TARTU ÜLIKOOL
Sotsiaalteaduste valdkond
Johan Skytte poliitikauuringute instituut

Laura Oolup

KÜBERRÜNNAKUTE RAKENDAMINE HÜBRIIDSÕJAPIDAMISE MEETODINA EESTI, GRUUSIA JA UKRAINA NÄITEL

Bakalaureusetöö

Juhendaja: Raul Toomla, PhD

Tartu 2017

Olen koostanud töö iseseisvalt. Kõik töö koostamisel kasutatud teiste autorite seisukohad, ning kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

……..

/Laura Oolup/

Kaitsmine toimub ……../kuupäev/ kell ……../kellaaeg/ ……../aadress/ auditooriumis ……./number/.

Retsensent: …….. /nimi/ (……./teaduskraad/), …….. /amet/

LÜHIKOKKUVÕTE

Hübriidsõda on pärast Krimmi annekteerimist ’roheliste mehikeste’ poolt kujunenud aktuaalseks terminiks, mille üle järjepidev diskussioon aset on leidnud. Küsimus ei seisne vaid selles, mis hübriidsõda täpselt on, vaid ka kontekstis, kas taoline eraldi sõjapidamise viis üldse eksisteerib.

Võimalikest hübriidsõjapidamise meetoditest on autor valinud uurimisobjektiks küberrünnakud, sest küberruumist ollakse üha enam sõltuvam, mis teeb ühiskonna sedavõrd haavatumaks küberrünnakutele. Tugevdamaks valmidust taolisele julgeolekuriskile vastu seista, on vajalik mõista vastava ohu olemust. Käesoleva töö eesmärgiks on uurida, kuidas rakendatakse küberrünnakuid hübriidsõjapidamise meetodina ja seeläbi on püstitatud hüpotees, et sõja olukorraga kaasnevad ulatuslikumad, intensiivsemad ning kõrgema raskusastmega küberrünnakud.

Eesmärgi saavutamiseks viib autor läbi võrdleva analüüsi kolme juhtumi baasilt, kus hübriidsõjapidamise meetodit küberrünnakuna rakendati: Eesti vastu 2007. aastal, Gruusia vastu 2008. aastal ning Ukraina vastu perioodil 2013. aasta november kuni 2015. aasta detsember. Küberrünnakute ulatuse, intensiivsuse ja raskusastme määramiseks teeb autor mõõtmised tulenevalt rakendatud küberrünnakute ründetüübist, küberrünnakute teostajate varieeruvusest. Küberrünnakute intensiivsust mõõdab autor kontekstis, kas tegu oli relvastatud rünnakuga võrdväärse küberrünnakuga või mitte. Ulatus sõltub küberrünnakute sihtmärkidest.

Kolme juhtumi mõõtmistulemuste võrdlusest selgus, et küberrünnakute raskusaste oli kõigil juhtudel kõrge tulenevalt rünnakutest informatsiooni terviklikkuse vastu. Küberrünnakute intensiivsus oli kõrge vaid Ukraina puhul, kuna teostati edukas füüsiliste tagajärgedega rünnak Ukraina elektrijaama vastu. Sõja olukorras Gruusia ja Ukraina puhul kaasnesid ulatuslikumad küberrünnakud ning intensiivsus rünnakute läbiviijate kontekstis oli kõrge erinevalt Eesti juhtumist. Seeläbi ei pea paika püstitatud hüpotees, sest ainult sõja olukorraga ei kaasne kõrgema raskusastme ning tingimata intensiivsemad küberrünnakud hübriidsõjapidamise meetodina. Võrdluse tulemusena aga selgus, et sõja olukorraga kaasnevad ulatuslikumad küberrünnakud ning intensiivsemad rünnakute teostajate kontekstis.

SISUKORD

SISSEJUHATUS

Hübriidsõda on tõusnud aktuaalseks terminiks peamiselt seoses ’roheliste mehikeste’ ilmumisega Ukrainasse, mille tulemusena Venemaa annekteeris Krimmi (Renz 2016:285). Seeläbi on mitmed autorid omistanud hübriidsõja kontseptsiooni ja selle rakendamise Venemaale, mis tuleneb suuresti Valeri Gerassimovi doktriinist, kus on kirjeldatud sõjalisi taktikaid, mida Venemaa on rakendanud Ukraina puhul, kuid hübriidsõda pole seal mainitud (Renz 2016:286). See on olnud üks põhjus, mis on tekitanud segadust hübriidsõja mõistmisel.

Kuigi hübriidsõja kui eraldi sõjapidamisviisi eksistentsiaalsuse üle esineb vastakaid arvamusi (Bachmann ja Gunneriusson 2015:81-82; Kofman ja Royansky 2015; Puyvelde 2015), siis Lääs on võtnud suuna hübriidohte sellise nimetuse all aktsepteerida. NATO Varssavi tippkohtumisel 2016. aasta suvel otsustasid Liitlased implementeerida koostöös Euroopa Liiduga strateegia, mis kätkeb vastuhakku hübriidsõja vastu (NATO 2016). Euroopa Komisjon andis 2016. aasta aprillis välja raamdokumendi selle kohta, kuidas Euroopa Liit peaks võitlema hübriidohtude vastu, viidates, et tänapäeval on hübriidohud reaalsus (Euroopa Komisjon 2016) ning 11. aprillil 2017 kirjutati alla Euroopa hübriidohtude kompetentsikeskuse asutamisele (NATO 2017).

Hübriidohtude ühine määratlemine on olnud problemaatiline, mis põhjendab osalt, miks Euroopa Komisjoni dokumendiski hübriidohu definitsiooni osas paindlik tahetakse olla. Seepärast on raamistikus viidatud, et vajalik on uurida hübriidohte lähemalt, määramaks riikide nõrgad kohad hübriidohtude suhtes ja mõista, mis determineerib teatud ohu hübriidsuse (Euroopa Komisjon 2016). Seda käesolev bakalaureusetöö plaanibki teha.

Antud töö raames on eesmärk uurida ühe konkreetse hübriidohu tüübi või täpsemini ühe hübriidsõjapidamise meetodi olemust, milleks on küberrünnak, kuna varasem uurimus nii konkreetselt sellel teemal puudub. See on aga vajalik, kuna hübriidsõda peetakse tänapäeva ning tuleviku sõjaks ning küberrünnakuid nähakse järjekindlalt nende osana. Nagu James Andrew Lewis on märkinud, ei seisne küberruumi kasutamine vaid informatsiooni edastamises, vaid seda saab rakendada teiste sõjapidamise domeenide käe pikendusena (Lewis 2014:2). Seepärast mõistmaks julgeolekuriski küberrünnaku näol

hübriidsõja meetodina ja osata ette valmistuda taolise ohu realiseerimiseks, on vaja mõista nende rakendamise olemust.

Seeläbi ongi töö keskne uurimisküsimus, kuidas rakendatakse küberrünnakuid hübriidsõjapidamise meetodina. Seda uurib autor Eesti, Gruusia ja Ukraina vastu sooritatud küberrünnakute alusel vastavalt konflikti toimumisaegadele 2007., 2008. ja 2013-2015. aastal. Hüpotees, mille eesmärgi saavutamiseks on autor seadnud, on järgmine: sõja olukorraga kaasnevad intensiivsemad, ulatuslikumad ja kõrgema raskusastmega küberrünnakud.

Töö on jaotatud kahte ossa. Esimeses osas toob autor välja teoreetilise baasi olemasolevate käsitluste alusel sellest, mis on hübriidsõja kontseptsioon ning milles väljendub küberrünnak hübriidohuna. Töö teises osas viib autor läbi kvalitatiivse analüüsi, rakendades võrdlevat meetodit ning tehes seda toetudes esimeses osas kirjeldatud muutujate mõõtmisele juhtumite keskselt. Analüüsitavad juhtumid, milleks on Eesti vastu 2007., Gruusia vastu 2008. ja Ukraina vastu aastatel 2013-2015 sooritatud küberrünnakud, on valitud lähtuvalt teoorias kirjeldatud hübriidsõjapidamise kontseptsioonile. Analüüsis kasutatavad andmed pärinevad erinevatest avalikult kättesaadavatest raportitest, artiklitest meedias ja varasemalt tehtud uurimustest.

Andmestiku kogumine on raskendatud, kuna küberrünnakutest alati ei raporteerita, tegu on sensitiivse infoga, mistõttu on infole ligipääs piiratud. Samuti on probleeme ka küberrünnakute atributeerimisega, mistõttu kogutud andmestikus esineb selles kontekstis abstraktsust. Vajaliku teoreetilise materjali kogumine oli autori jaoks samuti keeruline, kuna hübriidsõda terminina on uus ning tegevust küberruumis pole hübriidsõja kontekstis otseselt uuritud. Seega materjali limiteerituski kinnitab vajadust teemat uurida.

1. HÜBRIIDSÕJA KONTSEPTSIOON

Käesolevas osas selgitab autor, mida hübriidsõda endas kätkeb, tuues esmajoones välja hübriidsõja kontseptsiooni kujunemise tausta. Seejärel toob autor välja, milles väljendub küberrünnaku olemus hübriidohuna ja kirjeldab seeläbi teooriaid, tuues välja ka muutujad, millest hiljem lähtub autor võrdluse läbiviimisel empiirilises osas.

1.1 UUS SÕJAPIDAMISVIIS

Carl von Clausewitz on kirjutanud, et sõda on poliitika tegemine teiste vahenditega ning sealjuures lisanud, et sõda on jõu kasutamine sundimaks vastast käituma ning tegutsema ründaja tahte järgi (Clausewitz 1993:83,99). Sõjapidamise eesmärk ja selle põhiidee pole aja vältel muutunud, hoolimata vahendite ning seeläbi sõja tunnusjoonte muutumisest (Mansoor 2012:1). Kuid sõda on oma olemuselt muutunud komplekssemaks. Tulenevalt globaliseerumise ning tehnoloogia arengust või õigemini viimase revolutsioonist proovitakse arendada keerukaid võimekusi, mis oleksid nii sõjalised (konventsionaalsed, traditsioonilised meetmed ning vahendid) kui ka mittesõjalised (näiteks terrorism, mässuliste tegevus) ning osapoolteks on lisaks riikidele ka riigivälised tegutsejad (Cruceru 2014:235).

