TALLINNA TEHNIKAÜLIKOOL
Majandusteaduskond
Õiguse instituut

Lauri Esko

# EESTI VÄLISPOLIITILISTE EESMÄRKIDE MÕTESTAMINE KÜBERJULGEOLEKU TEMAATIKA NÄITEL

Bakalaureusetöö
Õppekava RAHVUSVAHELISED SUHTED

Juhendaja: Holger Mölder, PhD

Tallinn 2019

Deklareerin, et olen koostanud töö iseseisvalt ja olen viidanud kõikidele töö koostamisel kasutatud teiste autorite töödele, olulistele seisukohtadele ja andmetele ning ei ole esitanud sama tööd varasemalt ainepunktide saamiseks.

Töö pikkuseks on 5940 sõna sissjuhatusest kuni kokkuvõtte lõpuni.

Lauri Esko ……

(allkiri, kuupäev)

Üliõpilase kood:

Üliõpilase e-posti aadress: realestenteprise@gmail.com

Juhendaja: Holger Mölder, PhD

Töö vastab kehtivatele nõuetele

……

(allkiri, kuupäev)

Kaitsmiskomisjoni esimees:

Lubatud kaitsmisele

……

(ametikoht, nimi, allkiri, kuupäev)

SISUKORD

# SISSEJUHATUS

Käesolev bakalaureusetöö keskendub Eesti välispoliitiliste eesmärkide mõtestamisele küberjulgeoleku temaatika näitel. Selleks toetutakse kahele teoreetilisele kontseptsioonile: välispoliitika eesmärgid Holsti järgi ning julgeolekustamise teooria (Buzan, Waever, de Wilde). Täpsemalt uuritakse Eesti rolli/eesmärki välispoliitikas küberjulgeoleku vallas. Töö empiirilises osas analüüsitakse Eesti julgeolekupoliitika seisukohti ja eripärasid. Töö teoreetiline raamistik toetub Kalev Holsti (1995) kirjeldatud riikide välispoliitiliste eesmärkide ja strateegiate kontseptsioonile. Töö eesmärgiks selgitada, kuidas avalduvad antud teema näitel Eesti välispoliitika eesmärgid ning nende saavutamise viisid. Rõhk on eelkõige küsimusel, kas Eesti üritab küberteema puhul saavutada individuaalset kaitsevõimekust. Julgeolekustamise teooria rakendamine aitab mõista, kuidas Eesti on pärast 2007. aastal toimunud küberrünnakuid oma rolli/eesmärki rahvusvaheliste suhete süsteemis rakendanud. Uurimismeetodiks on valitud diskursuseanalüüs, kuna küberjulgeoleku analüüsimisel on oluline eelkõige tekstides öeldu.

Töö võib jagada mõtteliselt kolmeks osaks, mis omakorda jagunevad peatükkideks: esimene osa keskendub Eesti julgeolekupoliitika eesmärkidele ja poliitikale üldiselt ning teine peatükk konkreetselt Eestis toimuvale küberjulgeoleku diskursusele ja selle analüüsile. Kolmandas osas keskendutakse Eesti osalemist erinevates organisatsioonides ja kuidas Eesti julgeolek oma eesmärke täitnud läbi küberjulgeoleku. Kõikides peatükkides on keskseks teemaks küberjulgeolek Eestis, mistõttu teisi valdkondi ja probleeme on käsitletud vähem. Töö teises pooles, kus käsitletakse Eesti julgeolekut küberjulgeoleku aspektist, siis ei pääse mööda 2007. aastal toimunud küberrünnakutest, mis ühtlasi tõstatas teema ka rahvusvahelisel tasandil. Toimunud sündmust on identifitseeritud kui „ajaloo esimest küberrünnakut", mis pani erinevad riigid ja organisatsioonid mõtlema infoühiskonna haavatavuste kohta (Volker 2009). Sealjuures on oluline märkida, et rünnakuid on suudetud tõlgendada nõnda, et need ei olnud suunatud Eestile lähtuvalt kehvast kaitsevõimest, vaid just tulenevalt Eesti heast reputatsioonist kübervaldkonnas (*ibid*).

Töö eesmärgiks on selgitada, kuidas avalduvad antud teema näitel Eesti välis- ja julgeoleku poliitika eesmärgid ning nende saavutamisele viisid. Rõhk on eelkõige küsimusel, kas Eesti küberteematikale rõhumine aitab saavutada eesrindlikus küberjulgeolekus ning kindlustada riigi julgeolekut läbi küberjulgeoleku. Selleks hinnatakse esiteks 2007. aastal toimunud küberrünnakute mõju kübervaldkonnale Eestis ja maailmas 12 aastat hiljem, seejärel luuakse ülevaate rahvusvahelise koostöö olemusest ning vaadeldakse, millist rolli on Eesti selle koostöö raames mänginud.

## Uurimusküsimused + eesmärgid

- Millised on Eesti peamised välis- ja julgeolekupoliitilisede eesmärgid ja nende saavutamise viisid kübervaldkonnas?
- Kas konkreetsele kübersuunale keskendumine on Eesti välispoliitikas mõistlik?
- Kas küberjulgeolekule rõhumine on Eesti jaoks peamine julgeoleku kindlustaja ja on vajalik Eestile silmapaistmiseks rahvusvaheliselt?

## Põhilised teesid on järgmised:

• Eesti eneseusalduslikkus ehk individuaalne võimekus küberkaitse vallas on küll üsna silmapaistev, kuid võrdluses teiste riikidega suuremate riikidega on kaitsevõime eelkõige ressursipuuduste tõttu küsitav.
• Rahvusvahelise koostöö puhul on Eesti kübervaldkonnas näidanud teerajaja rolli, osaledes aktiivselt erinevates rahvusvahelistes organisatsioonides.
• Küberjulgeoleku taseme rahuldava seisundi saavutamine on selgelt küberjulgeoleku näitel Eesti välispoliitika üks eesmärke.
• Eesti on läbi teinud seoses küberohtudega julgeolekustamise protsessi: Eesti esitles 2007. aastal toimunud küberrünnakuid avalikkusele kui julgeolekuliselt murrangulist sündmust, mis ühelt poolt tõstis esile Eesti suutlikkuse/olulise rolli küberkaitse vallas ning teisalt andis tõuke probleemiga rahvusvaheliselt tegutsemiseks.
• Väikeriigi oluline julgeoleku alustala on rahvusvaheline koostöö. Sellest tulenevalt saavad võimekamad liitlased väikeriikidele nende julgeoleku tarbija rolli ette heita.

# 1. EESTI JULGEOLEKU POLIITIKA EESMÄRGID JA PRIORITEEDID

Eesti julgeolekupoliitika alustes on välja toodud, et Eesti eesmärgid ja prioriteedid olid taasiseseisvumise järgselt väga selgesti määratletud – kõigepealt sooviti saavutada rahvusvaheline tunnustus omariiklusele ning seejärel võeti juba selge kurss Euroopa Liidu ja NATOga liitumisele. Nüüdseks on EL ja NATOga liitumisest möödas juba viisteist aastat, mis on piisav aeg julgeolekupoliitika kohaldamiseks uute oludega.
Eestis on kõrgemateks julgeoleku strateegiadokumentideks „Julgeolekupoliitika alused". 2010.a sai uue sisu ja ka vormi julgeolekupoliitika raamdokument – „Julgeolekupoliitika alused 2010". Sellest lähtuvalt on muutunud ka üldine diskursus Eesti julgeolekupoliitikast. Tegemist on tulevikku suunatud praktilise dokumendiga, mis kirjeldab ka hästi olevikku.

Julgeolekupoliitika alustes on välja toodud, et erinevalt paljudest teistest Euroopa riikidest, lähtub Eesti tänane julgeolekudiskursuse raamistik peamiselt riigi säilitamisest, mis on põhjendatav lühikese taasiseseisvumise aja kurbade kogemuste ning geopoliitilise asukohaga. Enamus Euroopa riike seostavad julgeolekut enamjaolt rahva heaolu, turvalisuse, inimõiguste, põhivabaduste, peamiste inimlike väärtuste ja rahuga (Mattheus, 2016). Julgeolek ei ole aga võrreldav moevooluga, millega peab kaasas käima ning kõik, mis mujalt tuleb ei pruugi sobida eestlasele.

