p. v) kui ka internet, võttis vastu 2015. aastal esimese riigina eraldiseisva küberheidutuse poliitika (*cyber deterrence policy*) heidutamaks vaenlasi küberruumis (White House, 2015). USA järel on teisedki riigid hakanud küberjulgeoleku strateegiates prioritiseerima heidutust, näiteks 2016. aastal vastuvõetud küberjulgeoleku strateegiad Suurbritannias (HM Government, 2016) ja Austraalias (Australian Government, 2016) käsitlevad heidutust. Tagamaks tugevat küberturvalisust Euroopa Liidus (edaspidi EL), võeti 2017. aastal vastu uus strateegia, mis

baseerub kolmel lähenemisel: küberrünnete vastupidavusvõimel, tulemuslikul küberheidutuse väljatöötamisel ja rahvusvahelise koostöö tugevdamisel (Euroopa Liidu Komisjon, 2017).

Eelnevast tuleneb käesoleva töö **aktuaalsus** – arvestades pingestunud julgeolekukeskkonda, Eesti geopoliitilist asendit ja igapäevaseid küberründeid, tuleb Eestil tugevdada oma julgeolekut vastavalt muutunud olukorrale. Eesti küberjulgeoleku-alast haavatavust on rõhutanud küberjulgeolekuga tegelevad asutused oma viimastes aastaraamatutes (Kaitsepolitseiamet, 2018, lk-d 20–21; Riigi Infosüsteemi Amet, 2018c; Välisluureamet, 2018, lk-d 52–57). Näiteks kaardistatakse pidevalt Eesti avaliku sektori andmesidevõrke, hindamaks Eesti võimet küberrünnetele vastu pidada (Riigi Infosüsteemi Amet, 2017a, lk 4; Teabeamet, 2016, lk 44). Välisluureameti hinnangul ohustab Eesti julgeolekut jätkuvalt ainult üks riik – Venemaa Föderatsioon – mis väidetavalt on pidevas infosõjas lääneriikidega ning arendab ja kasutab oma tegevuses ära küberruumi võimalusi (Teabeamet, 2016, lk 43; Välisluureamet, 2017, lk 4; Välisluureamet, 2018, lk 52). Ka Kaitsepolitseiamet on hoiatanud, et Venemaa kasutab küberrünnakuid, suunatud infolekkeid, desinformatsiooni ja otsest valet, et mõjutada avalikku arvamust ja diskrediteerida demokraatlikku valimisprotsessi (Kaitsepolitseiamet, 2016, lk 6).

Heidutus ei ole Eestis võõras kontseptsioon. Selle relevantsust rõhutatakse julgeolekupoliitika alusdokumendis "Eesti julgeolekupoliitika alused 2017", kus üheks eesmärgiks on heidutuse loomine, mis hoiaks ära ründed riigi ja elanike vastu ning millega seeläbi tagatakse stabiilsus. Eesti heidutust kindlustab NATO kollektiivkaitse (sh tuumaheidutus), kogukondlik lähenemisviis ja iseseisvalt väljaarendatud sõjalised võimed. (Riigikogu, 2017, lk-d 3, 6, 10, 12) Lisaks tähtsustab heidutust ka "Riigikaitse Arengukava 2017–2026": heidutus peab olema nähtav ja usutav hõlmates nii iseseisvat kaitsevõimet, NATO kollektiivkaitset kui mittesõjalisi võimeid (Riigikantselei, 2017, lk 17). "Eesti küberjulgeoleku strateegia 2014–2017" sõnastab ühe eesmärgina, et heidutus küberruumis peab toimuma sarnaselt füüsilisele maailmale (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk 10).

Autor leidis ainult ühe bakalaureusetöö, mis on Eestis kirjutatud küberheidutuse teemal: "Ameerika Ühendriikide normatiivse küberheidutuspoliitika analüüs 2016. aasta presidendivalimiste küberrünnakute näitel" (Kivistik, 2017). Töös analüüsitakse USA küberheidutuspoliitika tõhusust võttes aluseks 2016. aasta USA presidendivalimiste ajal toimunud küberrünnakuid Demokraatliku Partei serveritele ja presidendikandidaadi vastu.

Tulemusena selgus, et rahvusvahelises ja siseriiklikus seadusandluses on puudusi (nt küberspionaaži osas, üldine küberruumi vähene reguleeritus ning juriidiliselt siduvate normide puudus); USA ja Venemaa bilateraalsed kokkulepped ei ole osutunud efektiivseteks ning heidutusstrateegias ei ole arvestatud võimalusega, et riik võiks sekkuda teise riigi siseasjadesse küberruumi kaudu. (Kivistik, 2017) Käesoleva töö autor tõdeb, et heidutuse efektiivsust on keeruline mõõta, sest alati ei saa kindlalt väita, et teatud konflikti hoidis ära just valitud heidutusstrateegia ja mitte mõni muu tegur. Heidutuse mittetöötavus on aga palju paremini näha, sest lisaks muudele meetmetele ei takistanud ka heidutus konflikti tekkimist või eskaleerumist. Autor leiab, et ebaõnnestunud heidutusjuhtumid ei ole põhjuseks, miks peaks heidutuse rakendamisest loobuma, vastasel juhul ei oleks ka näiteks kaitsepoliitikal mõtet, sest maailmaajaloos on näiteid, kus vastaspoole rünnak oli kaitsest tugevam ja võitis konflikti.

Rahvusvahelisel tasandil on küberheidutus-alaste uurimistööde arv viljakam (Moore, 2008; Hansen, 2012; Rivera, 2012; Wong, 2012; Hemmer, 2013; Cirenza, 2015). Nimetatud uurimistööd on üheselt seisukohal, et küberruum kätkeb endas riske, mille maandamiseks võib võimaliku lahendusena kasutada küberheidutust. Töödes on keskendutud võimalikele küberheidutusstrateegiatele; küberruumis leiduvatele ohtudele ja haavatusele; küberheidutuse kontseptsiooni uurimusele; küber- ja tuumarelvaheidutuse erisustele jne. Tööde tulemusena jagatakse soovitusi ja tähelepanekuid, mida arvestada küberheidutusstrateegia arendamisel (Moore, 2008; Hansen, 2012; Rivera, 2012; Wong, 2012; Hemmer, 2013).

Kavandatav magistritöö on seega **uudne**, sest sellega uuritakse Eestis esmakordselt küberheidutuse kontseptsiooni kasutamise võimalusi Eesti küberjulgeolekupoliitikas. Samuti lisab see valdkonda uudisteadmist, magistritöö tulemused on algupärased ja rakendatavad.

Magistritöös võetakse näidis-eeskujuks Ameerika Ühendriigid seetõttu, et tegemist on küberruumis ühe eesrindlikuma ja kaugele arenenuma riigiga ning kus on rajatud ja edasi arendatud heidutusteooriat. Samuti on Eesti ja USA liitlased, kellel on ühine julgeolekuoht – Venemaa Föderatsioon – (Lewis, 2016) ning kelle küberohud (nt teenustõkestusründed) ja haavatavused (nt kasutatakse sama tarkvara) on sarnased. Nagu eelpool nimetatud, siis USA on ka esimene riik, kus küberheidutuspoliitika on eraldiseisva poliitilise dokumendina deklareeritud ning mis on jätkanud küberheidutuse kohaldamist riigi kaitseks (aprillis 2018 esitati USA Kongressile seaduseelnõu mitteriiklike tegutsejatega võitlemiseks küberruumis (Yoho, 2018)).

Käesolev magistritöö keskendub ainult riigi tasandile, sest uurimuse alla on võetud riigi küberjulgeoleku tugevdamise võimalused teise riigi praktika eeskujul. Küberruum pakub olulist uut konteksti poliitilisel maastikul – madal ressurss, anonüümsus, asümeetria haavatavustes tähendab, et ka keskmised ja väikesed riigid saavad teostada kõva ja pehmet jõudu (*hard and soft power*), erinevalt teistest traditsioonilistest domeenidest, kus suurriigid on ilmselgelt tugevamad (Nye, 2010, pp. 1, 19). Töö fokuseerib ainult riigi tasemele ja ühele riigile sellepärast, et jääda magistritöö etteantud mahu piiresse.

Kuna küberheidutust kaalutakse riikides kui ühte võimalikku lahendust võitlemaks küberruumist tulenevate ohtude vastu ning heidutust peetakse üheks meetmeks, mis hoiab ressurssi kokku, siis ehk on võimalik ka Eesti küberjulgeolekut tugevdada läbi küberheidutuse. Ei ole välistatud seegi, et küberheidutusega oleks võimalik heidutada ka füüsilise maailma ohte. Siit tuleneb ka uurimistöö keskne **uurimisprobleem**: kuidas tugevdada Eesti küberjulgeolekut läbi küberheidutuse? Uurimisprobleemi täpsustavad järgmised **uurimisküsimused**:

1. Kes ohustavad Eesti ja USA küberjulgeolekut?
2. Millised on heidutusteooriast tulenevad küberheidutuse tingimused?
3. Millised on Eestis ja USAs kehtivad küberheidutuse strateegilised meetmed?
4. Milliste küberheidutuse strateegiliste meetmetega saaks Eesti küberjulgeolekut tugevdada?

Magistritöö **eesmärk** on selgitada välja, milliste küberheidutuse strateegiliste meetmetega oleks võimalik tugevdada Eesti küberjulgeolekut. Kuna heidutusteoorias puuduvad konkreetsed heidutuse meetmed, siis töö käigus selgitatakse välja, missuguseid küberheidutuse strateegilise meetmeid on USA deklareerinud küberheidutuse strateegiates ning sama tõlgendusviisi kasutatakse ka Eesti dokumendianalüüsi puhul. Eelnevast järeldub seega, et tegemist on kaardistava uuringuga (Hirsjärvi, Remes ja Sajavaara, 2010, lk 129).

Eesmärgi saavutamiseks püstitati järgmised **uurimisülesanded**:

1. Selgitada välja Eesti ja USA küberjulgeoleku ohustajad.
2. Analüüsida heidutuse teooriat rahvusvaheliste suhete tasandil, heidutuse definitsiooni, kuidas heidutusteooria on kujunenud, millistele tingimustele see peab vastama ja millised

on võimalikud heidutusstrateegiad ning asetada heidutusteooria julgeolekuteoreetilisse konteksti.

3. Selgitada välja Eesti ja USA küberjulgeolekuga seotud strateegiadokumentides kasutatud küberheidutuse meetmed.
4. Analüüsida Eesti julgeolekupoliitika kujundajate seisukohti küberheidutuse meetmetest.
5. Analüüsida dokumendianalüüsi ja ekspertintervjuude tulemusi ning teha ettepanekuid Eesti küberjulgeoleku tugevdamiseks.

Magistritöö on **kvalitatiivne empiiriline uurimistöö**, kus on kasutatud uurimisstrateegiana juhtumiuuringut, täpsemalt põimunud üksikjuhtumiuuringut. Tegemist on käsitlusega, kus analüüsitakse juhtumit tervikuna selle kontekstis (Yin, 2014, pp. 53–56), käesoleval juhul küberheidutuse kasutamise võimalusi Eesti küberjulgeolekus. Uurimisobjektideks on Eesti ja USA küberjulgeolekuga seotud strateegiad ja Eesti julgeolekupoliitika kujundajate seisukohad.

Käesolevas töös kasutatakse **andmekogumise meetoditena** dokumendianalüüsi, poolstruktureeritud ekspertintervjuusid ja ankeetküsitlust, mille valimid on eesmärgistatud. Dokumendianalüüs põhineb Eesti ja USA küberjulgeolekuga seotud strateegiatel, mis on avalikkusele kättesaadavad. Poolstruktureeritud ekspertintervjuudesse kaasati kaheksa eksperti, kaks eksperti vastasid ankeetküsitlusele. Respondendid on praegused või endised teenistujad või töötajad Eesti riigikaitse ja julgeolekuga seotud asutustest või isikud, kes töötavad nimetatud valdkondadega seotud teadusasutustes või erasektoris. **Andmete analüüsimisel** kasutatakse kvalitatiivset suunatud sisuanalüüsi.

Magistritöö on jagatud kahte sisulisse peatükki. **Esimene peatükk** on teoreetiline, kus sõnastatakse heidutuse definitsioon, kirjeldatakse heidutusteooria evolutsiooni ning asetatakse heidutusteooria julgeolekuteoreetilisse konteksti. Peatükis kirjeldatakse ka heidutuse jaoks vajalikke tingimusi ja erinevaid heidutusstrateegiaid. Kuna küberheidutusel puudub eraldiseisev teoreetiline raamistik, siis käsitletakse seda osana heidutuse üldkontseptsioonist, millest tuletatakse vajalik teooria. **Teine peatükk** keskendub praktikale, kus uuritakse, milliseid küberheidutuse meetmeid kasutavad USA ja Eesti oma küberjulgeoleku tugevdamisel ning analüüsitakse ekspertintervjuude põhjal, milliseid neist oleks Eestil võimalik kasutada. Peatükk lõpeb tööd kokkuvõtvate ettepanekutega, milliste küberheidutuse meetmetega saaks Eesti küberjulgeolekut tugevdada.

1. HEIDUTUSEST KÜBERHEIDUTUSENI: TEOORIA

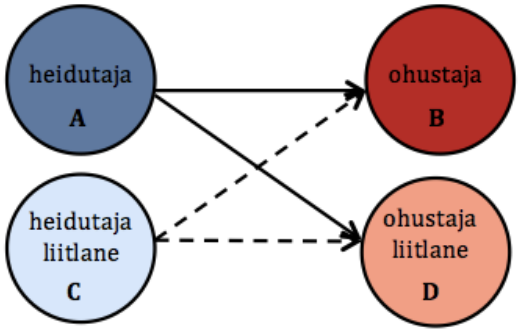
Esimese peatüki eesmärgiks on anda arusaam heidutusest ja küberheidutusest; analüüsida, milliseid tingimusi on heidutuseks vaja täita; millised on võimalikud strateegilised suunad; millega on võimalik vastast heidutada. Selleks, et mõista paremini heidutust ja sellega kaasnevaid kitsaskohti, olemasolevaid probleeme ning vältida levinud väärarusaamu, antakse ülevaade heidutusteooria kujunemisest ehk evolutsioonist, misjärel asetatakse see julgeolekuteoreetilisse konteksti. Siinkohal tuleb märkida, et küberheidutusel ei ole eraldi küberheidutusteooriat, vaid see tuginebki üldisele heidutuse teooriale. Kogu esimese peatüki eesmärgiks on luua magistritöö teoreetiline raamistik uurimisinstrumentide disainimiseks ja uurimistulemuste analüüsiks. See tähendab, et teoorias kirjeldatu põhjal analüüsitakse teises peatükis dokumente ja hinnatakse, kas tegemist on küberheidutusega, mis on selle sisuks ning nende tulemuste põhjal koostatakse intervjuu küsimused ekspertidele.

1.1. Definitsioon ja teooria evolutsioon

Heidutusel (ladina keeles "*dēterrere*" – hirmutama ära või eemale (Bendiek & Metzger, 2015, pp. 4–5)) on palju erinevaid definitsioone, kuid valdavalt kõiki iseloomustab järgnev: ajendada oponenti loobuma oma kavatsus(te)st. Definitsioonid erinevad näiteks määral, et see võib hõlmata ka võimalikke heidutusstrateegiaid (heidutatakse läbi karistuse või tõkestamise) (Mearsheimer, 1983, p. 14, Morgan, 1977, p. 17 ref Moore, 2008, p. 13; Lebow & Stein, 1990, p. 1, Rühle, 2015), keskendutakse konkreetsete huvide kaitsmisele (Cheng, 2015, p. 1, Bunn, 2007, p. 2), kahju-kasu tasakaalule (*cost-benefit calculus*) (Nye, 2017; Defense Science Board, 2017, p. 3; Bunn, 2007, p. 3; Marquez, 2011, p. 10) või rõhutatakse *status quo* osatähtsust (Quackenbush, 2010, p. 60) jne. Variatsioone on küllaldaselt, mida on mõjutanud nii ajastu kontekst kui (sotsiaal)teaduse trendid ja arengud. Näiteks kujunemise alguses mõjutas heidutusteooriat tugevalt realismi teooria (definitsioonis keskendutakse jõu kasutamisele, *status quo* säilitamisele) (Jervis, 1979, pp. 289–290). Hiljem kasutati heidutuse mõtestamiseks mänguteooriat (nt Alperovitch, 2011, pp. 87–88) ja 21. sajandil räägitakse heidutuse kontekstis pigem (elutähtsate) huvide kaitsmisest (vt White House, 2015).

Heidutust eristatakse kohustamisest (*compellance*), kus kasutatakse ähvardusi, et teine pool lõpetaks mingi mitte soovitava tegevuse või teeks hoopis midagi muud. Kuigi erisus tundub olevat abstraktne, leiavad analüütikud, et kohustamine on nö rangem, karmim heidutusest, sest juba alustatud alustatud tegevust, mida on üldjuhul eelnevalt planeeritud, on keerulisem peatada. Arvatakse, et alles algfaasis (mõtlemisel või arutlemisel) olevat käitumist on lihtsam muuta ja mõjutada, kui juba tegutsemisfaasis olevat käitumist. Viimasel juhul on kaalutud erinevaid võimalusi ja tegevusi ning selle tulemusena on langetatud otsus ja alustatud täideviismist. Samas on olukordi, kus mõlemad nii heidutus kui kohustamine on olemas. (Morgan, 2003, p. 2)

Heidutavaid osapooli võib olla rohkem kui üks, kuigi varasemalt on valdavalt siiski kasutatud kirjeldamisel kahte osapoolt – heidutaja, kes on ohus heidutatava tegevusest ja heidutatav, kes oma planeeritava tegevusega ohustab heidutajat (Quackenbush, 2011, p. 744). Lisaks heidutajale ja heidutatavale võivad osapoolteks olla ka ühe või teise poole liitlased, kellel võivad olla teatud huvid heidutaja või heidutatava suhtes. Näiteks abistab USA oma liitlasi, pakkudes neile oma sõjalist jõudu heidutusena vaenlaste vastu.



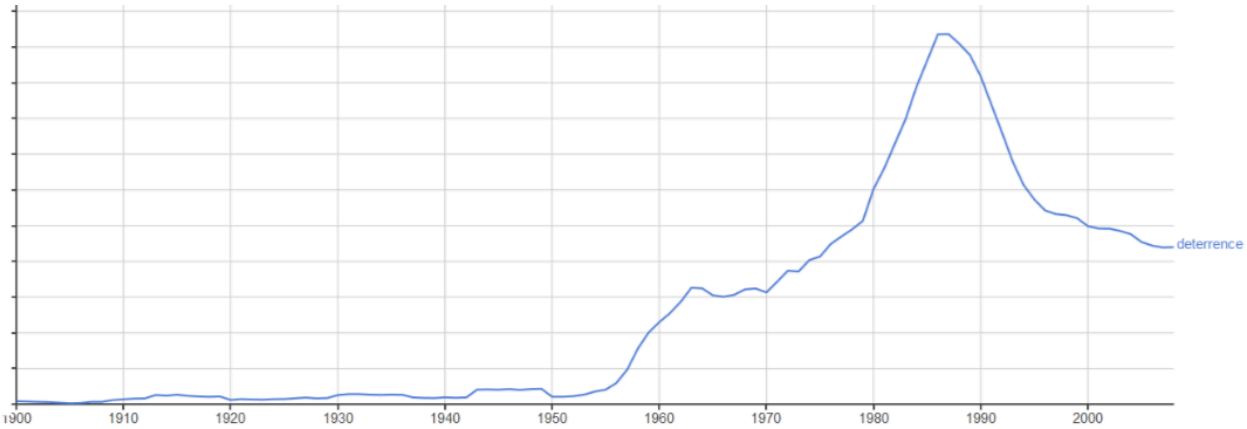
Joonis 1. Võimalik stsenaarium heidutavatest osapooltest ja nooltega on märgitud heidutuse suund (autori koostatud)

Joonisel 1 on kujutatud ühte võimalikku stsenaariumi heidutuse osapooltega. Parema arusaadavuse nimel nimetab autor heidutatavat ohustajaks. Ohustaja B soovib muuta *status quo*d rünnates heidutajat A. Heidutaja A deklareerib, et kui ohustaja B ründab, siis heidutaja A ründab küberrelvaga ohustaja B kriitilise informatsiooni infrastruktuuri. Heidutajat A toetab liitlane C, kes täiendavalt deklareerib, et kui heidutajat A rünnatakse, siis ründab liitlane C ohustajat B tuumarelvaga. Stsenaariumis võib ka olla, et ohustajat B toetab omakorda liitlane D, kes saab

kasu ohustaja B rünnakust. Heidutaja A ja liitlane C võivad suunata oma heidutuse ka ohustaja liitlase D vastu.

Teooriana kujunes heidutus välja alles 20. sajandi esimeses pooles, mil püüti leida vastust küsimusele, kuidas ära hoida sõdu (Zagare & Kilgour, 2000, p. 3). Sõdadest hoidumist võib muuhulgas põhjendada sellega, et 20. sajandi eel ja kestel koges kogu maailm, milliseks on sõjad kujunenud inimkonna ja tehnoloogia arengu käigus. Seda iseloomustab hästi Bernard Brodie (1946, p. 62) seisukoht, kes on väitnud, et enne 1945. aastat oli sõjaväe institutsiooni peamine eesmärk võita sõdu, kuid alates 1945. aastast on see eesmärk muutunud – ennetada neid. Lisaks sellele, et heidutuse abil sooviti vältida sõdadega kaasnevaid õudusi, leiti, et heidutus on ka kulude poolest kokkuhoidlikum lahendus (Lebow & Stein, 1990, pp. 1, 5 ref Rits, 2013, lk 28).

Heidustusteooria kujunemine ei ole olnud järjepidev, seda on arendatud ja uuritud perioodiliselt. Robert Jervis (1979) on jaotanud heidutusteooria kolme “lainesse”, sest nagu lainetuski, kord tõuseb, kord langeb – iseloomustab selline liikuvus ka heidutusteooria senist arengut. Jervise poolt pakutud laineid (1940–1950; 1955–1970; 1970–1990) on võimalik eristada joonisel 2, kus on kajastatud sõna “heidutus” kasutamine publikatsioonides aastatel 1900–2008.



Joonis 2. Sõna "deterrence" (heidutus) kasutamine publikatsioonides aastatel 1900–2008 (Lewis, 2015, p. 1)

Esimese laine algusaja leidub erinevaid seisukohti. Jervis koos teiste teadlastega on leidnud, et heidutusteooria hakkas kujunema kohe pärast Teist Maailmasõda, mil teadlased Bernard Brodie, Arold Wolfers ja Jacob Viner püüdsid mõista tuumarelvade olemasolu tähendust poliitikas ning rahvusvahelistes suhetes (Jervis, 1979, p. 291; Lupovici, 2010, p. 706). Kuid näiteks

Quackenbush ja Zagare (2016, p. 1), kes on käesoleva sajandi heidutusteooria edasiarendajad, väidavad, et heidutusteooria töötati välja juba varem – pärast Esimest Maailmasõda. Seda kinnitab ka näiteks Taddeo (2017), kes kirjutab, et heidutusstrateegiatele keskendunud debatid toimusid juba 1920-ndatel ja 1930-ndatel, kuid tunnistab, et heidutus muutus päevakajaliseks alles pärast Teist Maailmasõda. Igal juhul on õige väita, et heidutuse teoreetiline raamistik algas 20. sajandi esimeses pooles ning selle idee levimise üks põhjusi on tuumarelva loomine. Õigupoolest on levinud arusaam, et heidutus tähendabki tuumarelvaga heidutust, mis ei ole õige. Tuumaheidutus on ainult kitsas ristlõige heidutuse mõttest (Jackson, 2015).

Esialgsetel heidutuse ideedel oli poliitikale suhteliselt väike mõju. Neil puudus süsteemsus ja sarnaselt realismi kriitikale heideti varajastele ideedele ette liialt laiali valguvust. Üheks põhjuseks, miks heidutusteooria sai algselt vähest tähelepanu, oli asjaolu, et akadeemikud keskendusid muudele, tol ajal päevakajalisematele, küsimustele kui abstraktsetele ja pikemaajalisematele. (Jervis, 1979, pp. 290–291; Lupovici, 2010, p. 706)

Teine laine, mida peetakse heidutusteooria kuldseks ajastuks (Lebow & Stein, 1990, p. 5), algas 1950-ndatel, mil mänguteooria mudelid (eriti nn "argpüksimäng", ing kl *the chicken game* või *the game of chicken*, vt Lisa 1) lisati heidutusteooria uuringutesse. Kuigi seeläbi hakati osapoolte taktikalist käitumist paremini mõistma ja heidutus muutus populaarseks, saatis seda endiselt kriitika (Lupovici, 2010, p. 707). Üks peamisi etteheited heidutusele oli asjaolu, et see andis vähe informatsiooni teiste osapoolte motiivide muutmise võimalustest ega saanud olla kindel, et just heidutus on olukorda kuidagi muutnud. Kriitikana toodi välja sedagi, et heidutusteooria hindab osapoolte ratsionaalset mõtlemist üle, nt ei arvesta see emotsiooni najalt tehtud otsuseid, kuigi mõistlik inimene (otsustaja, *decision-maker*) oleks võibolla käitunud teisiti. Antud kriitikale vastasid heidutusteooria pooldajad, et heidutus peabki olema selline, et ka emotsionaalne, lühinägelik ja nõrgamõistuslik vastane saab aru – sõja alustamine on kõige hullem alternatiiv, mida otsustada. (Jervis, 1979, pp. 292, 299) Samast perioodist pärineb ka tuntud filmilooja Stanley Kubricku (1964) film "Dr Strangelove ehk kuidas ma lõpetasin muretsemise ja õppisin armastama pommi", mis keskendub tuumasõja hirmule. Filmi üks põhitõdemusi, mis on ühtlasi heidutuse üks tingimustest ja reaalelus kehtiv, on asjaolu, et heidutus peab olema avalik (kommunikeeritud). See tähendab, et vastane peab olema heidutavast meetmest teadlik. Vastasel juhul, mis on viimsepäeva relvast kasu, kui vastane ei ole sellest teadlik ja kalkuleerib oma tegevust seetõttu valesti. Üks näiteid, kus teadmatuse tõttu kalkuleeris riik oma tegevusi ekslikult

on Suurbritannia ebaõnnestunud heidutus 1982. aasta Falklandi saarte konflikti eel. Suurbritannia oli ilmselgelt Argentiinast sõjaliselt võimekuselt üle, aga kuna Argentiina ei olnud Suurbritannia tegevusest teadlik (asjaolust, et piirkonda on saadetud tuumaallveelaev ja seda toetavat kaks fregatti), tegi ta vale kalkulatsiooni järeldades, et Suurbritannia ei ole tegelikult (sõjaliselt) valmis saari kaitsma, vaid üksnes blufib. (Paul, 1994, pp. 146, 163–164) Kui Arengtiina oleks teadnud, et Suurbritannia saatiski pärast ähvardust sõjalise üksuse Falklandi saartele, oleksid nad tõenäoliselt loobunud oma plaanist ja verine konflikt oleks jäänud ära (Till, 2012, lk 418). Seepärast on oluline, et heidutus oleks avalik, see oleks vastasele teada ja arusaadav, kui ta oma tegevusi planeerib.

Kolmas heidutusteooria laine algas 1970-ndatel. Sarnaselt teisele lainele jätkus kriitika – heidutusteooriat toetavad näited oli väga vähe ja teooria ise oli liialt deduktiivne. Näiteks, kui tihti tegelikult riigimehed või otsustajad tegelikult hävitavad kasutusel olnud kommunikatsiooni kanali selleks, et nende otsust ei oleks võimalik enam muuta või mõjutada, nagu seda tegi näiteks Vene sõjaväejuht 1914. aastal lõhkudes telefoni pärast seda, kui oli veennud tsaari kuulutama välja mobilisatsiooni, et viimane ei saaks anda teada oma ümbermõtlemisest. (Kahn, 1960, pp. 472–473; Jervis, 1979, pp. 289, 301–302; George & Smoke, 1974, pp. 61–71 ref Jervis, 1979, p. 301) Tänapäeva maailmas, kus kommunikatsiooni viise on palju erinevaid ning need on kiired, on muidugi palju keerulisem end kättesaamatuks teha. Kolmas laine näitas, et heidutusteooriat peab täiendama osas, mis puudutab riski võtmist, premeerimist, tõenäosust, väärarusaamu ning siseriiklikku ja bürokraatlikku poliitikat (Jervis, 1979, pp. 303–314).

Lupovici (2010) on täiendanud Jervise (1979) lainete perioodi veel neljandagagi, mis algas pärast külma sõda. Ta väidab, et külma sõja lõpp, uued ohud ja tõlgenduste areng (*development of interpretative approaches*) andis tõuke neljandale heidutusteooria lainele, kuid erinevalt eelnevatest, uuritakse empiirikat ja teooriat isoleeritult. (Lupovici, 2010, pp. 705, 710) Ka teised teadlased on täheldanud heidutusteooria uuesti tõstatamist päevakorda. Näiteks kirjutab Rits (2013), et heidutuses nähakse ühte võimalust astumaks vastu ja hoidmaks ära terroristide plaanitavaid rünnakuid. Lowther (2013) argumenteerib, et kiirelt arenevad strateegilised väljakutsed, keerulised eelarvelised tingimused ja soov uuendada riiklikku julgeolekupoliitikat annavad uue elu vanale kontseptsioonile – heidutusele. Seda kinnitab näiteks ka asjaolu, et 2006. aastal välja antud USA QDR raportis (*Quadrennial Defense Review Report*), mis peegeldab kaitseministeeriumi tsiviil ja militaarvaldkonna liidrite mõtlemist ning kaitsepoliitika suundumist,

on sõnastatud, et USA liigub üks-heidutus-kõigile-ja-kõigele (*one size fits all*) mõtteviisist kohandatud heidutusele (*tailored deterrence*), et paremini heidutada arenenud sõjaliste võimekusega riike, massihävitusrelva omajaid ja mitteriiklike terroriste (Department of Defense, 2006; Bunn, 2007, pp. 1–2). See tähendab, et USA nägi heidutuse edasises arendamises kasutatavat lahendust oma julgeoleku ohtudele. Enam ei oldud seisukohal, et heidutada on vaja ainult ühte riiki (Nõukogude Liitu) läbi karistava heidutusstrateegia, vaid tarvis on heidutada selliste meetmetega, mis vastavad olukorrale kõige paremini. Samuti on heidutust võimalik kasutada ka teiste vastaste puhul.

21. sajandi uued ohud ja arenenud võimekus, globalisatsioon, interneti mõju jne, pakuvad ühelt poolt uusi erinevaid meetmeid heidutamiseks, kuid teisalt on loodud ka uusi subjekte, keda on vaja heidutada. Seega ei kuulu heidutusfääri mitte enam ainult lähinaaberriigid või suurriigid, vaid ka organiseeritud kurjategijate rühmitused, mitte enam ainult füüsiline maailmas, vaid ka küberruum, kus piir lubatu ja keelatu vahel on ebaselge.

Esimest korda kasutati terminit "küberheidutus" 1994. aastal, kui professor James Der Derian arutles, milline heidutav mõju võib olla võrgutehnoloogial (*network technology*) füüsilisele lahinguväljale (Derian, 2009, pp. 210–217). Arvatavasti keskendus Derian ainult füüsilise maailma heidutusele, kuna sellel ajal ei olnud ühiskond veel küberruumist nii palju sõltuvuses ega haavatav. Ent kaks aastat hiljem, 1996. aastal, arutles akadeemik Richard Harknett stsenaariumi üle, kus konflikt leiab aset küberruumis ning analüüsis, kuidas seda uut sõjapidamisviisi heidutada (Harknett, 1996). Peaaegu 25 aastat hiljem puudub küberheidutusel endiselt üheselt mõtestatav definitsioon.