Uute tehnoloogiate areng, mis võimaldab eesmärgini jõuda kiiremini ning lihtsamini, aitab minimaliseerida konventsionaalsete vahendite kasutamist ning näiteks küberrünnakud omavad sellist eripära (Geers 2011:136). See-eest täielikku edu sõjalises kontekstis konventsionaalsete vahendite kasutamiseta ei saavutata (Băhnăreanu 2016:60). Frank Hoffman on kirjeldanud taolist komplekssust kui erinevatest vahenditest unikaalse kombinatsiooni otsimist ja seejärel selle rakendamist (Hoffman 2014:330). Sõjapidamise keerukuse kasvava tendentsiga on kaasnenud valdkonna terminoloogia laienemine ning uued teooriad ja kontseptsioonid, mida proovitakse kohaldada niivõrd-kuivõrd uuele nähtusele.

Neljanda ja viienda generatsiooni sõjapidamisviisid on näited kahest pakutud teooriast tänapäeval ning tulevikus aset leidvale sõjale. Need kaks lähenemist, mida on kirjeldanud Cristian Băhnăreanu, hõlmavad riikide osatähtsuse vähenemist sõjalises vastasseisus, professionaalsete armeede teket, asümmeetriliste taktikate ning tehnikate kasutamist, mis

sunnivad vastast rakendama mittekonventsionaalseid meetmeid. Lisaks tuuakse välja, et vastased on riigivälised tegutsejad ja konventsionaalsete meetodite kasutamine seguneb ebatraditsiooniliste ründevahenditega. Sealhulgas rakendatakse mittevägivaldseid operatsioone, kuhu kuuluvad näites infooperatsioonid, ning konfliktipõhjused omavad poliitilist, usulist ja sotsiaalset tausta (Băhnăreanu 2015:59-60).

Veel üks kontseptsioon, millega on proovitud kirjeldada väljatoodud keerulist sõjapidamisviisi, on liitsõjapidamise (ingl k *compound warfare)* meetod, mis hõlmab konventsionaalsete ja mittekonventsionaalsete jõudude rakendamist (Băhnăreanu 2015:58-59). Erinevus hübriidsõjast seisneb selles, et kontseptsioon ei seleta tänapäevase ning tuleviku sõja komplekssust näiteks erinevate meetodite samaaegse rakendamise poolest (Hoffman 2014:333).

Frank Hoffman, keda võib nimetada hübriidsõja kontseptsiooni autoriks või vähemalt kaasautoriks, on toetunud selle loomisel nende samade väljatoodud koolkondade teooriatele, mis proovivad seletada sõjapidamisviise tänapäeval ning tulevikus. Neljanda generatsiooni sõjapidamisviisi ideedest on Hoffman hübriidsõja kontseptsiooni haaranud konfliktis esinevad hägusad piirid kasutatavate meetodite vahel ning riigi ülemlikkuse vähenemise vägivaldsete tegevuste rakendamises. Liitsõjapidamisviisi teooriast on ta arvesse võtnud konventsionaalsete ning mittekonventsionaalsete meetodite koostoimest tuleneva või saadava mõju ning tõhususe (Hoffman 2007:30).

1.2 HÜBRIIDSÕJA OLEMUS

Kui Clausewitz määratles sõja poliitiliste eesmärkide täideviimisena, ainult et teiste vahenditega, siis hübriidsõja puhul on vahenditeks erinevate meetodite rakendamine, mis pärinevad erinevatest konfliktimoodustest (Hoffman 2009). Sõdades on varasemaltki rakendatud tehnikaid, mis on nii regulaarsed kui ka korrapäratud (ingl k *irregular),* kuid hübriidsõjas tehakse seda ühe osapoole poolt samal sõjatandril, seega erinevad jõud ning võimekused on rohkem segunenud, võrreldes traditsioonilise sõjaga (Hoffman 2007:29).

Hübriidsõja kui termini on omaks võtnud mitmed akadeemikud, kuid definitsioonid siiski varieeruvad. Näiteks Ioniță on kirjeldanud hübriidsõda kompleksse sõjapidamisviisina, mis hõlmab erinevate meetodite segunemist ja nende rakendamise koostoime esinemist (Ioniță 2014:66). Băhnăreanu on toonud välja, et tulevikus aset leidvad konfliktid on

kombinatsioon konventsionaalsetest ja ebaregulaarsetest meetoditest, kuid konventsionaalset ja asümmeetrilist meetodit ei pruugita rakendada hübriidsõjas alati samaaegselt ehk võidakse kasutada ka vaid ühte neist (Băhnăreanu 2015:64).

Hoffman ise on defineerinud hübriidsõda sõjapidamisviisina, mis koondab erinevaid konfliktimooduseid, milleks on konventsionaalne võimekus, ebakorrapärased taktikad ja vormid, terrorirünnakud ja kuritegeliku loomuga segadust tekitavad tegevused (ingl k *criminal disorder)* (Hoffman 2007:14). Tema definitsioon tugineb enamjaolt 2005. aasta Ameerika Ühendriikide kaitsestrateegias väljatoodud uutele eesseisvatele ohtudele. Nimelt nähti sel ajal peamiselt nelja tüüpi ohte: traditsioonilisi, korrapäratuid, katastroofilisi ning segadust tekitavaid (The National Defense Strategy of the United States of America 2005:2). Ohud, mida strateegias konkreetselt veel hübriidohtudeks ei nimetatud, tulenesid USA hegemooniks olemisest konventsionaalse võimekuse poolest, mistõttu teised riigid ning mitteriiklikud tegutsejad on pidanud hakkama leidma alternatiivseid võimalusi, millega tagada eelist USA ees (Mattis ja Hoffman 2005; The National Defense Strategy of the USA 2005:2-3).

Mida aga hõlmavad väljatoodud ohukategooriad? Tulenevalt USA 2005. aasta kaitsestrateegiast, nähakse traditsiooniliste ohtudena konventsionaalsete meetmete rakendamist. Nendeks on teiste seas sõjavägi, merevägi ja õhujõud. Kuna traditsioonilised meetmed on kulukad, võibki oodata vastase tegutsemist mõnel teisel areenil teistsugust meetodit rakendades (The National Defense Strategy of the USA 2005:2-3). Ebakorrapärased on üheks neist. Need ohud hõlmavad mässuliste ning terroristide akte, mille realiseerimise eesmärgiks on õõnestada riigi usaldusväärsust ning mõjuvõimu (The National Defense Strategy of the USA 2005:3).

Hoffman eraldab siinkohal terrorismi korrapäratud meetoditest, mille ta defineerib omakorda kui valimatu vägivalla ja sunnimeetmete kasutamisena (Hoffman 2014:331). Korrapäratud meetmed, mille alla grupeeruvad ka küberrünnakud, omavad olulist rolli just konventsionaalsete võimekuste rakendamisel. Nad aitavad tagada eeliseid traditsiooniliste jõudude kasutamiseks näiteks spionaaži kaudu (Cruceru 2014:232).

Katastroofilisi tagajärgi omavad ohud, mis USA kaitsestrateegia kontekstis omistati massihävitusrelvade kasutamisele, ning segadust tekitavad ohud, mis olid defineeritud

kui militaarsete ja uute tehnoloogiliste arenduste rakendamisena (The National Defense Strategy of the USA 2005:2-3), asendas Hoffman kuritegevusliku loomuga segadust tekitava konfliktimoodusega (Hoffman 2007:14). Kuritegevusliku olemusega meedet näeb Hoffman destabiliseeriva meetodina, mis avaldab vastavat mõju eelkõige riigi valitsusele (Hoffman 2014:330).

Nagu Hoffman ka välja toob, sõltub sõja hübriidsus sellest, milliseid vahendeid rakendatakse ning, kes on need rakendajad (Hoffman 2007:28). Rakendajate ehk osapooltena hübriidsõjas kirjeldab Hoffman kolme võimalust: riike, riigi poolt toetatud gruppe, ühinguid või rühmitusi ning riigiväliseid tegutsejaid (Hoffman 2007:29). Mitteriiklikud tegutsejad võivad olla näiteks terroristlikud rühmitused, etnilised ja organiseeritud kuritegevuslikud grupid (Schroefl ja Kaufman 2014:868).

1.2.1 KÜBERRÜNNAK HÜBRIIDSÕJAPIDAMISE MEETODINA

Kenneth Geers on välja toonud, et kõik poliitilised ja sõjalised konfliktid hõlmavad küberdomeeni, mille ulatust ning mõju on keeruline ette ennustada. Lisaks võib tegevus küberruumis muutuda olulisemakski, võrrelduna sellega, mis traditsioonilisel viisil maal, meres ja õhus võib toimuda, sest küber- kui asümmeetrilisele rünnakule võib olla keerulisem vastu hakata kui näiteks massihävitusrelvale (Geers 2011:9).

Kohane on küberrünnakut pidada hübriidohuks, mida on kinnitanud Gunneriusson ja Ottis, põhjendades, et küberrünnak ei kategoriseeru ainult konventsionaalse või mittekonventsionaalse meetodi alla, vaid asub nende kahe vahel või teisisõnu on olemuselt ühisosa neist kahest (Gunneriusson ja Ottis 2013:99). Ka Thomas Rid on rõhutanud, et rakendatud küberrünnakuid kübersõja alla koondada on ennatlik, sest tulenevalt Clausewitzi sõja definitsioonist, ei vasta olnud ning suure tõenäosusega ka tulevikus toime pandavad küberrünnakud sõja kontseptsiooni elementidele (Rid 2012:7, 29).

Seda, mida hõlmab endas küberrünnak, on defineeritud mitmeti, mida illustreerib ka suur varieeruvus definitsioonides NATO Küberkaitsekeskuse koduleheküljel (CCDCOE). Dunn Cavelty on mõistnud küberrünnaku all kahju tekitavat juhtumit või olukorda, mis on inimeste poolt juhitud (Dunn Cavelty 2015:402). Martin Libicki defineerib küberrünnakut kui ühe riigi süsteemi toimimise katkestamise või rikkumisena teise riigi

poolt (Libicki 2009:23). Hübriidsõja kontseptsioonist tulenevalt jääb Libicki seletuse juures vajaka aspekt, et osapoolteks ei pruugi olla ainult riigid, mida toob välja ka Leonard Kahn (Kahn 2013:384).