Lisaks Eesti enda siseriiklikele tegevustele julgeolekut kindlustada, on Eestil võimalus ära kasutada ja endale sobivas suunas mõjutada mitmeid rahvusvahelisi initsiatiive, olles Euroopa Liidu, NATO, ÜRO ning teiste rahvusvaheliste organisatsioonide liige (Välisministeerium). Olulise tegevusena võib seega välja tuua vajaduste olemasolevates organisatsioonides enda positsiooni tugevdada ning oluliste rahvusvaheliste organisatsioonidega liituda ning arendada kahe- ja mitmepoolseid suhteid. Peamine eesmärk on seega võimalikult paljudes kohtades kaasa rääkida. Arvestades Eesti võimaluste piiratust kõikidel teemadel kaasa rääkida, on erilise tähtsusega õige teemade valik.

Eesti julgeolekupoliitika üldmulje võtab kokku kõige paremini just dokumendist endast võetud lause: "*Eesti püüab saavutada välispoliitikas julgeoleku kindlustamiseks vajalikku rahvusvahelist keskkonda...*" Juba kasutusel olevate loogikate ja mõistete kõrval peaks siseriiklikku ja ka rahvusvahelisse debatti lisama ka uusi teemasid. Uued loogikad ja lähenemisviisid aitavad üldpilti näha uues valguses. Üldiselt peaks nii siseriiklikus transatlantilises debatis kui ka rahvusvahelisel (NATO) tasandil rõhutama koostööd ja "kollektiivse julgeoleku" põhimõtet. Ehkki NATO tasandil on „kollektiivne julgeolek" juba vanem mõiste, peaks seda transformeerima ka suhetesse teiste riikide ja organisatsioonidega. Koostöö julgeoleku nimel ei pea reeglina tähendama koostööd ainult teatud organisatsiooni raames vaid ka välispoliitikas üldiselt.

NATO on Eesti jaoks oluliseks julgeolekugarantiiks (Välisministeerium, 2013), kuid toob endaga kaasa ka Venemaa vastureaktsiooni. Eesti on nii NATO kui ka maailma tähelepanu tervikuna Venemaa horisondil hoidnud (näiteks küberrünnakutega). Kahe ja mitmepoolsete suhete osas jääb oluliseks partneriks USA. Varasemat on olnud mõlema riigi Venemaasse suhtumises olulisi sarnasusi: Venemaa suhtes on põhimõte: loodame parimat, valmistume halvimaks. Kui nüüd uue USA presidendi Donald Trumpi suhtumine Euroopa Liitu ja Euroopa panusest NATO-sse on tekitanud kõvasti segadust nii Euroopas kui ka meil Eestis.

Eesti julgeoleku sõnavarast ei ole kuhugi endiselt kadunud ka "Vene oht", mis on mingil määral mõistetav. Suhted Venemaaga ei arene eriti mitte kuidagi. Kuna puudub välispoliitiline kontseptsioon, reaalne, mis mingi suuna kätte annaks, kuigi erinevad huvigrupid üritavad Venemaa teemat sisse suruda igasse võimalikku majandusvaldkondlikku poliitika dokumenti. Ehkki selle mõiste võiks juba ammu välistada, ei ole praktikas see siiski ilmselt kunagi välistatud. "Vene oht" ei kao eestlase mõtetest ilmselt niipea.

Kuigi sõjaline oht Venemaalt tundub Eestile ohuna pigem tulenevalt ajaloost, reaalset ohtu ei ole Idast juba päris pikka aega olnud, kuid tõsi, päris välistada seda ei saa. Ka 2019 aasta välisluureameti raport on välja toonud selle, et *„Eesti peamised välised julgeolekuohud tulenevad Venemaa käitumisest, mis õõnestab rahvusvahelist korda"*.

Ühiskonna väärtused ja -hinnangud on pidevas muutumises nii siseriiklikus kontekstis kui ka rahvusvahelisel tasandil. Inimesed on aru saanud, et niimoodi enam jätkata ei saa nagu siiani on elatud, saadakse aru, et materiaalsed väärtused ei ole enam peamised ning ka teistel asjadel siin maailmas on olemas väärtus. Maailm liigub juba, tõsi küll aeglaselt, nende suunas. Kuna kõik asjad on kuidagi üksteisega seotud, muutuvad sellest tulenevalt ka julgeolekupoliitilised väärtused. Kui varasemalt seisti oma riigi eest peamiselt sõjaliste vahenditega, on "kõva" julgeoleku kõrvale järjest rohkem tekkimas ka teisi valdkondi. Kui inimesed väärtustavad rohkem üksteist, riigid arvestavad rohkem teiste riikide ja organisatsioonidega, käitutakse "inimlikumalt" siis muutub ka julgeolekus koostöö ja teineteisega arvestamine olulisemaks. Väärtustel, et hoolida maailmast ja maailma julgeolekust üheskoos, on julgeolekupoliitikale oma mõju.

## 1.1 Välispoliitika eesmärgid Holsti järgi Eesti kontekstis

Eesti välispoliitiliste eesmärkide analüüsimiseks tuuakse järgnevas töö osas ülevaade võimalikest riikide välispoliitiliste eesmärkide määratlusest, mis põhineb Kalevi Holsti 1995. aasta toesele „International politics: a framework for analysis".

Esimeseks riikide välispoliitiliseks eesmärgiks on välja toodud julgeoleku saavutamine, mille Holsti seob hirmu kontseptsiooniga. Et nimetatud hirme vältida ning riiklikku julgeolekut tagada, valivad riigid erinevate strateegiate vahel. Esimeseks võimalikuks viisiks on isolatsioon (Holsti 1995:87-88), mis tänapäeval ning antud töö raames kindlasti enam rolli ei mängi. Teise strateegia võimalikkuse üle võib aga Eesti ja küberjulgeoleku valdkonna puhul juba arutada. Selleks on niinimetatud enese usalduslikkus, mis tähendab riigi eesmärki tagada ainult oma võimetele toetudes kaitse või heidutus võimalike vaenlaste eest (*ibid*, 1995:91). Holsti seostab selle pigem suurriikide võimalikkusega ning juba sellest lähtudes on Eesti kui väikeriigi täielik individuaalne võimekus kaheldav. Siiski on paslik küsida, kuivõrd on õigustatud võimalik kuvand Eesti küberjulgeoleku alasest suutlikkusest rahvusvahelises kontekstis. Järgnevaks võimalikuks julgeoleku tagamise strateegiaks on neutraliteedi kuulutamine (*ibid*, 1995:88-89) või n-ö mitteühinemisliikumine, mida võiks analüüsida Eesti puhul küll 1938. aasta kontekstis, kuid NATO liikmelisus välistab selle välispoliitilise

eesmärgi võimalikkuse. Seoses Eesti kuuluvusega erinevatesse rahvusvahelistesse organisatsioonidesse, on kolmas võimalik julgeolekupoliitiline strateegia liitlasstrateegia, mida saab tänapäeval ka kõige tavapärasemaks riikide välispoliitilisteks eesmärkideks pidada. Antud käitumisviisi puhul on niisiis tegu liitlaste leidmisega, kes peaksid tõstma läbi kollektiivse tegutsemise riigi julgeolekut. Eesti saab selgelt määratleda üldjoontes selle strateegia kindlaks järgijaks. Oli ju selgelt pärast iseseisvumist kindel välispoliitiline eesmärk liituda NATOga, mis ka 2004. aastal saavutati. Täpsemalt saab Eesti ja NATO puhul liitlasstrateegia puhul rääkida alaliigist, mida iseloomustab riikidevaheline relvajõudude, kaitsevõime ühendamine. Küberjulgeoleku temaatikat analüüsides kerkibki küsimus, kuivõrd on Eesti oma küberkaitsevõime näitel kasutanud nimetatud strateegiat ehk ühendanud „küberrelvajõude“ nii NATO kui ka teiste organisatsioonide kontekstis.