Üks võimalusi küberheidutuse defineerimiseks on kasutada tuumaheidutuse analoogiat. Kuna tuumaheidutuse all mõeldakse tuumarelvaga heidutamist, siis selle tõlgenduse kohaselt võib küberheidutus tähendada heidutamist küberrelvaga. Küberrelva ehk arvutikoodi eesmärgiks on ähvardada või põhjustada füüsilist, funktsionaalset või vaimset kahju struktuuridele, süsteemidele või elusolenditele (Rid & McBurney, 2012, p. 7). Üks erinevusi tuumarelvaga ja küberrelvaga heidutamise vahel seisneb selles, et tuumaheidutuses peab vastane olema teadlik tuumarelvast, aga küberrelvaga heidutamisel peab vastane olema veendunud, et riigil on küberrelva loomise või kasutamise võime, kuid selle täpset olemust ei tohiks teada. Vastasel juhul kaotab küberrelv oma mõtte – vastane saab oma infosüsteeme tugevdada küberrelvas kasutatava haavatavuse vastu või

tugevdada oma infosüsteeme selliselt, et küberrelv ei avaldaks oma mõju või seda ainult vähesel, marginaalsel määral.

Eelpool kirjeldatud tõlgendus kitsendab küberheidutust oluliselt, sest tegelikult on võimalik küberruumis rakendada ka oluliselt laiemat heidutust. Näiteks Suurbritannia küberjulgeoleku strateegias on küberheidutavate meetmetena nimetatud tõkestus- ja karistusheidutust ning rahvusvaheliste normide arendamist (Lonsdale, 2016, p. 54). 2016. aastal loodud töörühm "strateegilise küberheidutuse ülevaade" (*landscaping strategic cyber deterrence*), käsitles viit erinevat küberheidutuse võimalust: tõkestus- ja karistusheidutus, assotsiatsioon (*association*) ehk avalikult süüdlase nimetamine ja seeläbi häbistamine (*naming and shaming*), rahvusvahelised normid ja tabud ning kaasakiskumine (*entanglement*) ehk vastase heidutamine läbi teiste valdkondade nagu näiteks majandusliku, poliitilise või diplomaatilise sfääri (Ryan, 2017, p. 1).

Erinevate valdkondade kaudu heidutamine on sarnane rist-domeenilise heidutusstrateegia kontseptsioonile (vt alapeatükki 1.3). Nimelt leidub küberruumis erinevaid meetmeid, mis võivad vastasele mõjuda heidutavalt nii küberdomeenis (küberruumis) kui ka teistes domeenides (vesi, maa, õhk, kosmos). Näiteks diskuteeritakse Ameerika Ühendriikides võimaluse üle kasutada vastuseks küberrünnakule hoopis väikese võimsusega tuumarelva (Tucker, 2018). Rist-domeenilise heidutusstrateegia kontseptsioonist lähtuv tõlgendus on selgem küberheidutuse käsitlus erinevalt näiteks nende teadlasteste lähenemisest, kes sisustavad heidutust läbi erinevate komponentide või võtmeelementide, põhjendamata sealjuures oma valikuid. Näiteks, Moore (2008, p. 49) on oma uurimistöös võtnud aluseks neli komponenti: tõkestus, karistus, lävend ja selgelt sõnastatud riiklik poliitika. Kui vastane ületab riiklikus poliitika dokumendis sätestatud lävendi ehk nn punase joone (*red line*), siis sellele vastatakse tõkestuse või karistusega. Goodman (2010, p. 105) on uurinud küberheidutust läbi kaheksa komponendi: huvi, heidutav deklaratsioon, tõkestavad meetmed, karistavad meetmed, usutavus, garantii (*reassurance*), hirm ja kasu-kahju kalkulatsioon. See tähendab, et riik, püstitades strateegia mingi huvi kaitsmiseks, annab välja usutava ja garanteeriva deklaratsiooni, mis sisaldab endas ühtlasi kirjeldust, mis juhtub siis, kui vaenlane tegutseb teatud viisil. Deklaratsioonis lubatav peab mõjuma vaenlasele hirmutavalt ning seetõttu arvestab ta oma kavatsuste planeerimisel ja elluviimisel, kas saadud kasu kaalub üles sellega kaasnevad kahjud (Goodman, 2010, p. 106). Komponendid jagunevad seega heidutusmeetmeteks ning lisatingimusteks, millele heidutus peab vastama täiendavalt heidutusteooriast tulenevatele üldistele tingimustele (vt ptk 1.3). Nii Moore' kui Goodmani

valitud komponentides on kattuvusi, kuid nad ei selgita, millest nad oma valikutes on lähtunud, milliseid veel kaalusid ja miks nad välja jäid.

Denning (2015, p. 11) toob välja, et küberheidutus tõstatab nii palju küsimusi ja on raskesti mõistetav seepärast, et sellel on väga laialivalguv tähendus. Teistes sõjapidamise domeenides ei vaadelda heidutust kogu domeeni ulatuses (nt ei ole olemas maaheidutust või kosmose heidutust), vaid räägitakse konkreetsest objektist (tuumarelv, tavajõud (*conventional forces*)) või muust tegevusest (majanduslikud sanktsioonid), millega heidutatakse. Ka tuumaheidutus nagu eelnevalt kirjutatud, on tuumarelvaga heidutamine, kuid see ei tähenda, et tegemist on kogu maadomeeni heidutusega. Ent küberdomeen on komplekssem ja teised domeenid on sellest sõltuvuses. Seejuures tuleb rõhutada, et laialivalguv käsitlus ei ole kuidagi väär või halb, vaid eeldab erinevatest valdkondadest head arusaama.

Eelpool toodut üldistades võib öelda, et küberheidutust on võimalik tõlgendada kolmel viisi: kitsalt, laialt ja valikuliselt (vt tabel 1). Kokkuvõetuna: kitsastõlgendusviis tähendab ainult küberrelvaga heidutamist, ülejäänud heidutusmeetmed on lai tõlgendusviis ning seejuures pole piiranguid, mitmest domeenist heidutusmeetmed pärinema peavad. Kui täiendavalt heidutusmeetmetele sisaldab heidutuse strateegia lisatingimusi (nt kaitstavad huvid, punased jooned jne), siis on tegu valikulise tõlgendusviisiga.

Tabel 1. Küberheidutuse kolm tõlgendamisviisi (autori koostatud)

Tõlgendamisviis	**Küberheidutus tähendab ...**
Kitsas	heidutamist küberrelvaga (analoogia tuumaheidutusega)
Lai	johtuvalt rist-domeenilisest heidutusstrateegia kontseptsioonist leidub küberruumis erinevaid meetmeid, mis võivad vastasele mõjuda heidutavalt nii küberdomeenis (küberruumis) kui ka teistes domeenides (vesi, maa, õhk, kosmos) ja teised mittesõjalised meetmed (nt diplomaatilised ja poliitilised)
Valikuline	teatud komponentide olemasolu, näiteks: huvi, heidutav deklaratsioon, tõkestavad meetmed, karistavad meetmed, usutavus, garantii (*reassurance*), hirm ja kasu-kahju kalkulatsioon.

Käesolevas alapeatükis kirjeldas autor heidutuse definitsiooni ja teooria evolutsiooni kasutades selleks Jervise laine mudelit ja Lupovici täiendust sellele ning erinevaid võimalikke küberheidutuse tõlgendusversioone. Nagu tihtipeale juhtub, siis pealtnäha igapäevaselt kasutatavatel mõistetel puuduvad tegelikkuses kokkulepitud üheselt mõistetav definitsioon, nii on see ka heidutuse puhul. Üldiselt mõistetakse heidutust kui kellegi heidutamist ehk hirmutamist millegagi, millest hoiduda. Riikide omavahelistes suhetes mõistetakse heidutust üldjuhul kui

loobumist plaanist teist riiki rünnata, kuid tegelikult nagu hiljem heidutusstrateegiate avamisel selgub, saab heidutada igal ajahetkel, ka siis, kui ründamisega või muu tegevusega on alustatud. Samuti ei pea olema heidutatav ainult vaenlane vaenuliku riigi mõttes, vaid ka muidu heades või normaalsetes suhetes riik, mis võib ohustada oma tegevuse või veel planeerimisjärgus oleva tegevusega riigi teatud huvi. Selles avaldub ehk kõige paremini realismi teooria maailmakäsitlus – igaüks peab iseenda (huvide) eest seisma. Kuid viise, kuidas mõjutada teisi riike on veelgi ja sellisel juhul ei pea tegemist olema ilmtingimata heidutamisega. Näiteks eristatakse veel lisaks eelpool kirjeldatud kohustamisele ka sundlust (*coercion*) – teise sundimist teatud viisil käituma – ja hoiatust (*dissuasion*) – vastase keelitamine loobuma mingi võime arendamisest (Yost, 2003).

1.2. Heidutusteooria julgeolekuteoreetilises kontekstis

Tuntud sõjastrateeg Carl von Clausewitz (1997) on väitnud, et kuigi teooria ei pruugi anda meile otseseid vastuseid, siis aitab teooria vältida igakordset ratta leiutamise vajadust ja seetõttu võimaldab see efektiivselt hoomata olulisi aspekte ja seoseid ning teha lõppkokkuvõttes paremaid valikuid tõhusamalt (Heuser, 2002, lk 578 ref Till, 2012, lk 84). Autor nõustub antud seisukohaga – teooria aitab mõtteid korrastada ja kuigi heidutuse kontseptsiooni on kasutatud aastatuhandeid, siis teooria olemasolu aitab olla efektiivsem ja annab selle rakendajale teatud eeliseid selle rakendajale. Heidutuse teooria peamine tugevus seisneb selles, et see pakub lahendusi, millega säilitada rahu, hoides ära konflikte või nende eskaleerumist.

Nagu eelpool öeldud, siis heidutuse teooria on noor ja seetõttu on teoreetilised käsitlused killustatud. Mõned akadeemikud (Zagare, 1996; Morgan, 2003; Taipale, 2010, p. 12; Quackenbush & Zagare, 2016, p. 1) väidavad, et enamuse heidutuse alasest teaduskirjandusest võib kategoriseerida üheks teooriaks – **klassikaliseks ehk ratsionaalseks heidutusteooriaks**. Klassikalist heidutusteooriat iseloomustab realism ja jõudude tasakaalu põhimõte (Zagare & Quackenbush, 2016, p. 2). See tähendab, et rahvusvahelist süsteemi iseloomustab hobbeslik maailm, kus toimub kõigi sõda kõikide vastu. Seetõttu peab iga riik tagama iseenda julgeoleku. Kõige efektiivsem võimalus rahu saavutamiseks on tagada riikide vahel võimalikult võrdne jõudude jaotumine. Kui jõud jaguneb võrdväärselt, siis riigid ei soovi *status quo*'d muuta ega teisele riigile väljakutset esitada. (Zagare, 1996, pp. 365–368) Teisisõnu jõud (nt tuumarelv või

militaarjõud) on see, millega heidutatakse konflikti tekkimise eest. Kui jõud on võrdväärselt jagunenud, siis heidutavad riigid end vastastikku ja seeläbi on tagatud rahu.

Esialgu tundub mõistetav, et riigid on rahul, kui jõud on võrdväärselt jaotatud, kuid ei saa välistada, et riigi ambitsioon ei pruugi sellega pikka aega rahulduda ja et ühel hetkel soovitakse rohkemat. Seda kinnitab omakorda ka neorealismi teooriast väljaarenenud ofensiivne ehk ründava realismi tees, mille kohaselt riigid üritavad maksimeerida oma (mõju)võimu ja seetõttu ei saa riik kunagi oma julgeolekus kindel olla ning peab suhtuma kahtlustustega teise riigi võimu suurenemisesse või olukorda, kus oma tegevusega vähendatakse teise riigi võimu (Wohlforth, 2010, p. 139). Kirjeldatud maailmas on ratsionaalne, et riigil on välja arendatud oma heidutusstrateegia, mis tagaks selle, et vastasel ei tuleks mõtetki ründamiseks.

Zagare (1996) on analüüsinud heidutuse kirjandust ja selle põhjal leidnud, et klassikaline heidutusteooria jaguneb kaheks – strukturaalseks ja otsustus-teoreetiliseks. Teised autorid sellist eristust ei tee, kuid kuna see aitab paremini mõista heidutusteooria kujunemist ja seda mõjutanud ajastu eripärasid, siis on magistritöö autor otsustanud kirjeldada Zagare jaotust. Seega edasist lugedes tuleb arvestada, et teised autorid näevad kirjeldatud teooriat koos ühe tervikuna.

Strukturaalne ehk neorealistlik heidutusteooria on täiendanud klassikalist heidutusteooriat, täpsustades: kui suurriikide vahel on jõud jaotatud võrdväärselt, siis see tagab rahvusvahelise rahu. Siit tuleneb ka heidutusteooria nimetus – süsteemi struktuuris seisneb lahendus, kuidas vältida konflikti. Suurriigid heidutavad teineteist vastastikku, kuna ühel puudub eelis teise ees. Näiteks, tuumarelvaheidutus on oma olemuselt stabiilne – riigid, kellel on tuumarelv, on võrdväärse jõuga ja seega heidutavad nad vastastikku üksteist. (Zagare, 1996, p. 368) Ka Margaret Thatcher on kord öelnud: "Tuumarelvadeta maailm oleks vähem stabiilne ja palju ohtlikum meile kõigile" (Margaret Thatcher Foundation, 2017). Samas ei kujutatud tõenäoliselt ette, et 21. sajandi hakul on tuumariike lausa üheksa (Arms Control Association, 2017), kelle arvamusega tuleb teatud küsimustes arvestada hoolimata sellest, kas nad on suurriigid või mitte. Külma-sõjaaegsed poliitika kujundajad on tunnistanud oma seisukoha muutumist: tuumarelva omavate riikide nimekirja pikenemisel on maailm muutunud hoopis ebastabiilsemaks (Schultz, Perry, Kissinger & Nunn, 2007).

Teisisõnu, teooria väidab, et kui sõjaline võime on ebavõrdselt jaotunud (asümmeetriliselt), siis heidutus on ebatõenäoline. Nõrgem riik annab väljapressimisele järele või tugevam riik lihtsalt ründab ja surub oma nõuded peale (Quackenbush, 2011, p. 743; Quackenbush & Zagare, 2016, p. 3) Samas ei ole siinkohal teadlased selgitanud võimalikku olukorda, kus keskmised ja väikeriigid seisavad suurriigi tegevusele üheskoos vastu ega ole põhjendanud, miks asümeetrilises olukorras riigid ei ole alati oportunistlikult käitunud. Samuti ei ole arvestatud tehnoloogilist eelist. Näiteks ulatuslikku kahju tekitavate küberrünnete korraldamine on jõukohane ka küberkurjategijatele.

Samas väidab realismi teooriat edasiarendav teooria – neorealism – et suurvõimude sõda on multipolaarses maailmas tõenäolisem ja sagedasem kui bipolaarses maailmas (Wohlforth, 2010, p. 137). Selleks pakub strukturaalne heidutusteooria lahenduse sidudes sõja tekkimise tõenäosuse võimalike sõja kulutustega. Võrdväärsetes tingimustes on sõja tekke tõenäosus seotud kulutuste-kahjudega. See tähendab, et mida kulukam sõda, siis seda väiksem on tõenäosus selle tekkimiseks (va nö "kogemata tekkinud sõjad") (Quackenbush, 2011, p. 743; Quackenbush & Zagare, 2016, p. 3). Ümberpööratult öelduna: kui sõjakulutused on väikesed, siis seda suurem on tõenäosus konflikti tekkeks. Eelnevalt kirjeldatu on lihtsustatud versioon, sest alati on riigil ka muud huvid, vajadused jne, mis mängivad olulist rolli. Magistritöö autor leiab, et nimetatud teooriateesi tuleks täiendada. Lisaks võrdväärsele jõule tuleks arvestada näiteks ka osapoole sõjapidamisoskusega, sest kuidas muidu saavad võrdväärse jõuga riik tekitada kahju. Seda võtabki arvesse otsustus-teoreetiline heidutusteooria.

Otsustus-teoreetiline heidutusteooria, mis on samuti edasiarendus klassikalisest heidutusteooriast, keskendub osapoolte vastastikku mõjutavatele tulemustele, eelistustele ja (ratsionaalsetele) valikutele, mille alusel kujuneb käitumine riikidevahelistes konfliktides (Zagare, 1996, pp. 365, 368, 373). Otsustus-teoreetilist heidutusteooriat seletatakse läbi mänguteooria mudeli, mis tugineb kolmele eeldusele. Esiteks, mängijatel (st riikidel) on ebatäielik informatsioon olukorrast ja seetõttu on neil keeruline otsustada, milline on kõige optimaalsem otsus või tegu, mida teha tuleks. Teiseks, subjektiivsuse eelduse kohaselt ei ole mängija kindel, millise strateegia kasuks teine otsustab, vaid saab ainult subjektiivselt hinnata teise arvatavat käitumist (nt luureteabe, varasemate kogemuste jms põhjal). Kolmandaks, ratsionaalsuse eeldus väidab, et kasutades tõenäosuse ja kasulikkuse hinnangut, käitub mängija kasu maksimeerimise eesmärgist lähtuvalt. (Zagare, 1996, p. 375)

Klassikalisele heidutusteooriale on pakkunud Zagare ja Kilgour (2000) alternatiivse lähenemise – **ideaalne heidutusteooria** (*perfect deterrence theory*). Ideaalne heidutusteooria ei tee kindlaid järeldusi ähvarduste usutavuse osas, kuna selle üle otsustab osapool ise. Arvesse võetakse teiste osapoolte huvisid ja nende usutavust ähvarduste tegemisel. See tähendab, et usutavus on muutuses (muutuja, *variable*) ja sõltub olukorrast, osapooltest ja nende huvidest ning osapoolte võimest. Seejuures on veel oluline informatsioon, mis on erinevatele osapooltele teada. Kui ei omata täit teadmist, siis võib ka kalkulatsioon olla "vale" ehk teod põhinevad vääratel järeldustel. (Quackenbush & Zagare, 2016, pp. 7–8) Ideaalne heidutusteooria väidab, et kõik (heidutuse) ähvardused peavad olema usutavad. Siit tuleneb ühtlasi ka teooria nimetus: osaleja peab tegema ratsionaalseid valikuid iga otsuse puhul ehk tegu on nn perfektsuse kriteeriumiga. (Quackenbush & Zagare, 2016, p. 11) Kuigi Zagare on kritiseerinud varasemat heidutusteooriat ja heitnud ette, et see ei moodusta tervikut, siis koostöös Quackenbushiga välja pakutud ideaalne heidutusteooria ei ole heidutuse teooriat kõikehõlmavamalt selgitanud. Selleks, et paremini mõista eeltoodud heidutusteooria kirjeldust, on magistritöö autor koondanud teooria põhimõtted tabelisse 2.

Tabel 2. Heidutusteooria põhimõtted (Zagare, 1996; Quackenbush, 2011; Zagare & Quackenbush, 2016; autori koostatud)

<table>
<tr><th colspan="2">Klassikaline ehk ratsionaalne heidutusteooria</th><th>Ideaalne heidutusteooria</th></tr>
<tr><td colspan="2">• realism
o jõudude tasakaal tagab rahu
o igaüks peab tagama iseenda julgeoleku (hobbeslik maailmakäsitlus)
• riigid ei soovi status quo'd muuta, kui jõud jaguneb võrdväärselt ja see tagabki rahvusvahelise stabiilsuse
• ratsionaalsus</td><td rowspan="3">• ei tee kindlaid järeldusi ähvarduste usutavuse kui eelduse osas
• võtab arvesse teiste osapoolte huvid ja nende usutavuse ähvarduse tegemisel
• oluline on info, mis on osapooltele teada
• mänguteooria kohaselt on halvim rünnatava osapoole jaoks ründaja võit</td></tr>
<tr><th>Strukturaalne ehk neorealistlik heidutusteooria</th><th>Otsustus-teoreetiline heidutusteooria</th></tr>
<tr><td>• täpsustab: rahvusvahelise rahu tagab süsteemi struktuur, kui <u>suurriikide</u> vahel on võim jagunenud võrdväärselt, st suurriigid heidutavad teineteist vastastikku
• ümberpöördult: kui sõjaline võime on ebavõrdselt jaotunud, siis heidutus on ebatõenäoline
• tuumarelvaheidutus on oma olemuselt stabiilne – riigid, kes omavad tuumarelva, on võrdväärse jõuga ja seega heidutavad nad vastastikku üksteist
• võrdväärsetes tingimustes on sõja tekke tõenäosus seotud kulutuste-kahjudega, st mida kulukam sõda tõotab tulla, seda väiksem on tõenäosus selle tekkeks (va kogemata sõjad)</td><td>• keskendub osapoolte vastastikku mõjutavatele tulemustele, eelistustele ja (ratsionaalsetele) valikutele, mille alusel kujuneb käitumine riikidevahelistes konfliktides
• mänguteooria mudelite rakendamine
• valiku-teoreetiline raamistik</td></tr>
</table>

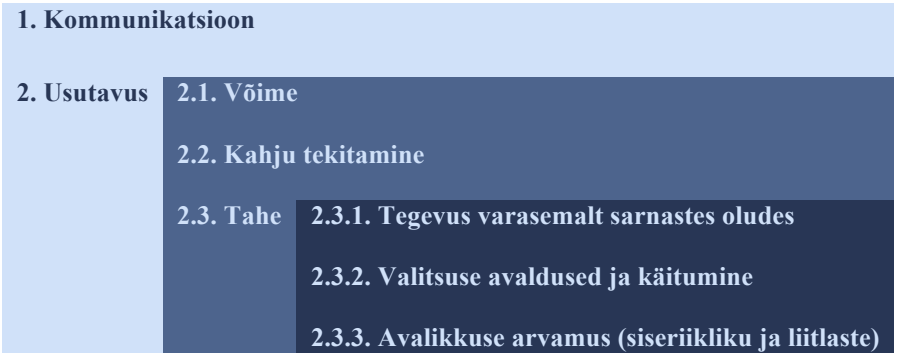
Leidub autoreid (Moore, 2008, p. 49; Goodman, 2010, p. 105), kes nendivad, et heidutusteooria on killustatud ning koostavad nimekirja heidutuse komponentidest, et uurida valitud heidutuse nüansse. Selline lähenemine on sarnane küberheidutuse defineerimisele (vt käesolev töö, lk 17). Näiteks pakub Goodman (2010, p. 105) välja kaheksa elementi küberheidutuse uurimiseks: huvi, heidutav deklaratsioon, tõrjuvad meetmed, karistavad meetmed, usutavus, garantii (*reassurance*), hirm ja kasu-kahju kalkulatsioon. Moore (2008, p. 49) on piirdunud nelja võtmeelemendiga: tõrjumine, karistamine, lävend (*thresholds*) ja selgelt sõnastatud riiklik poliitika. Morgan (2003) mõtestab heidutusteooriat läbi võtmeelementide, milleks on: tõsise konflikti esinemise eeldus, ratsionaalsuse eeldus, vasturünnaku ohu kontseptsioon, talumatu kahju kontseptsioon, usutavuse ideed ja stabiilse heidutuse ideed. Hoolimata killustatusest, on olemasolevate teooria fragmentide põhjal võimalik siiski analüüsi teostada nagu paljud teadusalased uuringud seda kinnitavad.

Käesolev alapeatükk kirjeldas heidutusteooriat julgeoleku kontekstis, kasutades selleks Zagare ja Quackenbushi käsitlust ning Zagare ja Kilgouri alternatiivset lähenemist. Selgus, et on teadlasi, kes leiavad, et kogu heidutuse teooria koondub üheks tervikuks – klassikaliseks ehk ratsionaalseks heidutusteooriaks. Kuid on ka teadlasi, kes jaotavad klassikalise heidutusteooria omakorda strukturaalseks ja otsustus-teoreetiliseks. Selline jaotus järgib realismiteooria arengut ning on paremini arusaadav. Heidutusteooriat on ka edasi arendatud ja täiendatud uue suunaga – ideaalne heidutusteooria, kus on püütud arvesse võtta varasemalt heidutusteooriale etteheidetavat kriitikat, arvestatud muutunud julgeolekuolukorraga ja uute teadusarengutega sotsiaalteadustes.

1.3. Heidutuse tingimused ja heidutusstrateegiad

Mitte igasugune tegevus ei liigitu heidutuseks. Selleks on tarvis täita teatud tingimusi, seejuures ühe puudumisel ei pruugi heidutus enam oma eesmärki täita ja seda suurem on tõenäosus, et heidutus ebaõnnestub. Samas, mida rohkem on erinevaid tahke, mis veenavad vastast oma kavatsustest loobuma, seda tugevamaks võib heidutust pidada ja seda tõenäolisem on ka selle õnnestumine. Kuid tuleb pidada meeles, et lõpuks otsustab heidutuse toimivuse üle heidutatav – kas ta otsustab olla heidutatud või ei hooli ta heidutavatest meetmetest ja otsustab oma kavatsused täide viia. Alati on olemas ka võimalus, et vastane ei olnud heidutusest teadlik või näiteks ei osanud johtuvalt kultuurilistest erisustest seda tõlgendada vastavalt heidutaja

eesmärkidele. Heidutuse absoluutset õnnestumist ei garanteeri ükski meede. Järgnevalt kirjeldab töö autor, millistele tingimustele peab heidutus vastama (vt joonis 3).



Joonis 3. Heidutuse tingimused (Kaufmann, 1954; pp. 6–8; autori koostatud)

Esmalt peab heidutus olema hästi kommunikeeritud (*communication*) ja see peab olema usutav (*credible*) (Kaufmann, 1954, pp. 6–8). Selleks, et heidutus hoiaks ära teatud sündmused, on oluline roll kommunikatsioonil, st potentsiaalse vaenlase informeerimine sellest, mis juhtub siis, kui viimane peaks otsustama oma kavatsuse ellu viia. Tegu on võimalike kulutuste-kahjude ja riskide prognoosimisega, mis on seotud valmisolekuga oma ähvardust ellu viia. See tähendab, kui heidutuse tegemisel blufitakse või ei mõelda seda tegelikult tõsiselt, siis oponent ei pruugi enam tulevikus heidutust enam tõsiselt võtta. Kui heidutus olekski ainult bluffimine, siis kaotaks kogu kontseptsioon oma mõtte – kui kõik teavad, et heidutust ei mõelda tõsiselt, siis milleks peaks tühje sõnu oma plaanides arvesse võtma. Riski minimeerimiseks on teine oluline tingimus – usutavus. (Kaufmann, 1954, pp. 6–7) Selleks, et vaenlasele avaldaks heidutus usutavana mõju, on vaja teada, kes ta on. Selleks, et usutavus oleks loodud, on vaja: võimet (*capability*), suutlikkust tekitada talumatut kahju (*cost*) ja tahet (*intentions*). Vaenlast peab suutma veenda, et heidutajal on olemas võime tegutseda, et vaenlane kannab palju suuremaid kahjusid (*cost*), kui loodetav kasu seda väärt on ning heidutaja tõepoolest tegutseb nagu oma avalduses lubab (heidutus seisneb). Seega ei piisa pelgalt sellest, et heidutajal on teatud arv sõjalist tehnikat, vaenlane peab uskuma, et heidutaja on reaalselt on valmis seda ka kasutama ja tagajärgi kandma, mida heidutustegevus kaasa tuua võib. Näiteks Ameerika Ühendriikide endine president Barack Obama ähvardas Süüriat militaarse sekkumisega, kui viimane peaks kasutama keemilist relva. Aasta hiljem ründaski Süüria sõjavägi mässuliste poolt kontrollitud piirkonda Damascuses keemiarelvadega. Sellega ületas Süüria selgelt Obama seatud punast joont. Selmet saata koheselt vastureaktsioonina teele USA-poolne sõjaline rünnak otsustas Obama pöörduda USA Kongressi poole, et küsida sõjalise sekkumise jaoks luba. Selle otsusega seadis ta kahtluse alla oma

väljendatud heidutuse usutavuse (Chollet, 2016). Antud usutavust on samas parandanud USA praegune president Donald Trump, kes on näidanud konkreetsemat otsustavust sõjalise jõu kasutamisel. 2017. aastal, kolm päeva pärast Bashar al-Assadi režiimi poolt organiseeritud keemiarünnakut Süüria loodeosas, korraldas president Trump 59 Tomahawk tiibraketi tulistamise Süüria õhuväebaasi suunas (Samost, 2017).

Riigi tegeliku tahte tõlgendamisel lähtutakse kolmest aspektist: tegevus varasemalt sarnastes oludes, valitsuse avaldused ja käitumine ning nii siseriikliku kui liitlaste avalikkuse arvamus. Järjepidev välispoliitiline käitumine tõstab usutavust. Seetõttu on keerulisem olukord, kus pikaaegne nõrk valitsus on asendunud tugevaga, kuna sel juhul tuleb riigil end rohkem tõestada, ning *vice versa* ehk pikaaegselt tugeva valitsusega riiki usutakse paremini. Ent oluline on, et valitsuses endas oleks harmoonia, st kui ühe ministri avaldused on teisega vastukäivad, siis on see vaenlasele järjekordne nõrkuse märk. Avalikkuse toetuseta on riigil raske püsida, mistõttu on mõistlik arvestada heidutuse hindamisel nii heidutaja riigi kui ka liitlaste (kui neid on) avalikku arvamust. (Kaufmann, 1954, p. 8)

Nimetatud heidutuse tingimused peavad vastama mistahes valitud heidutusstrateegiale, viisile või meetodile, kuidas heidutust läbi viiakse, nii ka küberheidutuse puhul. Küberheidutus peab olema seega kommunikeeritud ning see peab olema usutav nii võimelt, valmiduselt kahjusid tekitada kui tahetelt lubatut täide viia. Kommunikatsiooniks on võimalusi palju, näiteks deklareerida heidutus strateegia dokumendis, (riigijuhi) kõnes või öelda vahetult arvatavale ähvardajale (nt otseliin (*hotline*) riikide vahel) vm viisil. Igal juhul kõige selgem on väljendada konkreetselt, mis on punane joon, mida vastane ületada ei tohi, mis on see tegevus, mille ületus võib vallandada (Lindsay & Gartzke, 2017, p. 18). Näiteks, riik A lubab nakatada viirusega (küberrelvaga) riigi B sõjalisi infosüsteeme, kui riik B peaks murdma riigi A kriitilisse infosüsteemi sisse ning šaboteerib seda viisil, mille tagajärjel seatakse inimelud ohtu. Heidutuse sisu võib edastada ka konflikti ajal (vt allpool üldine ja vahetu heidutus). Oluline on, et vastane mõistaks, mida tema teod kaasa võivad tuua.

Kommunikeeritud küberheidutus peab olema usutav: heidutajal on võime ja tahe heidutuse deklaratsioonis lubatut täide viia ning ta on valmis kahju tekkeks. Eelneva näite jätkuks seisneb usutav heidutus asjaolus, et riigil A on võime luua või kasutada küberrelva, ta on valmis kandma kahjusid, mis küberrelva kasutamisega võivad kaasneda (näiteks arvestades infoühiskonna ja

teenuste ristsõltuvust võivad nakatuda ka teised infosüsteemid, mis võib tuua kahju, mida ei osatud esialgu ette näha) ning tal on tahe nii toimida. Siinkohal mängivad olulist rolli vähemalt kaks asjaolu: omistamine (*attribution*) ja lekked infosüsteemide haavatavustest. Nimelt seisneb küberruumi üks suurimaid eripärasid anonüümsuses, st et küberrünnaku läbiviijaid on keeruline kindlaks teha ehk omistada. See ei ole probleem, kui heidutatav (punast joont ületanu) on kindlalt teada, näiteks keelatud tegu seisnes riigi piiri rikkumises. Kuid kui tegu seisneb näiteks infosüseemist andmete kopeerimises, mille käigus saadi teada uue infotehnoloogia kavandid (majanduslik küberluure, *economic cyber espionage*), siis on juba keeruline kindlalt väita, kes oli tegelik punase joone ületaja. Kirjeldatud näidet ilmestab USA ja Hiina-vaheline pikalt kestnud konflikt, mida USA on püüdnud lahendada erinevate meetmetega ning mis tipnes 2015. aastal presidentide Obama ja Xi Jinpingiga kokkuleppega, et Hiina valitsus ei teosta ega luba majanduslikku küberluuret teostada (Strawbridge, 2016, p. 836). Kusjuures vahetult pärast kokkuleppe sõlmimist väitis küberjulgeoleku ettevõtte CrowdStrike, et tuvastas uusi majandusliku küberluure katseid, mis on omistatavad Hiina häkkeritele (Alperovitch, 2015).