Käesoleva töö puhul järgitakse NATO definitsiooni rünnakust arvutivõrgu vastu, mida küll peetakse üheks küberrünnaku osaks. Definitsiooni kohaselt on tegu seega rünnakuga, mille eesmärk on „häirida, takistada, kahjustada või hävitada informatsiooni, mis resideerub arvutis/arvutivõrgus, või arvutit/arvutivõrku ennast“ (NATO 2014:2-C-11). Kuna küberrünnaku puhul on erinevaid definitsioone, siis käesolevas töös on õigustatud kasutada viimast definitsiooni, kuna kohaldub edukalt küberrünnakutele hübriidsõja kontekstis, mida antud töö puhul uuritakse.

Kenneth Geers on välja toonud, et küberrünnakute peamine eelis seisneb selles, et küberruum ja Interneti arhitektuur eelkõige omavad mitmeid nõrkusi. Seeläbi suudavad ründajad, teisisõnu häkkerid mõjutada vähemalt ühte infoturbe kolmest alustalast: informatsiooni terviklikkust, käideldavust või konfidentsiaalsust (Geers 2011:135, 137). Geers jaotab vastavalt infoturbe komponentidele ka küberrünnaku vormid.

Geers toob välja, et informatsiooni konfidentsiaalsuse rünne hõlmab endas informatsiooni omamist, milleks puudub igasugune volitatus. Siia alla kuuluvad näiteks kommunikatsiooni (sidevõrkude) jälgimine ja pealt kuulamine. Kuna globaalne sidevõrkude kaitse ja julgeolek on arengult maha jäänud, võrreldes kuivõrd seotud on need sidevõrgud omavahel üle maailma, on häkkeritel üsnagi lihtne suures mahus informatsiooni varastada ning seeläbi ka info konfidentsiaalsust rünnata (Geers 2011:137).

Kui informatsiooni, informatsiooniallikaid või andmebaase üleüldiselt mittevolitatult modifitseeritakse ründaja poolt, toimub informatsiooni terviklikkuse vastane rünne. Näiteks toob Geers välja, et informatsiooni sabotaaž poliitilistel, kuritegelikel või sõjalistel eesmärkidel kuulub siia kategooriasse. Kolmas rünnakutüüp on informatsiooni käideldavuse vastane rünne. Sellisel juhul on ründaja eesmärgiks piirata või ennetada ligipääsu tagamist teatud andmetele või süsteemile terviklikult volitatud isikule. Teenustõkestusrünne (ingl k *denial of service – DoS*) on tüüpiliseimaks vahendiks sellise ründe läbi viimiseks (Geers 2011:137).

Nendest kolmest rünnakuvormist võiks raskusastmelt pidada kõige tõsisemaks rünnakut informatsiooni terviklikkuse vastu. Seda põhjusel, et taolist rünnakut saab teostada erineva raskusastmega, võimaldades sealjuures tekitada füüsilist kahju ning omades seeläbi ka suuremat mõju. Näiteks kuulub veebilehekülgede näotustamine (Brangetto ja Veenendaal 2016:123) siia ründe kategooriasse, mis ei too kaasa märkimisväärseid tagajärgi. Samas kategoriseerub siia alla ka rünnak Iraani tuumajaamade vastu 2010. aastal, mis on tuntud Stuxneti kui rünnaku läbiviimiseks kasutatud pahavaralise ussi all. Eesmärgiks oli saboteerida Iraani tuumaprogrammi arengut, mida suudeti edukalt teha, kahjustades uraani rikastavaid tsentrifuuge, muutes viiendiku nendest kasutuskõlbmatuks, mis omakorda viis Iraani tuumaprogrammi 2 aasta võrra arengust tagasi (Zetter 2014). Seega ründega informatsiooni terviklikkuse vastu on võimalik tekitada märkimisväärset füüsilist kahju. Andmed, et rünnakud informatsiooni konfidentsiaalsuse või käideldavuse vastu on tekitanud füüsilist kahju, puuduvad.

Küberründe vahendeid või meetodeid on mitmeid, kuid Pascal Brangetto ja Matthijs Veenendaal on välja tulnud teooriaga küberoperatsioonide kohta, mis omavad psühholoogilist mõju inimestele ehk peaksid mõjutama inimeste käitumist (ingl k *influence cyber operations)* (Brangetto ja Veenendaal 2016:115). Seega teatud küberrünnakute rakendamine sõltub sellest, kas eesmärgiks on inimeste mõjutamine vägivallavabal moel. Taoline taktika kohaldub ka hübriidsõja kontseptsioonile, sest eesmärk on minimaliseerida konventsionaalsete vahendite rakendamist ning saavutada elanikkonna üle psühholoogiline mõjuvõim teiste meetodite abil (Cruceru 2014:232). Kübervõimekus antud juhul on üks võimalus selleks (Brangetto ja Veenendaal 2016:118).

Küberrünnakud, mis teooria kohaselt peaksid mõjutama inimeste suhtumist ja käitumist, on madala intensiivsusega ehk ei kategoriseeru relvastatud rünnaku alla (Brangetto ja Veenendaal 2016:121). Kõrge intensiivsusega või teisisõnu relvastatud rünnakuks võib nimetata küberrünnakut, mis on loomult kineetiline ja toob kaasa näiteks teatud objekti füüsilise hävingu või kahjustuse (Schmitt 2012:288). Madala intensiivsusega rünnakuviisiks on informatsioonisüsteemi sisse häkkimine, näiteks kriitilise taristu vastu teostatav rünne, mille teostamisel võidakse süsteemis olevaid andmeid modifitseerida (Brangetto ja Veenendaal 2016:121). Teine meetod on libaoperatsiooniline küberrünnak

(ingl k *false flag attack*), mis tähendab, et rünnak omistatakse algselt valele isikule, grupile või riigile (Brangetto ja Veenendaal 2016:122).

Teenustõkestusrünne, mis hõlmab süsteemi ülekoormamist enamjaolt massiivsete infopäringutega ning seeläbi teenuse ligipääsmatuks tegemist (Brangetto ja Veenendaal 2016:122-123; Geers 2011:134), nagu ka veebilehekülgede näotustamine (ingl k *defacement)*, mis tähendab mittevolitatult informatsiooni muutmist veebilehekülgedel, mõjutavad negatiivselt riigiasutuste usaldusväärsust elanikkonna silmis (Brangetto ja Veenendaal 2016:123). Viimane psühholoogilist mõju avaldav küberrünnak on salastatud või privaatse informatsiooni varastamine ning selle avaldamine (ingl k *doxing*), mille eesmärk on sihtmärki avalikult häbistada ja seeläbi alandada (Brangetto ja Veenendaal 2016:124).

Küberrünnaku läbiviimist saab jaotada samuti kolme kategooriasse Gunneriussoni ja Ottise teooria kohaselt. Nende seletusest lähtuvalt teostatakse küberrünnakuid kas konventsionaalsete vägede toetuseks, iseseisva asümmeetrilise rünnakuna mittesõjaliste objektide suunal või küberruumi ekspluateerimisel millegi võimaldava või takistava vahendina. (Gunneriusson ja Ottis 2013:101-103).

Gunneriusson ja Ottis kirjeldavad, et konventsionaalsete vägede ja jõudude toetuseks rakendatud küberrünnakuga on tegu, kui sihtmärgiks on valitud näiteks arvuti poolt juhitavad süsteemid (näiteks droonid ja raketid), kontrolli- ja logistikasüsteemid. Peamiseks sihtmärgiks sõjalise küberoperatsiooni korral on vastase logistika- ning kommunikatsioonisüsteem, mis on küberrünnakutele enim haavatavamad. Kuid rünnak ei pea selles kategoorias omama tingimata pikaajalist mõju või efekti, teinekord võib ainult lühiajaline vastase kontrollsüsteemi rikkumine või häirimine ainuke eesmärk olla (Gunneriusson ja Ottis 2013:101).

Tõenäoliseimaks mittesõjaliseks sihtmärgiks üksikute küberrünnakute puhul peavad Gunneriusson ja Ottis kriitilist taristut selle suure sõltuvuse tõttu ühiskonnas. Lisaks võivad nende hinnangul selle küberrünnakute kategooria puhul rünnakute alla sattuda mitmed teised IT-lahendused, mis on küberruumiga seotud. Kolmas kategooria võib hõlmata inimeste koondamist küberruumi kaudu, kuid ka limiteerida nende ligipääsu teatud teenustele Internetis. Eelkõige viitavad autorid selles kategoorias küberruumile kui

keskkonnale, mida on võimalik ekspluateerida näiteks propaganda levikuks, luureinfo kogumiseks (Gunneriusson ja Ottis 2013:102-103).

Küberrünnakuid on tihti keeruline atribuuteerida (Geers 2011:136). Cilluffo ja Clark'i väidetele tuginedes on realiseeritud hübriidohtu problemaatiline omistada kahel põhjusel. Esimesel juhul ei pruugi kaitsja meelest ründaja omada piisavalt võimekust, et rünnaku eest vastutavat otsida. Teisel juhul on ohu realiseerija vältinud teadlikult enese avalikustamist näiteks siis, kui eesmärk on viivitada kaitsja vastusega mingile teisele rünnakule (Cilluffo ja Clark 2012:50). Applegate ja Stavrou määratlevad küberrünnakute läbiviijaid kohaldatavalt hübriidsõjapidamise kontseptsioonile riiklikeks või riigivälisteks tegutsejateks (Applegate ja Stavrou 2013:441). Cilluffo ja Clark aga märgivad, et rünnakut võidakse läbi viia agendi või teisisõnu läbi vahendaja *(*ingl k *proxy-actor)* (Cilluffo ja Clark 2012:49), mis põhjendab samuti rünnaku atributeerimise komplekssust.