Teiseks laiemaks eesmärgiks on Holsti välja toonud autonoomia, mis seostub tihedalt suveräänsusega ehk riigi võimuga olla oma otsustes iseseisev (*ibid*, 1995:16). Kolmandaks oluliseks eesmärgiks on välja toodud materiaalne heaolu, millel võivad omakorda olla erinevad käitumisstrateegiad (autarkia, merkantilism, vabakaubandus) (*ibid*, 1995:225). Mõlema eesmärgi üle saab küll Eesti kontekstis arutleda, kuid küberjulgeoleku kontekstis jäävad pigem suveräänsuse ning majandusliku heaolu küsimused tagaplaanile.

Siiski ei jää antud töö raames tagaplaanile Holsti kirjeldatud neljas riikide välispoliitilise eesmärgi tüüp, milleks on soov saavutada rahvusvaheline seisund. Holsti kirjeldab staatuse küsimust kui midagi riikidele omast – poliitiliste käitujate soovi tekitada austust, vahel isegi kadedust enda suunas. Antud eesmärgi näideteks toob Holsti välja näiteks sõjalise võimsuse demonstreerimise, soov presenteerida end tehnoloogiakeskusena või isegi spordivõistlusi (*ibid* 1995:17). Eesti ja küberjulgeoleku puhul tekibki küsimus, kas Eestile langenud „rambivalgus“ pärast 2007. aasta rünnakuid ning Eesti poliitikute ning ametiisikute sõnavõtud põhinevad eelkõige soovil arendada Eesti rahvusvahelist seisundit või saab Eesti rolli objektiivselt, võrreldes teistega, pidada tõeliselt edukaks.

Rääkides mainest ja seisundist pole Holsti kirjeldanud põhjalikumalt põhjuseid, miks riigid seda otsivad. Eesti, kes on selgelt valinud üheks eesmärgiks oma väiksuse tõttu eelpool kirjeldatud liitlasstrateegia, motivatsiooni tõsta oma mainet küberjulgeoleku vallas on suhteliselt kerge põhjendada. Väikeriiki on kerge pidada rahvusvahelises organisatsioonis nagu NATO eelkõige julgeoleku tarbijana. Seetõttu võib väikeriikidel olla „kõrgendatud“ eesmärk tõestada end julgeoleku pakkujana. Ja see pakkuja roll on mõistagi seotud sellega, kuidas riik suudab end rahvusvahelisel areenil esitleda.

# 2. KÜBERJULGEOLEK

Keskmise Eesti elaniku jaoks on kübermaailm on nii tavaline ja kasutatav vahend, et väga ei mõeldagi, et selle kaudu võidakse teha rünnakuid või koguni alustada riikide vahel kübersõda. Ilmselt enne 2007. aastat olid vaid vähesed riigid teadvustanud küberjulgeoleku rolli olulisust, arvestades kui nõrk ta võib tegelikult olla. Küberrünnak Eestile kui maailmas tuntud e-riigile tõestas, kui haavatav igapäevaselt kasutatav võrgusüsteem internetiajastul tegelikult on. Eesti oli üks esimesi juhtumeid, kus küberrünnak nii laiahaardeline oli. See sündmus vapustas maailma ning tõi riigid reaalsusesse, et küberrünnak on võimalik relv sõjaks. Kuidas aga konkreetsemalt mõjutas Pronksiöö järgne Eestile tehtud küberrünnak 2007. aastal nii Eestit kui ka maailma, ongi autor peamiseks uurimisküsimuseks seadnud.

Eesti on läbi teinud seoses küberohtudega julgeolekustamise protsessi: Eesti esitles 2007. aastal toimunud küberrünnakuid avalikkusele kui julgeolekuliselt murrangulist sündmust, mis ühelt poolt tõstis esile Eesti olulise rolli küberkaitse vallas ning teisalt andis tõuke probleemiga rahvusvaheliselt tegutsemiseks (Hansen ja Nissenbaum 2009). Eesti eneseusalduslikkus ehk individuaalne võimekus küberkaitse vallas on küll näiliselt silmapaistev, kuid võrdluses teiste riikidega on kaitsevõime eelkõige ressursipuuduste tõttu küsitav. Rahvusvahelise koostöö puhul on Eesti kübervaldkonnas näidanud n-ö teerajaja rolli, osaledes aktiivselt erinevates rahvusvahelistes organisatsioonides.

## 2.1 Küberrünnak Eestile 27. aprill 2007

27. aprillil, vahetult pärast Pronksiöö sündmusi, algas Eestile suunatud küberrünnak, eesmärgiga häirida Eesti erinevate infotehnoloogiliste süsteemide käideldavust, mis kokku kestis 22 päeva. Rünnakuid tehti enamasti väljaspool Eestit asuvatest arvutivõrkudest. Ametlikud Eesti riigi suhtluskanalid internetis olid pideva ründe all 27. aprillist kuni 19. maini (Randel 2007).
Küberründed said alguse sellest, kui venekeelsetes foorumites ja veebiajakirjades esitati üleskutseid käivitada MS Windows käsurealt käsk ping foorumis toodud parameetritega

serveri koormamiseks. Hiljem lisandusid BAT failid, mis automatiseerisid ping-käsu kasutamise (Randel 2007). Tegu oli DDoS rünnakuga ehk inglise keeles nimetatuna *distributed denial-of-service* (Richards 2009). Sihtmärkidena levitati reeglina riigi veebilehtede aadresse, nagu www.riik.ee, www.valitsus.ee, www.peaminister.ee ning mõnede valitsuserakondade veebisaitide aadresse. (Randel 2007). Rünnaku tipphetkedel kaasati rohkem kui miljon arvutit ja tekitati mõnel lehel enam kui 5000 klikki sekundis (Kalvet 2007:25). Sellel samal tipphetkel ehk 8. mail kell 11 õhtul saadeti sekundis välja 4 miljonit paketti, mis sisaldasid kahte tüüpi andmeid - infot, et see jõuaks vastava aadressini, ning kasutaja lisatud andmeid (Davis 2007).

Pingimisele lisandusid vigased veebipäringud, mida esitati massiliselt eelkõige riigi ja meediaväljaannete veebilehtedele. Nende päringute kasutusele võtmine vihjas spetsiaalsete vahendite kasutamistele (Randel 2007). Lisaks kasutati nakatunud arvutitest virtuaalset arvutivõrku, mida nimetatakse botnet'iks, mis on vabalt kättesaadava pahavarana internetis (Richards 2007). Seda kasutati eelkõige pankade ründamiseks. Hansapanga vastu suunatud peamised ründed toimusid 10. ja 15. mail, viimasel kuupäeval lisandusid sihtmärkide hulka ka SEB Eesti Ühispank ja Krediidipank. Botneti kasutati ka suuremate meediaväljaannete ning portaalide ründamiseks (Randel 2007).

Kahju Eesti majandusele polnud suur, kuid Hansapanga kohta ei saa ilmselt sama öelda. Nimelt riigi suurim pank oli sunnitud sulgema internetipanga süsteemid. See oli mitmel viisil kahju tekitav, sest alustuseks tegid 97% ulatuses eestlastest oma pangaülekandeid Internetis. Lisaks ei saanud inimesed kasutada pangaautomaate ega oma deebetkaarte välismaal maksmiseks (Richards 2009). Seega majandust ei puudutanud ehk nii palju, aga ebamugavusi tavainimestele igapäevases elus küll.

Ründeid riigi vastu võis algselt tõlgendada poliitiliste protestidena, kuid süstemaatiline kommertsstruktuuride ründamine viitab riigi vastu suunatud organiseeritud tegevusele, mida võib nimetada nii küberterrorismiks kui ka küberrünnakuks. Rünnakute eesmärk oli tõkestada info edastamist. Nendega halvendati ka väikefirmade olusid, sest

äritegevus oli e-posti serverite, võrguseadmete ja veebiserverite ülekoormatuse tõttu häiritud (Randel 2007).

Küberrünnakut hakkas lahendama CERT Eesti, mis on rahvuslik turvaintsidentide lahendamise meeskond (*Computer Emergency Response Team – CERT)*. Peamine eesmärk on tiimil tagada Eesti riigi infosüsteemide ja kriitiliste infosüsteemide pidev toimimine. Nimetatud atakis oli CERT Eesti peamine ülesanne tagada riigi infokanalite kättesaadavus nii Eestis kui ka välismaal ning tõkestada riigi vastu suunatud rünnakut nii riigis kui ka väljaspool. Selleks koondati lisaks CERT Eesti IT spetsialistidele kokku ka Soome CERT meeskond, kelle abil tehti koostööd välismaiste teenusepakkujate (Randel 2007). Rünnakule vastupanu aitasid osutuda väljaspool Eestit samuti Saksamaa ja Sloveenia turbemeeskonnad (Harwell 2007).