Teine oluline asjaolu usutavuse tingimuse täitmisel küberruumis on see, et viimastel aastatel on üha enam lekkinud avalikkusele nn null-päeva haavatavusi (*zero-day vulnerabilities*), mida muuhulgas saab ära kasutada küberrelva loomisel. Null-päeva haavatavus on turvaauk, mille kõrvaldamiseks ei ole veel väljastatud turvapaika (Cybernetica, 2018a). Näiteks NotPetya pahavara rünnak Ukraina infosüsteemide vastu 2017. aastal kasutas ära tarkvara Microsoft Windowsi haavatavust (Riigi Infosüsteemi Amet, 2017b, lk 2). Üks tuntumaid lekkeid on Vault 7, mida WikiLeaks on publitseerinud 2017. aasta kevadest ning mis põhineb USA Luure Keskagentuuri (*Central Intelligence Agency*) poolt kogutud haavatavustel, eesmärgiga kasutada neid kübersõjapidamises (*cyber warfare*) (WikiLeaks, 2018). Kui varem oli vaja ulatuslike ja keerulisemate küberrünnakute jaoks nii inim- kui rahalist ressurssi, siis nimetatud lekked on muutnud küberrelva loomise lihtsamaks. Seetõttu võib öelda, et kui heidutus seisneb küberruumis korraldatava küberrelva kasutamises, siis vastast veenda küberrelva olemasolus on lihtsam võrreldes teiste heidutavate meetmete või vahenditega ning kuna küberrünnaku korraldajat on keerulisem kindlaks teha, siis on riigid ka altimad seda kasutama erinevalt nt kineetilisest sekkumisest. Lisaks on küberrelva kasutamine ehk rahvusvahelise õiguse kohaselt proportsionaalsem meede (sõltub muidugi juhtumist), kuna teadaolevalt on senised kahjud küberrünnaku tagajärel piirnenud materiaalse kahjuga, mitte inimelude või -tervise rikkumisega.

Heidutusteooria aluspõhimõttetele tugineb heidutusstrateegia. Heidutusstrateegia hõlmab spetsiifilisi sõjalisi hoiakuid, ähvardusi ning viise, kuidas neid kommunikeerida riikidele, keda soovitakse heidutada. (Morgan, 2003, p. 8) Ehk teisisõnu, kuidas jõuda teoorias kirjeldatud maailmani – vältida konflikti ja tagada rahvusvaheline rahu. Heidutusstrateegiaid on palju erinevaid, keskendudes vastavalt: osapooltele (unilaterlaane ja ühine), reaalsele või potentsiaalsele ohule (üldine ja vahetu heidutusstrateegia), huvidele (laiendatud heidutusstrateegia), kaitsele või ründele (tõkestav ja karistav heidutusstrateegia), spetsiifilisele olukorrale või subjektile (kohandatud heidutusstrateegia) või mitmetele domeenidele (rist-domeeniline heidutusstrateegia). Riigi koostatud strateegia dokument võib sisaldada nii üht kui mitut heidutusstrateegiat. Järgnevalt kirjeldab autor nimetatud heidutusstrateegiaid lähemalt.

Morgan (2003, p. xvi) eristab kahte heidutusstrateegiat: üldine heidutus (*general deterrence*) ja vahetu heidutus (*immediate deterrence*). Külma sõja ajal keskenduti peamiselt vahetule heidutusele, ohud olid siis päevakajalised ja julgeolekukeskkond pinev, sest kardeti, et peagi puhkeb taas sõda. **Vahetu heidutus** tähendab, et peatselt, vaenlase järgmise sammuna, saabub rünnak ning seda on vaja vahetult või koheselt heidutada. Tegelikult leiab Morgan, et vahetut heidutust esineb väga harva ja rohkem tähelepanu peaks pöörama üldisele heidutusele. **Üldine heidutus** tähendab, et on olemas potentsiaalsed ohud, mis võivad tihti olla alles hüpoteetilisel tasandil, seejuures ei pruugita täpselt teada, kes on ründaja. Heidutus on disainitud selliselt, et heidutada vaenlasi isegi rünnaku mõtlemise alustamisest või potentsiaalsest väljakutsujast. (Morgan, 2003, pp. xvi–xvii) Huth ja Russett (1984, p. 496) eristavad siinkohal veel **laiendatud heidutust** (*extended deterrence*), see tähendab, et ei heidutata mitte end ohustava rünnaku või soovimatu tegevuse eest, vaid kolmanda osapoole, nt liitlase, kaitseks.

Olukorras, kus on osapooli mitu ja sõltuvalt nende soovist säilitada *status quo*'d pakub Quackenbush (2011) välja, et on olemas unilateraalne (*unilateral*) ja ühine (*mutual*) heidutusstrateegia. Kui ainult üks riik soovib säilitada *status quo*'d, siis on tegemist **unilateraalse heidutusstrateegiaga**, kuid kui mitu riiki soovivad ühiselt säilitada *status quo*'d, siis on tegemist **ühise heidutusstrateegiaga**. Tõenäoliselt aitab selline eristamine luua parema ülevaate sellest, millistes huvides saab loota liitlastele ning millistes asjades tuleb loota iseendale.

Johtuvalt kaitse tasemest ja vasturünnaku tugevusest eristatakse veel tõkestavat ja karistavat heidutusstrateegiat. **Tõkestav heidutusstrateegia** (*deterrence by denial*) veenab vastast, et ta ei

saavuta oma eesmärki rünnaku õnnestumisel (Mearsheimer, 1983, pp. 14–15 ref Moore, 2008, pp. 18–19). Ehk teisisõnu, kui vastane otsustab riiki rünnata, siis tema rünnaku mõttetust peaks veenma asjaolu, et riik on nii tugev, et tõrjub igasuguse ründe eemale ja vastane sellisel juhul ainult kurnaks ja kulutaks ressursse mõttetult. See-eest **karistav heidutusstrateegia** (*deterrence by punishment*) tähendab vasturünnakut, ehket kui vastane otsustab oma tegevusega jätkata, siis sellele järgneb vastutegevus (Mearsheimer, 1983, pp. 14–15 ref Moore, 2008, pp. 18–19).

2006. aastal kasutati esimest korda mõistet **kohandatav** (*tailored*) **heidutusstrateegia**, mis tähendab, et vastavalt olukorrale kohandatakse vastav võime, sõnumid ja tegevused, et heidutada vastast. Mõneti võib pidada seda minekut tagasi aega, mil räägiti sõjast kui kunstivormist, sest ka heidutus on selle käsitluse kohaselt justkui kunstiline vorm. (Moore, 2008, p. 24; Bunn, 2007) Näiteks heidutatakse mingit riiki erinevalt kui terroristlikku ühingut. Samuti võib olla heidutus erinev erinevate terroristlikke ühingute heidutamisel. Kõik see sõltub paljuski kontekstist. Arvestades tänapäeva maailma kompleksust, siis tundub selline lähenemine mõistlik olevat. Igaühele ei pruugi üks ja sama deklareeritud heidutus olla heidutava mõjuga.

2000. aastal sai alguse veelgi üks heidutusstrateegiline võimalus: **rist-domeeniline heidutusstrateegia** (*cross-domain deterrence*, CDD). Domeene, kus viiakse läbi sõjalisi operatsioone on kokku viis: maa, õhk, vesi, kosmos ja küberruum. Rist-domeeniline võib tähendada nii seda, kust domeenist rünnatakse või mida rünnatakse, mis domeenis asub objekt, aga ka seda, millises domeenis (domeenides) avaldub mõju. Näiteks küberrünnak (rünnak küberdomeenist) vastase sõjaväe võrkude vastu (samuti küberdomeenis olev sihtmärk) avaldab mõju ka teistes domeenides – näiteks ei ole võimalik juhtida või omada olukorrast ülevaadet teistes domeenides (juhtida või suunata õhu-, maa- või merevägesid). Rist-domeeniline strateegia ei ole uus kontseptsioon, modernses sõjapidamises saab näiteks õhuvägi kasutada jõudu mereväeüksuste vastu, mereväeüksused saavad omakorda kasutada jõudu õhuväeüksuste vastu ja nii õhu- kui mereväeüksused saavad kasutada jõudu maaväeüksuste vastu. (Manzo, 2011, p. 2). Seega rist-domeeniline heidutusstrateegia tähendab, et ühes domeenis deklareeritud heidutus võib heidutada vastase tegevust teises domeenis. Näiteks majanduslikud sanktsioonid või sõjaline rünnak kui heidutus küberrünnakule (Lindsay & Gartzke, 2017, p. 1).

Küberruum on laiendanud riikide tööriistakasti. Näiteks arvatakse, et USA ja Iisrael kasutasid Stuxneti küberrünnakut, et häirida Iraani tuumaprogrammi ilma vajaduseta alustada sõda ja

Venemaa mõjutas USA 2016. aasta presidendivalmisi ilma, et USA sellele oleks konkreetse ja silmnähtava vastuse andnud (Lindsay & Gartzke, 2017, p. 1). Tõendeid alles kogutakse, kuid selge omistamine on keeruline.

Käesolev teoreetiline peatükk kirjeldas heidutuse teekonda küberheidutuseni. Evolutsiooni kirjeldus näitas, kuidas heidutusteooria on ajas arenenud. Heidutusteooriale on mõju avaldanud: realismi koolkonna prevaleerimine teadusmaastikul, bipolaarne maailm ja tuumarelva teke. Teooria arengu peatükis jõudis autor analüüsi käigus tõdemuseni, et kõige paremini kirjeldab tänapäevast olukorda ideaalne heidutusteooria. Kuna riikide seas valitseb pidev soov oma võimu (jõudu) suurendada, siis iga riik peab seisma iseenda eest väljas ja seega ka omama mingisugust heidutusstrateegiat. Teooria peatükk kirjeldas, millised on võimalikud heidutusstrateegiad. Nagu heidutusteooria puhul, nii on ka heidutusstrateegiad ajas arenenud. 21. sajandi algul tänu internetitehnoloogiale ja seetõttu ka uue sõjapidamisdomeeni lisandumisest on hakatud rääkima ka küberheidutusest. Küberheidutus võib tähendada ühelt poolt nii küberrelva kasutamist kui ka teisalt on see eraldi küberdomeenis heidutamine või küberruumis leiduvate meetmete heidutus teistes domeenides.

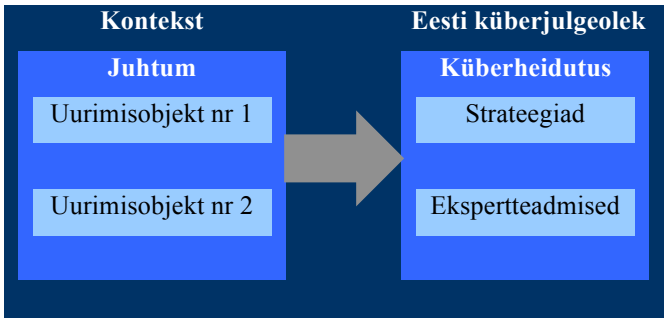
Teooria peatüki eesmärk oli luua raamistik, millega oleks võimalik läbi viia dokumendianalüüsi ja hinnata, kas tegemist on küberheidutusega või mitte, mis on selle küberheidutuse sisu. See annab omakorda aluse, mille pinnalt küsida julgeolekupoliitika kujundajatelt ehk ekspertidelt, kas teoorias ja dokumendianalüüsis avastatud küberheidutuse meetmed oleksid rakendatavad ehk Eesti küberjulgeolekut tugevdavad või mitte.

2. KÜBERHEIDUTUSE KASUTAMISE VÕIMALUSED EESTI KÜBERJULGEOLEKU TUGEVDAMISEKS

Teises peatükis kirjeldatakse esmalt uurimuse metoodikat ja valimeid, sh kirjeldatakse valitud andmekogumise meetodeid ja andmeanalüüsi tehnikaid ning töö käigus kasutatud rakendusi. Teises ja kolmandas alapeatükis viiakse läbi analüüs ja tehakse järeldused valitud andmekogumise meetodite – dokumendianalüüsi, ankeetküsitluse ja ekspertintervjuude – põhjal ning vastatakse sealhulgas püstitatud uurimisküsimustele. Neljandas alapeatükis tehakse ettepanekuid Eesti küberjulgeoleku strateegia arendamisel – küberjulgeoleku tugevdamiseks.

2.1. Uurimuse metoodika ja valim

Eelmises peatükis tuvastati, et heidutusteooria, mis sai alguse 20. sajandi esimeses pooles, on alles kujunemisjärgus ning küberheidutus on veelgi uudsem idee, mis on hakanud levima alates 1990ndatest. Seetõttu on oluline uurida valitud teemat võimalikult laiahaardeliselt kasutades selleks erinevaid uurimismeetodeid. Kõige paremini sobib selleks juhtumiuuring (*case study*), mis võimaldab teostada põhjalikku ja igakülgset uurimist kindlas kontekstis erinevaid uurimismeetodeid kasutades (Yin, 2014, pp. 50–56; Strömpl, 2014). Kuna valitud teema puhul on tegemist ühe konkreetse juhtumiga (Eesti küberjulgeoleku tugevdamine läbi küberheidutuse) kindlas kontekstis (Eesti küberjulgeolekus), mida plaanitakse uurida läbi kahe uurimisobjekti (strateegiadokumentide ja ekspertteadmiste kaudu), siis valitakse uurimisstrateegiaks **põimunud üksikjuhtumiuuring** (*embedded single case study*) (Yin, 2014, pp. 53–56). Ka Merriami (1998 ref Strömpl, 2014) tõlgenduse kohaselt on tegemist juhtumiuuringuga, sest autor plaanib küberheidutust intensiivselt ja terviklikult kirjeldada ning analüüsida, samuti on uuringu tulemus selle osa. (Strömpl, 2014) Eelnevat illustreerib joonis 4.



Joonis 4. Põimunud üksikjuhtumiuuring (Yin, 2014, p. 50; autori koostatud)

Uurimistöös kasutatakse **andmekogumise meetoditena** dokumendianalüüsi ja poolstruktureeritud ekspertintervjuud, mis aitavad leida vastuseid püstitatud uurimisküsimustele (vt tabel 3).

Tabel 3. Uurimistöö probleemi toetavate uurimisküsimuste uurimismeetodid (autori koostatud)

Uurimisprobleem	**Uurimisküsimused**	**Uurimismeetod**
Kuidas tugevdada Eesti küberjulgeolekut läbi küberheidutuse USA näitel?	1. Kes ohustavad Eesti ja USA küberjulgeolekut?	1.1. Teooria analüüs
		1.2. Dokumendi analüüs
		1.3. Ekspertintervjuu ja ankeetküsitlus
	2. Millised on heidutusteooriast tulenevad küberheidutuse tingimused?	2.1. Teooria analüüs
	3. Millised on Eestis ja USAs kehtivad küberheidutuse strateegilised meetmed?	3.1. Dokumendi analüüs
		3.2. Ekspertintervjuu ja ankeetküsitlus
	4. Milliste küberheidutuse strateegiliste meetmetega saaks Eesti küberjulgeolekut tugevdada USA näitel?	4.1. Ekspertintervjuu ja ankeetküsitlus

Dokumendianalüüs on süsteemne protseduur analüüsimaks dokumentide sisu (Bowen, 2009, p. 27), mille eelised seisnevad spetsiifilisuses, stabiilsuses ja erapooletuses (Yin, 2013, p. 106). See tähendab, et dokumentides on kirjas täpsed nimetused, faktid ja need on põhjalikult läbimõeldud, iga sõna on kaalutletud ja omab mingit tähendust. Samuti on võimalik sisu juurde korduvalt tagasi tulla, see ei ole pidevalt muutuv, see ei ole kallutatud ega spetsiifiliselt uurimisteema jaoks loodud, vaid kajastab riigi seisukohti ja prioriteete. Tavapäraselt võib dokumendianalüüsi üks puudusi olla kättesaadavus või juurdepääsupiirang. Antud juhul lähtub töö autor põhimõttest, et heidutus peab olema avalik ja vastane olema sellest teadlik (vt alaptk 1.3), seega analüüsitakse alla ainult avalikult kättesaadavaid dokumente. Riigi strateegiadokumendid on riigiasutuste veebilehtedelt kättesaadavad ning kirjutatud kas autori emakeeles või ingliskeeles, mille autor on omandanud vähemalt B2 tasemel.

Poolstruktureeritud intervjuu kui andmekogumise meetodi suurimaks eeliseks on andmete kogumise paindlikkus: vastavalt intervjuu kulgemisele ja eksperdile on võimalik saadud vastuseid lasta täpsustada ja saada põhjalikku teavet paludes põhjendada väljendatud seisukohta, mida näiteks struktureeritud intervjuu puhul või suletud küsimustega teha ei saa. Intervjuu on

sobiv meetod, kui soovitakse saada põhjalikku teavet ja uuritakse kompleksseid teemasid. Intervjuu üks suurimaid ohte on antud juhul näiteks intervjueeritava kalduvus anda sotsiaalselt soovitavaid vastuseid, sest soovitakse endast jätta eeskujuliku ning erudeeritud inimese muljet (Hirsjärvi, Remes ja Sajavaara, 2010, lk-d 193–194).

Intervjuu eesmärk on esitada kõik plaanitud küsimused, kuid intervjueerida loomulikult, kindlast järjestusest kinni pidamata, arvestades intervjuu käigu ja iseloomuga. Teemad on ülesehitatud üldisemat laadi sissejuhatavast küsimusest alates ja liikudes edasi spetsiifilisemate, ekspertteadmist vajavate küsimustega. Intervjuu viiakse läbi iga eksperdiga individuaalselt. Seetõttu saab intervjueeritav tunda end vabalt, mis omakorda tagab usaldusväärsema tulemuse (Grönfors, 1982, p. 109 ref Hirsjärvi, Remes ja Sajavaara, 2010, lk 197). Intervjuu vastused jäädvustatakse intervjuu läbi viimisel diktofoniga, mis võimaldab keskenduda suhtlemisele, mitte kirjutamisele, ja hiljem vestlus transkribeeritakse. Autor kaalus ka pilootintervjuu läbiviimist, kuid arvestades, et tegu on poolstruktureeritud intervjuuga, siis saab esiti ebaselge küsimuse korral täpsustada, mida küsimuse all mõeldakse või soovitakse teada saada.

Dokumendianalüüsi valim on **eesmärgistatud** (*purposive sampling*), mis tähendab, et valimi moodustamisel lähtutakse ühikute (antud juhul dokumendi) teatud omadustest ja uurimisküsimustest, st need valitakse kindla eesmärgiga (Babbie, 2013, pp. 128–129). Eesmärgiks on antud juhul uurida strateegilisi dokumente, mis käsitlevad küberheidutust (vt tabel 4). Eestis on strateegilisel tasandil neli küberjulgeoleku ja -heidutusega seotud strateegilist dokumenti. Ameerika Ühendriikides johtuvalt riigi suurusest on küberjulgeolekuga tegelevaid asutusi märkimisväärselt rohkem (vt nt Ameerika Ühendriikide kaitseministeeriumi poolt koostatud küberjulgeoleku poliitikaga seotud dokumentide loetelu, Cyber Security & Information Systems Information Analysis Center, 2018), kuid siinkohal lähtuti kahest aspektist. Esiteks, võeti sarnaselt Eesti asutuste loogikale vaatluse alla riigi tasand (Eestis Riigikantselei, USAs Valge Maja) ja siis küberjulgeoleku ja riigikaitse eest vastutavad asutused (ehk nii Eestis kui USAs Kaitseministeerium ja Eesti puhul lisaks Majandus- ja Kommunikatsiooniministeerium). Teiseks, kuna Ameerika Ühendriigid on vastu võtnud oma küberheidutuse poliitika eraldiseisva dokumendina, siis teised strateegilised dokumendid kinnitavad või kordavad üle poliitika dokumendis juba nimetatud meetmeid – st et tekkis andmete saturatsioon ehk küllastus, midagi uut enam ei lisandu, meetmed hakkasid korduma (Laherand, 2008, lk 67). Seetõttu piisas valitud

dokumentidest. Kuigi autor nendib, et heidutavatena võivad mõjuda ka sellised meetmed, mille põhieesmärgiks ei ole vastase heidutamine.

Tabel 4. Dokumendianalüüsis kasutatud dokumentide nimekiri (autori koostatud)

1. Eesti küberjulgeoleku-alased strateegiadokumendid			
Jrk	**Välja antud**	**Asutus**	**Dokumendi pealkiri**
1	2014	Majandus- ja Kommunikatsiooniministeerium	Eesti küberjulgeoleku strateegia 2014–2017
2	2017	Riigikogu	Eesti julgeolekupoliitika alused 2017
3	2017	Kaitseministeerium	Kaitseministeeriumi valitsemisala arengukava 2018–2021
4	2017	Riigikantselei	Riigikaitse arengukava 2017–2026
2. Ameerika Ühendriikide küberjulgeoleku-alased strateegiadokumendid			
Jrk	**Välja antud**	**Asutus**	**Dokumendi pealkiri**
5	2011	White House	International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World
6	2015	Department of Defense	The DoD Cyber Strategy
7	2015	White House	Report on Cyber Deterrence Policy
8	2017	White House	National Security Strategy of the United States of America
9	2018	Department of Defense	Summary of the 2018 National Defense Strategy of the United States of America

Ka **ekspertintervjuude valim** on **eesmärgistatud**. Ekspertintervjuusid viidi läbi isikutega (vt tabel 5), kelle kogemused kübervaldkonna eksperdina on huvipakkuvad (Flick, 2009, p. 165) ning kellelt sooviti koguda kübervaldkonna ja julgeoleku kohta faktiteadmisi (Kolb, 2008, p. 142). Kuna küberheidutus on kompleksne valdkond ja töö eesmärgiks on katta teema võimalikult mitmekülgselt, siis valiti eksperdid lisaks kübervaldkonna ja Eesti julgeolekukeskkonna teadmistele, kas riigikaitse, õiguse või rahvusvaheliste suhete taustaga, Euroopa Liidu, NATO või teadustöö kogemustega. Enamus eksperte on juhtivatel kohtadel, mis sobis töö strateegia tasandiga hästi kokku ja vältis liigset detailsusesse laskumist. Süvatehnilisi teadmisi intervjuu ei eeldanud ning vajalike tehniliste teadmiste olemasolu kinnitas asjaolu, et eksperdid töötab valdkonnas, kus tal on neid niigi baastasemel tarvis.

Ekspertidega kontakteeruti e-maili teel. Võimalusel eelistati intervjuud läbi viia vahetult, ent arvestades, et mõned valitud eksperdid resideeruvad välismaal, siis jäeti võimalus nendega

telefoni või e-kirja teel intervjuu läbiviimiseks, kuna nende-poolset sisendit pidas autor oluliseks antud teema uurimisel. Samuti ei olnud võimalik lühikese ajaperioodiga vajalike teadmiste või kogemustega uusi eksperte asemele leida.

Tabel 5. Intervjueeritud eksperdid (autori koostatud)

Jrk	**Nimi**	**Amet**
1	Andrus Padar	Kaitseliidu küberkaitse üksuse pealik
2	Gert Auväärt	Riigi Infosüsteemi Ameti rahvusvaheliste suhete juht (endine Välisministeeriumi küberasjade koordinaator)
3	Hannes Krause	Majandus- ja Kommunikatsiooniministeeriumi Euroopa Liidu ja rahvusvahelise koostöö osakonna endine nõunik alalises esinduses Euroopa Liidu juures (telekommunikatsioon); Riigi Infosüsteemi Ameti analüüsi ja poliitika osakonnajuhataja
4	Heli Tiirmaa-Klaar	Euroopa Liidu välisteenistuse küberpoliitika koordineerimise juht
5	Jonatan Vseviov	Kaitseministeeriumi kantsler
6	Kadri Kaska	teadur NATO Küberkaitsekoostöö Keskuses (ajavahemikus jaanuar 2017 kuni mai 2018 Riigi Infosüsteemi Ameti juhtivanalüütik)
7	Mihkel Tikk	Kaitseministeeriumi küberpoliitika ja infotehnoloogia osakonnajuhataja
8	Piret Pernik	Rahvusvahelise Kaitseuuringute Keskuse teadur
9	Taimar Peterkop	Riigi Infosüsteemi Ameti peadirektor
10	Toomas Vaks	Swedbanki küberriskide juht (aastatel 2011–2017 Riigi Infosüsteemi Ameti peadirektori asetäitja küberturvalisuse alal)

Kaks ekspertintervjuude küsimust (viies ja seitsmes, vt lisa 2) koostati dokumendianalüüsi tulemuste põhjal. Kuna dokumendianalüüsis tuvastati palju võimalikke heidutusmeetmeid, siis selleks, et ekspertidel oleks mugavam vastata esitas autor küsimuse esitamisel paberkandjal meetmeid sisaldava tabeli (vt lisa 2, tabel 17). Sellisel viisil oli ekspertidel võimalik küsimuses sisalduvaid meetmeid paremini hoomata kui suulisel ettekandmisel. Viimasel juhul võivad esimesena nimetatud meetmed ära ununeda juba küsimust lõpetades. Selleks, et mitte piirata andmestikku olemasolevate meetmetega ja anda ekspertidele valikuvabadus, küsiti ka täiendavalt, milliseid heidutusmeetmeid võiks Eesti kaaluda, mida dokumendianalüüsi tulemusena kaasatud ei olnud. Kui autor ei oleks kaasanud etteantud meetmeid ja oleks küsinud ainult, milliseid heidutusmeetmeid Eesti võiks küberheidutuseks kasutada, siis oleks tõenäoliselt eksperdid toonud vähem meetmeid välja (seega ka vähem analüüsitavat andmestikku). Lisaks tuleb arvesse võtta, et küberheidutus on piisavalt uudne ja spetsiifiline teema, millel on vähe ekspertteadmisega

isikuid. Samuti ei pea valitud eksperdid antud spetsiifilist teadmist omama, vaid oskama hinnata ja analüüsida võimalusi ja puuduste esinemisel esitama võimalikke täiendavaid ettepanekuid. Ei oleks olnud ka mõistlik eeldada, et eksperdid oleks pidanud tegema intervjuuks põhjaliku eeltööd. Ka ankeetküsitlus ei oleks olnud antud juhul sobiv lahendus, sest siis oleks jäänud ära võimalus küsida täiendavaid küsimusi, mida intervjuu võimaldab.

Ekspertidelt andsid sisukamaid vastuseid rohkemate meetmete esitamisel, kui üldistatud koodidega oleks saavutanud. Liigne üldistatus ei oleks andnud piisavalt analüüsitavat sisendit ja magistritöö tulemusena ei oleks saanud rakendatavaid ettepanekuid esitada, sest need oleks jäänud liiga üldistatuks ja seega oleks töö praktiline väärtus jäänud marginaalseks. Näiteks kaitsemeetmete alla kuuluvad nii infosüsteemidesse juurdepääsu piiramine kui ka infosüsteemide moderniseerimine, kuid pelgalt kood "kaitsemeetmed" ei oleks andnud antud sisu piisavalt hästi edasi.

Ekspertintervjuude kestus jäi umbkaudu 30–60 minuti vahele. 10 eksperdist kaks eksperti saatsid oma vastused e-kirja teel, sest vahetut intervjuud ei olnud võimalik läbi viia. Nende vastuseid eristatakse tulemuste analüüsimisel. Anonüümsuse tagamiseks määrati igale eksperdile oma number, mida tähistati tähega "E" ja numbriga, näiteks E1. Numbrite määramisel kirjutas autor kümnele paberilipikule eksperdi initsiaalid ja murdis paberid kokku selliselt, et kirjutatut näha ei oleks. Seejärel segas autor lipikud omavahel, et ei oleks võimalik järjestada kirjutatud lipikuid. Järgmisena seadis autor lipikud üks haaval ritta ning omastas vasakult paremale numbrite järjekorra ühest kümneni. Seejuures kontrollis autor, et eksperdile sattunud number ei kattuks töös esitatud intervjueeritud ekspertide tabelis 5 oleva järjekorra numbriga. Näiteks ekspert Kadri Kaska, kes asub tabelis 6 kuuendal kohal, ei tohi olla eristatav sümboliga "E6". Kui number kattus järjekorra numbriga, siis murdis autor lipiku uuesti kokku ning segas alles jäänud lipikud omavahel uuesti ja asetas taaskord need üks haaval ritta jätkates numbrite määramisega. Ekspertidele omastatud numbrid on teada ainult autorile. Tärniga tähistatud on eksperdid, kes saatsid oma vastused e-kirja teel.

Arvestades, et ekspertide näol on tegemist küberjulgeoleku valdkonnas tuntud inimestega, kelle elulugu on internetist kergesti leitav, jäeti analüüsis välja sotsiaaldemograafilised andmed ja seosed, sest sellega ei oleks autor saanud tagada lubatud anonüümsust. Samuti leiab autor, et sotsiaaldemograafilised andmed ei oleks töös palju lisandväärtust andnud, sest töö eesmärk ei ole

uurida põhjusi, miks juura eriala omandanud ekspert pooldas teatud meetmete hulka rohkem kui majanduse erialal töötav ekspert, vaid teada saada küberjulgeoleku kui erialateadmistega ekspertidelt, millised heidutavaid meetmeid on Eestil võimalik rakendada arvestades riigi praegust julgeolekukeskkonda. Samuti on enamuse ekspertide ametikohtadel tarvilik kõrghariduse olemasolu, seega ka see teadmine ei anna tööle palju juurde.

Andmete analüüsimisel kasutati kvalitatiivset **suunatud sisuanalüüsi ehk kontentanalüüsi**, mida kasutatakse tekstide sisu ja kontekstiliste tähenduste uurimiseks. Sisuanalüüsi tugevuseks on näiteks asjaolu, et seeläbi on võimalik pöörata tähelepanu ka harva esinevatele või unikaalsetele nähtustele tekstis (Laherand, 2008 ref Kalmus, Masso ja Linno, 2015). Näiteks ekspertintervjuudes ei anna meetme esinemissagedus midagi juurde, sest meedet saab esineda umbes ühel-kahel juhul konkreetse küsimuse juures ning esinemise hulgas võib olla ka pelgalt meetme kohta käiv kommentaar, mis ei tähenda, et ekspert meedet kuidagi prioritiseeriks või olulisekski peaks. Oluline on meetmete rakendatavuse võimalikkus arvestades küberjulgeoleku keskkonda ja Eesti riigi võimalusi. Samuti ei saa ka dokumendianalüüsis teha põhjapanevaid järeldusi esinemissageduse järgi, sest mõni oluline meede jääks sellisel juhul tähelepanuta.

Sisuanalüüsi nõrkuseks on jällegi see, et antud analüüs ei võimalda läbi töötada suuri valimeid, mis tingib vähese üldistatavuse. Tekib oht valikulise tõendusmaterjali kogumiseks, mis toimub sageli mitteteaduslikult ja uurijale meelepäraste hüpoteeside kinnitamiseks. (Kalmus, Masso ja Linno, 2015) Nimetatud nõrkust aitab ületada kindlate protseduurireeglite järgimine. Käesolevas töös on selle vältimiseks püstitatud uurimisküsimustele vastavad põhikategooriad, mis aitavad fokuseerida uuritavale, et mitte laiali valguda, siis on teooriast tulenevalt ette antud kindel raam, milles püsida. Oluline on jääda igal sammul objektiivseks, ka siis, kui see võib minna vastuollu isiklike veendumuste ja kogemustega.