Seega küberrünnakute rakendamine sõltub mitmest tegurist: mida rünnatakse, millal ja mis eesmärgil seda teostakse. Nendest lähtuvalt seab käesoleva töö autor hüpoteesiks, et sõja olukorraga kaasnevad intensiivsemad, ulatuslikumad ja kõrgema raskusastmega küberrünnakud. Seda hakkab autor testima järgmises osas.

2. EMPIIRILINE ANALÜÜS

Käesolevas peatükis on eesmärk testida teoorias püstitatud hüpoteesi: sõja olukorraga kaasnevad intensiivsemad, ulatuslikumad ja kõrgema raskusastmega küberrünnakud. Hüpoteesi testimiseks kasutab autor võrdlevat meetodit, mille teostamist kirjeldatakse järgneva alapeatüki all.

2.1 ANDMESTIK JA MEETOD

Vastamaks püstitatud uurimisküsimusele, kuidas rakendatakse küberrünnakuid hübriidsõjapidamise meetodina ja testimaks seeläbi hüpoteesi, kas sõja olukorraga kaasnevad intensiivsemad, ulatuslikumad ja kõrgema raskusastmega küberrünnakud, viib autor läbi võrdleva analüüsi kolme juhtumi näitel, mil küberrünnakuid vastava sõjapidamisviisi taktikana rakendati Eestile 2007. aastal, Gruusiale 2008. aastal ja Ukrainale 2013-2015. aastatel.

Põhjus, miks autor valis just need juhtumid, seisneb omakorda nende juhtumite vastavuses töö esimeses osas kirjeldatud hübriidsõja kontseptsioonile (Maigre 2015, Bachmann ja Gunneriusson 2014:82). Uurimaks küberrünnakuid hübriidohuna, oli vaja valida juhtumid, kus on rakendatud hübriidsõjapidamise meetodeid. Eesti puhul ei toimunud hübriidsõda, kuid rakendati hübriidtaktikaid kuritegevusliku loomuga segadust tekitavate ning ebakorrapäraste meetoditena tänavatel toimunud demonstratsioonide ning küberrünnakute näol. Gruusias ja Ukrainas toimuvale on võimalik kohaldada hübriidsõja kontseptsioon, sest lisaks küberrünnakutele ebakorrapärase meetodina, rakendati uuritavatel perioodidel samaaegselt ka konventsionaalseid vahendeid.

Lisaks ühendab kolme juhtumit Venemaa pidamine potentsiaalseks rünnakute eest vastutavaks. Teoorias sai välja toodud hübriidtaktikate ning sealjuures küberrünnakute omistamise problemaatilisus, kuid Venemaad võib siiski suure tõenäosuse alusel pidada vastutavaks enamike toime pandud küberrünnakute eest, sest esineb suurel määral viiteid seostele rünnakute läbiviijate ja Vene valitsuse vahel (Project Grey Goose:Phase I Report 2008:4; Richards 2014:34; Shakarian 2011:67; Weedon 2015:70).

Iga juhtumi puhul mõõdab autor kolme tegurit: küberrünnakute raskusastet, intensiivsust ja ulatust. Mõõtmise läbiviimiseks on juhtumite kohta vaja koguda infot selle kohta,

millal küberrünnakud aset leidsid, kes olid rünnakute teostajad ning milliseid rünnakuid läbi viidi. Viimase puhul on oluline leida info sihtmärkide ning rakendatud ründemeetodite kohta. Need andmed on autor toonud iga juhtumi puhul ka eraldi tabelites (vt tabel 1, 17-18; tabel 2, 19-20; tabel 3, 21-22) välja. Kogutud andmestik pärineb erinevatest raportitest, varasematest uurimustest ning ka usaldusväärsetest artiklitest meedias, kus oli avaldatud informatsiooni toimunud küberrünnakute kohta.

Küberrünnakute raskusastet mõõdetakse Geers'i (2011:137) poolt väljatoodud rünnakutüüpide alusel, mille puhul rünnak informatsiooni terviklikkuse vastu on raskem rünnakutüüp, võrreldes rünnakutega informatsiooni käideldavuse vastu. Rünnakute tagajärgi raskusastme mõõtmisel ei arvestata. Seega raskusaste on kõrge, kui rünnakud informatsiooni terviklikkuse vastu on toimunud ning madal, kui piirdutud on vaid rünnetega informatsioon konfidentsiaalsuse ning käideldavuse vastu.

Intensiivsus jaotub kaheosaliseks. Rünnakumeetodite kontekstis sõltub see, kas rakendatud küberrünnakud kategoriseeruvad madala intensiivsusega rünnakute alla, mida on kirjeldanud Brangetto ja Veenendaal (2016:121), või on tegu kõrge intensiivsusega (Schmitt 2012:288), mis eeldab küberrünnaku võrdväärseks pidamist relvastatud rünnakuga. Lisaks mõõdetakse intensiivsust rünnakute toimepanijatest lähtuvalt. Intensiivsemate rünnakutega nende teostajate kontekstis on tegu juhul, kui riik või riigi poolt toetatud grupp või rühmitus on küberrünnaku toime pannud. Lisaks sõltub intensiivsus ka sellest, kui suur oli rünnakute toimepanijate variatiivsus. Ehk tegu on kõrge intensiivsusega rünnakute toimepanijate kontekstis, kui neid on toime pannud häkkerite grupid ja kellel on leitud võimalikud sidemed Vene valitsusega.

Kolmas mõõdik ulatus sõltub küberrünnakute sihtmärkidest. Ehk, kas need olid riigisisesed või ka riigivälised. Ulatus sõltub ka Gunneriussoni ja Ottise (2013:101-103) väljatoodud küberrünnakute rakendamise erisustest: kas rakendatakse neid konventsionaalse jõu toetamiseks, mittemilitaarsete objektide vastu või millegi takistava või võimaldava vahendina küberruumi kui keskkonda ära kasutades. Ulatus on seda suurem, mida enam on erinevatel eesmärkidel ja erinevatele sihtmärkidele rünnakuid teostatud. Ulatus on suur, kui küberrünnakuid sooritati ka konventsionaalse jõu toetamiseks lisaks iseseisvatele asümmeetrilistele rünnakutele ning millegi takistava või võimaldava vahendina. Ulatus on seega väike, kui konventsionaalsete jõudude

toetamiseks küberrünnakuid ei rakendatud ning küberrünnakute sihtmärkideks olid riigisisesed asutused.

Järgnevalt viiakse läbi mõõtmised ulatuse, intensiivsuse ja raskusastme suhtes iga juhtumi põhjal eraldi. Seejärel võrreldakse saadud tulemusi mõõdikutepõhiselt ning tehakse järeldused püstitatud hüpoteesi osas.

2.1.1 KÜBERRÜNNAKUD EESTI VASTU 2007. AASTAL

26. aprillil algasid Eesti pealinnas Tallinnas rahutused etniliste venelaste ja eestlaste vahel seoses Pronkssõduri teisaldamisega ning sõdurite haudade üles kaevamisega, mis asetsesid kuju ümber (Swedish Emergency Management Agency 2008:8; Stiennon 2010:87). 27. aprilli ööl teisaldati kuju, mis oli 1947. aastal tehtud tähistamaks Nõukogude Liidu võitu Natsi-Saksamaa üle, salajasse kohta. Sama päeva õhtul ehk vähem kui 24h pärast leidsid aset esimesed küberrünnakud Eesti vastu (Swedish Emergency Management Agency 2008:8-9, 11). Lisaks küberrünnakutele ja tänavatel toimunud demonstratsioonidele levitati ka propagandat ning toimus Eesti saatkonna blokaad Moskvas (Tiirmaa-Klaar 2008:157).

Tabel 1. Eesti-vastased küberrünnakud 2007. aastal.

Küberrünnakute kestvus	27. aprill 2007 – 18. mai 2007 (Tikk, Kaska, Vihul 2010:33).
Rünnaku vastavus poliitiliselt olulisele perioodile konfliktis	27. aprill 2007 – Pronkssõduri teisaldamine, algas esimene küberrünnakute faas (Tikk, Kaska, Vihul 2010:18). 8. mai õhtul (9. mai varahommikul Moskva aja järgi) – Venemaal Võidupüha tähistamine, Eesti serveritele massiivne DDoS-rünnak (Swedish Emergency Management Agency 2008:16; Tikk, Kaska, Vihul 2010:20).
Teostaja	Riigivälised iseseisvad tegutsejad, häktivistid (Tikk, Kaska, Vihul 2010:33).
Sihtmärk	DNS-serverid; pangad (Hansapank, SEB-pank); valitsuse, ministeeriumite, presidendi, parlamendi, Reformierakonna,

	Postimehe, väiksemate omavalitsusüksuste, maakoolide ja mitme teisegi asutuse veebileheküljed; Interneti teenusepakkujad (sidevõrgud) (Stiennon 2010:87; Swedish Emergency Management Agency 2008:11, 13, 15-16; Tikk, Kaska, Vihul 2010:19-20).
Ründemeetod	DoS (ingl k *denial of service* – teenustõkestusrünne), DDoS (ingl k *distributed denial of service* – hajus teenustõkestusrünne), pahavara levitamine, veebilehekülgede näotustamine, rämpsmeilide ja -kommentaaride edastamine (Tikk, Kaska, Vihul 2010:33).

Küberrünnakud algasid rahutustega samaaegselt ning kestsid valdavalt 18. maini. Rünnakud toimusid mitmes faasis: 27. aprillist - 29. aprillini ning 30. aprillist 18. maini (Tikk, Kaska, Vihul 2010:18, 33). Suuremahulised küberrünnakud leidsid aset Võidupühal Moskva aja järgi 9. mai kesköösl, mil rakendatud botnetid hõlmasid üle miljoni arvuti (Swedish Emergency Management Agency 2008:16), teostamaks seeläbi DDoS-rünnakut.