Poliitiliste institutsioonide tasandil jäi kriisi lahendamise vastutus eelkõige valitsusele, mida pooldas täielikult selleaegne Riigikogu koosseis. Riigikogu enda ülesandeks jäi selgitada toimuvat olukorda väliskolleegidele (Ergma 2007). Eesti valitsus, üritades küll tõrjuda DDoS rünnakuid, pidi blokeerima rahvusvahelise infovoolu, mistõttu lõigati Eesti ülejäänud maailmast välja. Kuigi see oli radikaalne meetod, osutus see siiski õnnestunuks, sest tänu sellele vähenes rünnatavate veebilehtede koormus ja 19. mail lõppesid küberrünnakud (Richards 2009).

## 2.2 Küberrünnakuga kaasnenud probleemid

Oluliseks probleemiks saab kindlasti pidada seda, et Eesti polnud valmis taoliseks rünnakuks. Eesti võis olla selleks ajaks arendanud oma tehnoloogiat suurel määral, mida peegeldas 2005. aastal kasutusele võetud e-valimiste süsteem ja et ligikaudu 60% elanikest sõltus olulisel määral igapäevatoimingutes Internetist, aga küberjulgeolek oli nõrk (Richards 2009). Eesti e-rühm moodustati vaid aasta enne rünnakut ehk 2006. aastal (Ryan 2006). Raha suunati pigem telekommunikatsiooni ja teiste internetipõhiste teenuste uurimiseks ning arendamiseks, kuid turve nimetatud valdkonnas jäi tahaplaanile – kõik see tegi Eestist haavatava riigi (Richards 2009).

Teine küsitav koht peitub selles, kuidas oleks maailm pidanud reageerima ning tegutsema antud olukorras. Tõsi, appi tulid teiste riikide CERT meeskonnad, Rootsi Internetifirmad tõrjusid mitmeid rünnakuid enne, kui need Eestini jõudsid, NATO saatis välisvaatleja Eestisse ja aitas hiljem koos EL-ga rünnakut uurida, kuid kas oleks ehk pidanud kehtima NATO riikidele Artikkel 5? (Välisministeerium 2007:67, 60)

Jaak Aaviksool oli see võimalus, kuid ilmselt oli tal raske selle välja kuulutamisega vähese toetuse tõttu NATO liimetelt (Rehman 2013). Vähene toetus tulenes sellest, et puudus selge definitsioon, mis küberrünnak on, ning üldjuhul ei teata, kes selle on täpselt toime pannud, kas mõni riik või eraisikud. Puudusid rahvusvahelised õiguskonventsioonid, mis oleksid deklareerinud, kuidas selliste olukordade puhul käituda, kuna taoline rünnak juhtus vaid teist korda pärast USA arvutitele suunatud rünnakut Hiina poolt 2003-2006. aastal (Rehman 2013). Samuti pole ühelgi riigil otsest kontrolli Interneti üle, sest see on universaalne ressurss (Ryan 2007).

Eesti rünnaku puhul kasutati mitmeid termineid: kübersõda, küberterrorism ja küberrünnak. Tundub, et esimesed kaks ei sobi rünnaku iseloomustamiseks, kuna sõja puhul on vaja kahte poolt, kes sõdiksid. Sellisel juhul tõkestab üks pool teise rünnakuid, samas teeb ka vastutegevust – antud juhul Eesti piirdus vaid oma infosüsteemide kaitsmisega. Teiseks küberterrorism eeldab terroriakte, mis oleksid suunatud riigi kaitse nõrgestamisele, antud juhul oli tegu vaid veebsaitide ründamisega (Ühtegi 2007). Terminist hoolimata oli rünnak oluline alarm ning näitas, et küberrünnak on uus poliitiline vahend ning kujutab endast tõsist ohtu. Ülejäänud maailma polnud suutnud seda endale teadvustada ning seepärast võttis Eestilgi probleemi lahendamine kauem aega, kui oleks võinud (Ryan 2007). Küberrünnakute lahendamise puhul tekitab suurt peavalu ning konfliktsust rünnaku taga seisvate isikute kättesaamine. Näiteks on IP-aadressidega, mis on peamine moodus rünnaku korraldaja jälitamiseks, võimalik jälgi peita, suunates neid läbi teiste riikide (Richards 2009).

On võetud seisukoht, et 2007. aasta oli ilmselt organiseeritud tegevus, kuna tegutseti sõjaväelise täpsusega. Esiteks lõppesid rünnakud alati 00.00 südaööl (Ilves 2007). Teiseks pärinesid ründed *botnet*-võrgustiku vahendusel rohkem kui kümnelt tuhandelt

n-ö arvutizombilt välismaistelt IP-aadressidelt 50-st riigist nii Venemaalt, USAst, Jaapanist, Vietnamist, Hiinast ja ka Egiptusest. Eesti süüdistas küll Venemaad, kuna kokkusattumus Pronksiöö sündmustega andis selleks liigagi suure tõenäosuse, kuid NATO ja EL-i informaatikaeksperdid ei leidnud piisavalt tõendeid. Muidugi tõukas ka Venemaa kõik süüdistused tagasi. Samuti ei nõustunud ta Eestiga Venemaa prokuratuur Eestiga juhtumi uurimisel koostööd tegemast (Välisministeerium 2007:60).

Samas suudeti identifitseerida mõningad rünnakus osalejad kohe alguses Interneti aadressite järgi – paljud olid venelased ning pärit mõnest Venemaa riigiinstitutsioonidest (Traynor 2007). 2008. aastal leiti üks isik, kes osales rünnakus – Dmitri Galushkevich. Ta oli marurhvuslasest vene õpilane, kes osales oma laptopiga DDoS rünnakus Reformierakonna veebilehele, tehes selle kasutamise võimatuks kümneks päevaks. (Richards 2009)

## 2.3 Küberrünnaku tagajärjed

Küberrünnakud olid toona niivõrd uudne temaatika, et selle mõistmiseks, oli vaja reaalset juhtumit ning Eestile suunatud rünnak selle ka lõi. Uudsuse tõttu puudusid erinevad õiguskonventsioonid ning seadused, kuidas peaksid teised riigid (nt NATO liikmed) sellistes olukordades käituma ja reageerima (Rehman 2013).

Eestile suunatud küberrünnak oli oluline häirekell, näidates, kui nõrgad on küberkonflikti lahendamismeetodid rahvusvahelisel tasandil. Eelkõige puudulik küberrünnaku täpne definitsioon ning kiire reageerimine, sest NATO ei tõlgendanud siis veel küberrünnakut sõjalise aktsioonina (Välisministeerium 2007:68). Küberrünnakutesse peab suhtuma tõsisemalt ning võrdsustama sõjalise rünnakuna. E-riigi puhul sõltuvad enamik toimingutest internetist, seega 2007. aasta küberrünaku tagajärjeks oleks võinud olla suurem kaos. Niisiis kuulutatigi 2014. aasta Wales'i tippkohtumisel küberkaitse osaks NATO kollektiivkaitse põhiülesannetest (NATO 2014).

Positiivne on ka see, et 2008. aasta augustis avati Eestisse NATO küberkaitsekeskus *(NATO Cooperative Cuber Defense Center of Excellence – CCD COE)* Tallinnas, eesmärgiga arendada reageerimist küberterrorismile ning koostada standartne protokoll küberrünnakule reageerimiseks (Richards 2009). Lisaks hakkasid Euroopa Komisjonis arutelud kuritegevuse vastu võitlemise eriüksuse loomist, et tõkestada efektiivsete meetoditega küberkuritegevust (Välisministeerium 2007:71). Eestigi seadis endale rünnakust tulenevalt arengukava, et selline situatsioon paremate meetmetega edaspidi lahendada.