Sisuanalüüsi tegemiseks on kombineeritud omavahel kaks tehnikat: **juhtumiülene ehk horisontaalne analüüs ja seosemustrite väljaselgitamine**. Juhtumiülese analüüsi puhul vaadeldakse korraga mitut analüüsitavat juhtumit, mis tulenevad uurimisküsimustest ja moodustavad põhikategooriad. Vastavalt vajadusele jaotatakse põhikategooriad täpsustatud alamkategooriateks, kui need sisaldavad endas mitut komponenti. Ühele uurimisküsimusele võib vastuse saada nii dokumendianalüüsis kui ka intervjuudest. Seosemustrite analüüsimisel keskendutakse mitmele analüütilisele dimensioonile, st ei leita mitte ainult erinevusi-sarnasusi,

vaid tähenduslikke ja olemuslikke seoseid, vaadeldakse, mil viisil teatud nähtused on omavahel interaktsioonis. (Kalmus, Masso ja Linno, 2015)

Dokumendianalüüsi ja ekspertintervjuu analüüsi puhul kasutati esialgu rakendust NVivo for Mac, kuid kuna sellel versioonil puudusid vajalikud funktsionaalsused (seosekaartide loomine) konverteeriti fail ümber ja kasutati edasi Windowsi operatsioonisüsteemile mõeldud rakendusega NVivo 11 Pro. Kuigi kasutatakse **suunatud kodeerimist**, mille puhul toimub kodeerimine vastavalt uurimisküsimustele ning muud teemad jäetakse andmestikus kõrvale (Kalmus, Masso ja Linno, 2015), siis on loodud kaks eraldi kategooriat: mõisted ja tähelepanekud. Need aitavad kiiresti leida üles dokumentides kasutatud mõistete definitsioone, et kontrollida, kas neist on üheselt arusaadud ning tähelepanekud sisaldavad väiteid, mida võib analüüsis vaja minna täiendava selgitusena.

Dokumentide ja ekspertintervjuude kodeerimisel loodi vastavalt uurimisküsimustele kaks põhikategooriat: **1. Küberjulgeoleku ohustajad** ja **2. Küberheidutuse meetmed**. Põhikategooriale **2. Küberheidutuse meetmed** alla loodi seitse alamkategooriat: **2.1 Diplomaatiline ja poliitiline**, **2.2 Informatiivne**, **2.3 Militaarne**, **2.4 Tehniline**, **2.5 Juriidiline**, **2.6 Majanduslik** ja **2.7 Heidutust toetavad meetmed**. Esimesed kuus alamkategooriat loodi juhindudes kohandatud mudelist DIME. DIME on võimu elementide mudel, mille konstruktsioon võimaldab otsustajal (*decision-maker*) tõhusalt saada informatsiooni situatsiooni analüüsimiseks ja edasise tegevusplaani otsustamiseks. Mudel jaguneb diplomaatiliseks, informatiivseks, militaarseks ja majanduslikuks, kuhu on täiendavalt juurde võetud poliitiline ja juriidiline, kuid arvestades tehnoloogilist revolutsiooni tuleb elemente täiendandada veel ühega – tehniline. (Wingfield & Tikk-Ringas, 2010, pp. 17–18) Käesolevas töös hõlbustab mudeli kasutamine heidutusmeetmete analüüsi ja hiljem ettepanekute esitamisel.

Ekspertintervjuud helisalvestati diktofoniga Sony ICD-UX200 ja transkribeerimisel kasutati transkribeerimistarkvara Express Scribe.

2.2. Küberheidutus Eesti ja Ameerika Ühendriikide küberjulgeolekus: dokumendianalüüs

2.2.1. Dokumendianalüüsi tulemused

Dokumendianalüüsi tulemusena tuvastas autor, et valitud riikide küberjulgeolekut võivad ohustada: **riigid**, **küberkurijategijad**, **mitteriiklikud tegutsejad** (*non-state actor*), **pahatahtlikud tegutsejad** ja **siseringiohustajad** (*insider threat*) (vt joonis 5). Ohustada võivad üks või mitu nimetatut ohustajat (nt riik või riigid ja mitteriiklikud tegutsejad), kuid autor kasutab lihtsuse mõttes töös läbivalt mitmuse vormi.

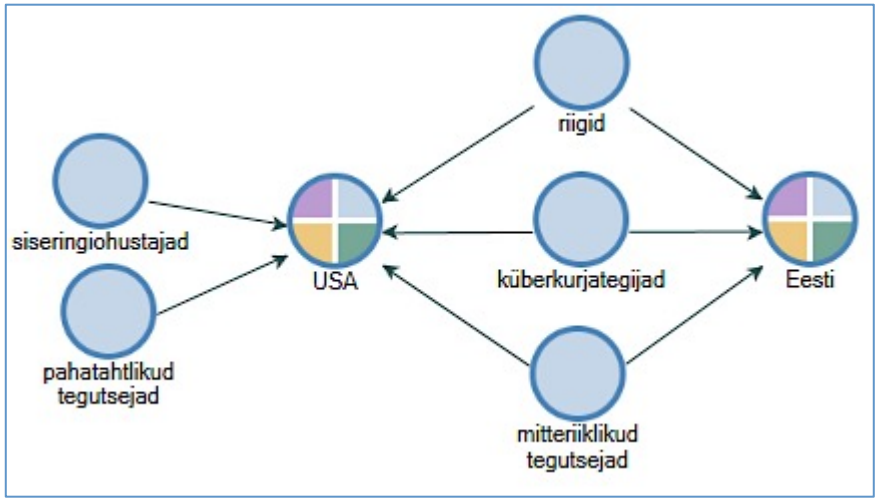
Joonis 5. Kategooria "Küberjulgeoleku ohustajad" koodipuu dokumendianalüüsis (autori koostatud)

Kõigis Eesti strateegiadokumentides tuvastas autor ohustajana **küberkurjategijaid**, mis ohustavad väga laia osa Eesti julgeolekust ja mitte ainult küberruumis, vaid ka füüsilises maailmas toimuvat – inimelu (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk 6). Küberkurjategijate hulka võivad kuuluda: organiseeritud kuritegelikud ühendused, terrorirühmitused, üksikisikud ja grupeeringud, kelle tegevust võivad toetada või suunata riigid (Riigikogu, 2017, lk 6).

Lisaks küberkurjategijatele tuvastati Eesti küberjulgeoleku ohustajatena **mitteriiklike tegutsejaid**. Mitteriiklikud tegutsejad võivad olla nii individuaalsed häkkerid kui ka grupeeringud, kes võivad muuhulgas oma tegutsemisel olla ka motiveeritud poliitilistest ajenditest (nt protestida riigi immigratsioonipoliitika vastu) või tegutseda mõne riigi suunamisel (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk 5).

Küberkurjategijatele ja mitteriiklikele tegutsejatele tuvastati Eesti küberjulgeoleku ohustajatena ka **riigid**, mis arendavad ja kasutavad aktiivselt oma küberründe võimet ning mis võivad toetada või suunata mitteriiklikke tegutsejaid (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk 5; Riigikogu, 2017, lk 5).

Nimetatud kolm küberjulgeoleku ohustajat olid kattuvad USA dokumentides välja toodud ohustajatega (vt joonis 6). USA dokumentides nimetati täiendavalt veel järgmisi ohustajaid: **siseringiohustajaid** ja **pahatahtlikke tegutsejaid** (*adversary*). Siseringiohustajad on isikud, kes teadlikult või tahtmatult jagavad rünnatava(te) infosüsteemi(de) kohta rünnaku seisukohalt olulist teavet või küsivad seda teistelt isikutelt (kolleegidelt); korrumpeerivad süsteeme või andmeid või mõjutavad organisatsioonis tehtavaid otsuseid selliselt, mis kahjustaksid infosüsteeme või võimaldavad sooritada rünnet (White House, 2015, p. 4). Pahatahtlikud tegutsejad on ohustajate üldistatum koondnimetus, mis jätab võimaluse laiendata küberheidutust ka neile, keda ei ole otsesõnu nimetatud.



Joonis 6. Eesti ja USA **Küberjulgeoleku ohustajate** seosemustrikaart dokumendianalüüsi tulemusena (autori koostatud)

Nimetatud küberohustajad võivad näiteks läbi küberspionaaži, küberrünnakute, teenusetõkestus- jm rünnakute ohustada: riigi julgeolekut, majanduslikke huve, elutähtsaid teenuseid, kriitilist informatsiooni infrastruktuuri, riigi toimimist üldiselt, usaldust teenuste vastu jpm (vt tabel 6).

Tabel 6. Valik tsitaate Eesti küberohustajatest ja haavatavustest (autori koostatud)

"*Kasvab riiklike toimijate hulk küberruumis, kes on seotud Internetiga nii ühendatud kui ka suletud arvutivõrke sihtiva küberspionaažiga, mille eesmärgiks on koguda teavet nii riigi julgeoleku kui ka majandushuvid kohta. Suureneb küberründevõimekust omavate riikide hulk ja aktiivsus.*" (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk 5)
"Eesti riigi ja ühiskonna toimimine, iga inimese majanduslik ja sotsiaalne heaolu, elu ning tervis sõltuvad üha enam kasutatavate infosüsteemide ja teenuste turvalisusest. Strateegia üks põhieesmärk on kirjeldada meetmeid elutähtsate teenuste katkematuks toimimiseks ja vastupidavuseks ning kriitilise informatsiooni infrastruktuuri kaitseks küberohtude eest." (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk 7)
"*Eesti digitaalsed teenused on riigi lahutamatu osa, milleta riik ei saa tänapäevasel viisil enam toimida, ja see*

suurendab võimalike rünnete mõju riigi julgeolekule. Side- ja infosüsteemide seotuse tõttu võib ühe elutähtsa või olulise teenuse katkemine mõjutada veel paljude teiste teenuste kättesaadavust, ühtlasi ohustada riigi toimimist tervikuna. Küberjulgeolek ja digitaalsed teenused on valdkonnad, milles Eestil on rahvusvaheline usaldusväärsus ... ." (Riigikogu, 2017, lk 5)
"*Lisaks riiklike toimijate aktiviseerumisele kasvab poliitiliselt motiveeritud üksikisikute ja ühenduste suutlikus panna väheste vahenditega toime teenusetõkestus- jm ründeid, samuti oma tegevust sotsiaalvõrgustikes organiseerida.*" (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk 5)
"*Lisaks tuleb tuua esile et küberrünnaku ohtude maandamiseks on tugevdatud sisejulgeoleku valdkonna infosüsteemide turvalisust.*" (Kaitseministeerium, 2017, lk 15)

Põhikategoorias **2. Küberheidutuse meetmed** tuvastati kokku 15 koodi, mida esines 401 korral, neist USA dokumentides esines 15 koodi 225 korral ja Eestis 14 koodi 65 korral. USA ja Eesti dokumentides kattusid 14 koodi ning erinesid kahe koodi osas. Eesti ja USA küberheidutusmeetmete sarnasused ja erinevused on toodud välja lisas 3. Kuna põhikategoorias on uuritavaid subjekte ainult kaks, ent koode 15, siis ei ole seosemustri kaardil antud juhul mõtet. Ühelt poolt oleks seosemustrikaart kirju ja visuaalselt keeruline töösse mahutada, teisalt ei kajastaks see endas olulist informatsiooni, sest mittekattuvaid koode oli ainult kaks. Seega jättis autor seosemustri kaardi loomata.

Alamkategooria **2.1 Diplomaatilised ja poliitilised** meetmed sisaldas endas kolme meedet: **rahvusvahelise võime arendamine ja koostöö**, **riikide käitumisnormide arendamine küberruumis** ning **sanktsioonide kehtestamine**. Neist kõige enam esines **rahvusvahelise võime arendamist ja koostööd** – USA strateegiadokumentides 26 korral, kuues dokumendis (st kogu dokumendi valimi ulatuses). **Rahvusvahelise võime arendamine ja koostöö** seisneb laia ampluaaga lähenemises alates võrguturvalisusest kuni rahvusvahelise õiguse jõustamiseni paljudes erinevates tegevustes. Täpsemalt tuvastati USA strateegiadokumentides järgmised tegevused (Department of Defense, 2015, 2018; White House 2015, 2017):

- olukorrateadlikkuse (*situational awareness*) loomine (sh küberohtude teadlikkuse tõstmine);
- info ja parima praktika vahetamine (nt standardsete operatiivsete protseduuride jagamine, digitaalne ekspertiis, tööjõu arendamine, penetratsiooni ja kerksuse testid) ning vastavate asutuste ja isikutega kontaktide loomine ja hoidmine;
- kollektiivse kaitse loomine ja arendamine;

- kollektiivse riski maandamine;
- küberturvalisuse kultuuri loomine;
- eelhoiatussüsteemi jagamine;
- multistakeholderismi (põhimõte, mis kaasab kõiki huvegruppe) initsiatiivide soodustamine;
- treeningute ja muude ressursside võimaldamine (nt küberoperatsioonide planeerimine ja harjutamine);
- riigi võime toetamine intsidendi haldusel;
- avaliku ja erasektori partnerluse (*public private partnership*, PPP) loomisel ja arendamisel toetamine;
- erasektori toetamine investeerimisel;
- konverentside korraldamine (nt kriitilise info infrastruktuuri kaitsmise teemal);
- õiguskaitseorganite tegevuse tõhustamine, sh vajaliku õigusloome täiendamine, mis puudutab süütegude uurimist, menetlemist, süüdimõistmist, arvutiekspertiisi kasutamist ning samuti isikute koolitamine (nt ekspertiisi spetsialistide, juristide, seadusandjate).

Nimekiri ei ole lõplik ja täiendavalt võidakse kokkuleppida vastavalt olukorrale ka muudes tegevustes, mis puudutab rahvusvahelise võime arendamist ja koostööd.

USA strateegilised liitlased ja partnerid on üle kogu maailma: samameelsed riigid, arenguriigid, NATO liikmesriigid, rahvusvahelised organisatsioonid (nt NATO, Ameerika Riikide Organisatsioon (*Organization of American States*, OAS), Aasia ja Vaikse ookeani majanduskoostöö foorum (*Asia-Pacific Economic Cooperation*, APEC), Ühinenud Rahvaste Organisatsioon, Kagu-Aasia Maade Assotsiatsioon (*Association of Southeast Asian Nations*, ASEAN), Grupp Seitse (*The Group of Seven*, G7)) ning spetsiifilised regioonid (Lähis-Ida, Aasia ja Vaikne ookean ning Euroopa). Uusi liite, koalitsioone ja partnereid luuakse vastavalt muutunud olukorrale ja vajadusele.

Ka Eesti strateegiadokumentides esines meedet **rahvusvahelise võime arendamist ja koostööd** kõige enam – 21 korral, kõigis allikates. Eesti koostöö osapoolteks on lähinaabrid, samameelsed riigid, liitlased ja partnerid ning NATO ja Euroopa Liidu liikmesriigid. Koostöö seisneb: info jagamise tõhustamises, töösse panustamises, küberteadlikkuse tõstmises, uuteks ohtudeks

valmisoleku parandamises ja suutlikkuses nendega tegeleda, abikäepoliitikas ning oskusteabe ja kogemuste jagamises (Riigikogu, 2017, lk-d 16–17). Järjepideva koostööga tõstetakse kogu maailma küberjulgeoleku taset, kuid selle käigus parandab Eesti ka enda oskusi (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk 7).

Kokku 56 korral esines Eesti strateegiadokumentides NATO organisatsiooni, täpsemalt keskenduti koostööle ja kollektiivkaitsele. Rõhutatakse vajadust olla liitlastega ühtsed, tõhustada infovahetust ning luua ja arendada küberjulgeolekualaseid võimeid, standardeid, väljaõppe- ja treeningvõimalusi (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk 10). Seejuures peab NATO olema suuteline reageerima ja tegutsema kõigis domeenides kogu alliansi ulatuses (Riigikogu, 2017, lk 11).

Riikide käitumisnormide arendamine küberruumis on nii USA kui Eesti strateegiadokumentides vähe esinev, vastavalt seitsmel ja kahel korral. USA on rõhutatud vajadust kokku leppida riikide käitumisnormides (*norms of behavior*) küberruumis, ehket mis on aktsepteeritav käitumine ja milline mitte ning kuidas ja milliste vahenditega karistada neid, kes on lubatud piiri ületanud (nt küberrünnaku korral teise riigi vastu). USA on nimetanud strateegiadokumendis neli rahuaja käitumisnormi, millele ta otsib toetust rahvusvahelisel tasandil: (1) riik ei tohi korraldada või teadlikult toetada sellist tegevust küberruumis, mis tahtlikult kahjustab kriitilist infrastruktuuri või muul viisil kahjustab kriitilise infrastruktuuri kasutamist, mis pakub teenuseid avalikkusele; (2) riik ei tohi korraldada või teadlikult toetada tegevust, mille eesmärk on takistada CERTi tööd küberintsidendiga tegelemisel. Samuti ei tohi riik kasutada CSIRTi selleks, et võimaldada küberruumis tegevust, millega tehakse kahju; (3) riik peab tegema koostööd, mis on järjepidev tema siseriikliku õiguse ja rahvusvaheliste kohustustustega, kui teine riik palub abi uurides küberkuritegevust, kogudes digitaalseid tõendeid ja tegelema oma territooriumilt lähtuva küberkuritegevusega; (4) riik ei tohi korraldada või teadlikult toetada intellektuaalse omandi rikkumisi, sh müüa ärisaladusi või muud konfidentsiaalset äriinformatsiooni eesmärgiga võimaldada konkurentsieeliseid riigi ettevõtetele või kommertssektorile (White House, 2015, p. 17).

Eesti ei ole strateegiadokumentides sisustanud, milliseid konkreetseid käitumisnorme arendada tuleks, kuid soovib kaasa rääkida ühiste arusaamade kujundamises (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk-d 11–12; Riigikogu, 2017, lk 17).

USA dokumentides on marginaalselt tähelepanu pööratud **sanktsioonide kehtestamisele**. USA on seisukohal, et sanktsioneerida tuleb ka neid, kes mitte ainult ei ole küberrünnakute korraldajad, vaid ka kaasaaitajad või võimaldajad (White House, 2015, pp. 5, 11). Eesti strateegiadokumentides autor sanktsioonide kehtestamist ei tuvastanud.

Alamkategoorias 2.2 **Informatiivne** tuvastati kokku kaks peamist meedet: **info** ja **parima praktika jagamine**. **Info jagamine** on meede, millega USA soovib muuhulgas tõhustada riigi olukorrateadlikkust ja sellest lähtuvalt valmistuda rünnakuteks ning parendada infosüsteemide kerksust. Selleks on vajalik hinnata, mis info on vajalik ja jagada seda kiirelt ning võimaldada vastavad saladuse tasemed (White House, 2017, p. 13). Eestis on nimetatud olulisena infovahetuse tõhustamist partneritega ning küberkuritegevusega seotud info operatiivset vahetamist riikidega (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk-d 6, 10).

Meedet **parima praktika jagamine** esines USA dokumentides kahel korral rohkem kui **info jagamist**. USA usub, et kollektiivse kaitse tugevdamiseks on küberjulgeoleku parima praktika rakendamine vajalik ning on seetõttu välja andnud ka globaalselt tunnustatud standardid ja praktika, mis aitaksid orgnisatsioonidelgi küberriske mõista, kommunikeerida ja hallata (White House, 2015, pp. 6, 8). Parima praktikaga kasutuselevõtuga loodetakse ka moderniseerida föderaalset infotehnoloogiat (White House, 2017, p. 13). Eesti strateegiadokumendis on viidatud oskusteabe (*know how*) ja kogemuste jagamisele, mida võib tõlgendada ka kui parima praktika jagamist (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk 12).

Alamkategoorias 2.3 **Militaarne** tuvastati samuti kaks meedet: **eelhoiatussüsteem** ning **küberoperatsioonide arendamine ja läbiviimine**. Meedet **eelhoiatussüsteemi** arendamine ja rakendamine esines nii Eesti kui USA strateegiadokumentides. Eelhoiatus, nii füüsilises maailmas kui küberruumis, on vajalik õigeaegseks rünnakutele reageerimiseks (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk 10; Riigikogu, 2017, lk 11) ja USA kasutab seda täiendavalt ka infosüsteemide kerksuse tagamiseks (White House, 2015, p. 10). Lisaks on USA strateegiadokumendis nimetatud, et eelhoiatussüsteemi jagatakse liitlaste ja partneritega, mis võimaldab töötada üheskoos nii rahu kui kriisi ajal (White House, 2011, p. 10).

USA strateegiadokumentides esines **küberoperatsioonide arendamist ja läbiviimist** kõige enam, Eestis vaid paaril korral. USA on võtnud eesmärgiks tõhustada kübervahendeid kogu konflikti spektrumi ulatuses, et kaitsta riigi vara, kriitilist infrastruktuuri, info terviklikkust ja konfidentsiaalsust (White House, 2017, p. 32). Ühtlasi soovitakse tõhustada võimet ja protseduure, et vaenlaste vastu oleks võimalik küberoperatsioone läbi viia (White House, 2017, p. 32). Eesti loob oma sõjalise kaitse arendamiseks küberväejuhatuse, kelle täpseid ülesandeid strateegiadokumentides ei ole käsitletud, (Kaitseministeerium, 2017, lk 2) ning arendatakse kübersõjapidamise võimeid, kuhu kaasatakse ka erasektor ja vabatahtlikud (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk 10; Riigikogu, 2017, lk 11).

Alamkategoorias 2.4 **Tehniline** hõlmas endas kõige enam meetmeid, mistõttu koondati need nelja koodi alla: **tuvastamine**, **kaitsemeetmed**, **võime arendamine** ja **kerksus**. USA strateegiadokumentides hõlmab **tuvastamine** endas: infotehnoloogiliste haavatavuste, sh nullpäeva haavatavuste, identifitseerimist seeläbi nende mõju vähendades (Department of Defense, 2015, p. X); küberohtude ja -rünnete ennetamist (White House, 2015, pp. 7, 9; White House, 2017, p. 13); internetivõrgu seiramist (White House, 2015, pp. 20, 22). Eesti dokumendianalüüsis leiti aga järgnevad tulemused: küberohtusid ja -ründeid on võimalik ennetada ja nendele kohaselt reageerida läbi tuvastamise või ka läbi internetivõrgu seiramise (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk-d 7–8; Riigikantselei, 2017, lk 5).

Kaitsemeetmeid võib olla mitmesuguseid ja nende nimekiri ei ole seejuures ammendav. USA strateegiadokumentides toodi kaitsemeetmetena välja järgmiseid tegevusi: kerksust tagavad turvalist IT-arhitektuuri rakendatavad infosüsteemid (White House, 2015, p. 5); uuendatud ja asjakohastatud föderaalsed võrgud, seejuures tuleb kõrvaldada innovatsiooni takistav bürokraatia ning võtta kasutusele odavamad ja juba olemasolevad (*off-the-shelf*) infotehnoloogilised lahendused (White House, 2017, pp. 13, 29); üldist küberturvalisust tõstvate tunnustatud küberturbestandardite rakendamine (White House, 2015, p. 8), sh tuleb sõjalisekaitsega tegelevatele tööstusettevõtetel võtta kasutusele veel täiendavad standardeid (Department of Defense, 2015, p. 23).

Eesti dokumendianalüüsis peeti oluliseks ka aktiivset kaitset (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk 10) ning selle tõhusa juurutamise vajadust, sh tuleb Eesti ühiskonna jaoks olulisi teenuseid kaitsta küberriskide vastu (Riigikogu, 2017, lk 7).

Küberruumi kaitset arendab riik pidevalt: jälgides küberruumi, kontrollides infoturbenõuete rakendamist riigi ja oluliste teenuste osutajate infosüsteemides, sh koolitab ja nõustab teenuse osutajaid (Riigikogu, 2017, lk 16). Kriitilisi andmeid hoitakse ja töödeldakse kõrgturvalistes andmekeskustes, mida varundatakse välismaal (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk 8). Infosüsteemide seisukordi jälgitakse pidevalt, neid ajakohastatakse vastavalt vajadusele ja uute süsteemide loomisel võetakse arvesse turvariske, sh tugevdatakse ka sisejulgeoleku valdkonna infosüsteemide turvalisust (Riigikogu, 2017, lk 15; Majandus- ja Kommunikatsiooniministeerium, 2014a, lk 8; Riigikantselei, 2017, lk 15). Riigi toimimiseks vajalikele institutsioonidele töötatakse välja alternatiivsed lahendused sideteenusele ning tuleb salastatud teabe edastamiseks laiendada väljatöötatud krüpteeritud võrkude kasutusele võttu (Riigikogu, 2017, lk 16).

Eesti dokumendianalüüsis on väljatoodud **võime arendamise** all riigikaitsealase võime arendamist, mille tsiviil-, sõjalisel ja rahvusvahelisel koostööl põhinevad ressursid peavad toimima ka küberruumis – kõik sektorid üheskoos tagavad küberruumi kaitse (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk 5–6, 10). USA dokumendid kirjeldavad üldiselt küberjulgeoleku võimet, millega tõhustatakse infosüsteemide turvalisust, sh avastatakse ja ennetatakse pahatahtlikku kübertegevust (White House, 2015, p. 9).

USA strateegiadokumentides on nimetatud **kerksust** kui võimet vastupidada ja taastuda kiirelt rünnakutest, õnnetusjuhtumitest jms sündmustest, mis takistab vaenlasel oma eesmärki saavutada; see on osa tõrjuvast heidutusstrateegiast. Kerksust on võimalik tugevdada, kui infosüsteeme arendatakse lähtudes turvalisest IT-arhitektuurist ning omatakse head olukorrateadlikkust. (White House, 2015, pp. 5, 10, 13–14; White House, 2017, p. 13) Lisaks kriitilisele infrastruktuurile peab USA valitsus rakendama kerksust võrkudele, süsteemidele ja andmetele (White House, 2015, pp. 5, 10). Eesti dokumendianalüüsis mõistetakse **kerksust** ennekõike ühiskonna kontekstis, mille eesmärgiks on suurendada Eesti ühiskonna vastupidavust hädaolukordadega toime tulekuks, sh ka siis kui küberriskid oluliste teenuste osas realiseeruvad (Riigikogu, 2017, lk 7).

Alamkategoorias 2.5 **Juriidiline** loodi kokku kolm koodi: **küberriskide ja ristsõltuvuste haldamine**, **õiguskaitseorganite tegevuse tõhustamine**, **õiguskorra muutmine ja täiendamine**.

Eesti ja USA rõhuasetused **küberriskide ja ristsõltuvuste haldamise** osas on erinevad. Näiteks Eesti keskendub lisaks küberriskidele ka ristsõltuvuste hindamisele ja vastavalt vajadusele alternatiivsete lahenduste väljatöötamisele (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk-d 7–8). USA dokumendid ristsõltuvusi ei uuri ja alternatiivsetele lahendustele ei mõelda, küll aga prioritiseeritakse võtmetähtsusega kriitilist infrastruktuuri, kuna ressurssi ja tähelepanu kõigeks ei jätku. Küberriskide osas nähakse üheselt vajadust neid hinnata ja hallata. (White House, 2017, p. 13)

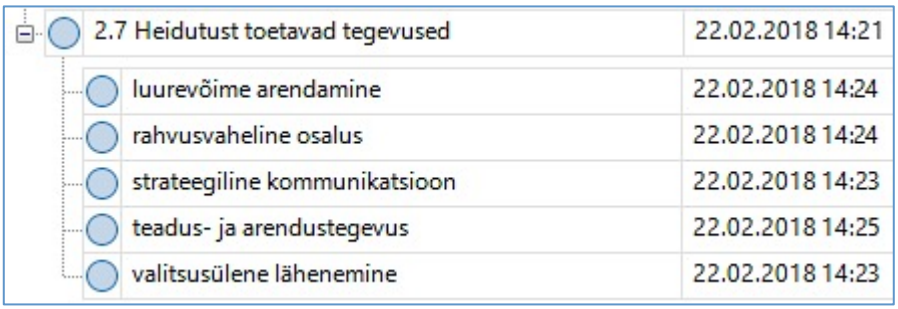
Õiguskaitseorganite tegevuse tõhustamine on eriti tähtis arvestades, et küberkuritegevust peetakse küberjulgeolekule üheks suurimaks ohuks. Eesti on selleks seadnud eesmärgina korrastada korrakaitsestruktuuri ja töökorraldust, suurendada küberkuritegevusega tegelevat isikkoosseisu ning arendada vajalikke võimeid (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk-d 5, 9). USA keskendub õiguskaitseorganite töövahenditele ning küberkurjategijate vastutusele võtmisele (White House, 2017, p. 49). USA on eesmärgina seadnud ka õiguskaitseorganitele võimaluse keelata juurdepääsu infrastruktuurile, kui küberruumis viiakse läbi pahatahtlikku tegevust (White House, 2015, p. 10). Antud meetme all püütakse ka läbi rahvusvahelise koostöö ja üldise võime parendamisega luua heidutust, sest tänu oskuslikule küberkurjategijate avastamisele, süüdistava materjali kogumisele ja menetlemisele avaldab see küberkurjategijatele pikema meetmena rohkem mõju. Samuti kutsub USA üles teisi riike liituma Budapesti konventsiooniga, mis sisaldab endas kolme võtmekontseptsiooni: (1) kindlustab, et õiguskaitseorganitel on pädevus ja vahendid uurimaks küberkuritegevust ja tegelemaks digitaalsete tõenditega; (2) rakendama küberkuritegevuse materiaalõigust (*enacting substantive cybercrime laws*); (3) kasutades mehhanisme nagu 24/7 selleks, et tagada effektiivset ja õigeaegset rahvusvahelist koostööd. (White House, 2015, p. 12)

Õiguskorra muutmine ja täiendamine eeldab, et õigusruumi kehtivat regulatsiooni vaadatakse üle teatud regulaarsusega ning tehakse täiendusi ja muutusi vastavalt muutunud oludele. Siinkohal on Eesti strateegia küberruumi turvalisuse tagamisel ajakohane õigusruum (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk-d 6, 9, 11). USA on samuti nimetanud õiguskorra ajakohastamist (Department of Defense, 2015, p. 7), aga ka harmoneerimise vajadust riikide vahel (White House, 2011, p. 20) ning kutsub riike üles Budapesti konventsiooniga liitumist (vt käesolev töö, lk 47). Lisaks on USA keskendunud info jagamise põhimõtete täpsustamisele

seadustes, mis puudutab nii asutuste kui ka ettevõtete vahelist info vahetamist, sest küberohtudest jagatud olukorrateadlikkus võimaldab parandada ilmsiks tulnud haavatavusi ning seeläbi oma infosüsteeme kaitsta. Seejuures järgitakse info kaitsmise vajadusi, mis puudutab näiteks ettevõtlusega seotud konfidentsiaalset infot. (White House, 2015, pp. 7–8)

Alamkategoorias 2.6 **Majanduslik**e meetmetena tuvastati **investeerimine küberturvalisusesse**. USA valitsus investeerib palju küberturvalisusesse, mis ühtlasi tagab ka tõhusama infosüsteemide kerksuse, samuti võtab valitsus vastutusele asutused, kes küberturvalisusesse ei panusta (White House, 2015, pp. 6, 9). Eesti strateegiadokumentides märgiti, et küberjulgeoleku tagamisse on tarvis investeerida, täpsemalt: ohtude maandamiseks tuleb investeerida tehnoloogiasse, usaldusväärsete ja konkurentsivõimeliste küberlahenduste tagamiseks tuleb tagada riigi tark tellimus ning kogetu tuleb uuesti investeerida innovaatilistesse lahendustesse (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk 6). Eesti riik on küberjulgeolekusse investeerimisel eeskujuks ka erasektorile (Riigikogu, 2017, lk 16).