Tikk, Kaska ja Vihul on kirjeldanud, et teenustõkestusrünnakute toimepanemiseks koondati venekeelsetes foorumites häktiviste, kes olid rahvuslikult ja poliitiliselt motiveeritud isikud. Nendes Interneti-foorumites jagati juhiseid, kuidas rakendada *ping*-käsklust teatud parameetritega MS Windowsi käsurealt, mis võimaldab kontrollida sihtmärgiks valitud arvuti või serveri kättesaadavust ja ligipääsu ning seeläbi need üle koormata ja kättesaamatuks muuta. Hiljem muudeti avalikuks .bat-failid, mis, kopeerides arvutitesse, viisid *ping*-käsu automaatselt läbi ja muutsid rünnatavad veebileheküljed ligipääsmatuteks (Tikk, Kaska, Vihul 2010:18, 33).

Intensiivsus rünnakute teostaja kontekstis oli madal, sest ühelegi häkkerite rühmale ei ole rünnakuid omistatud, tegutsejateks olid iseseisvad riigivälised häktivistid. Samas koordineeritud küberrünnakuid teises rünnaku faasis esines (Tikk, Kaska, Vihul 2010: 33), mis võib viidata antud juhul Vene valitsuse toetusele. Samas rünnakute tipphetkel 9. mail oli botneti kaasatud ligi miljon arvutit (Swedish Emergency Management Agency 2008:16), kuid paljud arvutiomanikud polnud suure tõenäosusega teadlikud, et nende arvuti on kaasatud rünnakusse.

Madal intensiivsus kohaldub ka läbiviidud rünnakutele, sest teostatud rünnakud ei olnud võrdväärsed relvastatud rünnakule, kuid raskusaste korraldatud rünnakute puhul on kõrge, kuna teostati ründeid informatsiooni terviklikkuse vastu. Informatsiooni terviklikkuse vastane rünne väljendub näiteks veebilehekülgede näotustamises.

Rünnakute ulatus ei olnud suur. Esiteks ei rakendatud konflikti käigus konventsionaalseid meetmeid, seeläbi ei toimunud küberrünnakuid konventsionaalsete vägede toetuseks. Sihtmärkideks olid valitud riigisisesed asutused, enamasti riigiinstitutsioonide veebileheküljed, kuigi 9. mai rünnakute tagajärjel muutus 58 veebilehekülge ligipääsmatuks (Tikk, Kaska, Vihul 2010:20). Seega teostati küberrünnakuid mittesõjaliste sihtmärkide pihta kui ka Gunneriussoni ja Ottise poolt väljatoodud kolmanda kategooria rünnakuid, mis on loomult kas takistavad või võimaldavad (Gunneriussoni ja Ottise 2013:102, 103).

2.1.2 KÜBERRÜNNAKUD GRUUSIA VASTU 2008. AASTAL

2008. aastal toimus Gruusias sõda Gruusia ja Venemaa vahel. Sõda toimus Abhaasia ja Lõuna Osseetia üle, mille iseseisvumist Gruusiast pooldas Venemaa (Stiennon 2010:96; Tikk, Kaska, Vihul 2010:89). Küberrünnakud Gruusia domeeniga olevatele veebilehekülgedele, nagu Gruusia presidendi, valitsuse, välis- ja kaitseministeeriumi kui ka Gruusia-meelsete meediaväljaanete omadele, algasid samal päeval 8. augustil, kui Vene väed sooritasid õhurünnaku Gruusia militaarobjektidele (Tikk, Kaska, Vihul 2010:70; Stiennon 2010:97). Lisaks toimusid küberrünnakud veebilehekülgedele, mida Gruusia kasutas kommunikeerimiseks oma rahva ja ülejäänud maailmaga, ka 7. augusti õhtul (Stiennon 2010: 97).

Tabel 2. Gruusia-vastased küberrünnakud 2008. aastal.

Küberrünnakute kestvus	8. august – 28. august 2008 (Tikk, Kaska, Vihul 2010:89).
Rünnaku vastavus poliitiliselt olulisele perioodile konfliktis	8. august – Vene väed teevad õhurünnaku Gruusia militaarobjektide pihta (Stiennon 2010:97). Samal päeval algavad küberrünnakud Gruusia domeeniga veebilehekülgedele (Tikk, Kaska, Vihul 2010:70).

Teostaja	Häktivistid, häkkerite grupid (Russian Business Network), riigivälised tegutsejad (Shakarian 2011:67; Stiennon 2010:99; Tikk, Kaska, Vihul 2010:75).
Sihtmärk	Erinevad Gruusia domeeniga veebileheküljed, sealjuures Gruusia presidendi, keskvalitsuse, välis- ja kaitseministeeriumi, Gruusia-meelsete ning Gruusia meediaväljaandeid (nt apsny.ge, News.ge), Lääne meedia, muude eraettevõtete, finants- ja haridusasutuste veebileheküljed, rünnati ka Gruusia suurimat kommertspanka (Shakarian 2011:64, 66; Tikk, Kaska, Vihul 2010:70-72).
Ründemeetod	DoS, DDoS, veebilehekülgede näotustamine, pahavara levitamine, rämpsmeilide saatmine (Tikk, Kaska, Vihul 2010:89).

Gruusia juhtumi puhul teostati küberrünnak ka kuu enne konflikti algust 19. juulil, mil tehti DDoS-rünnak Gruusia presidendi veebileheküljele sõnumiga *win+love+in+Russia*, mille tagajärjel muutus veebilehekülg 24h-ks kättesaamatuks (Tikk, Kaska, Vihul, 2010:69). Lisaks olid maas ka teised samal serveril asuvad veebileheküljed (Stiennon 2010:97). On oletatud, et tegu oli proovirünnakuga konflikti vältel toimunutele (Shakarian 2011:66).

Intensiivsus rünnakute tegijate kontekstis on kõrge, sest lisaks iseseisvatele mitteriiklikele häktivistidele, keda osalt koondati Internetis venekeelses häkkerite foorumis (Project Grey Goose: Phase I Report 2008:8; Tikk, Kaska, Vihul 2010:75), on rünnakuid omistatud ka häkkerite grupile Russian Business Network'le, millel on sidemeid Vene valitsusega (Shakarian 2011:67; Stiennon 2010:99). Ehk tegu võib olla häkkerite grupiga, mis oli toetatud Vene valitsuse poolt. Sealjuures on kindlaks tehtud, et mitmed DDoS-rünnakud pärinesid Venemaal asuvatest serveritest (Richards 2014:34). Samas oli tegu madala intensiivsusega rünnakutega, sest ükski rünnak polnud võrdväärne relvastatud rünnakuga. See-eest rünnakute raskusaste on kõrge, kuna rakendati ründeid informatsiooni terviklikkuse vastu, mis väljendub näotustamise teostamises.

Rünnakute ulatus oli suur kontekstis, et küberrünnakuid rakendati ka konventsionaalsete vägede toetuseks. Otseselt kommunikatsiooni- ja logistikasüsteeme ei rünnatud, kuid sihtmärkideks valitud veebileheküljed omasid Stiennoni (2010:97) sõnul olulist rolli

konflikti vältel, sest tagasid infovahetuse Gruusia valitsuse ja Gruusia elanikkonna ning ülejäänud maailma vahel. Lisaks ründasid Vene häkkerid veebilehekülge, kus oli võimalik rentida elektrigeneraatoreid, mis võis olla toetav rünnak konventsionaalsetele rünnakutele Gruusia elektritaristu vastu (Shakarian 2011:66). Rünnakute ulatus on sellegi võrra suur, et ei piirdutud vaid riigiasutuste ja riigisiseste ettevõtete ründamist, vaid sihtmärkideks osutusid ka USA ja UK saatkonnad Tbilisis (Stiennon 2010:98).

2.1.3 KÜBERRÜNNAKUD UKRAINA VASTU AASTATEL 2013-2015

2013. aasta novembris, mil tookordse Ukraina presidendi Viktor Yanukovichi kabinet keeldus Ukraina - Euroopa Liidu Assotsiatsiooni leppest, vallandusid Kiievis valitsusvastased protestid, millega kaasnesid ka surmajuhtumid. Krimmi ilmusid 27. veebruaril 2014 venemeelsed relvastatud 'rohelised mehikesed', annekteerides Krimmi. Sama aasta aprillis vallandus relvastatud konflikt Ida-Ukrainas, mis kestab tänase päevani (Geers 2015:10). Kuna tegu on kestva kriisiga ning arvestades ka käesoleva töö mahulimiiti, piirdus autor rakendatud küberrünnakute uurimisega perioodil 2013 november kuni 2015. aasta detsember. Samuti tuleb meeles pidada, et esitatud nimistu küberrünnakutest pole ammendav, kuna konflikt on olnud pikaajaline, analüüse küberrünnakutest pole laialdaselt Ukraina kriisi kontekstis tehtud ning tõenäoliselt pole ka kõigist rünnakutest raporteeritud. Seega analüüsib autor siinkohal enim kõneainet pakkunud rünnakutest.

Tabel 3. Ukraina-vastased küberrünnakud aastatel 2013-2015.

Küberrünnakute kestvus	November 2013 - detsember 2015 (nt Lee et al 2016:iv, vi; Pakharenko 2015:61; Weedon 2015:76).
Rünnaku vastavus poliitiliselt olulisele perioodile konfliktis	02.12.2013 – protestid Maidanil jätkusid, samaaegselt algasid küberrünnakud Ukraina opositsiooni veebilehekülgede vastu (Pakharenko 2015:61). Märts 2014 – Vene väed sisenesid Krimmi, teiste seas Ukraina valitsuse veebilehekülg võeti 72h-ks rünnaku tõttu maha (Weedon 2015:76). Rünnati USA luuredroone, mis üle Krimmi lendasid,

	NATO veebilehekülgi, sealhulgas NATO Küberkaitsekeskuse veebilehekülge (Erol ja Oguz 2015:272-273; Schwartz 2014). 21-25 mai 2014 Ukraina presidendivalimised, samaaegselt rünnati Ukraina Keskvalimiskomisjoni viiruse ja näotustamisega (Geers 2015:11; Koval 2015:56). 23. detsember 2015 – Rünnak Ukraina elektrijaama SCADA süsteemile, millele eelnes Ukraina-meelsete aktivistide füüsiline rünne alajaamale, mis tagas elektrit Krimmi poolsaarele (Lee et al 2016:iv, vi; Zetter 2016)
Teostaja	Venemeelsed häktivistid, häkkerite grupid (CyberBerkut, Cyber-riot Novorossija, Advanced Persistent Threat Group 29, Russian CyberCommand) (Foxall 2016:7; Koval 2015:56; Maurer 2015:85; Pakharenko 2015:63; Weedon 2015:70, 77).
Sihtmärk	Ukraina meediaväljaannete, poliitikute, presidendi, Ukraina opositsiooni, valitsuse, Ukraina Informatsiooniagentuuri, Ukraina rahvusliku julgeoleku- ja kaitsenõukogu, Ukraina keskvalimiskomisjoni veebilehed; NATO, NATO Peaassamblee, NATO Küberkaitsekoostöö keskuse veebileheküljed, USA droonisüsteemid, Ukraina elektrijaama SCADA süsteem ja teised kriitilist taristut taganud ettevõtted (ICS-CERT 2016; Erol ja Oguz 2015:272-273; Foxall 2016:4; Weedon 2015:76).
Ründemeetod	DDoS, näotustamine, informatsiooni varastamine ja selle lekitamine *(*ingl k *doxing)*, pahavara levitamine (ICS-CERT 2016; Geers 2015:11; Koval 2015:56; Pakharenko 2015:61, 63-64; Weedon 2015:76).