Esimene eesmärk arengukavas oli, et Eestis oleks laialt rakendatud astmeline turvameetmete süsteem, mis tagab riigi küberjulgeoleku. Selle nimel kehtestati valitsuse määrus „Infosüsteemide turvameetete süsteem“ 2007. aasta detsembris. 2012. aastal tegi määrus „Infoturbe juhtimise süsteem“ riigiasutustele kohustuseks määrata ametisse infoturbejuhid. Nende inimeste ülesanneteks on hinnata asutuse infoturbe tõhusust, osaleda asutuse arendus- või IT-nõukogu töös ja infosüsteemide arendusprojektides. Samuti nõustab infoturbe riskide hindamisel, uute turvameetmete loomisel või olemasolevate parandamisel ja juurutab asutuses turvaintsidentide haldamise korra. (Raud 2012).

„*Eesti on väga suure infoturbealase kompetentsuse ja teadlikkusega riik*“ – see oli riigi teine eesmärk, mis sai sõnastatud 2008-2013 Küberjulgeoleku strateegias. Seegi sai samuti täidetud, sest 2012. aasta jaanuaris toimus Eestis eriline küberõppus „Küberpalavik 2012“. See oli esimeseks õppuseks valitsusele ja kriisikomisjonile (Eesti infoühiskonna aastaraamat 2011/2012: 38) Lisaks peab riik oluliseks ka rahvusvahelise koostöö arendamist, sest ühtsete küberriskide põhimõtete, arusaamade väljatöötamine ja tõhus ohtude maandamine on tänapäeva internetiseerunud maailmas oluline. Selleks osaleti 2011. aastal EL-USA küberõppuse „Cyber Atlantic“ planeerimisel ja läbimängimisel, mille käigus tutvustati EL liikmesriikide ja USA ning ELi institutsioonide kübereksperte nii tehnilisel kui ka poliitika planeerijate tasemel. (Raud 2012). Seega Eesti on end olulisel määral tõestanud küberjulgeoleku tagamisel kui ka koostöö edendamisel rahvusvahelisel areenil pärast rünnakut.

Olukorrale poliitiliselt lähenedes, tekitas negatiivse tagajärje see, et Eesti ning sealjuures ülejäänute Lääneriikidega hakkas Venemaad süüdistama. Nii pingestas Eesti veelgi suhteid Venemaaga (Myers 2007). Nimelt Inforturbefirma Arbor Networks Inc. vaneminseneri Jose Nazario arvates polnud Eestile suunatud küberrünnakud juhitud ühe Venemaalt pärit üksuse poolt, sest nagu ka EL ja NATO järeldusele jõudsid, ei leitud piisavalt tõendeid selleks. Ühtki selget rünnakusuunda Moskvast Tallinnasse ei leitud. See eest on avastatud, et rünnakutes oli osalejateks venekeelseid arvutispetsialiste. Tegu võis olla Vene natsionalismi mitte Vene valitsusega, kes tegutses Pronksiöö pingetest tulenevalt (Kirk 2007) .

Rünnakuid uurides leiti seoseid isegi Venemaa presidendi administratsiooni domeenidega, kuid nagu ennegi mainitud, on rünnakuid võimalik suunata läbi teiste IP-aadresside, mistõttu võis rünnaku eest vastutav olla ükskõik kes (Myers 2007). Selliste süüdistuste tõttu kehtestas Venemaa ajutiselt sanktsioonid Eestile toorainekuabanduse vahendamisel ning ka piirangud reisimisele Tallinna ja Peterburi vahel. Õnneks need ei kestnud kaua ning drastilisemat käitumist Venemaa poolt ei tulnud, kuid kindlasti oleks Eesti pidanud olema tagasihoidlikum oma süüdistustega, eriti veel nii kriitilisel ajal, nagu oli seda Pronkssõduri teisaldamise perioodil (Anderson 2007).

## 2.4 Julgeolekustamise teooria ja kübertemaatika julgeolekustamine

Uue julgeoleku ohu loomist nimetas Kopenhaageni koolkond julgeolekustamiseks. Riikidevahelistes suhetes võib ühe riigi poolt alustatud julgeolekustamine kaasa tuua teise riigi reaktsiooni, kus julgeolekustatakse esimese riigi julgeolekustamist. Kui mingi teema on julgeolekustatud, siis liigub ta edasi riigi välispoliitikasse ning saab rahvusvaheliste suhete teemaks (Buzan, Weaver, de Wilde 1998:24). Julgeolek on endale osutav praktika, sest paraktikas küsimusest saab julgeoleku küsimus, mitte kindlalt sellepärast, et tõeline eksistensiaalne oht eksisteerib vaid sellepärast, et küsimus on esitatud kui ohuna. Julgeoleku protsess on keele teoorias kutsutud kui kõneakt. See ei ole märgiks millegile enamale, vaid lausung ise on kutsutud kui kõneaakt (*ibid*:24-26).

Julgeolek võib olla nii füüsiline kui ka ideoloogiline. Julgeoleku oht tekib, kui mõni küsimus kujutab eksistentsiaalset ohtu määratud referentobjektile (*Ibid*:21).

Kui vaadata nüüd kübertemaatika julgeolekustamise vaatevinklist ja eesti võtmes, siis rünnakuid on analüüsinud ka julgeolekustamise teooria raames Lene Hansen ja Helen Nissenbaum (2009). Julgeolekustamine on protsess, mille käigus julgeolekustaja, kelleks on üldjuhul ametnikud või poliitikud, kirjeldavad teatud nähtust julgeolekuohuna (Buzan et al 1998). Kui julgeolekustamise protsess õnnestub, siis ei tegeleta viidatud nähtusega enam kui tavalise poliitilise küsimusena, vaid selle lahendamiseks rakendatakse kiireloomulisi, tavapäraseid protsesse (nagu poliitiline diskussioon, legaalsed piirangud) vältivaid samme (*ibid*). Hansen ja Nissenbaum (2009) on leidnud, et Eesti-poolsed julgeolekustajad suutsid edukalt maailmale esitada toimunud küberrünnakute eripära.

Eesti poliitikud suutsid muuta välismaailmale usutavaks selle, et toimunud sündmusi saab kirjeldada, nagu juba eelpool mainitud, kui „esimest kübersõda" (*ibid*:1169). Julgeolekustamise tegi osaliselt edukaks ka see, et mitmed rahvusvaheliselt tunnustatud pressiväljaanded nagu Washington Post või New York Times kajastasid teemat sarnaselt „väga reaalse näitena kübersõjast" ning osutasid NATO olulisusele selles küsimuses (*ibid*). Ainus, mida Eesti esindajad ei suutnud, oli oma tähtsaima publiku, NATO-liitlaste, veenmine, et ründed kujutasid ohtu Eesti suveräänsusele ning seetõttu võiks sarnaste rünnete suhtes rakendada artikkel viie põhimõtet (*ibid*).

Rünnakute tegelikku olemust vaadates ei kujutanudki aset leidnud sündmused niivõrd suurt ohtu, kuna kõige mõjukamad osad taristust jäid puutumata – rünnakud ei häirinud elektri-, finants-, energia- ega liiklusvõrke. Pigem olid rünnakud ebamugavaks, võib-olla piinlikuks vahejuhtumiks, mis tõid esile võimalikud ohud suhteliselt väheste tagajärgedega (valitsusasutuste veebilehtede, ajalehtede ning suuremate pankade töö oli häiritud, kuid reaalselt füüsilist kahju ei tekitatud). Lisaks peab veel mainima, et küberrünnakuid on tegelikult mitmeid korda esinenud ka enne Eesti juhtumit (Hansen ja Nissenbaum 2009). Siiski suutis Eesti esitleda sündmust nii, et andis tugeva tõuke NATOle küberkaitse temaatikat arendada. Aasta pärast rünnakuid võttis NATO vastu

oma küberjulgeoleku strateegia, lõi küberkaitse korraldusasutuse ning toetas Küberkaitse Kompetentsikeskuse loomist Eestisse. Kuid NATO pole ainuke organisatsioon, mille liige Eesti on ja mis tegeleb küberjulgeoleku küsimustega – oma rolli mängivad ka Euroopa Liit, Euroopa Nõukogu, ÜRO ja OECD (Tiirmaa-Klaar 2010). Lisaks on oluline märkida CERTi raames tehtavat koostööd, mis oli küberrünnakute ajal üheks oluliseks osaks (*ibid*). Nimetatud organisatsioonid on võis olla küll „esimene", kuid kindlasti on rahvusvahelist avalikkust hoiatanud ka 2008. aastal Gruusia ja Leedu kogemus Venemaa poolt tulnud rünnakutega (Tikk 2010). Eestis on tänu suurele teema käsitlusele kasvanud suuri rahvusvaheliselt tuntud küber ettevõtteid nagu näiteks Bytlife solutions, BHC Laborator, Bytlife Solutions, kes pakuvad oma ekspertiisi ülemaailma ja korraldavad ka küberõppuseid. Samuti on Eesti Välisministeerium nõustanud Gruusiat riigikaitseks vajalike võimete arendamisel (Välisministeerium).