Dokumendianalüüsi käigus selgus, et Ameerika Ühendriigid on oma küberheidutuspoliitikas toonud eraldi veel välja heidutust toetavad tegevused, mida teoorias küll ei käsitletud (va strateegiline kommunikatsioon), kuid katmaks teemat võimalikult laiahaardeliselt otsustas autor selle uurimise alla võtta ja täiendas alamkategooriaid seitsmenda alamkategooriaga 2.7 **Heidutust toetavad tegevused,** mille käigus tuvastati viis koodi: **luurevõime arendamine**, **rahvusvaheline osalus**, **strateegiline kommunikatsioon**, **teadus- ja arendustegevus ning haridus** ning **valitsusülene lähenemine ja kaasavpoliitika** (vt joonis 7).



Joonis 7. Alamkategooria 2.7 Heidutust toetavad tegevused koodipuu (autori koostatud)

Luurevõime arendamine, mille hulka kuulub teabe kogumine, analüüs ja operatsioonid, võimaldab tõhustada omistamist (*attribution*) ning küberrünnete korraldajate vastutusele võtmist.

Selleks on USA loonud infovahetuskeskkonna, et infokilde tervikpildiks ühendada. (White House, 2015, p. 16) Eelneva luureteabega on võimalik küberründeid ka ära hoida või vähendada mõju (Department of Defense, 2015, pp. 14, 24). Eesti strateegiadokumentides on märgitud: "*Põhiseaduslikku korda ohustava tegevuse ennetamiseks ja tõkestamiseks on vaja koguda ja töödelda asjakohast teavet ...*" (Riigikogu, 2017, lk 12), mis võib hõlmata ka küberruumi.

Rahvusvaheline osalus on sarnane **rahvusvahelise võime arendamisele ja koostööle** hõlmates: riikide käitumisnorme küberruumis; kollektiivset võrkude kaitse tõhustamist; koostöö toetamist võitluses küberkuritegevusega; liitude ja konsensuse loomist, mis puudutab reageerimist küberrünnetele kriitilise infrastruktuuri vastu (White House, 2015, p. 14). Eesti strateegiadokumentides on kajastatud osa, mis kattub rahvusvahelise võime arendamise ja koostööga ning õiguskaitseorganite tegevuse tõhustamisega (vt lisa 3).

Strateegiline kommunikatsioon, sh deklaratiivne poliitika, eesmärk on anda signaal vastasele, mis tagajärgi tema tegevus võib kaasa tuua. Lubatud piiri ületamisele järgneb sanktsioon. Seejuures võib signaali andmine olla nii otsene kui kaudne, avalik või privaatne. Selleks, et veenduda, kas vastane tõlgendas sõnumit õigesti, tuleb abiks jällegi luureteave. (White House, 2015, p. 15) Eesti strateegiates strateegilist kommunikatsiooni ei ole otseselt mainitud.

Teadus- ja arendustegevus, kuhu alla käib ka tehnoloogiline innovatsioon, eesmärgiks on mh kõrvaldada vaenlase asümeetriline eelis, näiteks arendades uusi võimeid, mis aitavad tuvastada vastase tegevust küberruumis või eemaldada eelis, mida küberohustajad hetkel ära kasutavad. Selleks tuleb luua uusi tehnikaid või vahendeid, mis mõjuvad heidutavalt ning tugevdavad kerksust ja kaitset (nt töötades välja lahenduse, kus ei peaks kasutama paroole, kuid mis säilitaks turvalisuse ja piiraks ligipääsu autoriseerimata isikutele). (White House, 2015, p. 18) Eesti dokumentides on küll nimetatud **teadus- ja arendustegevust** ning innovatiivseid lahendusi, kuid lisaks rõhutatakse ka teadlikkuse tõstmise vajadust. Teadlikkus ohtudest aitab maandada ja ennetada küberohte (nt kuidas ära tunda küberintsidenti ja kuidas sellele reageerida) ning selleks viiakse läbi koolitusi. (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk-d 6–7, 9–11)

USA tõdeb, et küberohtudega ei suuda ainult üks ametkond tegeleda, seetõttu tuleb küberintsidentidele reageerida **valitsusüleselt lähenedes**, sh ka riigi-üleselt. Iga asutusel on oma nišš, milles ta on tugev, ja ühiselt ning koordineeritult suudetakse vastata pahatahtlikule

kübertegevusele ja riigi tasandil kübersündmustele. Eesti strateegias on lähtutud sarnasest põhimõttest, kus avaliku, era- ja kolmanda sektoriga koostöös tagatakse riigi küberjulgeolek (Majandus- ja Kommunikatsiooniministeerium, 2014a, lk 7). See on ka osa riigikaitse laiast käsitlusest, "*mis koondab sõjalised ja mittesõjalised võimed, tegevused ja ressursid nii avalikust-, era- kui ka kolmandast sektorist*" (Riigikogu, 2017, lk 3).

2.2.2. Dokumendianalüüsi järeldused

Teooria peatükis selgus, et küberheidutusel on kolm võimalikku tõlgendusviisi: lai, kitsas ja valikuline (vt käesolev töö, lk 18). Vastavalt püstitatud magistritöö eesmärgile valis autor laia tõlgendusviisi, mida kasutati nii USA kui Eesti dokumendianalüüsis. Dokumendianalüüsis tuvastatud heidutava mõjuga meetmed kinnitavad, et küberheidutust võib käsitleda laiemalt kui pelgalt küberrelvaga heidutamist.

Laiendatud tõlgendusviisiga ühtisid Eesti ja USA dokumendianalüüsi 15 koodist 14 koodi. Samas ei tähenda koodide kattuvus, et Eesti ja USA heidutuse strateegiad oleksid samasugused. Kui vaadata lähemalt iga koodi taga olevaid meetmeid, siis selgub, et Eesti dokumentides on üldiselt nimetatud koodid küll olemas, kuid nende sisu ei avata või avatakse vähesel määral (vt lisa 3). Seega saab pigem järeldada, et üldistatuna on strateegiate põhimõtted kattuvad (nt rahvusvahelist koostööd tehakse, infot jagatakse, kaitsemeetmeid rakendatakse jne), kuid konkreetsemalt erinevaid meetmeid ning see, kuidas neid põhimõtteid sisustatakse, on USA heidutuse strateegias märgatavalt rohkem käsitlust leidnud. Näiteks tehakse USAs rahvusvahelist koostööd rohkematel tasanditel kui Eestis ning koostöösuunad on konkreetsemad (vt käesolev töö, lk-d 40–41). On üldmõistetav, et USA on suurriik, millel on rohkem ressursse kui väikeriigil Eestil ning seepärast peab Eesti oma tegevusi prioritiseerima. Sellegipoolest leiab autor, et on tegevusi, mis ei nõua olulist täiendavat ressurssi või on võimalik leida efektiivsemaid viise heidutuse tugevdamiseks. Näiteks mõnede meetmete osas võib juhtuda, et Eesti juba täidabki neid, kuid need ei ole strateegilisel tasandil deklareeritud. Heidutus on seda tugevam, mida selgem ja arusaadavam ta võimalikele vastastele on ning deklareerimine iseenesest ei võta palju ressurssi. Näiteks kuigi üheski Eesti strateegiadokumendis ei tuvastatud sanktsioonide kehtestamist, siis siiski on Eesti võtnud osa välispoliitikas teise riigi sanktsioneerimisest.

Teooriast selgus veel, et heidutus peab vastama kahele põhi- ja kuuele alatingimusele (vt käesolev töö, lk 24). Magistritööga saab kontrollida ainult ühte – kommunikatsiooni tingimuse täidetavust. See jääb käesoleva töö raamidesse, sest töös uuritakse võimalikke võimalusi (heidutuse meetmeid) küberjulgeoleku tugevdamiseks. Meetme tõhususe hindamine ja reaalne mõju jääb magistritöö raamidest välja, kuid seda võib uurida edasi järgmiste uuringutega. Dokumendianalüüsis on eelduslikult kõik meetmed kommunikeeritud, sest need on leitud avalikest avaldatud strateegia dokumentidest. Iseküsimusi on, kui selgelt ja arusaadavalt seda on tehtud, st vastane ei pea pingutama analüüsimaks, kas rünnataval riigil on heidutus ja mis on selle sisu. Kuna Eesti heidutuse strateegia ei ole eraldiseisev dokument, vaid killustatult laiali erinevates strateegiadokumentides, siis see raskendab kommunikatsiooni heidutaja ja vastase vahel. Infokao vastu aitab, kui koondada Eesti küberjulgeoleku tugevdamiseks mõeldud heidutus küberjulgeoleku strateegiasse või kaaluda, sarnaselt USAle, küberheidutuspoliitika dokumendi koostamist.

Dokumendianalüüsi tulemused on osalt kooskõlas maailmakorraga, mida kirjeldati teooria peatükis. Nimelt arvatakse ainsateks rahvusvahelise süsteemi subjektideks riike (vt ptk 1.2.), kuid dokumendianalüüsi tulemusena selgus, et Eesti ja USA küberjulgeolekut ohustavad ka nö mitteriigid ehk küberkurjategijad; mitteriiklikud tegutsejad, kes ei tegutse riigi korraldusel; kasutajad ning siseringiohustajad. Muud heidutuse teooriast tulenevad põhimõtted jäävad käesoleva töö raamidest välja ennekõike mahu piirangute tõttu, kuid seda võib uurida edasi järgmiste uuringute käigus.

Teoorias kirjeldati ka erinevaid võimalikke heidutusstrateegiaid (vt käesolev töö, lk-d 25–29). Dokumendianalüüsis tuvastatud meetmete pinnalt järeldub, et paralleelselt on nii USAs kui Eestis kasutatud mitut erinevat heidutusstrateegiat korraga (vt lisa 3). Näiteks leidus USA heidutusstrateegias elemente nii laiendatud (USA heidutuse ulatus teistele NATO liikmesriikide kaitseks), tõkestavat (tõhusad kaitsemeetmed, mis takistavad ründajal rünnet läbi viia), karistavat (sanktsioonid) jne heidutusstrateegiat. Eestis leidus samuti kõige enam laiendatud (Eesti on NATO liikmesriik ning peab samuti teise liikmesriigi ründel aitama liikmesriiki) ja tõkestavat (kaitsemeetemete rakendamine) heidutusstrateegiat.

Dokumendianalüüsi tulemusena selgus, et Eesti ja USA küberjulgeoleku ohustajad kattuvad, va siseringiohustajate osas. Sellest võib järeldada, et Eestis ei ole seni peetud strateegilisel tasandil siseringiohustajatega seotud küberründeid piisavalt suureks ohuks, et nendega peaks tegelema.

Diplomaatilise ja poliitilise valdkonna heidutusmeetmete osas ei ole Eestis deklareeritud ühte – sanktsioonide kehtestamist, kuigi Eesti on osalenud näiteks Euroopa Liidu kaudu teise riigi sanktsioneerimises. Riikide käitumisnormide arendamise osas puuduvad Eestil konkreetselt seatud eesmärgid, mida soovitakse täita. Ühelt poolt annab see paindlikkuse leida diskussioonis liitlasi ning seega võimaluse mõnes muus Eestile välispoliitiliselt olulises küsimuses partnereid juurde saada (nn *tit-for-tat*). Teisalt on Eestil tugev küberriigi maine, mida võetakse eeskujuks ning seetõttu selgete ettepanekute puudumine võib seda mainet kahjustada. Rahvusvahelise võime arendamise ja koostöö all on Eesti selgelt keskendunud NATOle ning olemasolev kattub USA meetmetega.

Paljud meetmed olid seotud olukorrateadlikkusega, mis sõltub info jagamisest. Näiteks rahvusvahelise võime arendamine ja koostöö eesmärkideks on tõsta teadlikkust ohtudest, parandada valmisolekut ohtudega tegelemisel, tõhustada süütegude uurimist ja menetlemist (ka karistamist) ning selle kõige eelduseks on info jagamine, mis moodustab olukorrateadlikkuse. Info võimaldab mõista olukordi, mida need tähendavad, millist mõju need võivad avaldada, samuti, kuidas tuleks reageerida, näiteks tugevdades kaitsemeetmeid, mis omakorda aitab tõhustada kerksust ning parandada leitud haavatavusi või teisalt neid ära kasutada. Info võib toimida ka eelhoiatusena, kui näiteks on kogutud luureteavet ning analüüsi tulemusena ilmnevad vastase tegevusplaanid ning vastavalt valmistada ette ka oma kodanikke eelseisneva ees läbi strateegilise kommunikatsiooni. Viimase heaks näiteks on Tšehhi teadlaste avastus ID-kaardi turvariskist, millele Eesti suutis õigeaegselt reageerida ja suurem oht jäi realiseerimata.

Parima praktika jagamist sisustatakse USAs palju laiemalt kui Eestis. Eestis on nähtud vajadust jagada kitsalt oskusteavet ja kogemusi rahvusvahelise koostöö raames, kuid ei ole toodud välja näiteks siseriiklike asutuste vahelist parima praktika jagamist (nt Eestis puutuvad küberjulgeolekuga kokku Riigi Infosüsteemi Amet ning Politsei- ja Piirivalveamet jt asutused).

Militaarses valdkonnas on mõlemas riigis prioritiseeritud eelhoiatussüsteemi õigeaegseks reageerimiseks, kuid lisaks jagab USA seda oma liitlaste ja partneritega, mis võimaldaks töötada

üheskoos nii rahu kui kriisi ajal. Selline ühetaolisus aitab kiirendada otsustamist ja tagab ladusama tegutsemise ka konflikti ajal. Küberoperatsioonide arendamine ja läbiviimine on Eestis selgelt veel kujunemisjärgus. Esimese sammuna on loodud küberväejuhatus, kuid täpne funktsioon ja tegevused on strateegia tasandil avalikkusele teadmata.

Tehnilises valdkonnas kõige uudsemaks meetmeks võiks pidada kerksuse rakendamist küberruumile. Eesti on seni kasutanud kerksuse kontseptsiooni ühiskonna toimetulekuks hädaolukorras (sh küberriskidega seotult oluliste teenuste osas), kuid võiks kaaluda selle laiendamist. Jällegi on tõenäoliselt meetmeid, mis võiksid kuuluda kerksuse alla, kuid eesmärk võib olla muu, seega tuleks üle vaadata, mis olemasolevatest tegevustest ja põhimõtetest võiksid täita ka kerksust ning mida võiks selle pinnalt edasi arendada. Selge arusaam ja ülevaade ning vastav deklareerimine on jällegi signaaliks vastasele, et Eesti küberruumis on oma eesmärke keeruline saavutada.

Eesti on tugevalt keskendunud kaitsemeetmetele võrreldes nt USAga, millel strateegilisel tasandil oli palju vähem meetmeid nimetatud. Märkimisväärsem erinevus seisnes näiteks USA seisukohas võtta kasutusele juba olemasolevaid (nn *off-the-shelf*) IT-lahendusi, mis on eritellimustest odavamad. Tuvastamise osas teevad mõlemad riigid võrguseiret ja ennetustööd, kuid Eesti võiks USA eeskujul kaaluda võimalust otsida infotehnoloogilisi haavatavusi. Kui see nõuab liialt ressursse, siis võib jääda lootma rahvusvahelise koostöö käigus saadetud infole ning küberhügieeni tugevdamisele.

Juriidilises valdkonnas on Eesti USAst küberriskide ja ristsõltuvuste haldamises eesrindlikum, kuna on võtnud eesmärgiks lisaks küberriskidele ka ristsõltuvusi hinnata ning töötada välja alternatiivseid lahendusi halvemateks stsenaariumiteks. Õiguskaitseorganite tegevuse tõhustamisel on märgata erinevaid prioriteete. Näiteks Eesti keskendub õiguskaitseorganite struktuurile, töökorraldusele ja võimete arendamisele, kuid USA nende töövahenditele ja võimalikele tegevustele (vastutusele võtmise ja infrastruktuurile juurdepääsu keelamisele). Siit võib järeldada, et USA on sammuvõrra Eestist ees, kuigi tegeleb endiselt ka organisatoorsete tegevustega.

Mõlemas riigis on olulise meetmena välja toodud õigusruumi ajakohastamine, kuid USA täpsustab lisaks, et vaja on ka riikide omavahelist õigust harmoniseerida ning pakub ühe

võimalusena Budapesti konventsiooniga liitumist, mis annab baasnõuded küberkuritegevusega võitlemisel. USA on näinud vajadust reguleerida ka infojagamise põhimõtteid seaduse tasandil, mida Eestis probleemse või vajaliku tegevusena ei nähta.

Samuti panustavad mõlemad riigid küberturvalisusesse investeerimisele. Eesti on näinud vajadusena näidata riigina eeskuju erasektorile, kuid USA on avalikus sektoris läinud sunniteed– kes ei panusta küberturvalisusesse, see võetakse vastutusele.

Heidutust toetavad tegevused on kontseptsioon, mida heidutusteooria ei ole käsitlenud, kuid USA on toonud selle oma küberheidutuse poliitikasse sisse. Jääb selgusetuks, mille alusel selline valik tehtud sai. Näiteks piir rahvusvahelise osaluse kui heidutust toetava tegevuse osas ning rahvusvahelise võime arendamise ja koostöö kui küberheidutuse meetme osas on hägune. Kui tehakse rahvusvahelisel tasandil koostööd, siis see võib hõlmata ka näiteks rahvusvahelistes koostööformaatides, organisatsioonides vmt tegevustes osalemist. Seetõttu võiks jätta ainult ühe alles või võiks olla täpsustatud, kuidas neid eristada.

Strateegiline kommunikatsioon ühelt poolt hõlmab endas heidutuspoliitika või -strateegia olemasolu, kuid teisalt peaks aitama heidutussõnumite edastamise vastasele. Pikaajalise dokumendi nagu näiteks strateegia muutmine võtab kaua aega, kuid lähenev konflikt eeldab kiiret tegutsemist, seega on strateegilisel kommunikatsioonil oluline roll kanda.

Kõigi meetmete osas, mida USA dokumentides on nimetanud ja Eestis ei ole, tuleks üle kontrollida, kas need meetmed on juba Eestis olemas või mitte. Kui meetmeid ei ole, siis tuleks kaaluda, kas neid võiks kasutusele võtta, mis kasu nendega taodeldakse jne. Nende meetmete osas, mis on olemas kehtivas strateegias või varasemalt nimetatud tuleks veenduda, et need on täidetud ja nende tõhusus on jätkuvalt kohane. Ühe osana saab seda kontrollida eksperintervjuudes, kus on võimalus ekspertidel anda oma hinnang olemasolevatele meetmetele, uute meetmete rakendatavuses, kuid niisamuti nende meetmete osas, millega tuleb jätkata, mida pole suudetud veel täielikult rakendada või mis on ja jäävadki pidevaks strateegilisel tasandil.

Eelneva kokkuvõtteks võib järeldada, et Eesti senine küberheidutus seisneb peaasjalikult kahel meetmel: rahvusvahelise võime arendamisel ja koostööl ning kaitsemeetmetes. Samuti võib

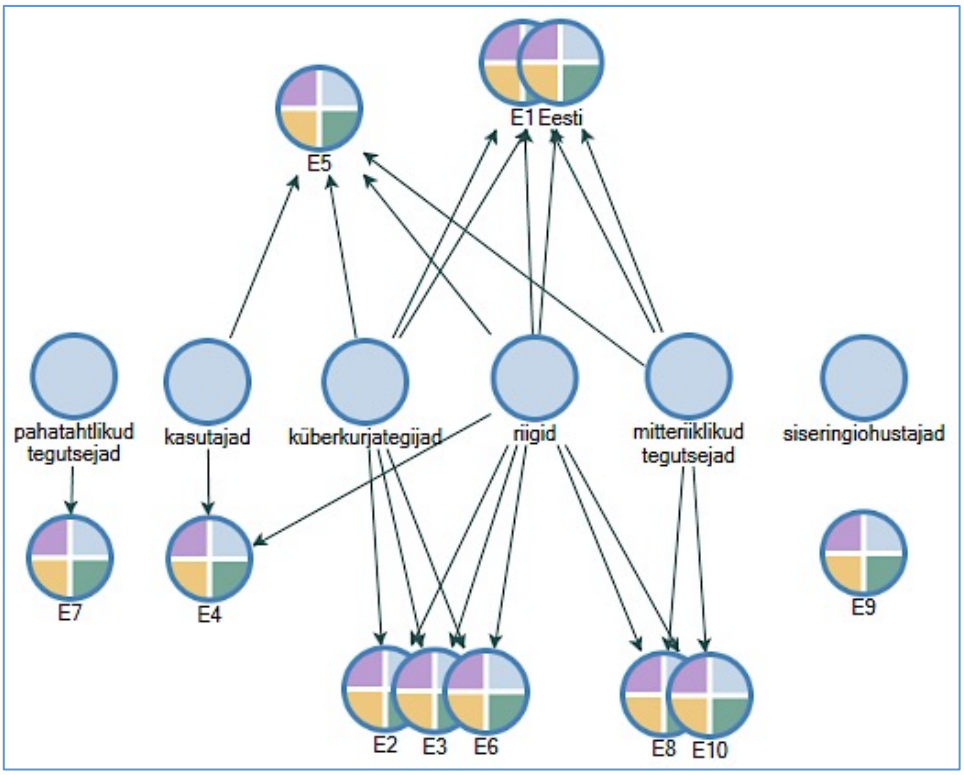
öelda, et hetkel kehtiv Eesti heidutuse strateegia koosneb järgnevatest strateegiatest: ühisest (läbi NATO), tõkestavast, üldisest (vahetut ohtu ei tuvastatud) ja rist-domeenilisest (küberdomeen).

Selleks, et uurida edasi, kuidas tugevdada Eesti küberjulgeolekut läbi küberheidutuse on tarvis küsida hinnangut Eesti julgeolekupoliitika kujundajatelt, kes omavad vastavaid erialateadmisi kübervaldkonnast ning mis abistab hinnata, milliseid heidutusmeetmeid võiks Eesti kaaluda.

2.3. Eesti julgeolekupoliitika kujundajate seisukohad küberheidutusest: ekspertintervjuu

2.3.1. Ekspertintervjuude tulemused

Ekspertintervjuude tulemused sarnanesid kategoorias **1. Küberjulgeoleku ohustajad** kolme koodi osas dokumendianalüüsi tulemustega, täiendavalt loodi juurde üks kood ning ühe koodi osas kattus eksperdi hinnang USA dokumendianalüüsis nimetatud ohustajaga, mida Eesti dokumendianalüüsis ei tuvastatud. Kaheksa eksperti kümnest nimetas Eesti küberjulgeoleku ohustajaks **riike**, viis eksperti **küberkurjategijaid** ja neli **mitteriiklikke tegutsejaid**. Sarnaselt USA dokumendianalüüsile, nimetas üks ekspert ohustajaks **pahatahtlikke tegutsejaid**. Analoogselt Eesti dokumendianalüüsile ei toonud ka ükski ekspert välja **siseringiohustajaid**, ent täiendavalt dokumendianalüüsile nimetas kaks eksperti ohustajateks **kasutajaid**. Eesti dokumendianalüüsi tulemustega kattusid kahe eksperdi hinnangud, kuigi ühel neist oli toodud veel üks ohustaja juurde. Kirjeldatud seoseid kajastab alljärgnev seosemustrikaart (vt joonis 8).



Joonis 8. Eesti küberjulgeoleku ohustajate seosemustrikaart (autori koostatud)

Kõige enam nimetati Eesti küberjulgeoleku ohustajateks **riike**. Täpsemalt nimetati ainult ühte riiki – Venemaad – mis reageerib välispoliitilistele sündmustele küberrünnakutega. Lisati, et riikide käitumine küberdomeenis peegeldab nende käitumist füüsilises maailmas. Sealjuures toodi välja, et küberruumis ei kehti geograafilised piirid nii nagu füüsilises maailmas (vt tabel 7).

Tabel 7. Valik ekspertide tsitaate riigist kui küberjulgeoleku ohustajast (autori koostatud)

"*riiki eelkõige ohustavad teised riigid /.../ viis aastat ettevaatavalt on kahtlemata Venemaa peamine oht Eesti riigile.*" (E1)
"*noh, aga vaata, mis venelaste* modus operandi *on. Tavaliselt, kui keegi neile nagu varba peale astub, siis nad nagu laiatavad sulle kohe küberiga. Kui türklased lasid lennuki alla seal kuskil, siis pärast seda lõid laiaulatuslikud küberrünnakud Anonymouse poolt justkui. /.../ kui hollandlased tegid koostööd selle USA valimiste häkki uurimisel, siis pärast seda Hollandi pangad said pihta kõvasti. /.../ dopingu skandaal venealste sportlastega, siis /.../ spordiorganisatsioonide kontod häkitakse ja varastatakse infot ja lekitatakse. /.../ kui me [Eesti] venelastele varba peale astume, küll ta siis ka küberründab meid*" (E1)
"*Küberdomeen riigipiire ei tunne /.../ näiteid riikidest, kes on küberdomeenis tegutsenud majanduslikest kaalutlustest lähtuvalt a la Põhja-Korea /.../. Riigid käituvad küberdomeenis üldjuhul sama poliitika kohaselt mis teistes domeenides.*" (E10*)

Samas ei pidanud mitte kõik eksperdid riike kõige suuremaks ohustajaks. Üks ekspertidest tõi välja, et suurim oht on ootamatu olukord, milleks Eesti valmistunud ei ole. Paralleeli siinkohal võib tuua kriisiks valmisolekuga, kus on elanikel soovitatud varuda hädaolukorra varu, et paremini hakkama saada (nn ühiskondlik kerksus, vt Riigikogu, 2017, lk-d 18–20).

"*esimesel kohal isegi ei ole täna mingisugused riiklikud ohud, vaid pigem ikkagi see, kus erinevate sõltuvuste kombineerimisel tekivad sellised olukorrad, mida me ei suuda ette näha ja mis on kõige hullem, et me ei ole ka nende tekkimisteks valmistunud /.../ seesama ID-kaart on nüüd hea näide*" (E4)

Küberkurjategijaid nimetasid kümnest eksperdist kuus, kes ütlesid, et see on kogu maailmas ühesugune oht ning nägid peamist põhjust küberkurjategijate soovis raha teenida. Kuigi üks ekspert hiljem täpsustas, et Eestis palju raha ei ole ning peamised motivatsioonid Eesti ründamiseks on kas sõjaline agressioon või Eesti kaudu NATO ja Euroopa Liidu intsitutsioonide õõnestamine.

"*peamine risk ühiskonnas on ikkagi ju kuritegevus, /.../ see on see, mis põhimõtteliselt lööb majandusele pihta /.../*" (E2)

"*laias laastus me oleme täpselt samades ohtudes, mis ülejäänud maailm, et on olemas kriminaalsed grupid, kes tahavad raha teenida. Neil nagu suhteliselt vahet ei ole, kus nad seda raha teenivad*" (E5)

"*otseselt siin [Eestis] ei ole väga mingisugust raha, onju. Me ei ole ka mingisugune raha vahenduskeskus nagu Šveits või mingisugune muu riik, et siin selles mõttes seda motivatsiooni on vähem /.../ reaalne motivatsioon Eestile midagi teha on nagu kaks, et üks on see, et kas tegelikult plaanitakse mingisugust suuremat aggressiooni siia suunas /.../ või siis teine on see, et näidata NATO-t läbi liikmesriigi või Euroopa Liitu halvas valguses*" (E5)

Viis eksperti nimetasid Eesti küberjulgeoleku ohustajaks **mitteriiklikke tegutsejaid**.

"*poliitilistel eesmärkidel motiveeritud, igasugu üksiküritajad ja need, kes lihtsalt nalja teevad, aga need on nagu ikkagi mitme järguvõrra väiksem oht ja võibolla rohkem tulevikus akuutseks muutuv*" (E1)

Kaks eksperti nimetasid Eesti küberjulgeoleku ohustajaks ka **kasutajaid**, kes teadlikult ei soovi halba, kuid oma teadmatusest tehnoloogiaga ümber käimisel loovad olukorra, mis võib riigi julgeolekut ohustada.

"*Eesti küberjulgeolekut tervikuna ohustab kõige rohkem ikkagi rumalus ja see rumalus selletõttu, et noh.. inimlik teadmatus, võimetus mitte niivõrd hinnata ohtu, vaid aru saada tehnoloogiast, mida siis tarvitatakse*" (E4)

Üks ekspertidest nimetas ka **pahatahtlikke tegutsejaid** (*malicious actor*), tõmmates paralleeli Euroopa Liidu uues küberjulgeoleku raamistikus kasutatava terminiga, mis on pehmem sõnastus võrreldes riigi vastutuse sätetega (*wrongful acts*).

"*ohustavad need tegijad või tegurid, kes toimetavad nö pahatahtlikkult küberruumis, ingliskeeles kasutasime väljendit Euroopa Liidu kontekstis* malicious actors*. Ehk, kelle eesmärk on pahatahtlik, kes eirab nö reegleid, rahvusvahelist õigust, kehtivat korda.*" (E7)

Üks ekspert ei nimetanud ühtegi olemasoleva koodiga kattuvat ohustajat, vaid tõi välja Eesti küberjulgeoleku ohuks riigi digitaalset eluviisi: "*ohustab ennekõike ülikergesti ärakasutatav ja mittemaandatav digitaalne eluviis. /.../ ma arvan, et /.../ ID-kaardiga seonduv oli tegelikult alles esimene /.../ .*" (E9)

Sarnaselt Eesti dokumendianalüüsi tulemustele ei pidanud ka ükski ekspertidest Eesti küberjulgeoleku ohustajaks **siseringiohustajaid**, mis tuvastati USA dokumendianalüüsis.

Kategoorias **2. Küberheidutuse meetmed** tuvastati 14 koodi, mis kattus Eesti dokumendianalüüsi 14 koodi osas. Kõige enam nimetati rahvusvahelise võime arendamist ja koostööd, riikide käitumisnormide arendamist küberruumis, info jagamist, tuvastamist, kaitsemeetmeid, kerksust, küberriskide ja ristsõltuvuste haldamist ning õiguskaitseorganite tegevuse tõhustamist. Kõige vähem toodi välja eelhoiatusüsteemi, võime arendamist, õiguskorra

muutmist ja täiendamist ning heidutust toetavaid tegevusi (täpsemalt, rahvusvahelist osalust, luurevõime arendamist ja valitsemisülest lähenemist) (vt lisa 3).

Alamkategoorias **2.1. Diplomaatiline ja poliitiline** tuvastati kolm koodi: **rahvusvahelise võime arendamine ja koostöö**, **riikide käitumisnormide arendamine küberruumis** ning **sanktsioonide kehtestamine**. Kõigi nimetatud koodide puhul vähemalt viis eksperti leidsid, et meetmed on heidutuse jaoks olulised ning ühel juhul – rahvusvahelise koostöö puhul – oli pooldav arvamus selgelt ülekaalus.

Üheksa eksperti nimetasid **rahvusvahelise võime arendamine ja koostöö** oluliseks heidutavaks meetmeks. Hetkel kehtivast ja jätkuvalt olulisena nimetati kõige enam rahvusvahelistes organisatsioonides NATO (kollektiivkaitse klausel) ja Euroopa Liidu liikmelisust. Üks ekspertidest tõi välja ka CERT-de enda koostöövõrgustiku (vt tabel 8).