Kui 2012. aastal toimusid tavapärased DDoS-rünnakud, siis 2013. aastal muutusid kasutatavad pahavarad ohtlikemaks (Koval 2015:55). Rünnakud on toimunud järjepidevalt kogu konflikti vältel ning olnud seoses konflikti kontekstis oluliste sündmustega. Näiteks 2013. aasta novembris ründasid Vene häkkerid näotustamise ja DDoS-rünnetega mitmeid Ukraina meediaväljannete ja poliitikute veebilehekülgi

(Weedon 2015:76). Kui protestid Maidanil polnud vaibumas, sooritati DDoS-rünnakuid vastavalt 2. detsembril 2013 Ukraina opositsiooni veebilehekülgedele (Pakharenko 2015:61). Kui Vene väed sisenesid Krimmi, tehti rünnak mitmele veebileheküljele. Üheks neist oli Ukraina valitsuse veebilehekülg, mis rünnaku tagajärjel oli ligipääsmatu 72h (Weedon 2015:76). Samaaegselt rünnati ka üle Krimmi lendavaid USA luuredroone (Erol ja Oğuz 2015:272-273). Krimmi annekteerimisega samal nädalal oli rünnaku all Ukraina parlamendiliikmete mobiiltelefonid (Tucker 2014). Ukraina presidendivalimiste ajal korraldati küberrünnak Ukraina keskvalimiskomisjonile (Geers 2015:11).

Kim Zetter on kirjeldanud, et 2015. aasta detsembris korraldati füüsilist kahju tekitanud küberrünnak Ukraina regionaalse elektrisüsteemi vastu, mille tagajärjel jäi 225 000 inimest elektrita. Täpsemalt rünnati SCADA (ingl k *Supervisory control and data acquisition*) ehk elektrijaama juhtimissüsteemi. Vahetult enne olid Ukraina-meelsed teinud füüsilise rünnaku ühele Ukraina alajaamadest, mis varustas Krimmi elektriga ning jättis ligi 2 miljonit Krimmi elanikku elektrita. SCADA-süsteemi rünnakut oldi varasemalt ette planeeritud, mida taheti ilmselt muul ajal teostada. Kuid Ukraina-meelsete rünne kiirustas SCADA-süsteemi rünnet tegema vastureaktsiooni või -meetmena (Zetter 2016). Enne SCADA-süsteemi sisse häkkimist ning selle terviklikkuse ründamist, teostati teisigi rünnakuid. DDoS-rünnak sooritati NATO veebilehekülgede vastu märtsis 2014 (Schwartz 2014) ning rünnati näiteks Hollandi Ohutuse Nõukogugi 13. oktoobril 2015, mis oli avalikustamas detailset raportit MH17 lennuõnnetuse kohta (Foxall 2016:6).

Rünnakute sooritajate kontekstis on intensiivsus Ukraina juhtumi puhul kõrge, lähtudes erinevate venemeelsete häkkerite gruppide nagu CyberBerkut, Cyber.riot Novorossija, Advanced Persistent Threat Group 29 (APT 29) seotusega küberrünnakute teostamises (Pakharenko 2015:63; Weedon 2015:70). Arvestada tuleb ka potentsiaalse võimalusega, et need võisid olla toetatud Vene valitsuse poolt. APT 29 on tugeva võimekusega küberspionaažigrupp, mille puhul võib kahtlustada Vene valitsuse sponsorlust, kuna finantstoetuseta ei suudetaks gruppi edukalt töös hoida (Weedon 2015:70). Lisaks olid rünnakute taga ka mitmed häktivistide grupid nagu Russian CyberCommand (Maurer 2015:85). Seega rünnakute sooritajate intensiivsuse kõrge tase tuleneb lisaks iseseisvatele mitteriiklikele tegutsejatele ka riigiväliste häkkerite gruppide osalusele, keda võis suure tõenäosusega Vene valitsus toetada.

Enamasti rakendati madala intensiivsusega rünnakuid, kuid SCADA-süsteemi vastane rünne, mis tõi kaasa ka füüsilise kahju, saab liigitada kineetilise küberrünnaku alla, mis võib olla võrdväärne relvastatud rünnakuga. Seega küberrünnakute intensiivsus on selle tõttu kõrge. Lähtudes rünnakutüüpidest, on tegu samuti kõrge raskusastmega, sest toimus informatsiooni terviklikkuse vastaseid ründeid.

Toimepandud küberrünnakute ulatus on suur, sest sihtmärkide variatiivsus on laialdane: lisaks riigisisestele sihtmärkidele on rünnatud ka riigiväliseid asutusi ja objekte. Samuti on konflikti vältel esinenud küberrünnakuid, mida on rakendatud konventsionaalsete jõudude toetamiseks, mis selgeimalt väljendus Krimmi annekteerimise puhul. Sündmust takistava juhtumina võib siinkohal näiteks tuua opositsiooniparteide lehekülgede vastase rünnaku 2013. aasta detsembris, kui neid pooldavad protestijad polnud Maidanilt lahkumas.

2.1.4 ANALÜÜS

Erisusi küberrünnakute rakendamise puhul kolme juhtumit võrreldes on märgata, mida illustreerib ka järgmine tabel kõigi juhtumite ning vastavate mõõdikute tulemustega.

Tabel 4. Juhtumite mõõtmistulemused.

	Eesti	**Gruusia**	**Ukraina**
Ulatus	Väike	Suur	Suur
Rünnakute intensiivsus	Madal	Madal	Kõrge
Rünnakute teostajate intensiivsus	Madal	Kõrge	Kõrge
Raskusaste	Kõrge	Kõrge	Kõrge

Eesti puhul oli küberrünnakute ulatus väike, kuna sihtmärkideks osutusid riigisisesed asutused, enamasti rünnati riigiinstitutsioonide veebilehekülgi ning rünnakud kategoriseerusid Gunneriussoni ja Ottise määratluse alusel iseseisvate küberrünnakute alla, arvestades näiteks rünnakuid DNS-serverite vastu. Lisaks kasutati küberruumi ära

ka valeinformatsiooni levikuks ja teenuste kättesaamise takistamiseks teenustõkestusrünnete ning näotustamise alusel.

Gruusia ja Ukraina puhul jaotusid sihtmärgid samade kategooriate alla, kuid sihtmärkideks olid ka riigivälised asutused ning lisandusid rünnakud konventsionaalsete jõudude toetamiseks, mis Ukraina puhul ilmnesid Krimmi annekteerimise ajal Ukraina valitsuse veebilehekülje ründamisega, muutudes seeläbi ligipääsmatuteks. Gruusia puhul kaasnesid Vene õhurünnakutega samal päeval küberrünnakud Gruusia domeeniga veebilehekülgede vastu. Seeläbi oli küberrünnakute ulatus Gruusia ning Ukraina puhul eeldatult suur.

Küberrünnakute intensiivsus oli Eesti ja Gruusia juhtumite puhul selgelt madalad, kuna rünnakud ei olnud võrdväärsed relvastatud rünnakutega. Ukraina puhul oli enamasti samuti tegu madala intensiivsusega rünnakutega, kuid SCADA-süsteemi vastane rünnak ei ole seda. Kuna nimetatud rünnak tõi kaasa füüsilise kahju ehk ligi 230 tuhat inimest pidi tagajärjena kannatama elektrikatkestuse all, võib rünnakut pidada relvastatud rünnakuga võrdväärseks. Põhjusel, et taoline rünnak esines, eristub Ukraina juhtum Eesti ning Gruusia omast, mistõttu saab intensiivsuse taseme rünnakute kontekstis kõrgeks määrata.

Seeläbi ei kehti püstitatud hüpoteesis ka faktor, et sõjaga kaasnevad intensiivsemad küberrünnakud, sest Gruusia puhul oli küberrünnakute intensiivsus madal, mida käesoleva töö autor eeldas vaid Eesti juhtumi kohta. Kuna Gruusia sõja ja Ukrainas toime pandud SCADA-süsteemi vastase küberrünnaku vahel on seitse aastat, võib oletada, et küberründevõimekus on arenenud selle perioodi jooksul, kuna küberruumis toimuv pole staatiline. Samas võis Gruusia puhul olla küberkaitsevõimekus tugevam, võrreldes Ukrainaga, kuid puuduvad andmed, et Gruusia suunas oleks üldsegi proovitud rünnakut SCADA-süsteemi vastu läbi viia.

Intensiivsus küberrünnakute toimepanijate kontekstis on siingi Eesti puhul madal põhjusel, et tegutsejateks olid iseseisvad riigivälised häktivistid. Ehk erinevalt Gruusia ja Ukraina juhtumitest, pole omistatud rünnakuid konkreetsele häkkerite grupile. Kuigi küberrünnakute puhul esines koordineeritust, mis võib viidata Vene valitsuse toetamisele. Gruusia puhul koondati küll sarnaselt Eestile iseseisvaid häktiviste venekeelsetes

Interneti keskkondades, kuid rünnakuid on omistatud ka konkreetsele häkkerite grupile, milleks oli Vene valitsusega sidemeid omav Russian Business Network. Seepärast on Gruusia puhul tegu kõrge intensiivsusega küberrünnakute teostajate kontekstis. Seda on Ukrainagi puhul, mida ilmestab suur hulk erinevaid häkkerite gruppe, kelle puhul on samuti leitud seoseid Vene valitsusega.