# 3. EDUKAS KOOSTÖÖ ORGANISATSIOONIDES JA RAHVUVAHELISE SEISUNDI SAAVUTAMINE

Eesti selge tahe olla küberjulgeoleku ohtude eeskostja avaldub ka 2008. aastal vastu võetud esimeses Küberjulgeoleku strateegias (tänaseks on ilmunud küberjulgeoleku strateegia aastateks 2014-2018 ja küberturvalisuse strateegia 2019-2022), mille üheks peamiseks eesmärgiks ongi kirja pandud globaalse koostöö soodustamine: *„Seoses 2007. aasta kevadel toimunud rünnakute ja nende käigus saadud kogemustega, aga ka meie endi järgnenud algatustega oodatakse Eestilt rahvusvahelisel tasandil suurt panust ja mõningatel juhtudel ka protsesside eestvedamist."* Küberjulgeolek eeldab juba olemuselt teatud koostööd riikide vahel – infotehnoloogia ja interneti ei saa kuidagi lokaalselt määratleda. Riigid rakendavad võimu nii, et juhinduvad oma väärtustest ja rahvuslikest huvidest, ning kübervõim pole erand (Pernik, 2015).

Küberjulgeolek väga laialivalguv määratlus – ründed võivad olla poliitilise sisuga, nii riikidevahelised kui ka riigisisesed, samas on suur osakaal ka küberkuritegevusel, mis puudutab eelkõige erasektorit. Seetõttu tegeletaksegi erinevate küberjulgeoleku tahkudega läbi erinevate tasandite ja organisatsioonide ehk teatud tasemel liitlasstrateegia kasutamine on antud teema suhtes vältimatu. Euroopa Liit on väljatöötamas oma kübersanktsioonide režiimi, millega reguleerida stabiilset küberruumi arengut (Tiirumaa-Klaar, 2019:43). Euroopa Nõukogu, kes ainukesena pakub riikidele võimalust liituda küberkuritegevuse vastu võideldava konventsiooniga, mis kohustab liikmetel küberkuriteod kriminaliseerida ja sealhulgas määrab küberkurjategijate väljaandmisekohustuse (Tiirmaa-Klaar 2010). Võiks eeldada, et Eestil oleks võimalus 2007. aasta kogemusele pakkuda eeskuju küberkuritegude kriminaliseerimisest seadusandluses, kuid Eestil ilmekat, põhjalikult koostatud näidet teistele selle vallas hetkel veel pakkuda ei ole. Siiski puudutab küsimust küberkaitse strateegia, mis jällegi keskendub eelkõige koostöö vajadusele ja kutsub üles arendama välja riikide suhtes nö mudelseadus, mis hõlbustaks koostööd (Eesti küberjulgeoleku strateegia 2014). Kui seadusandluse suhtes Eesti eeskujuks veel olla ei suuda, siis on nimetatud Küberjulgeoleku strateegia küll suhteliselt ainulaadseks dokumendiks –

paljud riigid ja asutused on sealt ideid üle võtnud, sealhulgas isegi USA küberkaitse eksperdid oma vastava strateegia koostamisel (Ilves 2011).

Sarnaselt Euroopa Nõukoguga, kes eelkõige keskendub küberkuritegevusele ja mitte niivõrd riikidevahelistele küberrünnakutele, on oluliseks organisatsiooniks Euroopa Liit, mis tegelebki eelkõige tsiviilotstarbeliste küsimustega. Selles kontekstis on Eesti samuti näidanud oma osa probleemi käsitlemisel. Näiteks korraldas majandus- ja kommunikatsiooniministeerium 2009. aastal ELi ministrite kohtumise, et ellu kutsuda ELi kriitilise informatsiooni infostruktuuri kaitse poliitika (Tiirmaa-Klaar 2010). Eestisse suhtumist näitab ka siia Euroopa IT agentuuri loomine, mille puhul siiski serverid jäävad Strasbourgi (E24 2010). Eesti on pead tõstnud ka näiteks Euroopa Julgeoleku- ja Koostööorganisatsioonis, kus Eesti juhtimisel on algatatud mitmed küberjulgeoleku teemalised seminarid, mille tulemusena on organisatsioon välja töötanud liikmetele suunatud juhise, kuidas küberjulgeolekut tõhusamalt tagada (*ibid*). Küberjulgeoleku temaatikaga tegeleb mõistagi ka ÜRO. Võrreldes eelpool nimetatud organisatsioonidega, tegeleb ÜRO NATO kõrval ainukesena ka kübersõdade ja küberterrorismiga (Tikk 2010). ÜRO eeliseks ja ka nõrkuseks on see, et see pakub võimalikest organisatsioonidest kõige laiema konsensuse võimalikkust. Ühelt poolt on võimalikult laiahaardeline koostöö küberjulgeoleku vallas oluline, teisalt seab lai liikmelisus piiranguid, kuna liikmed on väga erineva arengu- kui ka kompetentsitasemega. Eesti tahet ka ÜRO kontekstis silma paista on see väide, et Eesti toetas aktiivselt ka ÜRO globaalse küberkultuuri alase resolutsiooni vastuvõtmist (Tiirmaa-Klaar 2010).

Vaadates Eesti meediat, siis peetakse kõige väljapaistavaks edusammuks Eesti koostööd NATO raames, mis tuleneb kindlasti suures osas NATO CCD COE loomisest. NATO oli ka esimene organisatsioon, mis pärast rünnakuid kiiremas korras küberjulgeolekuga tegelema hakkas (Tiirmaa-Klaar 2010). Eestit on iseloomustatud kui ühe aktiivseima riigina NATO küberkaitsepoliitika väljatöötamisel (*ibid*).

Ühelt poolt võib tunduda pigem teadusuuringute koostamine ja eelkõige kompetentsi edastaja roll NATO kontekstis mõneti ebaoluline väärtus. Võrreldes teiste valdkondadega, on võib-olla kompetents ning teadustöö isegi kõige olulisem väärtus

kübersfääris, kuna siin ei mõõdeta võimekust tankide arvus vaid pigem nö ajupotentsiaalil keeruka valdkonnaga tegelemisel. Siinkohal on Eesti suutnud küberkaisekeksuse näol luua endale sobiva pinnase eesvedaja rolli mängimiseks, see aitab kinnistada Eesti identiteeti just antud valdkonna eksperdina. NATO pakub ka Eestile soodsa raamistiku koostöö edendamiseks, seda eriti küberjulgeoleku eripärasid arvestades (Tikk 2009). NATO suureks eeliseks on kübervallas suhteliselt üksmeelse tahte olemasolu, mis kiirendab erinevate poliitikate rakendamist (*ibid*). NATO poolne tahe uutele ohtudele keskenduda on jällegi soodustavaks asjaoluks Eestile. Lisaks keskendub NATO võrreldes teiste küberjulgeolekuga tegelevate organisatsioonidega just küberrünnakute ja kübersõdade valdkonnale (*ibid*). Esimene suurem tulemus tuntuse saavutamisel teadussfääris saadi mitmekümne eksperti toel kui NATO küberkaitsekeskus lõi „Tallinna manuaali“, mis sõnastab kübersõdade pidamise põhimõtted (NATO CCD COE).