Tabel 8. Valik ekspertide tsitaate rahvusvahelise võime arendamise ja koostöö sisustamisest (autori koostatud)

"*NATO. NATO. NATO*" (E5)
"*see, et me oleme NATO ja Euroopa Liidu liige*" (E9)
"*NATO CCD COE on käsitletav heidutusmeetmena, sest mingite inimeste /.../ arvamus on see, et tegemist on mingisuguse NATO nö rünnaküksusega, mis paikneb Eestis ja mis siis, kui Eestit rünnatakse hakkab kohe nagu vastu laskma. /.../ noh, et nad ikkagi selles mõttes nagu natuke mõtlevad, et milliseid jälgi nad siia näiteks maha jätavad ja milliseid signatuure siia täheldatakse, sest /.../ kui sa noh hakkad mingisugust riiki ründama, kellel on ikkagi olemas demonstreeritud võimekus või noh sa oled kuskilt lugenud, et tal on see võimekus, mis ei pruugi tõele vastata, kuid noh levitatakse sellist infot, siis sa ikkagi natuke mõtled, kas seda ründama hakata või siis mitte.*" (E4)
"*CERT ise, aga ka nende rahvusvaheline koostöö, /.../ mida nad teevad ju teiste CERT-dega Euroopa tasandil. CSIRT Networki ja kõigis sellistes formaatides.*" (E2)
"*kindlasti on Euroopa Liit. Meie integreeritud üldse Lääne institutsioonidesse /.../ kahepoolsed suhted teiste riikidega*" (E1)

Ekspertintervjuudest käis läbi ka Euroopa Liidu Nõukogu ühine diplomaatilse reageerimise raamistik, mis võeti vastu 2017. aasta lõpul Eesti eesistumise raames. Lisaks leidsid mõned eksperdid, et seda peaks Eesti tulevikus kindlasti ära kasutama. Näiteks üks ekspertidest tõi esile, et võiks paluda Euroopa Liidu ühtsel välisteenistusel esitada demarš riikidele, mis ei taha teha koostööd (vt tabel 9).

Tabel 9. Eksperdi kirjeldus diplomaatilise ja poliitilise meetme võimalikust kasutamisest (autori koostatud)

"*näiteks, kui Eestis saab kannatada /.../ mingite perioodiliste rünnakute läbi /.../ ja me näeme, et see kahepoolne pöördumine kompetentsi kanalite kaudu ei too tulemit, siis me võiksime täiesti vabalt kasutada selle jaoks ka välispoliitilisi kanaleid, /.../ näiteks /.../ Türgist tuleb Eesti pihta mingi rünnak, onju, mille puhul me näeme, et jäljed viivad Türki. Seda me ei tea, kuhu nad sealt edasi viivad. Siis võiksime meie vabalt paluda /.../ Euroopa Liidu ühtne välisteenistus, palun tehke Türgi suunas démarche ja siis vaadata, mis juhtub. Seda me ei ole kunagi proovinud. /.../ ja see on nüüd selle Euroopa Liidu paketis sees, et iga Euroopa Liidu liikmesriik saab seda teha, võib sisuliselt minna Brüsselis laua taha ja öelda, et mul oli massiivne küberrünnak. Sellele olid sellised ja sellised tagajärjed. Mina tean, et see otse läks Türki. Minu need CERT või luureteenistus /.../ on selle välja selgitanud. Seda ma ei tea, kas Türgi on selle eest vastutav. Ma palun, et tehke Türgi suunas* démarche*. /.../ selliste kolmandate riikide puhul töötab väga hästi see piinlikkuse argument. /.../ mingisugune president või /.../ välisminister /.../ kasvõi /.../ osakonna juhataja kuskil välisministeeriumis, ta ei taha teada, et tema riik tegeleb mingisuguse küberiga või et keegi kuskil midagi ründab. Ta ei taha, et see segab tema* grand design*'i nagu Euroopa Liidu suhtes. Ja kui sa muudad selle küberi mängu toomise alati süsteemseks, siis sa tegelikult /.../ lõpp-kokkuvõttes suurendad oma heidutushoiakut.*" (E9)

Üks ekspert tõi veel välja, et rahvusvahelise võime arendamine seisneb arengukoostöös, mille senist tegevust võiks siduda kübervaldkonna teemadega.

"*see on arengukoostöö, mida me teeme nii või naa, miks mitte siis siduda olemasolevat arengukoostööd ka küberiga ja /.../ see on miski, mida me oleme mõni aasta teinud ja mida me teeme ka edaspidi, et see kindlasti võiks olla selle strateegia osa. vähemalt see rahvusvahelise koostöö bloki all.*" (E7)

Kaheksa eksperti tähtsustas **riikide käitumisnormide arendamist küberruumis** heidutava meetmena ning üldiselt leiti, et sellel suunal tuleks edasi tegutseda. Kolm eksperti leidis, et selle kasutegur on pigem marginaalne või kaudne, sest Eesti küberjulgeoleku ohustaja rahvusvahelisest õigusest ise kinni ei pea ning teisalt on need ainult poliitiliselt siduvad (vt tabel 10).

Tabel 10. Valik ekspertide tsitaate riikide käitumisnormide arendamisest küberruumis (autori koostatud)

"*Eesti väike riigina on alati olnud hästi tugev selle põhimõtte toetaja, et rahvusvaheline õigus kehtib ka küberruumis. See on meie üks julgeolekugarante, /.../ meie eksistentsi tagabki nii-öelda teatud kehtiv reeglistlik õigusruumis. Et seda üle korrata ka siseriiklikult lihtsalt kasvõi ühe lausega üle korrata, et see kehtib ja see on olemas nagu on minu arust oluline*" (E7)
"*ma arvan, et Eesti on suhteliselt aktiivselt /.../ arvestades ikkagi meie väiksust, siis /.../ ma arvan, et me oleme seal*

väga hästi toimetanud ja väga aktiivselt, et seda kindlasti tuleb jätkata ja välisministeerium /.../ on seda jätkamas ka. /.../ et siin ma arvan, et see on kindlasti üks asi, millega me saame ja peame tegelema." (E1)
"*see tähendab seda, et meie oleme dzentelmenid, aga ma tean, et meie vastased ei ole. /.../ me ei saa arvestada, et nemad täidavad rahvusvahelise õiguse norme. Tõsi küll, meie ise ikkagi järgime oma väärtusi ja käitume väärikalt, aga see ei ole heidutus vastasele. /.../ ainuke moment, et me oleme ühtsed, et me kehtestame omad põhimõtted ja käitume nii, ta teab seda.*" (E6)
"*mul nagu usk on väike, eks ole. Need on ikkagi poliitiliselt siduvad ainult*" (E3)
"*Kaudse mõjuga; pigem fooniloov tegevus. Kasutatav heidutusena küll, aga kaudselt, sidudes soovimatu tegevuse teatud hulga automaatsete ja varem kokkulepitud sanktsioonidega*" (E10*)

Sanktsioonide kehtestamisel oli üldine ekspertide hinnang, et Eesti ainuüksi selle meetme rakendamisel toime ei tule ja seega on vaja selle meetme kasutamisel teha koos liitlastega, seejuures nähti peamise liitlasena Euroopa Liidu liikmesriike. Üks ekspertidest veel rõhus, et rahalised sanktsioonid peaksid olema suunatud ründe korraldaja, mitte teostajale ning teine, et see on potentsiaalselt pikaajalise heidutava mõjuga (vt tabel 11).

Tabel 11. Valik ekspertide tsitaate sanktsioonide kehtestamisest (autori koostatud)

"*ilmselt oleksid EL sanktsioonid tõhusamad kui Eesti enda omad*" (E8)
"*täpsustus: ainult EL sanktsioonid*" (E9)
"*sanktsioonid on mõjusamad läbi Euroopa Liidu. /.../ Eesti ei suuda oma sanktsioonidega väga palju mõju avaldada, kuid noh, võimalik ründaja tõenäoliselt impordib ja ekspordid meile nii mõndagi, aga lihtsalt see maht on niivõrd pisike, et see üksikuna ei toimi.*" (E6)
"*rahalised sanktsioonid, /.../ kui me räägime riigi-poolsetest rünnakutest /.../ siis pigem see sanktsioon peaks olema strateegiliselt kõrgemal tasandil, see, kes juhib seda, mitte selle läbiviijale"* (E3)
"*Jah, potentsiaalselt pikaajalise heidutava mõjuga, aga vaid reaktsioonina juba toimunud rünnakule eesmärgiga heidutada tulevasi rünnakuid korraldamast.*" (E10*)

Alamkategoorias **2.2 Informatiivne** pidas **info jagamist** seitse ja **parima praktika jagamist** oluliseks viis eksperti. Üks ekspertidest arvas, et parim praktika on küll kena kui on, aga ilma selleta saab ka hakkama. Kaks eksperti rõhutasid, et infot peaks jagama strateegilist partnerite ja liitlastega. Üks ekspertidest tõi välja pikema loetelu infost, mida tuleks jagada (nt signatuuride, analüüside, mustrite jne) ning ütles, et kogu maailmas on info jagamine probleemne. Eelnevat kinnitas veel üks ekspert, kes ütles, et info on olemas, aga seda tuleb analüüsida ning seejärel jagada nii Eestis sees kui ka rahvusvahelise tasandil (vt tabel 12).

Tabel 12. Valik ekspertide tsitaate info jagamisest (autori koostatud)

"*noo see on suurepärane, et ameeriklased on endale sellise strateegiliselt kirja pannud, aga võiksid käituda ka ehk* accordingly. *Selles suhtes, et kui sa tahad vastase /.../ rünnaku hinda tõsta, siis see tähendab eelkõige informatsiooni jagamist. /.../ see on nüüd asi, milles ma arvan on kogu maailm nõrk selles kübervaldkonnas.*" (E5)
"*signatuuride jagamine, konkreetsete analüüside jagamine, vastase MO – modus operandi – kuidas asju on läbi viidud, kust need kohad on neid märgata jne. Et nagu selliseid asju tehakse nagu kuskil siseselt, onju. /.../ sõjaväes me kutsume neid SOP-deks* [standard operating procedure] */.../ ja siis on TTP, /.../* training tactics procedures */.../ ja siukeste asjade jagamine, et sa jõuaksid sellesse, et sa suudaksid süsteemi tegelikult analüüsida äriliselt vaatest, et nagu see arusaam, et mis need nagu põhiväärtused on, /.../ neid asju täna ei jagata, neid asju ei teha. Et küber on ikkagi suhteliselt niši-*business*, minu arust täna. See on nagu tehnikute lõbu natukene*" (E5)
"*tegelikult seda infot on /.../ jagama teistega nii Eestis sees kui rahvusvaheliselt. See on kindlasti asi, mis on RIA teha ja mida /.../ rohkem analüüsima seda infot, mis /.../ on ja seda siis rohkem teistega jagama.*" (E1)

Alamkategoorias **2.3 Militaarne** tuvastati koodidena **eelhoiatussüsteem** ja **küberoperatsioonide arendamine ja läbiviimine**. **Eelhoiatussüsteemi** all toodi välja ennekõike olukorrateadlikkust (*situational awareness*), mida pidas oluliseks neli eksperti. Üks ekspertidest tõi välja, et olukorrateadlikkuses on kogukonnal oma tähtis roll kanda. Samuti nimetas ekspert, et selle abil on võimalik omistada küberründe id, mis teebki sellest meetmest heidutuse.

"*küberruumis see eelhoiatuse arendamine on midagi hoopis teistsugust. /.../ see on siis kogukonna põhine nagu kogu see meie küberkaitse on.*" (E1)

"*Kindlasti osa kaitsest. Kui eelhoiatuse all pidada silmas ka üldist situatsiooniteadlikkust, siis on ta väga oluline just atributsiooni vaatenurgast. Raske on – eriti veel veenvalt – küberrünnakut kellelegi omistada, kui puudub veenvus üldise situatsiooniteadlikkuse osas.*" (E10*)

Viis eksperti ütlesid, et **küberoperatsioonide arendamine ja läbiviimine** on oluline ennekõike kaitsmise eesmärgil, kuid nentisid, et seda on keeruline saavutada. Siinkohal toodi ka välja, et oluline on meetme koosmõju kommunikatsiooniga: vaenlane peab olema teadlik võimest ning millised on nö punased jooned, millise tegevuse puhul riik on valmis vastu ründama. Kommunikatsioonita võib heidutus ebaõnnestuda, sest ta ei oska olulisi asjaolusid arvesse võtta.

Üks ekspertidest tõi välja, et Eestis ei ole veel selget küberheidutuse diskussiooni tekkinud ning 2014–2017. aastal kehtinud küberjulgeoleku strateegiasse sai see ettevaatlikult ja üldiselt kirja

pandud. Kaheldi, mis signaali see võib anda ja kuidas seda tõlgendada võidakse – kas väljakutset esitavana või osutub see järjekordseks infosõja argumendiks, mida Eesti vastu kasutada (vt tabel 13).

Tabel 13. Valik ekspertide tsitaate küberoperatsioonidest (autori koostatud)

"*Vajalik enda kaitsmiseks elementaarsel tasandil, kuid heidutusefekt tekib alates teatud tehnilisest võimekusest, mida on keerulisem saavutada*." (E8)
"*ennekõike sul peab olema võimalus seda ründavat ja kaitsvat ründevõimekust järjepidevalt arendada. /.../ see /.../, kes sind ründab, ta peab teadma seda, et sa võid rünnata vastu ja sa võid ka paljastada tema anonüümsuse.*" (E4)
"*Võib olla oluline osa üldisest heidutushoiakust, kui kõrvuti võime arendamisega tegeletakse ka deklaratoorse poliitikaga (ehk sõnumite süstemaatilise väljutamisega teemal: millisel juhul, vastuseks missugusele rünnakule, on riik valmis omapoolset küberrünnet teostama; milline on see võime jne). Kui on ainult küberründevõime ilma selleta, et keegi teine teaks, et selline võime on, siis panustab see küll potentsiaalselt kaitsesse, aga mitte heidutusse. Kui on ainult deklaratoorne poliitika ilma võimeta (ehk bluff), siis on iseenesest kaitse null, aga heidutushoiak potentsiaalselt olemas eeldusel, et teine usub võime olemasolu ja see toimib tema kasude-kahjude analüüsis heidutaja poolt soovitud viisil. Võib ka toimida vastupidi: provokatiivselt.*" (E10*)
"*ma olen suht kindel, et Eestis ei ole nagu küberruumis heidutust keegi korralikult läbi mõelnud. Kõige lähemale mulle meenub /.../, kui tehti seda kehtivad küberjulgeoleku strateegiat. /.../ tõstatsin teema, et kui me kirjutame sinna sisse ründavate operatsioonide, küberründavate operatsioonide läbiviimise, et mida see teeb, kas see loob heidutust või vastupidi see nagu nõrgendab meie ütlust, provotseerib. /.../ ja siis /.../ tuli umbes vastus, et /.../ vahet pole, et kedagi ei huvita /.../ Seda strateegiat tehti ka nii, et umbes igaüks vaatas oma sisemist /.../ comprehensive /.../ lähenemist ei olnud. /.../ ja ka see mõte oligi siis, et nagu ärme siis nagu kirjutagi seda sellisena lihtsalt välja, sest /.../ meie suutlikkus /.../ on tegelikult salastatud, eks, /.../ et kui sa kirjutad sinna, et me teeme nagu rünnet, /.../ näidake siis, mis rünnet te siin teete. Või siis hakkabki süüdistama meid, et kuulge eestlased ründavad meid siin. Ja kuna meil ei õnnestunud tekitada sellist ametkondlikku arutelu või suuremat analüüsi /.../ sellel teemal, siis /.../ kirjutasime selle ettevaatlikult sisse, /.../ aga see oli selline mõtlemine siis.*" (E1)

Alamkategoorias **2.4 Tehniline** oli kodeeritud neli koodi: **kaitsemeetmed**, **kerksus**, **tuvastamine** ja **võime arendamine**. Kõige olulisemaks seitsme eksperdi poolt peeti **kaitsemeetmeid** ehk infosüsteemide moderniseerimist ning **kerksust** ning kõige vähem, ühe eksperdi poolt, nimetati kaitsemeetmetest juurdepääsu piiramist. Infosüsteemide moderniseerimise osas toodi välja, et see on oluline osa kaitsvast heidutusstrateegiast ning teine ekspert lisas, et riik peab abistama infovara ja -süsteemi omanikke selle tegemisel. Lisaks tõi üks ekspertidest välja Eesti eripärana, et riik suunab kasutajaid uuendama infosüsteemide, muidu ei saa kasutada riigi poolt pakutavaid e-teenuseid (nt ID-kaarti). Selle meetme õigustatavust näitas näiteks suurt kahju tekitanud pahavarade kampaaniad WannaCry ja NotPetya – Eesti jäi suures osas puutumata.

"*ID-kaardi tehnika toimimiseks sa pead oma windowsi operatsiooni süsteemi uuendama, see peab koguaeg uuendatud olema. /.../ see oli ka üks oluline vahend, miks meist WannaCry ja NotPetya mööda läksid, eks. /.../ ameeriklastel ei olegi sellist keskset vahendit, kuidas mõjutada. Et meie jaoks on need tegelikult nagu governance vahendid, kuidas mõjutada neid teatud kriteeriumi täitma kõiki erinevaid osapooli nii era kui avalikus sektoris.*" (E1)

Kerksust nähti seitsme eksperdi poolt üheselt kõige rakendatavama heidutusmeetmena, mis on Eestis tehtav ning millega tuleks kindlasti jätkata. Sellegi poolest üks ekspertidest kõhkles kontseptsiooniliselt, sest pidas liigseks ohuks kerksuse seotust militaar valdkonnaga (vt tabel 14).

Tabel 14. Valik ekspertide tsitaate kerksusest (autori koostatud)

"*Kerksus – mina toetaks seda kõige enam. /.../ et make it hard. /.../ muuda end nö ebaatraktiivseks sihtmärgiks. Alati leitakse keegi, kes on lihtsam ja kergem, kergemini haavatatavam ja üldiselt minnakse lihtsama vastupanu teed. /.../ ma arvan, et see peaks väga tugevalt nagu sees olema, et sellele panustamine ja mitte ainult nii öelda aja ja töö mõttes, vaid ka rahaliselt panustamine, et seda kerksust nagu koguaeg saaks arendada. see ma arvan on üks nagu olulisemaid asju siin.*" (E7)
"*see on nagu peamine meie väärtus, mida meie loome heidutuse jaoks.*" (E1)
"*mina ei poolda nende sõjaliste terminite niimoodi ülevõtmist, /.../ ta on ikkagi suhteliselt noh, kitsas kontseptsioon ja kui sa nüüd laiendada teda kõigile, see on mõnes mõttes nagu militaariseerid kõike /.../*" (E3)

Kuigi dokumendianalüüsis oli **tuvastamine** ennekõike seotud haavatavuste, küberrünnakute ja -ohtude ning võrguseirega, siis kolm eksperti mõistsid selle all ennekõike üldist situatsiooniteadlikkust, mida peeti väga oluliseks. Üks ekspertidest täiendas, et tuvastamisel on väga oluline roll inimanalüütikul, sest tehnika ei ole veel suuteline seda ise tegema (nt nägema anomaaliaid, neid mõistma ja konteksti asetama).

"*aga see tuvastamine ei ole võimalik ainult tehnikaga, siin on inimanalüütikut ka vaja, sest tehisintellekt ei ole täna nii tasemel. Üldse spionaazi tüüpi ründeid, et sa otsid anomaalialid, ebaharilikku tegevust, mida püüab teinekord väga hästi maskeerida. Ja isegi, kui sa arened tehniliselt, siis tänapäeval inimene peab ikkagi seda juhtima. võibolla 50a pärast tehisintellekt ületab seda.*" (E5)

Võime arendamist seostas kolm eksperti militaarse valdkonna küberopatsioonide arendamise ja läbiviimisega, mida peeti oluliseks. Üks ekspert rõhutas, et nii kaitseväe poolel

küberoperatsioonide arendamine kui tsiviilvaldkonda jääv võime arendamine peaksid omavahel olema integreeritud, sest see loob tervikuna vajaliku ja rakendatava oskuse. Kaitseväe poolelt nähakse väga kindlat konteksti, kuid ei pruugita mõista üldist julgeolekulist tähendust, mis jääb kaitseväe pädevusest välja. Ekspert tõi näitena Tšehhi teadlaste teavituse ID-kaardi turvaveast, kus Kaitseväel vastav krüptograafia-alane kompetents puudub mõistmaks selle mõju e-riigi ökosüsteemile. Üldiselt ekspertintervjuudest jäi kõlama, et Eestis on vähe kõrgetasemelise kompetentsiga eksperte.

Oli ka eksperte, kes leidsid, et Eesti teeb juba enamust, kuid samas nenditi, et arenguruumi on, sest olemasolevat ei tehta tõhusalt või on nendega muid probleeme. Kaks eksperti rõhutasid täiendavalt, et kõik peaksid mõtlema julgeolekuliselt, kuna see ei ole ainult ühe asutuse vastutada (vt tabel 15).

Tabel 15. Valik ekspertide tsitaate tehnilise valdkonna meetmetest (autori koostatud)

"*me teeme kõike neid /.../ samu asju, aga nagu omamoodi ja mingites asjades me oleme kindlasti ees kui näiteks USA*." (E5)
"*kõik peavad tegema. See on siukene kultuuriline asi, et nagu kõik peavad mõtlema julgeolekuliselt, et /.../ Ida piiri taga /.../ kellelgi on plaanis see pikali joosta ja halvata meie ühiskonna toimimist. /.../ kogu kogukond peab hakkama mõtlema julgeolekuliselt. See on see väljakutse, /.../ see on see, mis loob selle kerksuse. /.../ ma arvan, et see on siuke töö, mis kunagi ei lõppe. /.../ teiste riikidega võrreldes meil on natuke parem seis, aga noh üldiselt on see väljakutse ikkagi võimas.*" (E1)

Alamkategoorias 2.5 Juriidiline pidas seitse eksperti oluliseks **küberriskide ja ristsõltuvuste haldamist**. Üks ekspertidest nentis, et tal puudub usk juriidilistesse meetmetesse, kui neid ei suudeta kohaldada.

"*kui ma Eestis midagi välja tooks, millega meil on probleeme, millega on teistel veel rohkem probleeme on see sama ristsõltuvuste haldamine ja küberriskide maandamine*" (E5)

"*aga kindlasti seda, et mul puudub absoluutselt igasugune usk juriidilistesse meetmetesse, mida sa ei suuda tegelikult kohaldada.*" (E4)

Kaheksa eksperti pidasid oluliseks **õiguskaitseorganite tegevuse tõhustamist**, kuid täpsemalt seda ei sisutatud, mis lisaks olemasolevale paremini olema peaks. Seejuures hetkel kehtivatest

heidutusena mõjuvatest asjaoludest nimetati Eesti karistusseadustikku ja süüteo toimepannute väljaandmist.

"*kui me räägime heidutusest näiteks küberkurjategijate vastu, /.../ üks väga konkreetne näide: kuna Eestis on praktika küberkurjategijad, kes on näiteks oma kuriteo toime pannud Ameerika Ühendriikides /.../, siis on noh praktika need välja anda. Seda paljudel riikidel ei ole. ja see on üks heidutusmeetmetest. /.../ sa tead, et kui sa paned /.../ küberkuriteo toime, siis /.../ Eesti annab su välja. Eesti ei hakka sind kaitsma.*" (E4)

Täiendavalt olemasolevatele meetmetele lisas üks ekspert, et Eestis mõjub heidutavalt ekstreemne avatus.

"*heidutusväärtust omab tegelikult /.../ meie e-ühiskonnast ja meie kogukonna väiksusest tulenev ekstreemne avatus. /.../ iga pahalane tegelikult, kes vähegi analüüsib Eestit kui targetit saab aru, et Eestis on väga keeruline midagi selliselt korraldada, et see ei jää teadmata. /.../ see ID-kaardi värk näitas tegelikult väga ilmekalt, kui me saame mingist riskist teadlikuks või kui kusagil on mingisugused anomaaliad, siis* it's going to be out there." (E9)

Vaid neli eksperti nimetas olulisena **õiguskorra muutmist ja täiendamist**. Eraldi toodi välja, et uurida tuleks õiguskorda RIA korrakaitsepädevuse osas. Samuti nimetati peatselt jõustatavat küberturvalisuse seadust, millega õiguskorda muudetakse konkreetsemaks, kuid nenditi, et on üldine probleem, et kübervaldkonda reguleerivad seadused, mis kehtivad ajast, kui interneti ei olnud veel loodud.

"*RIA korrakaitsepädevust kui ... kriminaalmenetluse, eriti piiriülese kriminaalmenetluse, tõhustamist*" (E2)

"*meil on üsna hea ja nüüd, kui hakkab kehtima see KÜTS, siis muutub see veel konkreetsemaks, aga üldiselt nagu paljude riikide pealt on näha, et endiselt reguleerivad seda valdkonda seadused, mis kehtivad ajast, mil internetti polnud olemas*" (E7)

Alamkategoorias 2.6 **Majanduslike** meetmete hulgas nimetatud **küberturvalisusesse investeerimist** pooldasid viis eksperti.

USA dokumendianalüüsist lisandunud alamkategooria 2.7 **Heidutust toetavate meetmete** osas toodi välja kõige enam ainult ühte – **teadus- ja arendustegevust**. Selle all nimetati näiteks vajadust ajakohastada haridussüsteemi ning samuti leiti, et üldine teaduse arendamine on väga väike Eestis.

"*mitte ainult see, et sa kannad läbi formaalhariduse, vaid see ka, et ... spetsiifilisi oskusi neis valdkondades tegutsemiseks ikkagi vaja on, mida sa noh, baasoskustega ülikooli lõpetades sa pead niikuinii hakkama kusagil, kuhu sa lähed, kohanema, selle konkreetse töökoha vajadusega. ... me omandame mingisugused standardiseeritud klotsid, onju ... lõpetame gümnaasiumi oma standardiseeritud klotsiga, läheme ülikooli, omandame seal selle standardiseeritud klotsi ja siis tõmbame joone vahele ja siseneme tööturule ... haridus võiks olla oluliselt integreeritum*" (E2)

2.3.2. Ekspertintervjuude järeldused

Ekspertintervjuude põhjal võib järeldada, et enamus eksperte lähtuvad küberheidutuse tõlgendamisel laiast käsitlusest. Kõige paremini mõisteti heidutavaid meetmeid oma valitud eriala valdkonnast lähtuvalt ning vastupidi, vähem pöörati tähelepanu eriala-välistest heidutuse meetmetest. Kaks eksperti lähtusid pigem kitsast küberheidutuse tõlgendusviisist, kuid nentisid intervjuus, et teised meetmed võivad kaudselt heidutusena mõjuda. Nendel juhtudel jäi ka mulje kõrgetest ootustest küberheidutusele – oodati justkui hõbekuuli, mis lahendaks tuumaheidutusele sarnase konkreetsusega võimalikke konflikte. Siiski suurem osa eksperte suhtusid küberheidutusse avatult. Autor leiab, et kui küberheidutuse võimalikest rakendamise võimalustest ollakse paremini teadlikud ning kui jõutakse järeldusele, et kitsas tõlgendus piirab põhjendamatult kasuliku kontseptsiooni rakendamist, siis ollakse avatumad küberheidutusse suhtumisel. Selleks oleks tarvis tekitada diskussioon ekspertide, akadeemikute ja poliitikute seas ning uurida küberheidutuse teemat edasi.

Nagu dokumendianalüüsi järeldustes nimetati, siis hetkel kehtivad heidutuse meetmed on kommunikeeritud (vt käesolev töö, lk 49), kuigi neid annaks efektiivsemalt kommunikeerida näiteks koondades küberheidutust puutuv osa ühte strateegiasse. Nende meetmete osas, mida ekspertintervjuudes arvati, et Eesti võiks veel lisaks kasutusele võtta, tuleb täiendavalt kommunikeerida. See saab täidetud näiteks siis, kui need kaasatakse uude Eesti küberjulgeoleku strateegiasse sisse.

Ekspertintervjuude analüüsi tulemused on sarnaselt dokumendianalüüsile ainult osaliselt kooskõlas maailmakorraga johtuvalt teoorias kirjeldatule (vt ptk 1.2), kuid samas nimetasid eksperdid selgelt välja riigi, mis ohustab Eestit kõige enam – Venemaa. Konkreetne ohustaja võib olla aluseks Eesti heidutuse strateegia kujundamisel. Nimelt on veel olemas kohandatav heidutusstrateegia, mis luuakse vastavalt olukorrale, võimalikule vastasele ja muudest asjaoludest lähtuvalt heidutuse sõnumid ja tegevused (vt käesolev töö, lk 28).

Siseringiohustaja hulka võib iseenesest hõlmata ka kasutajad, sest USA definitsiooni kohaselt võib siseringiohustaja ka eneseteadmata ja tahtmatult küberjulgeolekut kahjustada (vt käesolev töö, lk-d 38–39). Ekspertide arvamuse kohaselt ohustab kasutaja oma teadmatusest küberjulgeolekut (nt ei oska käsitleda õigesti tehnoloogiat, ei pea kinni baasküberhügieenist jne). Seega võib öelda, et koos dokumendi- ja ekspertintervjuude analüüsi tulemusena kattuvad Eesti ja USA küberjulgeoleku ohustajad. Nimetatud ohtu saab maandada ekspertide poolt välja käidud heidutust toetava meetmega – teadlikkuse tõstmine ja kaitsemeetme osas välja toodud baasküberhügieeni ning IT-standardite rakendamise ja neist kinni pidamisega (vt käesolev töö, lk-d 44–45).

Sarnaselt dokumendianalüüsi järeldustele oli ekspertide hulgas enim levinud laiendatud ja tõkestava heidutusstrateegia elemendid (vt lisa 3), mida üldistatult võib nimetada kaitsepoliitikaks. Dokumendianalüüsi ja ekspertintervjuude põhjal võib seega järeldada, et Eesti peaks jätkama senist kurssi.

Ekspertintervjuudes keskenduti rohkem meetmetele, mida saaks rakendada, ja vähem toodi välja meetmeid, millega Eesti ei peaks üldse tegelema (vt lisa 3). Kõige enam poolehoidu avaldatakse diplomaatiliste ja poliitiliste ning tehnilise valdkonna meetmete osas. Täpsemalt toodi välja rahvusvahelist koostööd ja kollektiivkaitset ning infosüsteemide moderniseerimist ja ristsõltuvuste haldamist. Teisalt oli võrdselt neid, kes leidsid, et rahvusvahelisest õigusest ja juriidikast üldiselt võiks abi olla ning neid, kes nägid nendel meetmetel marginaalset mõju olevat. Rahvusvahelises koostöös oli sarnaselt dokumendianalüüsile nimetatud NATOt, millel on Eesti küberheidutusel oluline roll kanda. Lisaks nimetati CERTi koostööpartnereid, kellega peaks rahvusvahelisel tasandil koostööd tegema.

Kaks eksperti tõid välja eelmise aasta lõpus Euroopa Liidu poolt vastuvõetud diplomaatilise reageerimise raamistiku, mida Eestis tuleks ka rakendada ja praktikasse võtta. Raamistik hõlmab endas näiteks ka ühist sanktsioonide kehtestamist. Seega võiks kaaluda uues Eesti küberjulgeoleku strateegias raamistiku olulisuse rõhutamisest ning et Eesti võib oma tegevuses võimaliku ründe või ohu korral aktiivselt kasutada raamistikus nimetatud võimalusi.

Info jagamise ja eelhoiatussüsteemi osas olid arusaamad vastukäivad. Need, kes pidasid oluliseks eelhoiatussüsteemi tõlgendades seda kui olukorrateadlikkust, ei pidanud samas info jagamist niivõrd prioriteetseks.

Mitmete meetmete puhul (sanktsioonide kehtestamine, eelhoiatussüsteemi ja küberoperatsioonide arendamist ja läbiviimist) lisati, et Eesti üksi seda tagada ei saa ja selleks tuleb liitlastega teha koostööd. Siia hulka võib veel nimetada ka riikide käitumisnormide arendamist küberruumis, mille jaoks on vajalik võimalikult paljude riikidega saavutada konsensus.