Raskusaste teostatud küberrünnakute baasilt on nii Eesti, Gruusia kui ka Ukraina puhul kõrge, sest kõigil juhtudel rakendati rünnakuid ka informatsiooni terviklikkuse vastu, mis on käesoleva töö kontekstis teooriast tulenevalt peetud tõsiseimaks rünnakutüübiks. Kuigi Ukraina puhul rünne erinevalt Eesti ja Gruusia vastu suunatud informatsiooni terviklikkuse vastastest rünnetest tõi kaasa ka füüsilise kahju, ei määra see rünnakute raskusastet, kuna raskusaste ei sõltu siinkohal rünnaku tagajärjest.

Erinevused Eesti kui rahumeelse konflikti ning sõja ajal Gruusia ning Ukraina vastu suunatud küberrünnakute vahel seisnevad rünnakute ulatuses ning küberrünnakute teostajate intensiivsuse kontekstis, mis sõja olukorras olid suuremad ning kõrgemad. Samas Gruusia ja Ukraina puhul erineb rünnakute intensiivsuse tase, mis Ukraina puhul on kõrgem. Lisaks on küberrünnakute raskusaste kõigi kolme juhtumi puhul sama. Seega sõja olukorras on rakendatud küberrünnakud ainult intensiivsemad rünnakute teostajate kontekstis ning teostatud küberrünnakute ulatus on suurem. Küberrünnakute intensiivsus erineb aga ka sõja olukordades ning raskustaseme osas erisusi pole sõja ega rahumeelse konflikti ajal.

Seeläbi ei kehti püstitatud hüpotees, et sõja olukorraga kaasnevad intensiivsemad, ulatuslikumad ja kõrgema raskusastmega küberrünnakud. Hübriidsõjapidamise meetodina rakendatud küberrünnakud on sõja olukorras intensiivsemad nende teostajate ning ulatuse poolest.

KOKKUVÕTE

Hoolimata hübriidsõja eksistentsiaalsuse üle käiva diskussiooni üle, on tegu siiski reaalse sõjapidamisviisiga. Seda on omistatud Venemaale ja terminit on seeläbi küll kasutatud ennekõike Krimmis toimunu kohta, pole siiski hübriidsõjapidamise meetodite rakendamine omane ainuüksi Ukrainas toimuvale, vaid on kasutatud ka varasemalt ning ka rahumeelse konflikti vältel.

Tulenevalt aga erinevatest arusaamadest ning seeläbi konsensuse puudumisest, milles seisneb hübriidoht ja hübriisõja kontseptsioon, uuris autor ühe hübriidsõjapidamise meetodi rakendamist, milleks on küberrünnak. Testitavaks hüpoteesiks seadis autor, et sõja olukorraga kaasnevad ulatuslikumad, intensiivsemad ja kõrgema raskusastmega küberrünnakud. Selleks uuris autor kolme juhtumit, kus küberrünnakuid hübriidsõjapidamise meetodina rakendati: Eesti vastu 2007. aastal, Gruusia vastu 2008. aastal ning Ukraina vastu perioodil 2013. aasta november – 2015. aasta detsember.

Jõudmaks vastuseni, kas püstitatud hüpotees kehtib, uuris autor väljatoodud juhtumite puhul rakendatud küberrünnakuid lähtuvalt, millal need aset leidsid, kes olid rünnakute teostajad, mis olid valitud sihtmärkideks ning millist ründetüüpi ja meetodit küberrünnakuks rakendati. Kenneth Geersi rünnakutüüpide jaotuse alusel mõõtis autor küberrünnakute raskusastet, ulatust tulenevalt Håkan Gunneriussoni ja Rain Ottise väljatoodud küberrünnakute rakendamise erisustest sihtmärkidest ja toimumisajast. Intensiivsust mõõtis autor vastavalt rünnakute teostajate varieeruvuse ning kas rünnakud oleksid võinud kategoriseeruda relvastatud rünnaku alla või mitte, tulenevalt Pascal Brangetto ja Matthijs Veenendaali teooriast.

Mõõtmistulemustest selgus, et sõjaolukorraga kaasnesid küll ulatuslikumad ning ründajate kontekstis intensiivsemad küberrünnakud, kuid raskusastmelt ja rünnakute intensiivsuse osas üldistust sõjaolukorras rakendatud küberrünnakutele teha ei saa. Nimelt oli raskusaste kõikidel juhtudel kõrge rünnete tõttu informatsiooni terviklikkuse vastu, mis on antud töö kontekstis raskusastmelt kõrgeim. Intensiivsus rünnakute kontekstis oli kõrge vaid Ukraina juhtumi puhul ning põhjusel, et toimus füüsilist kahju tekitanud elektrijaamavastane rünnak. Seega tulemustest järeldub, et püstitatud hüpotees

ei kehti. Selgub aga, et sõja olukorraga kaasnevad ulatuslikumad küberrünnakud ning intensiivsemad rünnakute teostajate kontekstis.

Käesoleva töö uurimistulemused toovad selgust ning tagavad esmase arusaama küberrünnakute rakendamisest hübriidsõjapidamise meetodina. Need tulemused annavad mõista, milles väljendub hübriidoht küberrünnaku näol ning kuidas võidakse küberrünnakuid rakendada nii rahumeelse konflikti vältel kui ka sõja olukorras. Seda on vajalik mõista, et olla paremini valmis vastava ohuga võitlemisel, kui see peaks realiseeruma. Ehk saadud töö tulemused võiksid aidata kaasa sobiva poliitika tegemise ning strateegiate loomisele hübriidohtude vastu võitlemises küberrünnakute kontekstis.

Saadud uurimistulemused on kasulikud edasise uurimise jaoks, mis on tingimata vajalik. Et veelgi enam mõista julgeolekuriski küberrünnakute näol hübriidsõjapidamise meetodina ning osata nende vastu õigeid vastumeetmeid rakendada, on täpsem küberrünnakute kaardistamine hübriidohtudena vajalik. Selles kontekstis saab ja tuleb uurida, mis põhjustas erisusi küberrünnakute rakendamisel kolme juhtumi puhul ja millest sõltus Ukraina puhul küberrünnakute intensiivsus või vastupidi, miks Gruusia puhul polnud küberrünnakud kõrge intensiivsusega.

KASUTATUD KIRJANDUS

1. Applegate, Scott D. & Angelos Stavrou. 2013. „Towards a Cyber Conflict Taxonomy.“ In *2013 5th International Conference on Cyber Conflict*, eds Karlis Podins, Jan Stinissen, Markus Maybaum. Tallinn: NATO CCD COE Publications, 431-448.
2. Bachmann, Sascha-Dominik & Håkan Gunneriusson. 2015. „Hybrid Wars: The 21st – Century's New Threats to Global Peace and Security." *Scientia Militaria, South African Journal of Military Studies* 43(1): 77 – 98.
3. Băhnăreanu, Cristian. 2015. „The Evolution of Warfare from Classic to Hybrid Actions.“ *Strategic impact* 2:57-66.
4. Brangetto, Pascal & Matthijas Veenendaal. 2016. „Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations.“ In *2016 8th International Conference on Cyber Conflict, Cyber Power,* eds Nikolaos Pissanidis, Henry Rõigas, Matthijs Veenendaal. Tallinn: NATO CCD COE Publications, 113-126.
5. CCDCOE. Cyber Definitions. https://ccdcoe.org/cyber-definitions.html (Külastatud 02.05.2017).
6. Cilluffo, Frank J. & Joseph R. Clark. 2012. "Thinking About Strategic Hybrid Threats—In Theory and in Practice." *PRISM* 4(1): 47-63.
7. Clausewitz, Carl von, Michael Howard, Peter Paret. 1993. *On War*. New York, Toronto & London: Alfred A. Knopf.
8. Cruceru, Valerică. 2014. "On Contemporary Warfare: Short Review of Specific Concepts." *Military Art and Science* 75(3):231-237.
9. Dunn Cavelty, Myriam. 2016. „Cyber Security.“ In *Contemporary Security Studies, 4th Edition*, ed Alan Collins. Oxford, New York: Oxford University Press, 400-416.
10. Erol, Mehmet Seyfettin & Şafak Oğuz. 2015. "Hybrid Warfare Studies and Russia's Example in Crimea." *Akademik Bakış* 17(9):261-277.
11. Euroopa Komisjon. 2016. „Ühisteatis Euroopa Parlamendile ja Nõukogule. Hübriidohtudega võitlemise ühine raamistik. Euroopa Liidu lahendus.“ 6. aprill. http://eur-lex.europa.eu/legal-

content/ET/TXT/HTML/?uri=CELEX:52016JC0018&from=ET (Külastatud 29.11.2016).

12. Foxall, Andrew. 2016. „Putin's Cyberwar: Russia's Statecraft in the Fifth Domani." *Russia Studies Center*, The Henry Jackson Society, 9.
13. Geers, Kenneth, ed. 2015. *Cyber War in Perspective:Russian Aggression Against Ukraine*." Tallinn: NATO CCD COE Publications.
14. Geers, Kenneth. 2011. *Strategic Cyber Security*. Tallinn: NATO CCD COE Publications.
15. Gunneriusson, Håkan & Rain Ottis. 2013. „Cyberspace from the Hybrid Threat Perspective." in *Proceedings of the 12th European Conference on Information Warfare and Security*, eds Rauno Kuusisto, Erkki Kurkinen. Academic Conferences and Publishing International, 98-105. https://cryptome.org/2014/12/ECIW2013.pdf (Külastatud 03.05.2017)
16. Hoffman, Frank G. 2007. „Conflict in the 21st century: The rise of Hybrid Wars." Arlington: Potomac Institute for Policy Studies.
17. Hoffman, Frank. 2009 „Hybrid vs Compound war." *Armed Forces Journal*, 1. oktoober. http://armedforcesjournal.com/hybrid-vs-compound-war/ (Külastatud 04.04.2017).
18. Hoffman, Frank. 2014. „On not-so-new Warfare: Political Warfare vs Hybrid Threats." 28. juuli. http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/ (Külastatud 29.11.2016).
19. ICS-CERT. 2016. „Cyber-Attack Against Ukrainian Critical Infrastructure." https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (Külastatud 26.04.2017).
20. Ioniță, Craișor-Constantin. 2014. "Is Hybrid Warfare something New?" *Strategic Impact* 4:61-71.
21. Kahn, Leonard. 2013. „Understanding Just Cause in Cyberwarfare." In *Routledge Handbook of Ethics an War, Just War Theory in the Twenty-First Century*, eds. Fritz Allhoff, Nocholas G Evans, Adam Henschke. New York ja London: Routledge Taylor ja Francis Group, 382-393.
22. Kofman, Michael & Matthew Rojansky. 2015. „A Closer look at Russia's 'Hybrid War'."*Kennan Cable* 7.