Jättes välja koostöö organisatsioonide raames, on Eesti oma küberkaitse arendaja rolli ka teistel viisidel näidanud. Näiteks eksisteerib Eestis küberkaitseliit, millega on seotud vabatahtlikud kübervaldkonna eksperdid. Omapärane idee on väidetavalt jällegi tekitanud rahvusvahelist tähelepanu (Tikk 2009). Küberkaitseliidust arenes välja 2018 aastal küberväejuhatus, mis tähendab seda, et nende ülesandeks on operatsioonide läbiviimine küberruumis (Kaitsevägi). 2012 Eestisse rajatud Euroopa Liidu IT-agentuuri peakontor EU-LISA, mida nimetatakse Eesti infotehnoloogilise eduloo järgmiseks progressiks. IT-agentuur EU-LISA vastutusalas on Schengeni infosüsteemi (SIS II), viisainfosüsteemi (VIS) ja Eurodaci ("suuremahulised IT-süsteemid") operatiivjuhtimisne. Agentuuri peakorter asub Tallinnas ja tehnilise infrastruktuuri on Strasbourgis (EU LISA).

Viimaseks võib välja tuua kõneka fakti, et Eesti on ülikooli õpingutes loonud jätkusuutliku pealekasvu koolitades välja kübervallas uusi tippspetsialiste. Selle eestvedamise on ende kätte võttu Tallinna Tehnikaülikool koostöös Tartu Ülikooliga. Innovaatilised ideed, mis maailmas huvi ja tähelepanu tekitavad, on jällegi sammudeks, mis kindlasti aitavad kaasa Eesti „kübereksperdi“ identiteeti luua ning mainet tõsta.

## 3.1 Individuaalne kaitsevõime

Kui edu rahvusvahelistes organisatsioonides on suhteliselt selge, siis järgnev töö osa üritab hinnata Eesti individuaalset suutlikkust tagada kübereksperdi staatust. Eesti edusse lähemalt uurides võib väita, et praegused saavutused võivad olla lihtsalt hiljutiste sündmuste paratamatu ja iseenesest realiseeruv järelmõju. Umbes 1,3 miljoni elanikuga riigilt ei saagi eeldada, et see suudaks iseseisvalt ja üksi särada. Koostöö esiletõstmine erinevates julgeolekuaspektides on väiksele riigile ainuvõimalik lahendus, eriti veel olukorras, kui peamise võimaliku ohu tekitaja on suurriik idanaaber, kelle raha varud on suuremad. Seetõttu on väikeriigi jaoks ainuke võimalus keskenduda tugevalt ainult kindlale valdkonnale. See valik on Eesti ja kübervaldkonna puhul õnnestunud. Eesti on olnud tegija esiteks alal, mis on ennast ise müüv, sest küberohud kerkivad esile järjest enam ning on tänapäeva maailma arenguid vaadates kindel. Lisaks on Eestil pigem vedanud, et 2007. aasta rünnakute ajal ei olnud küberohud maailmas niivõrd oluliselt esile kerkinud. Eesti sai väärtusliku õppetunni ning talle omistati märgiline tähendus kui esimene sarnaste probleemidega võitleja. Samas tekib siinkohal küsimus, mis seostub eelpool nimetatud riigisisese suutmatusega. Rääkides veel pigem õnnestunud valikutest, siis pakub NATO, nagu eelpool näidatud, hea raamistiku koostööks. Ilmselt Eesti jaoks kõike haaravate julgeoleku valdkodadega ning kõikide organisatsioonidele keskendumine mõeldamatu.

Üheks negatiivseks küberjulgeoleku aspektiks võib Eestile olla see, et tehnoloogia pideva arenemise tulemusena muutuvad ka aja möödudes küberohud. „*Ohud ei ole digitaliseerimise varjukülg, need on orgaaniline osa paketist. Tehnoloogia roll ühiskonna igapäevaelu toimimisele on jõudnud määrani, kus küberturvalisus ei ole enam lihtsalt tehnoloogiliste lahenduste kaitsmise summa, Eesti jaoks tähendab küberturvalisus digitaalse ühiskonna ja eluviisi kaitsmist tervikuna.*" (Maigre, Kaska, 2018). Positiivse küljena eelarve kontekstis saab siiski näha eesmärki kulutada üle 2% SKP-st kaitsekulutustele, mis tõstab Eestis teiste NATO liikmesriikide seas jällegi positiivselt esile. Eesti senise kübereksperdi staatust võib ohustada ka küberjulgeoleku muutumine täiesti tavapäraseks julgeolekupoliitika osaks. See tähendab, et

küberjulgeolekuga tegelemist nähakse tulevikus ilmselt võrdsena piltlikult näiteks õhutõrje loomise või jalaväelaste koolitamisega. Tehnoloogia pidev areng on kindel ning see toob kaasa ka paratamatu küberohtude suurenemise. Briti peaminister David Cameron on omakorda võrrelnud kübermaailma „valitsemist" 19. sajandi olukorraga, kus Briti impeeriumi eduks oli tarvis valitseda mereteid (The Guardian 2011). Julgeolekuanalüütikud ongi juba kübervaldkonda määratlemas „viienda sõjalise lahinguväljana" maa, õhu, vee ja kosmose kõrval (Schoenbohm 2011).

## 3.2 Eesti julgeoleku eesmärkide täitmine läbi küberjulgeoleku

Hinnates Eesti välispoliitiliste eesmärkide avaldumist küberjulgeoleku kontekstis, võib väita, et selgelt joonistuvad välja kaks omavahel seotud suunda. Nendeks on soov saavutada julgeolekut läbi kübervaldkonna ning sellega seostuv tahe näidata oma eelistatud seisundit. Eesti ressursi ja inimjõu puudusest tulenev vähene riigisisene individuaalne suutlikkus paneb meid suurriikide ja organisatsioonide liitudele toetama. Eesti on edukalt mänginud oma rolli erinevates rahvusvahelistes organisatsioonides kübervaldkonna arendajana. Lähiaastatel on oodata, et Eesti tugevdab suhteid kübervaldkonnas peamiste liitlasriikidega ning küberjulgeoleku algatusi rahvusvahelistes organisatsioonides (Tiirumaa-Klaar, 2019:43).

Kui käsitleda julgeoleku tagamist kõige tähtsama välispoliitilise eesmärgina ning küberjulgeolekut kui väga tähtsat selle eesmärgi võimendajat, siis saab väita, et Eesti individuaalselt vähevõimeka väikeriigina on küberjulgeoleku näitel selgelt oma esmase eesmärgi saavutanud. Edukalt on ära kasutatud küberrünnakutest tulnud tähelepanu enda kasuks, mis õigustab oma liikmelisust erinevates organisatsioonides.

# KOKKUVÕTE

Riigi üheks olulisemaks välispoliitiliseks eesmärgiks on tagada enda julgeolek. Julgeoleku tagamiseks on väga palju erinevaid viise, alustades kasvõi isolatsioonis olemisest ja oma ressursilise võimekuse suurendamisest, kuni kõikehõlmava rahvusvahelise koostööni sellistel teemavaldkondadel, mis esialgu ei näita sugugi otsest seotust riigi huvi oma julgeolekut kindlustada täpselt nagu on seda küberjulgeolek.

Samuti on Eesti üheks peamiseks eesmärgiks on Eestist positiivse kuvandi loomine (usaldusväärne partner, rahvusvahelisesse julgeolekusse panustaja, keskkonnasõbralik, edumeelne e-riik). Ühiskonna tugevuse kindlustamiseks peab tugevdama elutähtsate teenuste toimepidevust, elektroonilist sidet, küber- ja energiajulgeolekut, transpordi infrastruktuuri, finantssüsteemi ja keskkonnaturvalisust, ühtlast regionaalset arengut, lõimumist, psühholoogilist ja rahvatervise kaitset on välja toodud Kaitseministeeriumi „ühiskonna toimepidavuse ja sidusese“ eesmärkides .

Hinnates Eesti välispoliitiliste eesmärkide avaldumist küberjulgeoleku kontekstis, võib väita, et selgelt tuleb välja kaks omavahel seotud suunda. Nendeks on soov suurendada julgeolekut läbi kübervaldkonna ning sellega seostuv tahe näidata oma eesrindlikust sellel alal. Väikeriigi ressursipuudusest tulenev vähene riigisisene individuaalne suutlikkus sunnib otsima abi, suurriikidest liitlastele toetudes
Kui käsitleda julgeoleku tagamist kõige tähtsama välispoliitilise eesmärgina ning küberjulgeolekule keskendusmist kui hetkel kõige õigemat suunda, siis saab väita, et Eesti individuaalselt vähevõimeka väikeriigina on küberjulgeoleku näitel selgelt oma esmase eesmärgi saavutanud. Eesti suutis toonased rünnakud suhteliselt edukalt enda kasuks pöörata. Negatiivne kogemus kujundati pigem esilekerkivaks sündmuseks, mis lõi soodsa aluse Eestile antud probleemile oma välispoliitikas rõhku panna. Seega küberrünnak Eestile oli lõppkokkuvõttes hea õppetund ning teema tõsisus tõusis rahvusvahelisel areenil märkimisväärselt kõrgele.