2.4. Eesti küberjulgeoleku tugevdamise võimalused läbi küberheidutuse: järeldused ja ettepanekud

Magistritöö teises, empiirilises, peatükis uuriti, milliseid küberheidutuse meetmeid on Eesti ja USA oma strateegiadokumentides nimetanud ning mida arvavad neist Eesti julgeolekupoliitika kujundajad, seejärel analüüsiti tulemusi. Läbivalt järgis autor, et püsida teoorias ette antud kontekstis. Käesolevas peatükis koondatakse tulemused kokku ja vastatakse uurimisküsimustele eesmärgiga tuvastada, milliseid meetmeid võiks Eesti oma uues küberjulgeoleku strateegias kasutusele võtta.

Esimene uurimisküsimus uuris Eesti ja USA küberjulgeoleku ohustajaid, mille jaoks koguti andmeid nii teooriast, dokumendianalüüsist kui ekspertintervjuudest. Püstitatud uurimisküsimuse eesmärk oli vaadelda ja kontrollida, kas välja selgitatud küberheidutuse meetmed on sobivad olemasolevaid ohustajaid heidutama. Teooriast selgus, et rahvusvahelise süsteemi ainsateks subjektideks on riigid, mis ohustavad teisi riike, sest valitseb hobbesilik maailmakord ning seega peab igaüks tagama iseenda julgeoleku (vt käesolev töö, lk 22). Üheks viisiks julgeoleku tagamisel on rakendada heidutuse kontseptsiooni. Arvestades, et tänapäeval on tekkinud viies

sõjapidamise domeen ehk küberdomeen, siis on tarvis uurida ka meetmeid, mis heidutaksid lisandunud domeenis ohustajaid. Seetõttu uuriti juurde ka teisi andmekogumismeetodite tulemusi.

Dokumendianalüüsis selgus, et Eesti küberjulgeoleku ohustajateks on riigid, küberkurjategijad ja mitteriiklikud tegutsejad ning USA küberjulgeolekut ohustavad veel täiendavalt pahatahtlikkud tegutsejad ja siseringiohustajad. Kuigi pahatahtlikud tegutsejad ei ole otseselt eraldiseisev ohustaja, vaid pigem koondnimetus küberjulgeoleku ohustajatele, nö sünonüüm. USA küberjulgeoleku ohustajaid uuris autor seepärast, et kontrollida, kas need kattuvad suures osas Eesti ohustajatega ning kui, siis on see lisakinnituseks, et küberheidutuse meetmed, mida soovitada Eestis kohaldada on sobivad ka Eesti küberjulgeoleku ohustajatele.

Ekspertintervjuudes nimetati Eesti küberjulgeoleku ohustajateks veel lisaks dokumendianalüüsi tulemustele ka kasutajaid, kes ei oska oskuslikult infotehnoloogiaga ümber käia ning keda võiks paigutada USA siseringiohustaja definitsiooni kohaselt alla. Samuti nimetati pahatahtlikke tegutsejaid, mis tuleneb uuest Euroopa Liidu küberjulgeoleku raamistikust. Ekspertintervjuude tulemusena täpsustati, et riikidest ohustab Eestit kõige enam Venemaa.

Eelnevast tulenevalt saab vastata esimesele uurimisküsimusele järgnevalt: Eesti küberjulgeolekut ohustavad **riigid**, **küberkurjategijad**, **mitteriiklikud tegutsejad**, oskamatud **kasutajad** ja **pahatahtlikud tegutsejad** ning USA küberjulgeolekut ohustavad dokumendianalüüsi kohaselt: riigid, küberkurjategijad, mitteriiklikud tegutsejad, pahatahtlikud tegutsejad ja siseringiohustajad.

Teisele uurimisküsimusele, millised on heidutusteooriast tulenevad tingimused, millele küberheidutus peab vastama, leiti vastus teooria uurimisest. Ilmnes, et küberheidutusel ei ole omaette eritingimusi loodud ja heidutusele kehtivad igas domeenis ühesugused tingimused. Seega on vastus teisele uurimisküsimusele: heidutus peab olema võimalikule vastasele kommunikeeritud ning heidutus peab olema usutav, see tähendab, et riigil peab olema võime heidutuses lubatut täide viia, ta on valmis tekitama kahjusid ning ta omab tahet heidutuses lubatut täide viia. See tähendab, et tegu ei ole pelgalt blufiga. Selleks omakorda analüüsitakse: kuidas on varasemalt sarnastes oludes tegutsetud (st sõnum ja teod peavad olema järjepidevalt ühtsed); millised on valitsuse avaldused ja käitumine ning milline on avalikkuse arvamus olukorrast. (vt tabel 3, käesolev töö, lk 25)

Kolmandale uurimisküsimusele, millised on Eestis ja Ameerika Ühendriikides kehtivad küberheidutuse strateegilised meetmed, leiti vastused dokumendianalüüsi tulemusena. Erinevaid meetmeid identifitseeriti üle viiekümne, mis tõhusama situatsiooni analüüsimiseks ja otsustamiseks jaotati kohandatud mudeli DIME alusel viide valdkonda: diplomaatiline ja poliitiline, informatiivne, militaarne, tehniline, õiguslik ja majanduslik (vt lisa 3). USA dokumendianalüüsi tulemusena selgus, et heidutuse strateegiasse on kaasatud meetmeid, mis toetavad heidutust. Nimetatud meetmeid leiti kokku kuus: luurevõime arendamine, rahvusvaheline osalus, strateegiline kommunikatsioon, teadus- ja arendustegevus ning valitsusülene lähenemine. Heidutusteoorias selline käsitlus puudus, kuid seda võib kaaluda Eesti heidutuse strateegia arendamisel.

Eestis kehtivaid küberheidutuse strateegilised meetmeid leiti nii Eesti dokumendianalüüsist kui ka ekspertintervjuudes käigus. Erinevaid meetmeid selgitati välja alla kolmekümne, mis sarnaselt USA dokumendianalüüsile jaotati kohandatud mudeli DIME alusel viide valdkonda (vt lisa 3). Kuna USA dokumendianalüüsis ilmnes, et USA on kaasanud heidutuse strateegiasse ka heidutust toetavaid meetmeid, otsustas autor laiahõlmava uurimise eesmärgi täitmisel uurida Eesti dokumendianalüüsi käigus heidutust toetavate elementide kohta. Selgus, et teatud määral on Eesti heidutuse strateegias heidutust toetavad meetmed olemas. Rahvusvaheline osalus on sarnane rahvusvahelise võime arendamise ja koostööga; lisaks teadus- ja arendustegevusele rõhutati ka teadlikkuse tõstmise vajadust, mis toetab heidutust kaudselt ning valitsusülene lähenemine on sarnane riigikaitse laiale käsitlusele.

Neljandale uurimisküsimusele, millised on küberheidutuse strateegilised meetmed, millega Eesti saaks küberjulgeolekut tugevdada USA näitel, leiti vastused nii Eesti dokumendianalüüsist kui ka ekspertintervjuude käigus.

Dokumendianalüüsi ja ekspertintervjuude tulemusena selgus, et hoolimata asjaolust, et Eestis puudub eraldiseisev heidutuspoliitika, on Eestis heidutuse strateegia elemente juba praegu strateegiadokumentides olemas. Kuigi vastane võib heituda mingist asjaolust, mida riik ei ole teadlikult ja eesmärgipäraselt heidutusena sõnastanud ja teinud, siis heidutuse tõenäosust ja töötavust tõhustab, kui riik täidab heidutuse tingimusi, sest on ebatõenäoline, et vastane pingutab selleks, et kontrollida, kas riigil on olemas heidutus ja soov end kaitsta.

Vastavalt heidutuse teooriale peab heidutus olema kommunikeeritud. Tõepoolest, klassikalise heidutusteooria kohaselt on osapooled ratsionaalsed ja võiks eeldada, et enne *status quo*'d rikkudes kaalub vastane läbi võimalikud tagajärjed ja hindab, milline on rünnatava võimalik reaktsioon ja vastutegevus. Kuid ainuüksi sellele ei saa lootma jääda. Ideaalse heidutusteooria kohaselt võtab vastane arvesse asjaosaliste huvid, nende usutavuse ähvarduste tegemisel ja muu olulise info. See tähendab, et selgelt deklareeritud heidutuspoliitika tõstab usutavust.

Siit tulenevalt teeb autor **esimese ettepaneku**: tugevamaks ja töötavamaks heidutuseks on Eestil vaja selgelt deklareerida, milles Eesti heidutus seisneb. Selleks juba piisab, kui olemasolevatele eesmärkidele lisada juurde, et muuhulgas kannab see endas heidutavat eesmärki ning koondada küberheidutust puudutav ühtsesse dokumenti. See oleks vastasele esimene mõttekoht ja punane märguanne – Eesti ei lase end niisama lihtsalt rünnata.

Ekspertintervjuudes leiti, et küberheidutuseks peaks jätkama mõnede olemasolevate meetmetega. Näiteks, peaks jätkama rahvusvahelise võime arendamise ja koostööga. Kui riikide elanikel on parem küberhügieen, kui riigi küberturvalisusega tegelevad asutused suudavad tõhusamalt tuvastada, ennetada ja võidelda küberohtudega, kui õiguskaitseorganid suudavad efektiivsemalt menetleda ja küberkurjategijaid süüdi mõista, kui ühiskondlikult olulisi funktsioone tagades järgitakse baasinfoturbe põhimõtteid jne, siis see on tugev vastulöök pahatahtlikele tegutsejatele. Nagu mitmed eksperdid tabavalt ütlesid: kuritegevus läheb sinna, kus on kergem raha teenida. Ehk tugeva heidutuse korral leitakse end olukorrast, kus küberkuritegevus ei tasu enam ära.

Nii dokumendianalüüsi kui ekspertintervjuude tulemusena selgus, et Eesti heidutuspoliitika põhineb peamiselt ka tõkestaval heidutusstrateegial. Seetõttu tuleks jätkata kaitsemeetmete tõhustamisega (nt infoturbestandardite ja turvalise IT-arhitektuuri rakendamisega). Täiendavalt tuleks kaaluda uurimistulemustes leitud tõhusate heidutusmeetmetena hulgast, mis mõjuvad tõkestavalt: haavatavuste tuvastamine ja neile reageerimine, alternatiivsete lahenduste välja töötamine ning kerksus. Siit tulenevalt teeb autor **teise ettepaneku**, jätkata olemasolevatest strateegilistest heidutusmeetmetest: rahvusvahelise võime arendamise ja koostööga, kaitsemeetmetega ning õiguskaitseorganite tegevuse tõhustamisega. Parendada tuleks info jagamist ning küberriskide ja ristsõltuvuste haldamist.

USA heidutusstrateegia üks olulisi rolle on kerksusel. Eesti rakendab seni kerksuse kontseptsiooni ainult ühiskonnas, kuid nagu eksperdid kinnitasid on kerksusel oluline strateegiline eesmärk, mis on Eestis kasutatav ja esimesed sammud selles osas on tehtud. Arvestades Eesti piiratud võimalusi on kerksus üks paremini rakendatavaid heidutusmeetmeid. Kerksus võiks seejuures hõlmata kõigepealt ristsõltuvuste haldamist, st tuleb välja selgitada, millised on hetkel infosüsteemide sõltuvused ning alustada tuleks ennekõike kriitilisest infrastruktuurist, elutähtsatest teenustest. Samuti tuleks põhimõtetena kasutusele võtta selge siht turvalise IT-arhitektuuri ja infosüstemide moderniseerimisele. Mõlema meetme puhul peaks olema kaasatud ka erasektor, viimasel juhul kogu ühiskond. Siit tulenevalt teeb autor **kolmanda ettepaneku**, laiendada kerksuse kontseptsiooni küberruumi küberheidutuse meetmena.

Eelpool kirjeldatust selgub, et kõige paremini sobib Eesti küberheidutuse sisustamisel kohandatud ja tõkestav heidutusstrateegia, see on autori **neljas ettepanek**.

Tabel 16. Ettepanekud Eesti küberjulgeoleku tugevdamiseks läbi küberheidutuse (autori koostatud)

Nr	**Ettepanek**
1)	Deklareerida selgelt Eesti küberheidutuspoliitika koondades küberheidutust käsitlevad osad ühtsesse strateegiadokumenti.
2)	Jätkata olemasolevatest strateegilistest heidutusmeetmetest: rahvusvahelise võime arendamise ja koostööga, kaitsemeetmetega ning õiguskaitseorganite tegevuse tõhustamisega. Parendada tuleks info jagamist ning küberriskide ja ristsõltuvuste haldamist.
3)	Laiendada kerksuse kontseptsiooni küberruumi.
4)	Küberheidutuse sisustamisel lähtuda kohandatud ja tõkestavast heidutusstrateegiatest, st teha konkreetsetele ohustajatele võimalikult raskeks oma eesmärkide saavutamine.

Kõik ettepanekud koondati tabelisse 16 ning on suunatud Majandus- ja Kommunikatsiooniministeeriumile, kuna see on Eestis küberjulgeoleku strateegia koostamise eest vastutav ministeerium.

KOKKUVÕTE

Magistritööga otsiti vastust **uurimisprobleemile**: kuidas tugevdada Eesti küberjulgeolekut läbi küberheidutuse. Magistritöö **aktuaalsus** seisneb pingestunud julgeolekukeskkonnas, Eesti riigi geopoliitilises asendis ja ühiskonna sõltuvuses küberruumist ning igapäevastes küberrünnetes kui uues normaalsuses. Magistritöö **uudsus** seisneb esmakordses küberheidutuse kontseptsiooni kasutamise võimaluste uurimises Eesti küberjulgeolekupoliitikas ja magistritöö originaalsus seisneb küberheidutuse kontseptsiooni uurimises tuginedes Ameerika Ühendriikide heidutuse strateegiale ning kasutades juhtumiülest analüüsi.

Uurimisprobleemi abistab lahendada autori poolt püstitatud **neli uurimisküsimust**, millele vastati tuginedes teooria sünteesile, dokumendianalüüsile ja ekspertintervjuudele. Magistritöö eesmärgiks oli selgitada välja, milliste küberheidutuse meetmetega oleks võimalik tugevdada Eesti küberjulgeolekut. Eesmärgi saavutamist toetasid autori püstitatud **viis uurimisülesannet**. Töös saavutati püstitatud eesmärk, vastati uurimisprobleemile ja seda toetavatele uurimisküsimustele ning lahendati uurimisülesanded.

Esimene uurimisülesanne seisnes heidutuse teooria analüüsis rahvusvaheliste suhete tasandil, täpsemalt uuriti heidutuse definitsiooni, heidutusteooria kujunemisemist, heidutuse tingimusi ja võimalikke heidutusstrateegiad ning asetati see julgeolekuteoreetilisse konteksti. Teooria uurimisega analüüsiti heidutuse tähendust, milliseid tingimusi selleks on vaja täita, millised on võimalikud strateegilised suunad, millega on võimalik vastast heidutada ning kuidas on üldse heidutuse teooria kujunenud julgeolekuteoreetilises kontekstis. Heidutusel täpne definitsioon küll puudub, kuid valdavalt iseloomustab kõiki eesmärk mõjutada oponenti loobuma oma kavatsus(te)st. Ka küberheidutusel puudub oma kindel seletus. Autor tuvastas kolm peamist tõlgendusviisi: kitsas, lai ja valikuline. Töö autor lähtus töö kirjutamisel laiema tõlgendusviisist, sest see võimaldab leida sobivaimad küberheidutuse meetmed võrreldes kitsama tõlgendusega, millest on vähem võita. Laiem käsitlus on ka seniste uurimistöödega rohkem kooskõlas, sest enamikel juhtudel on küberheidutust vaadeldud laiemalt. Valikuline tõlgendusviis ei olnud sobiv, kuna sellel puudub teadusliku metodoloogia reeglitest kinni pidamine. Heidutuse teooria kujunemine jaguneb laias laastus nelja perioodi, mis suuresti kattub realismiteooria kujunemisega

20. sajandil: klassikaline ehk ratsionaalne heidutusteooria, strukturaalne ehk neorealistlik heidutusteooria, otsustus-teoreetiline heidutusteooria ja ideaalne heidutusteooria.

Töös jõuti järeldusele, et mitte igasugune tegevus liigitu heidutuseks, kuid heidutus ise võib täita ka muid eesmärke. Heidutuse tingimused on järgnevad: 1. kommunikatsioon ja 2. usutavus, mis jaguneb omakorda 2.1 võime, 2.2 kahju tekitamine ja 2.3 tahe. 2.3 tahe jaguneb veel kolmeks: 2.3.1 tegevus varasemalt sarnastes oludes, 2.3.2 valitsuse avaldused ja käitumine ning 2.3.3 avalikkuse arvamus. Heidutusstrateegiaid on palju erinevaid, mis võivad olla rakendatud samaaegselt korraga.

Teine uurimisülesanne oli selgitada välja Eesti ja USA küberjulgeoleku ohustajad, millele saadi vastus nii dokumendianalüüsi kui ka ekspertintervjuude tulemusena. Eesti küberjulgeolekut ohustavad riigid, küberkurjategijad, mitteriiklikud tegutsejad, oskamatud kasutajad ja pahatahtlikud tegutsejad ning USA küberjulgeolekut ohustavad dokumendianalüüsi kohaselt: riigid, küberkurjategijad, mitteriiklikud tegutsejad, pahatahtlikud tegutsejad ja siseringiohustajad.

Kolmas uurimisülesanne oli selgitada välja Eesti ja USA küberjulgeolekuga seotud strateegiadokumentides kasutatud küberheidutuse meetmed. Meetmeid tuli kokku üle viiekümne, mistõttu võttis autor kasutusele tõhusama situatsiooni analüüsimiseks ja otsustamiseks kohandatud mudeli DIME jaotates tuvastatud meetmed viide valdkonda (vt lisa 3).

Neljas uurimisülesanne oli analüüsida Eesti julgeolekupoliitika kujundajate seisukohti küberheidutuse meetmetest. Ekspertide heidutusmeetmed järgisid Eesti dokumendianalüüsis kasutatud heidutusstrateegiaid: ühine- (heidutus läbi NATO), tõkestav- (kaitsest läbi ei murda, eesmärke on raske saavutada) ja rist-domeeniline (küberdomeen).

Viies uurimisülesanne oli analüüsida dokumendianalüüsi ja ekspertintervjuude tulemusi ning teha ettepanekuid Eesti küberjulgeoleku tugevdamiseks. Kokku tegi autor neli ettepanekut, mis on suunatud kõik Majandus- ja Kommunikatsiooniministeeriumile.

Magistritöö tulemusi saab sisendina kasutada uue Eesti küberjulgeoleku strateegia koostamisel.

Magistritöö autor näeb vajadust teemat **edasi uurida** seatud küberjulgeoleku tugevdamise meetmete osas. Tuleks analüüsida ja hinnata sätestatud eesmärkide reaalset tulemuslikkust-mõõdetavust ning selgitada välja kitsaskohad ja põhjused. Ühelt poolt võivad esineda meetmeid, mis ongi järjepidevad, teisalt võivad esineda meetmeid, mis on ebaõnnestunult rakendatud ja vajaksid korrastamist, läbimõtlemist nende tõhusamaks rakendamiseks.

Nagu eksperdid ütlesid, siis küberturvaline mõtlemine peab kujunema kultuuriks nagu liikluskultuur. Riik üksi saab julgeolekut ja turvalisust tagada ainult teatud piirideni, kuid vajalik on ka kodanike panus. Viimaks, Eesti küberjulgeolek on täpselt nii tugev, kui on tema nõrgim lüli.

SUMMARY

The title of the Master's thesis is "*Strengthening Estonia's cyber security through cyber deterrence at the example of the United States of America*". The objective of the thesis was to find out which measures of cyber deterrence could improve Estonia's cyber security at the example of the United States of America.

To achieve the objective of the thesis five research tasks were set by the author:

1. To determine the cyber security threat actors of Estonia and US.
2. To analyze deterrence theory on the international level and also its definition, evolution, requirements, possible strategies and view deterrence within the context of security studies.
3. To determine current measures of cyber deterrence within the cyber security related strategies of Estonia and US.
4. To analyze opinions of experts in Estonian security policy on measures of cyber deterrence.
5. To analyze the results of document analysis and expert interviews and propose methods for strengthening Estonian's cyber security.

The thesis was designed within the framework of case study research strategy and consists of two chapters. The first chapter is theoretical one, where author defines deterrence, gives an overview of the evolution of deterrence and places deterrence in the security studies perspective. The second chapter focuses on the practical side of cyber deterrece, i.e. which measures of cyber deterrence are currently used in cyber security related strategies of Estonia and US and continues to analyze expert opinions on cyber deterrence to determine which of those measures could be implemented in Estonia. The method of the analysis used was qualitative content analysis and it was conducted using qualitative data analysis software NVivo for Mac and NVivo 11 Pro.

Based on the results of the research the author achieved the goal and proposed four strategical recommendations on how Estonia could strengthen its cyber security using cyber deterrence. The set research tasks were accomplished and the objective of the thesis was achieved.

VIIDATUD ALLIKATE LOETELU

Alperovitch, D., 2011. Towards Establishment of Cyberspace Deterrence Strategy. Rmt: C. Czosseck, E. Tyugu & T. Wingfield, toim-d. *3rd International Conference on Cyber Conflict*. Tallinn: NATO CCDCOE Publications.

Alperovitch, D., 2015. The Latest on Chinese-affiliated Intrusions into Commercial Companies. *CrowdStrike Blog.* [Võrgumaterjal] Leitav: https://www.crowdstrike.com/blog/the-latest-on-chinese-affiliated-intrusions-into-commercial-companies/ [Kasutatud 20.02.2018].

Arms Control Association, 2017. *Nuclear Weapons: Who Has What at a Glance*. [Võrgumaterjal] Leitav: https://www.armscontrol.org/factsheets/Nuclearweaponswhohaswhat [Kasutatud 21.11.2017].

Australian Government, 2016. Australia's Cyber Security Strategy: Enabling innovation, growth & prosperity. [Võrgumaterjal] Leitav: https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf [Kasutatud 29.04.2018].

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

Bendiek, A. & Metzger, T., 2015. *Deterrence theory in the Cyber-century: Lessons from a state-of-the-art literature review*. SWP Working Paper. Berlin: SWP-Berlin.

Bowen, G., 2009. Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, 9(2), pp. 27–40.

Brodie, B., 1946. Implications for Military Policy. Rmt: B. Brodie, F. S. Dunn, A. Wolfers, P. E. Corbett & W. T. R. Fox, toim-d. *The Absolute Weapon: Atmoic Power and World Order*. New York: Harcourt, pp. 57–89.

Bunn, M. E., 2007. Can Deterrence Be Tailored? *Strategic Forum*, 225, pp. 1–8.

Cheng, D., 2015. Prospects for Extended Deterrence in Space and Cyber: The Case of the PRC. *Lecture*, 1270, pp. 1–8.

Chollet, D., 2016. Obama's Red Line, Revisited. *Politico*. [Võrgumaterjal] Leitav: https://www.politico.com/magazine/story/2016/07/obama-syria-foreign-policy-red-line-revisited-214059 [Kasutatud 06.05.2018].

Cirenza, P., 2015. *An Evaluation of the Analogy Between Nuclear and Cyber Deterrence*. Thesis, Stanford: Leland Stanford Junior University.

Clausewitz, C., 1997. *On War*. London: Wordsworth Editions.

Cyber Security & Information Systems Information Analysis Center, 2018. *Build and Operate a Trusted DoDIN*. [Võrgumaterjal] Leitav: http://iac.dtic.mil/csiac/download/ia_policychart.pdf [Kasutatud 22.03.2018].

Cybernetica, 2017. Küberruum. *Andmekaitse ja infoturbe leksikon*. [Võrgumaterjal] Leitav: http://akit.cyber.ee/term/568-kuberruum [Kasutatud 28.12.2017].

Cybernetica, 2018a. Nullpäeva turvaauk. *Andmekaitse ja infoturbe leksikon*. [Võrgumaterjal] Leitav: http://akit.cyber.ee/term/490-zero-day-vulnerability [Kasutatud 20.02.2018].

Cybernetica, 2018b. Küberrünne. *Andmekaitse ja infoturbe leksikon*. [Võrgumaterjal] https://akit.cyber.ee/term/1186-kuberrunne [Kasutatud 28.04.2018].

Defense Science Board, 2017. *Defense Science Board (DSB) Task Force on Cyber Deterrence. Technical Report*. [Võrgumaterjal] Leitav: http://www.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf [Kasutatud 21.11.2017].

Denning, D. E., 2015. Rethinking the Cyber Domain and Deterrence. *Joint Forces Quarterly*, 77, 2nd Quarter, pp. 8–15.

Department of Defense, 2006. *Quadrennial Defense Review Report*. Washington, D.C.: Department of Defense.

Department of Defense, 2015. *The DoD Cyber Strategy*. [Võrgumaterjal] Leitav: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf [Kasutatud 02.11.2017].

Derian, D. J., 2009. Cyber-deterrence. Rmt: *Critical Practices in International Theory: Selected essays*. London: Routledge, pp. 210–217.

Eesti Keele Instituut, 2017. *Militerm – sõjandusterminoloogia andmebaas*. [Võrgumaterjal] Leitav: http://termin.eki.ee/militerm/ [Kasutatud 25.11.2017].

Eesti Keele Instituut, 2018. Eesti keele seletav sõnaraamat. [Võrgumaterjal] Leitav: http://www.eki.ee/dict/ekss [Kasutatud 01.04.2018].

Euroopa Liidu Komisjon, 2017. *Ühisteatis Euroopa Parlamendile ja Nõukogule. Vastupidavusvõime, heidutus ja kaitse: tugeva küberturvalisuse tagamine Euroopa Liidus. Ühisteatis. JOIN(2017) 450 final*. [Võrgumaterjal] Leitav: https://ec.europa.eu/transparency/regdoc/rep/10101/2017/ET/JOIN-2017-450-F1-ET-MAIN-PART-1.PDF [Kasutatud 27.12.2017].

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

Goodman, W., 2010. Cyber Deterrence: Tougher in Theory than in Practice? *Strategic Studies Quarterly*, Fall, pp. 102–135.

Gray, C. S., 2000. Deterrence in the 21st century. *Comparative Strategy*, 19(3), pp. 255–261.

Gray, C., 2003. The Reformation of Deterrence: Moving On. *Comparative Strategy*, 22(5), pp. 429–461.

Greenberg, A., 2017. North Korea's Sloppy, Chaotic Cyberattacks Also Make Perfect Sense. *Wired*. 15. juuni. [Võrgumaterjal] Leitav: https://www.wired.com/story/north-korea-cyberattacks/ [Kasutatud 28.12.2017].

Hansen, A. P., 2012. *Nothing New under the Sun: Benefiting from the Great Lessons of History to Develop a Coherent Cyberspace Deterrence Strategy*. Thesis, Norfolk: National Defense University.

Harknett, R. J., 1996. Information Warfare and Deterrence. *Parameters*, Autumn, pp. 93–107. [Võrgumaterjal] Leitav: http://ssi.armywarcollege.edu/pubs/parameters/articles/96autumn/harknett.htm [Kasutatud 10.02.2018].

Hemmer, P. T., 2013. *Deterrence and Cyber-weapons*. Thesis, Monterey: Naval Postgraduate School.

Hirsjärvi, S., Remes P. ja Sajavaara, P., 2010. *Uuri ja kirjuta*. Tallinn: Medicina.

HM Government, 2016. National Cyber Security Strategy 2016-2021. [Võrgumaterjal] Leitav: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf [Kasutatud 29.04.2018].

Huth, P. & Russett, B., 1984. What Makes Deterrence Work? Cases from 1900 to 1980. *World Politics*, 36(4), pp. 496–526.

Jackson, V., 2015. Stop Confusing Deterrence with Strategy. *The Diplomat*, 6 juuli. [Võrgumaterjal] Leitav: https://thediplomat.com/2015/07/stop-confusing-deterrence-with-strategy/ [Kasutatud 08.02.2018].

Jervis, R., 1979. Deterrence Theory Revisited. *World Politics*, 31(2), pp. 289–324.

Kaitsepolitseiamet, 2016. *Kaitsepolitseiamet: Aastaraamat 2016*. [Võrgumaterjal] Leitav: https://www.kapo.ee/sites/default/files/public/content_page/aastaraamat-2016.pdf [Kasutatud 20.06.2016].

Kaitsepolitseiamet, 2018. *Kaitsepolitseiamet: Aastaraamat 2017*. [Võrgumaterjal] Leitav: https://www.kapo.ee/sites/default/files/public/content_page/aastaraamat-2017.pdf [Kasutatud 12.05.2018].

Kalmus, V., Masso, A. ja Linno, M., 2015. Sotsiaalse analüüsi meetodite ja metodoloogia õpibaas. Tartu Ülikool. [Võrgumaterjal] Leitav: http://samm.ut.ee/ [Kasutatud 14.01.2018].

Kaufmann, W. W., 1954. *The Requirements of Deterrence*. New Jersey: Princeton University.

Kivistik, M., 2017. *Ameerika Ühendriikide normatiivse küberheidutuspoliitika analüüs 2016. aasta presidendivalimiste küberrünnakute näitel*. Bakalaureusetöö. Tallinn: Tallinna Ülikool.

Kubrick, S., 1964. *Dr Strangelove or: How I Learned to Stop Worrying and Love the Bomb*. Film.

Lebow, R. N. & Stein, J. G., 1990. When Does Deterrence Succeed and How Do We Know? *CIIPS Occasional Papers*, 8, pp. 1–90.

Lewis, J. A., 2015. Terminological Use of "Deterrence" 1900–2008. CSIS Strategic Technologies Program. [Võrgumaterjal] Leitav: http://csis-prod.s3.amazonaws.com/s3fs-public/150415_Terminological_Use_of_Deterrence.pdf [Kasutatud 11.02.2018].

Lewis, J. A., 2016. Indictments, Countermeasures, and Deterrence. Center for Strategic & International Studies. 25. märts. [Võrgumaterjal] Leitav: https://www.csis.org/analysis/indictments-countermeasures-and-deterrence [Kasutatud 20.02.2018].

Lindsay, J. & Gartzke, E., 2017. Cybersecurity and cross-domain deterrence: the consequences of complexity. Rmt: D. V. Puyvelde & A. F. Brantly, toim-d. *US National Cybersecurity: International Policits, Concepts and Organization*. London: Routledge, pp. 11–27.

Lonsdale, D. J., 2016. Britain's Emerging Cyber-Strategy. *The RUSI Journal*, 161(4), pp. 52–62.

Lowther, A., 2013. *Thinking About Deterrence: Enduring Questions in a Time of Rising Powers, Rogue Regimes, and Terrorism*. Alabama: Air University Press.

Lupovici, A., 2010. The Emerging Fourth Wave of Deterrence Theory – Toward a New Research Agenda. *International Studies Quarterly*, 54(3), pp. 705–732.

Majandus- ja Kommunikatsiooniministeerium, 2014a. *Küberjulgeolekustrateegia 2014–2017*. [Võrgumaterjal] Leitav: https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf [Kasutatud 12.11.2017].

Majandus- ja Kommunikatsiooniministeerium, 2014b. *Küberjulgeolekustrateegia 2014–2017. Lisa 2 Valdkondlik metoodika.* [Võrgumaterjal] Leitav: https://www.mkm.ee/sites/default/files/lisa_2_valdkondlik_metoodika.doc [Kasutatud 28.04.2018].

Margaret Thatcher Foundation, 2017. *Speech at Soviet Official Banquet*. [Võrgumaterjal] Leitav: http://www.margaretthatcher.org/document/106776 [Kasutatud 28.12.2017].