23. Koval, Nikolay. 2015. „Revolution Hacking.“ In *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed Kenneth Geers. Tallinn: NATO CCD COE Publications, 55-58.
24. Lee, Robert M., Michael J. Assante, Tim Conway. 2016. „Analysis of the Cyber Attack on the Ukrainian Power Grid.“ Electric Information Sharing and Analysis Center. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf (Külastatud 26.04.2017).
25. Lewis, James Andrew. 2014. „Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage.“ Center for Strategic & International Studies.
26. Libicki, Martin C. 2009. „Cyberdeterrence and Cyberwar.“ RAND Corporation. http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (Külastatud 10.04.2017).
27. Maigre, Merle. 2015. „Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO.“ The German Marshall Fund of the United States.
28. Mansoor, Peter R. 2012. „Introduction: Hybrid Warfare in History.“ In *Hybrid Warfare: Fighting Complex opponents from the Ancient World to the Present*, eds William Murray ja Peter R. Mansoor. Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, Sao Paulo, Delhi, Mexico City: Cambridge University Press, 1-17.
29. Mattis, James N. & Frank Hoffman. 2005 .”Future Warfare: The Rise of Hybrid Wars.” *Proceedins Magazine* 132(11).
30. Maurer, Tim. 2015. „Cyber Proxies and the Crisis in Ukraine.“ In *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed Kenneth Geers. Tallinn: NATO CCD COE Publications, 79-86.
31. NATO. 2014. „AAP-06, 2014 Edition.“ NATO Glossary of Terms and Definitions. http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6EN.pdf (Külastatud 13.05.2017).
32. NATO. 2016. Warsaw Summit Communiqué, 9. juuli. http://www.nato.int/cps/en/natohq/official_texts_133169.htm (Külastatud 11.05.2017).

33. NATO. 2017. „NATO Welcomes Opening of European Centre for Countering Hybrid Threats.“ 11. aprill. http://www.nato.int/cps/en/natohq/news_143143.htm (Külastatud 08.05.2017).
34. Pakharenko, Glib. 2015. „Cyber Operations at Maidan:A First-Hand Account.“ In *Cyber War in Perspective: Russian Aggression Against Ukraine*, ed Kenneth Geers. Tallinn: NATO CCD COE Publications, 59-66.
35. Project Grey Goose:Phase I Report. 2008. „Russia/Georgia Cyber War – Findings and Analysis.“ https://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report (Külastatud 26.04.2017).
36. Puyvelde, Damien von. 2015. „Hybrid War – does it even exist?“ *NATO Review.* http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm (Külastatud 29.11.2016).
37. Renz, Bettina. 2016. „Russia and 'hybrid warfare'.“ *Contemporary Politics 22(3):283-300.*
38. Richards, Julian. 2014. *Cyber War: The Anatomy of the Global Security Threat.* Basingstoke: Palgrave Macmillan.
39. Rid, Thomas. 2012. „Cyber War will not take place.“ *The Journal of Political Studies* 35(1):5-32.
40. Schmitt, Michael N. 2012. „ “Attack” as a Term of Art in International Law: The Cyber Operations Context.“ In *2012 4th International Conference on Cyber Conflict*, eds Christian Czosseck, Rain Ottis, Katharina Ziolkowski. Tallinn:NATO CCD COE Publications, 283-293.
41. Schroefl, Josef & Stuart J. Kaufman. 2014. “Hybrid Actors, Tactical Variety: Rethinking Asymmetric and Hybrid War.” *Studies in Conflict & Terrorism* 37:862-880.
42. Schwartz, Mathew J. 2014. „DDoS Attacks Hit NATO, Ukrainian Media Outlets.“*Dark Reading*, 17. märts. http://www.darkreading.com/attacks-and-breaches/ddos-attacks-hit-nato-ukrainian-media-outlets/d/d-id/1127742 (Külastatud 27.04.2017).
43. Shakarian, Pauolo. 2011. „The 2008 Russian Cyber Campaign Against Georgia.“ *Military Review* 63-68.
44. Stiennon. Richard. 2010. *Surviving Cyber War.* Lanham: Government Institutes.

45. Swedish Emergency Management Agency. 2008. „Sweden's emergency preparedness for Internet attacks." *SEMA´s Educational Series* 2. https://www.msb.se/RibData/Filer/pdf/26164.pdf (Külastatud 26.04.2017).
46. Zetter, Kim. 2014. „An Unprecedented Look at Stuxnet, the World's First Digital Weapon." *Wired*, 11. märts. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (Kasutatud 21.12.2016).
47. Zetter, Kim. 2016. „Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." *Wired,* 3. märts. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (Külastatud 02.05.2017).
48. Tiirmaa-Klaar, Heli. 2008. „The emerging cyber security agenda: Threats, Challenges and Responses." In *The Estonian Foreign Policy Yearbook 2008,* ed Andres Kasekamp. Tallinn: Estonian Foreign Poilicy Institute, 153-174.
49. Tikk, Eneken, Kadri Kaska, Liis Vihul. 2010. *International Cyber Incidents: Legal Considerations.* Tallinn: Cooperative Cyber Defence Centre of Excellence.
50. Tucker, Patrick. 2014. „Why Ukraine Has Already Lost The Cyberwar, Too." *Defense One*, 28. aprill http://www.defenseone.com/technology/2014/04/why-ukraine-has-already-lost-cyberwar-too/83350/ (Külastatud 29.04.2017).
51. United States Department of Defense. 2005. „The National Defense Strategy of the United States of America, Washington, D.C." http://archive.defense.gov/news/Mar2005/d20050318nds1.pdf (Külastatud 08.04.2017).
52. Weedon, Jen. 2015. „Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine." In *Cyber War in Perspective: Russian Aggression Against Ukraine,* ed Kenneth Geers. Tallinn: NATO CCD COE Publications, 67-78.

SUMMARY

„The Use of Cyber Attacks in the Context of Hybrid Warfare based on the Cases of Estonia, Georgia, and Ukraine“

Discussions about hybrid warfare that is supposed to characterize the modern conflicts intensified around the time when Crimea was annexed by the so called little green men in 2014. The discussions are not only about the concept of the hybrid warfare, but also about its existence. However, the hybrid threats are reality and the West has acknowledged it by establishing for example Centre of Excellence for Countering Hybrid Threats.

To agree on the countermeasures in fighting against the hybrid threats, it is necessary to understand their nature and how are the various methods related to hybrid warfare used. Therefore, current thesis is focusing on one specific means of conducting hybrid warfare which is cyber-attacks. Cyber-attacks are chosen to be the research object due to the growing dependence on the cyberspace in our societies, which makes us more vulnerable to cyber-attacks. Hence, cyber-attacks will remain to be great threat and will be used in various future hybrid conflicts, which illustrates the importance of doing a research on it.

The main research question of this thesis is how cyber-attacks as a hybrid threat are used as one of the means of hybrid warfare. To find the answer for the posed question the author has chosen three cases where the cyber-attacks as means of hybrid warfare were conducted. These were carried out against Estonia in 2007, Georgia in 2008 and Ukraine in 2013-2015. The cyber-attacks are probably still carried out in Ukraine, however, in this thesis the cyber-attacks conducted during the years of 2013-2015 are taken into consideration. The attacks used against these three countries will be measured separately in three categories: the intensity of the cyber-attacks, the extent and the degree of severity of the cyber-attacks.

The intensity will be measured in two subcategories. The intensity of the cyber-attacks will be measured in terms of whether the conducted cyber-attacks could be equal to armed attack or not. The intensity will also be measured in the context of the attackers: how large is the variety of the attackers. The extent of the attacks is measured based on the targets of the cyber-attacks and the degree of severity of the cyber-attacks depends on

which type of cyber-attacks were launched. Hereby, posed hypotheses for this thesis is that conducted cyber-attacks are more intensive, extensive and with higher degree of severity in war-time.

After conducting comparative analysis based on the results of the measurements, it was possible to conclude that the proposed hypothesis is false. The degree of the severity of cyber-attacks turned out to be high in each case, as the attacks against the information integrity were launched. Moreover, the intensity of the cyber-attacks was only high in terms of Ukraine, as a successful attack against SCADA-system was conducted, which brought along physical damage. The intensity of the attackers was high in the context of the attacks against Ukraine and Georgia. The extensive cyber-attacks were accountable to the attacks against Georgia and Ukraine. Therefore, it can be said that the cyber-attacks are only more extensive and intensive in terms of the attackers during the war time.

As this thesis has helped to understand the way cyber-attacks may be carried out as means of hybrid warfare during peace and war time, then its results may be helpful in creating appropriate policy on countermeasures against cyber-attacks as hybrid threats. However, before an exhaustive strategy for countermeasures can be created, further research is needed. The results of this thesis can be useful to do research on why the difference in the intensity of the cyber-attacks occurred between Georgian and Ukrainian cases.

Mina

_____

(autori nimi)

(isikukood:
_____)

annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose

_____

_____

_____,

(lõputöö pealkiri)

mille juhendaja on
_____,

(juhendaja nimi)

1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

2. üldsusele kättesaadavaks tegemiseks ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

3. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile;

4. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, _____ (kuupäev)

_____

(allkiri)