Marquez, P., 2011. Space Deterrence: The Prêt-á-Porter Suit for the Naked Emperor. Rmt: R. Butterworth, P. Marques, J. B. Sheldon & E. Sterner, toim-d. *Returning to Fundamentals: Deterrence and U.S. National Security in the 21st Century*. Washington D.C.: The George C. Marshall Institute, pp. 9–19.

Moore, R. J., 2008. *Prospects for Cyber Deterrence*. Thesis, Monterey: Naval Postgraduate School.

Morgan, P. M., 2003. *Deterrence Now*. Cambridge: Cambridge University Press.

Nye, J. S. Jr., 2010. *Cyber Power*. Cambridge, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs.

Nye, J. S. Jr., 2017. Deterrence and Dissuasion in Cyberspace. *International Security*, 41(3), pp. 44–71.

Paul, T. V., 1994. *Asymmertic Conflicts: War Initiation by Weaker Powers*. Cambridge: Cambridge University Press.

Quackenbush, S. L. & Zagare, F. C., 2016. Modern Deterrence Theory: Research Trends, Policy Debates, and Methodological Controversies. *Oxford Handbooks Online*. New York: Oxford University Press, 2016.

Quackenbush, S. L., 2010. General Deterrence and International Conflict: Testing Perfect Deterrence Theory. *International Interactions*, 36(1), pp. 60–85.

Quackenbush, S. L., 2011. Deterrence theory: where do we stand? *Review of International Studies*, 37, pp. 741–762.

Riigi Infosüsteemi Amet, 2017a. *Riigi Infosüsteemi Ameti küberturvalisuse teenistuse 2016. aasta kokkuvõte*. Tallinn: RIA. [Võrgumaterjal] Leitav: https://www.ria.ee/public/Kuberturvalisus/RIA-kuberturbe-aastaraport-2016.pdf [Kasutatud 02.11.2017].

Riigi Infosüsteemi Amet, 2017b. RIA Küberturvalisuse teenistuse kokkuvõte: juuli 2017. [Võrgumaterjal] Leitav: https://www.ria.ee/public/Kuberturvalisus/RIA-KTT-kokkuvote-juuli-2017.pdf [Kasutatud 20.02.2018].

Riigi Infosüsteemi Amet, 2018a. Turvaintsidentide käsitlemine CERT Eesti. [Võrgumaterjal] Leitav: https://www.ria.ee/ee/cert.html [Kasutatud 28.04.2018].

Riigi Infosüsteemi Amet, 2018b. RIA Küberturvalisuse teenistuse kokkuvõte: veebruar ja märts 2018. [Võrgumaterjal] Leitav: https://www.ria.ee/public/Kuberturvalisus/RIA-KTT-kokkuvote-veebruar-marts-2018.pdf [Kasutatud 28.04.2018].

Riigi Infosüsteemi Amet, 2018c. *Riigi Infosüsteemi Amet: Küberturvalisus 2018.* Tallinn: RIA. [Võrgumaterjal] Leitav: https://www.ria.ee/public/Kuberturvalisus/RIA-kuberturvalisus-2018.pdf [Kasutatud 12.05.2018].

Riigikantselei, 2017. *Riigikaitse Arengukava 2017–2026. Arengukava avalik osa.* [Võrgumaterjal] Leitav: https://riigikantselei.ee/sites/default/files/content-editors/Failid/rkak_2017_2026_avalik_osa.pdf [Kasutatud 26.12.2017].

Riigikogu, 2017. *Eesti julgeolekupoliitika alused*. [Võrgumaterjal] Leitav: https://www.riigiteataja.ee/aktilisa/3060/6201/7002/395XIII_RK_o_Lisa.pdf# [Kasutatud 12.11.2017].

Rits, M., 2013. *Strateegilise vaate muutus heidutusele Ameerika Ühendriikide ametlikus diskursuses ja laiemas välispoliitilises debatis globaalse terrorismivastase sõja kontekstis*. Magistritöö, Tartu: Tartu Ülikool.

Rivera, M., 2012. *Deterrence in Cyberspace*. Thesis, Norfolk: National Defense University.

Rühle, M., 2015. Deterrence: what it can (and cannot) do. *NATO Review*. [Võrgumaterjal] Leitav: https://www.nato.int/docu/review/2015/also-in-2015/deterrence-russia-military/EN/index.htm [Kasutatud 04.11.2017].

Ryan, N. J., 2017. Five Kinds of Cyber Deterrence. *Phiolosphy & Technology*, pp. 1–8.

Samost, A., 2017. USA tulistas Süüria lennuväebaasi üle 50 tiibraketi. *ERR*. 7. aprill. [Võrgumaterjal] Leitav: https://www.err.ee/588592/usa-tulistas-suuria-lennuvaebaasi-ule-50-tiibraketi [Kasutatud 19.02.2018].

Singer, D. E., 2012. Obama Order Sped Up Wave of Cyberattacks Against Iran. *The New York Times*, 1. juuni. [Võrgumaterjal] Leitav: https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html [Kasutatud 28.04.2018].

Singer, P. W., 2017. Cyber-Deterrence and the Goal of Resilience: 30 New Actions That Congress Can Take To Improve U.S. Cybersecurity. *Hearing on "Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities" Before the House Armed Services Committee*. 1 March.

Strawbridge, J., 2016. The Big Bluff: Obama, Cyber Economic Espionage, and the Threat of WTO Litigation. *Georgtown Journal of International Law*, 47, pp. 833–865.

Strömpl, J., 2014. *Juhtumiuurimus*. [Võrgumaterjal] Leitav: http://samm.ut.ee/juhtumiuurimus [Kasutatud 06.05.2018].

Zagare, F. C. & Kilgour, D. M., 2000. *Perfect Deterrence*. Cambridge: Cambridge University Press.

Zagare, F. C., 1996. Classical Deterrence Theory: A Critical Assessment. *International Interactions*, 21(4), pp. 365–387.

Taipale, K. A., 2010. Cyber-deterrence. *Law, Policy and Technology: Cyberterrorism, Information Warfare, Digital and Internet Immobilization*, IGI Global.

Teabeamet. 2016. *Eesti rahvusvahelises julgeolekukeskkonnas. Aastaraamat.* [Võrgumaterjal] Leitav: https://www.teabeamet.ee/pdf/2016-et.pdf [Kasutatud 20.06.2016].

Tikk-Ringas, E., ed., 2015. *Evolution of the Cyber Domain: The Implications for National and Global Security*. London: The International Institute for Strategic Studies.

Till, G., 2012. *Merevõim: teejuht 21. sajandisse*. 2. trükk. Tallinn: Eesti Ajalehed.

Tucker, P., 2018. No, the US Won't Respond to A Cyber Attack with Nukes. *Defense One*. 2. veebruar. [Võrgumaterjal] Leitav: http://www.defenseone.com/technology/2018/02/no-us-wont-respond-cyber-attack-nukes/145700/ [Kasutatud 19.02.2018].

Vabariigi Valitsus, 2018. *Seletuskiri küberturvalisuse seaduse juurde*. [Võrgumaterjal] Leitav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/K%C3%BCberturvalisuse%20seadus [Kasutatud 28.04.2018].

Välisluureamet, 2017. *Eesti rahvusvahelises julgeolekukeskkonnas*. [Võrgumaterjal] Leitav: https://www.valisluureamet.ee/pdf/TA_raport_2017_EST.pdf [Kasutatud 28.12.2017].

Välisluureamet, 2018. Eesti rahvusvahelises julgeolekukeskkonnas. [Võrgumaterjal] Leitav: https://xn--vlisluureamet-bfb.ee/pdf/raport-2018-EST-web.pdf [Kasutatud 12.05.2018].

Välisministeerium, 2017. *Rahvusvahelised sanktsioonid (piiravad meetmed)*. [Võrgumaterjal] Leitav: http://vm.ee/et/rahvusvahelised-sanktsioonid-piiravad-meetmed [Kasutatud 06.05.2018].

White House, 2015. *Report on Cyber Deterrence Policy*. [Võrgumaterjal] Leitav: http://federalnewsradio.com/wp-content/uploads/2015/12/Report-on-Cyber-Deterrence-Policy-Final.pdf [Kasutatud 20.06.2016].

WikiLeaks, 2018. *Vault 7: CIA Hacking Tools Revealed*. [Võrgumaterjal] Leitav: https://wikileaks.org/ciav7p1/ [Kasutatud 20.02.2018].

Wingfield, T. & Tikk-Ringas, E., 2010. Framework for International Cyber Security: The Cube, the Pyramid, and the Screen. Rmt: E. Tikk & A.-M. Talihärm, toim-d. *International Cyber Security: Legal & Policy Proceedings*. Tallinn: CCD COE.

Wohlforth, W. C., 2010. Realism. Rmt: C. Reus-Smit & D. Snidal, toim-d. *The Oxford Handbook of International Relations*. Oxford: Oxford University Press. pp. 131–149.

Wong, T. P., 2012. *Active Cyber Defense: Enhancing National Cyber Defense*. Thesis, Monterey: Naval Postgraduate School.

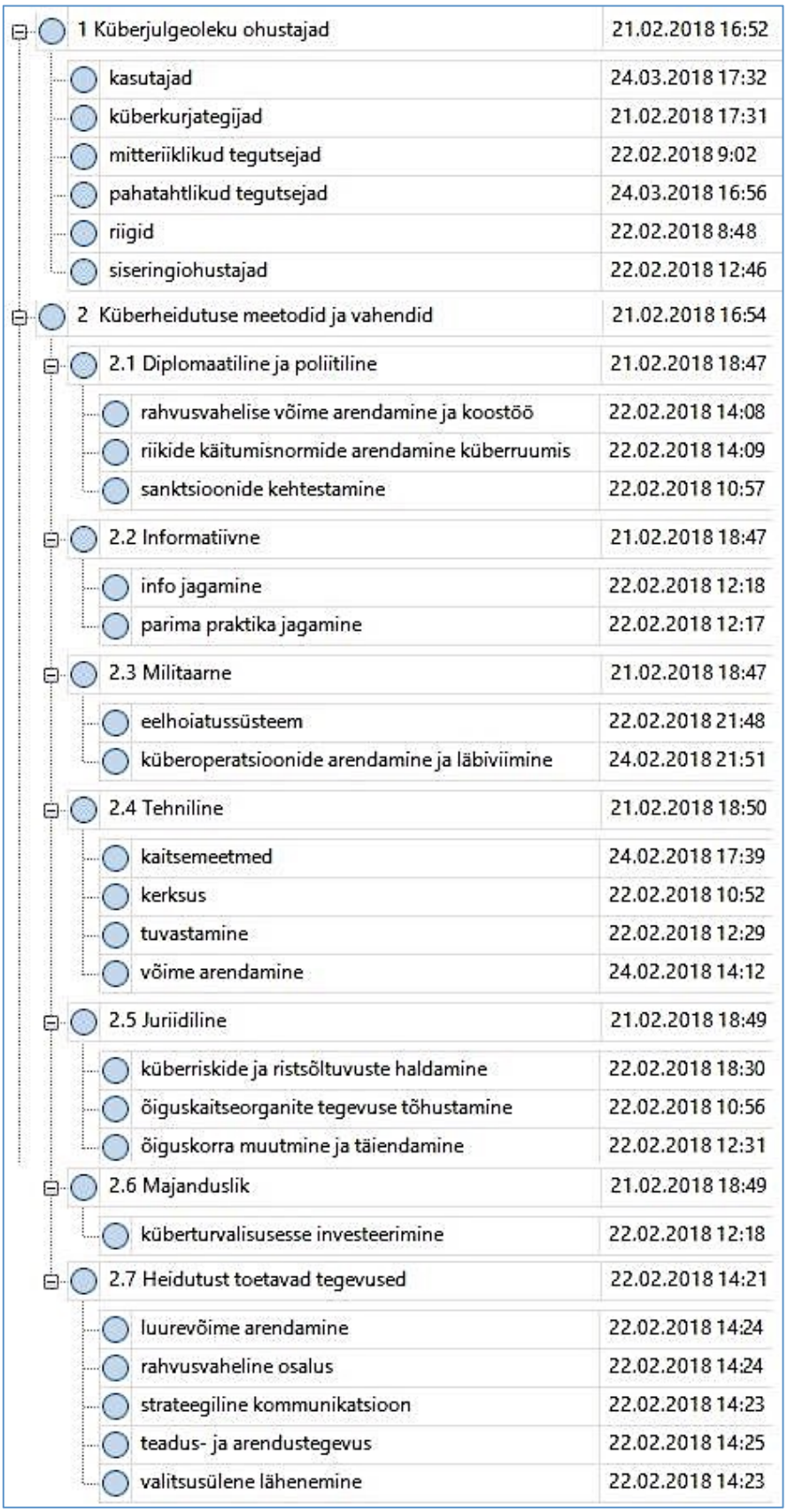
Yin, R. K., 2014. *Case Study Research. Design and Methods*. 5th ed. Thousand Oaks: SAGE Publications.

Yoho, T. S., 2018. *H.R. 5576 – Cyber Deterrence and Response Act of 2018*. 115th Congress, 2nd Session. 18. aprill 2018. [Võrgumaterjal] Leitav: https://www.congress.gov/115/bills/hr5576/BILLS-115hr5576ih.pdf [Kasutatud 12.05.2018].

Yost, D. S., 2003. Debating security strategies. *NATO Review*, Winter. [Võrgumaterjal] Leitav: https://www.nato.int/docu/review/2003/issue4/english/art4.html [Kasutatud 26.11.2017].

TABELITE JA JOONISTE LOETELU

LISAD



1 Küberjulgeoleku ohustajad	21.02.2018 16:52
kasutajad	24.03.2018 17:32
küberkurjategijad	21.02.2018 17:31
mitteriiklikud tegutsejad	22.02.2018 9:02
pahatahtlikud tegutsejad	24.03.2018 16:56
riigid	22.02.2018 8:48
siseringiohustajad	22.02.2018 12:46
2 Küberheidutuse meetodid ja vahendid	21.02.2018 16:54
2.1 Diplomaatiline ja poliitiline	21.02.2018 18:47
rahvusvahelise võime arendamine ja koostöö	22.02.2018 14:08
riikide käitumisnormide arendamine küberruumis	22.02.2018 14:09
sanktsioonide kehtestamine	22.02.2018 10:57
2.2 Informatiivne	21.02.2018 18:47
info jagamine	22.02.2018 12:18
parima praktika jagamine	22.02.2018 12:17
2.3 Militaarne	21.02.2018 18:47
eelhoiatussüsteem	22.02.2018 21:48
küberoperatsioonide arendamine ja läbiviimine	24.02.2018 21:51
2.4 Tehniline	21.02.2018 18:50
kaitsemeetmed	24.02.2018 17:39
kerksus	22.02.2018 10:52
tuvastamine	22.02.2018 12:29
võime arendamine	24.02.2018 14:12
2.5 Juriidiline	21.02.2018 18:49
küberriskide ja ristsõltuvuste haldamine	22.02.2018 18:30
õiguskaitseorganite tegevuse tõhustamine	22.02.2018 10:56
õiguskorra muutmine ja täiendamine	22.02.2018 12:31
2.6 Majanduslik	21.02.2018 18:49
küberturvalisusesse investeerimine	22.02.2018 12:18
2.7 Heidutust toetavad tegevused	22.02.2018 14:21
luurevõime arendamine	22.02.2018 14:24
rahvusvaheline osalus	22.02.2018 14:24
strateegiline kommunikatsioon	22.02.2018 14:23
teadus- ja arendustegevus	22.02.2018 14:25
valitsusülene lähenemine	22.02.2018 14:23

Lisa 1. Koodipuu

Lisa 2. Intervjuu küsimused

Sissejuhatavad küsimused

1. Mida peate oma senise kübervaldkonna karjääri kõige suurematekss saavutusteks?

Põhiosa küsimused

Küberohud

2. Mis või kes ohustab Eesti küberjulgeolekut? Palun põhjendage oma hinnangut.

Üldiselt heidutusest

3. Kuidas defineerite mõistet "heidutus"?
4. Millised on praegu Eestis kehtivad meetmeid, mis võivad mõjuda heidutavalt?

Küberheidutus

5. Ameerika Ühendriikide küberjulgeoleku strateegiadokumentide analüüsi tulemusena on autor jaotanud (küber)heidutavad meetmed valdkondadesse (vt tabel 17). Palun hinnata iga valdkonna juures meetme rakendamise võimalikust prioriteetsuse järgi arvestades Eesti praegust julgeolekupoliitilist keskkonda (st Eesti praegune seis, võime ja reaalsed võimalused). Palun põhjendage oma tehtud valikuid.
6. Lisaks tabelis nimetatutele, milliseid heidutuse meetmeid võiks veel kaaluda Eesti küberjulgeoleku tugevdamiseks?
7. Milliseid heidutust toetavaid tegevusi (nt teaduse arendamine, vabatahtlikke kaasamine, luurevõime arendamine, valitsusülene lähenemine jne) võiks Eesti kaaluda küberjulgeoleku tugevdamiseks?

Intervjuu lõpetamine

8. Kas soovite veel lisada midagi intervjuuga seoses?

Tänan veelkord, Teie vastused on selle teema uurimisel väga olulised. Kui mul tekivad lisaküsimused, kas võin Teiega veel ühendust võtta?

Tabel 17. Dokumendianalüüsi tulemusena jaotunud heidutavad meetmed (autori koostatud)

Valdkond	Heidutav strateegiline meede või vahend	Vastus
1. Diplomaatiline ja poliitiline	1.1 sanktsioonide kehtestamine	
	1.2 rahvusvaheliste õigusnormide loomine (riikide käitumisnormid (*responsible behaviour*) vm)	
	1.3 panustama üldise rahvusvahelise võime arendamiseks	
2. Informatiivne	2.1 info jagamine	
	2.2 parima praktika jagamine	
	2.3 usutavuse tõstmine	
	2.4 vaenlase otsustusprotsessi mõjutamine (*decision-making*)	
3. Militaarne	3.1 eelhoiatussüsteemi arendamine ja rakendamine	
	3.2 küberoperatsioonide arendamine ja läbiviimine (nt küberrelva arendamine)	
4. Tehniline	4.1 alternatiivlahenduste väljatöötamine	
	4.2 haavatavuste tuvastamine	
	4.3 kaitsemeetmed (vajab sisu)	
	4.4 kerksus (*resilience*)	
	4.5 juurdepääsu keelamine riigi informatsiooni infrastruktuurile	
	4.6 infosüsteemide ajakohastamine (riik omab pidevalt avaliku sektori infovarade nimekirja ja tugevdab neid süsteeme johtuvalt)	
	4.7 küberrünnakute ennetamine	
	4.8 küberrünnakute ja -ohtude tuvastamine	
	4.9 infosüsteemide arendamisel lähtutakse turvalisest IT-arhitektuurist (*security by design*)	
	4.10 turbestandardi väljatöötamine erisektorite organisatsioonidele	

	mõistmaks, kommunikeerimaks ja haldamaks oma küberriske	
	4.11 ründava ja kaitsva võime järjepidev arendamine	
	4.12 võrguseiramine ja info jagamine vastavate partneritega (nt S4A projekti edasiarendamine)	
5. Juriidiline	5.1 ristsõltuvuste järjepidev haldamine ja küberriskide maandamine	
	5.2 õiguskaitseorganite tegevuse tõhustamine	
	5.3 õiguskorra regulaarne hindamine ja muutmine vastavalt muutunud olukorrale	
	5.4 küberrünnakutega seotud korraldamiste toetamise karistamine	
6. Majanduslik	6.1 kulu (*cost*) tõstmise meetmed	
	6.2 kasu vähendamise meetmed	
	6.3 küberturvalisusesse investeerimine	

Lisa 3. USA ja Eesti küberheidutuse meetmed dokumendianalüüsi tulemusena ning ekspertide hinnangud (autori koostatud)

Tabel 18. USA ja Eesti küberheidutuse meetmed dokumendianalüüsi tulemusena ning ekspertide hinnangud (autori koostatud)

<table>
<tr><th rowspan="2">Ameerika Ühendriikides kehtivad küberheidutuse meetmed</th><th colspan="2">Eestis kehtivad küberheidutuse meetmed</th><th rowspan="2">Pigem meedet pooldavaid eksperte</th></tr>
<tr><th>Eesti dokumendianalüüsis</th><th>Ekspertide nimetatud</th></tr>
<tr><td colspan="4">I Diplomaatiline ja poliitiline</td></tr>
<tr><td colspan="4">1. rahvusvahelise võime arendamine ja koostöö</td></tr>
<tr><td colspan="3">• NATO liikmelisus, liitlaste kohalolu, kollektiivkaitse;
• ELi liikmelisus</td><td rowspan="3">9</td></tr>
<tr><td colspan="2">• küberohtude teadlikkuse tõstmine;
• info ja parima praktika vahetamine (Eestis: oskusteabe ja kogemuste; USAs: standardsete operatiivsete protseduuride jagamine, digitaalne ekspertiis, tööjõu arendamine, penetratsiooni ja kerksuse testid) ning vastavate asutuste ja isikutega kontaktide loomine ja hoidmine;
• kollektiivse kaitse loomine ja arendamine;
• Koostöösuunad: NATO (Eestis: ühtne lähenemine, infovahetuse tõhustamine, küberjulgeolekualaste võimete loomine ja arendamine, standardid, väljaõppe- ja treeningvõimalused)</td><td></td></tr>
<tr><td>• olukorrateadlikkuse loomine;
• kollektiivse riski maandamine;
• küberturvalisuse kultuuri loomine;
• eelhoiatussüsteemi jagamine;
• multistakeholderismi (põhimõte, mis kaasab kõiki huvegruppe) initsiatiivide soodustamine;
• treeningute ja muude ressursside võimaldamine (nt küberoperatsioonide</td><td>• töösse panustamine;
• abikäepoliitika</td><td>• ründe korraldajate välja selgitamine;
• ühine avalik häbistamine;
• õppused liitlastega;
• 2017. aastal vastu võetud ELi tööriistakast
<u>Täiendavalt kaaluda</u>:</td></tr>
</table>

planeerimine ja harjutamine); • riigi võime toetamine intsidendi haldusel; • avaliku ja erasektori partnerluse loomisel ja arendamisel toetamine; • erasektori toetamine investeerimisel; • konverentside korraldamine (nt kriitilise info infrastruktuuri kaitsmise teemal); • õiguskaitseorganite tegevuse tõhustamine, sh vajaliku õigusloome täiendamine, mis puudutab süütegude uurimist, menetlemist, süüdimõistmist, arvutiekspertiisi kasutamist ning samuti isikute koolitamine (nt ekspertiisi spetsialistide, juristide, seadusandjate)		• riikide ühine valmisolek rünnete omistamiseks; • ettevõtetega koostöö küberjulgeoleku tagamise eesmärgil **<u>Tuleb jätkata</u>**: • ELi tööriistakasti kasutamine	
Koostöösuunad: samameelsed riigid, arenguriigid, NATO liikmesriigid, rahvusvahelised organisatsioonid (nt Ameerika Riikide Organisatsioon, Aasia ja Vaikse ookeani majanduskoostöö foorum, Ühinenud Rahvaste Organisatsioon, Kagu-Aasia Maade Assotsiatsioon, Grupp Seitse ning regioonid (Lähis-Ida, Aasia ja Vaikne ookean ning Euroopa). Uusi liite, koalitsioone ja partnereid luuakse vastavalt muutunud olukorrale ja vajadusele	**Koostöösuunad**: lähinaabrid, NATO, samameelsed riigid, liitlased ja Euroopa Liidu liikmesriigid	**Koostöösuunad**: NATO CCDCOE, CERTid, rahvusvahelised "klubid"	
2. riikide käitumisnormide arendamine küberruumis			
• riikide käitumisnormide arendamine küberruumis			**8**
Täpsemalt: • ei tohi kahjustada kriitilist infrastruktuuri; • ei tohi takistada riikliku CERTi tööd ega kasutada seda rünnakute korraldamisel; • riik peab tegema koostööd teiste riikidega; • riik ei tohi toime panna intellektuaalse omandi rikkumisi	• rääkida kaasa riikide ühiste arusaamade kujunemises		
3. sanktsioonide kehtestamine			

• lisaks küberrünnakute korraldajatele ka kaasaaitajaid ja võimaldajaid	• meedet ei esinenud	**<u>Tuleb jätkata</u>**: • sanktsioonide kehtestamisega, sh rahaliste sanktsioonidega ning korraldajatele, mitte täideviijatele	**6**
II Informatiivne			
1. info jagamine			
• infovahetuse tõhustamine			**7**
• olukorrateadlikkuse tõhustamine; • hinnatakse kriitilise infrastruktuuri partnerite info vajadust, et tõsta operatiivsust	• küberkuritegevusega seotud operatiivne info riikide vahel		
2. parima praktika jagamine			
• eesmärgiga tõsta kollektiivselt kaitset küberruumis; • koostöö erasektoriga hindamaks võtmesüsteeme, mis peavad olema kaitstud ja implemeteeritud parimat praktikat; • NIST annab välja küberturbe raamistikku, mis viitab globaalselt tunnustatud standarditele ja praktikale aitamaks organisatsioonidel küberriske mõista, kommunikeerida ja hallata + moderniseerida föderaalset infotehnoloogiat	• oskusteabe ja kogemuste jagamine rahvusvahelise koostööna		**5**
III Militaarne			
1. eelhoiatussüsteem			
eelhoiatussüsteem on vajalik õigeaegseks reageerimiseks			**4**
• infosüsteemide kerksuse tagamiseks; • eelhoiatussüsteemi jagatakse liitlaste ja partneritega, mis võimaldab töötada üheskoos nii rahu kui kriisi ajal			

2. küberoperatsioonide arendamine ja läbiviimine			
• kübersõjapidamise võimete arendamine			
• tõhustada kübervahendeid kogu spektrumi ulatuses, et kaitsta riigi vara, kriitilist infrastruktuuri, info terviklikust ja konfidentsiaalsust; • ühtlasi soovitakse tõhustada protseduure, millega läbi viia küberoperatsioone vaenlaste vastu	• küberväejuhatuse loomine; • kaasatakse ka erasektor ja vabatahtlikud	• küberväejuhatus[1] • õppused	**5**
IV Tehniline			
1. Tuvastamine			
• võrguseire; • küberohtude ja -rünnete ennetamine			
• infotehnoloogiliste haavatavuste (sh nullpäeva haavatavuste) identifitseerimine vähendades nende mõju		• ekstreemne avatus, mis tuleneb e-ühiskonnast ja kogukonna väiksusest	**7**
2. Kaitsemeetmed			
• küberturbestandardite rakendamine			
• infosüsteemide ajakohastamine			
• tuleb kõrvaldada innovatsiooni takistav bürokraatia • kasutusele tuleb võtta odavamad ja olemasolevad (nn *off-the-shelf*) IT-lahendused	• aktiivne kaitse ja selle tõhusam juurutamine; • kaitsta tuleb küberriskide vastu ühiskonnale olulisi teenuseid; • teenuseosutajate koolitamine ja nõustamine;	• Eesti tugev küberkogukond, kes omavahel suhtlevad ja seetõttu tuvastatakse anomaaliaid ja suudetakse neile õigeaegselt reageerida, vahetatakse infot	**7**

[1] Eesti Küberjulgeoleku strateegias, mis võeti vastu 2014. aastal, seati eesmärgiks luua küberväejuhatus, kuid magistritöö kirjutamise ajal on see eesmärk juba täidetud.

	• kriitiliste andmete hoidmine ja töötlemine kõrgturvalistes andmekeskustes, mida varundatakse välismaal; • alternatiivsed lahendused sideteenustele • salastatud teabe edastamisel kasutada krüpteeritud võrke	kaitsemeetmete õigeaegseks rakendamiseks jne • ühiskonna järele aitamine ehk baasküberhügieen • *out-of-the-box* lahendused **Tuleb jätkata**: • baasküberhügieeni koolitamistega	
3. Võime arendamine			
• küberjulgeoleku võime, millega tõhustatakse infosüsteemide turvalisus, sh avastatakse ja ennetatakse pahatahtlikku kübertegevust	• riigikaitsealase võime arendamine	**Täiendavalt kaaluda**: • demonstreerima oma kübervõimeid	**4**
4. Kerksus			
• kerksus kui võime vastupidada ja taastuda kiirelt rünnakutest, õnnetusjuhtumitest jms sündmustest, mis takistab sealhulgas vaenlasel oma eesmärki saavutada; • kerksust tugevdab turvalise IT-arhitektuuri kasutamine ja hea olukorrateadlikkus	• ühiskonna kerksus, mille eesmärk on vastupidada hädaolukordadega toime tulekuks, sh ka siis kui realiseeruvad küberriskid oluliste teenuste osas	• RIA poolt pakutav kerksus • kriitilise infrastruktuuri turvalisusesse investeerimine; • turbelahendused; • haavatavuste ja rünnete tuvastamise võime; • ühiskonna kerksus; • sõjalise vastupanu suutlikkus **Tuleb jätkata**: • kerksuse arendamisega	**7**
V Juriidiline			
1. Küberriskide ja ristsõltuvuste haldamine			

• küberriskide hindamine ja haldamine			
• prioritiseeritakse võtmetähtsusega kriitilist infrastruktuuri	• ristsõltuvuste hindamine; • alternatiivsete lahenduste väljatöötamine	**Tuleb jätkata**: • küberriskide hindamise ja haldamisega	**7**
2. Õiguskaitseorganite tegevuse tõhustamine			
• õiguskaitseorganite töövahendid; • küberkurjategijate vastutusele võtmine; • võimaldada õiguskaitseorganitel keelata juurdepääs infrastruktuurile; • kutsub üles riike liituma Budapesti konventsiooniga	• korrakaitsestruktuuri ja töökorralduse korrastamine; • küberkuritegevusega tegeleva isikkoosseisu suurendamine; • vajalikke võimete arendamine	• küberkurjategijate väljaandmine teistele riikidele; • kehtiv karistusseadustik **Tuleb jätkata**: • õiguskaitseorganite tegevuse tõhustamisega	**8**
3. Õiguskorra muutmine ja täiendamine			
• õigusruumi ajakohastamine			
• vajadus harmoneerida õiguskorda riikide vahel (nt Budapesti konventsiooniga liitumine); • infojagamise põhimõtete täpsustamine seadustes, mis puudutab nii asutuste kui ka ettevõtete vahelist info vahetamist ja kaitsmist		**Tuleb jätkata**: • õiguskorra muutmise ja täiendamisega	**4**
VI Majanduslik			
1. investeerimine küberturvalisusesse			
• küberturvalisusesse investeerimine, mis tagab tõhusama infosüsteemide kerksuse; • asutuste, kes ei panusta küberturvalisusesse, vastutusele võtmine	• küberjulgeoleku tagamisse investeerimine, täpsemalt: ohtude maandamiseks, usaldusväärsete ja konkurentsivõimelistes küberlahenduste tagamiseks;		**5**

	• kogetu tuleb uuesti investeerida innovaatilistesse lahendustesse; • riik on eeskujuks küberjulgeolekusse investeerimisel erasektorile		
VII Heidutust toetavad tegevused			
• luurevõime arendamine (infovahetuskeskkonna loomine);	• teabe kogumine ja töötlemine põhiseaduslikku korda ohustava tegevuse ennetamiseks ja tõkestamiseks	• luurevõime arendamine	**1**
• rahvusvaheline osalus = rahvusvahelise võime arendamine ja koostöö			**0**
• strateegiline kommunikatsioon (deklaratiivne poliitika)		**Täiendavalt kaaluda**: • avalik kommunikatsioon; • rahva usaldus riigi institutsioonidesse	**3**
• teadus- ja arendustegevus (sh tehnoloogiline innovatsioon)			**6**
~~	• teadlikkuse tõstmise vajadus; • koolituste läbiviimine		
• valitsusülene lähenemine	• kaasavpoliitika; • riigikaitse lai käsitlus	•	**1**