Õnneks suudeti 2007. aasta küberrünnakust palju õppida. Siiani on palju probleeme lahendamata, aga vähemalt suudeti maailmas sellejärgselt teadvustada, kui oluline on küberkaitse ning kui ohtlikud on küberrünnakud. Eesti suutis end sellel teemal oluliselt kehtestada ning tänuks sellele loodi näiteks Tallinnase NATO küberkaitsekeskus ja koliti EU-LISA peakontor. Samuti on Eesti ise teinud palju selleks, et riigisisest küberturvalisust suurendada ning rahvusvahelist koostööd arendada.

Küberjulgeoleku (küberturvalisuse) strateegia iseloomustab ilmekalt Eesti tahet ning ka teatud määral suutlikkust olla märgatav rahvusvahelises koostöös kübervaldkonnas. Kui sätestatud riigisisesed eesmärgid on ilmselt eeskujuks teistele riikidele, siis puudutab dokument eraldi ka eelpool nimetatud organisatsioone ning nendega suhtes Eesti välispoliitilisi eesmärke. Juba see, et kõikide organisatsioonide suhtes on välja toodud eraldi konkreetsed suunised tegutsemiseks, iseloomustab Eesti tahet kui ka suutlikkust kübertemaatika edendajana tegeleda. Rääkides veel pigem õnnestunud kontsentreerumisest, siis pakub NATO, nagu eelpool näidatud, hea raamistiku koostööks ning kübervaldkonnas oleks ilmselt Eesti jaoks kõike puudutatavatele tahkudele ning kõikvõimalikele organisatsioonidele keskendumine ebareaalne.
Võib väite, et töös esitatud teesid pidasid paika ja leidsid ka uurimuse käigus kinnitust.

## Kasutatud kirjandus


Anderson, N (2007) „Massive DdoS Attacks Target Estonia; Russia Accused“ *Ars Technica,* 14. mai http://arstechnica.com/security/2007/05/massive-ddos-attacks-target-estonia-russia-accused/

Buzan M., O. Weaveri O. ja Wilde J. (1998) Security: A New Framework For Analysis. Boulder, CO: Lynne Rienner

Davis, J (2007) Wired 21 august „Hackers Take Down the Most Wired Country in Europe“ Veebilehel: https://www.wired.com/2007/08/ff-estonia/

Eesti Päevaleht (2011) Aaviksoo tahab Küberajateenistust. Veebilehel: http://www.epl.ee/news/eesti/article.php?id=51289682 02

Eesti Küberjulgeoleku strateegia 2008-2013 editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf

Eesti Küberjulgeoleku strateegia 2014-2017 Veebilehel: https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf

Eesti Küberjulgeoleku strateegia 2008-2013 Veebilehel: https://www.valitsus.ee/sites/default/files/contenteditors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf

Ergma, E (2007) „Küberjulgeolekule teed rajades“, *Riigikogu Toimetised,* 15 Veebilehel: http://www.riigikogu.ee/rito/index.php?id=11594&op=archive2

EU-Lisa https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems

Ilves, T H. Delfi (2009). „President Ilves: Pahatahtlikud küberrünnakud on vaja kriminaliseerida kõikides maailma riikides.“ Veebilehel: http://www.delfi.ee/news/paevauudised/arvamus/president-ilves-pahatahtlikud-kuberrunnakud-on-vaja-kriminaliseerida-koikides-maailma-riikides.d?id=25899659

Ilves, L K (2011). E-Eesti välispoliitika. *Diplomaatia,* nr 98, Oktoober.

Hansen, L. ja Nissenbaum, H. (2009) Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly* (2009) 53, 1155–1175

Holsti, K-J (1995) „International politics: a framework for analysis".

Kalvet, T (2007) „Eesti infoühiskonna arengud alates 1990. aastast" *Praxise toimetised,* 30, lk 25

Kaitseministeeriumi Kaitse-eelarve 2019 Veebilehel: http://www.kaitseministeerium.ee/et/eesmargid-tegevused/kaitse-eelarve

Kaitseministeeriumi "Ühiskonna toimepidevus ja sidusus" veebilehel: http://www.kmin.ee/et/eesmargid-tegevused/julgeolekupoliitka/uhiskonna-toimepidevus-ja-sidusus

Kaitseväe küberväejuhatus; veebilehel: http://www.mil.ee/et/kaitsevagi/Kybervaejuhatus

Kirk, J (2007) „Analysis: Russian Gov't not behind Estonia DDOS Attacks" *The Washington Post,* 2. juuni. Veebilehel: http://www.washingtonpost.com/wp-dyn/content/article/2007/06/02/AR2007060200126.html??noredirect=on

Küberkaitseliit: http://kyberkaitseliit.ee/

Myers, S L (2007) „Estonian Computer Blitzed, Possibly by the Russians" The New York Times, 19. mai. Veebilehel: http://www.nytimes.com/2007/05/19/world/europe/19russia.html?fta=y

Maigre M, Kaska K (2018), Diplomaatia, 14. september „Küberkaitsest, terviklikult" Veebilehel: https://diplomaatia.ee/kuberkaitsest-terviklikult/

Majandus ja kommunikatsiooniministeeriumi Eesti infoühiskonna aastaraamat 2011/2012, lk 38

Mattheus, Ü (2016) Ajaleht Sirp, "Euroopa väärtused ja postmodernistlik valitsus" 11. märts. Veebilehel: https://www.sirp.ee/s1-artiklid/c9-sotsiaalia/euroopa-vaartused-ja-eesti-postmodernistlik-valitsus-2/

NATO (2014) „Wales Summit Declaration“ *Press release*, 120, 5. september Veebilehel: http://www.nato.int/cps/en/natohq/official_texts_112964.htm

P. Pernik (2015) Diplomaatia oktoober 16. „Küberjulgeolek kui välis- ja julgeolekupoliitika küsimus.“ Veebilehel: https://diplomaatia.ee/kuberjulgeolek-kui-valis-ja-julgeolekupoliitika-kusimus/

Postimees, Majandus24 (2010) Euroopa IT-agentuur tuleb Eestisse. Veebilehel: https://majandus24.postimees.ee/324261/euroopa-it-agentuur-tuleb-eestisse

Postimees (2012) Briti minister: küberrünnakud võivad samuti käivitada NATO 5. Artikli. Veebilehel: http://www.postimees.ee/843952/briti-minister-kuberrunnakud-voivad-samuti-kaivitada-nato-5-artikli/

Randel, T (2007) „CERT Eesti tegevuse aastakokkuvõte 2007“ Veebilehel: https://www.ria.ee/sites/default/files/content-editors/CERT/cert_2007_aastakokkuv6te.pdf

Raud, H (2012) „Küberjulgeolekust“, Eesti Infosühiskonna Aastaraamat 2011/2012.

Rehman, S (2013) „Estonia Shows, How to Build a Defense against Cyberwarfare“ *US News,* 14. jaanuar. Veebilehel: http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare

Richards, J (2009) „Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security“, *International Affairs Review,* 18(2)Veebilehel: http://www.iar-gwu.org/node/65

Ryan, J (2007) „„I-sõda“: uus, käepärane ja üha valusamalt haavatav koht“, *NATO Teataja,* 4 Veebilehel: http://archive.today/NOF2b

Schoenbohm (2011). Germany Must Defend Against Cyber Attacks. *Atlantic-community.org.* Veebilehel: http://www.atlantic-community.org/index/articles/view/Germany_Must_Defend_Against_Cyber_Attacks_

The Guardian (2011) PM launches cyber security strategy. Veebilehel: http://www.guardian.co.uk/government-computing-network/2009/jun/25/office-cyber-security-strategy-25jun09?INTCMP=SRCH

Traynors, I. The Guardian (2007). Russia accused of unleashing cyberwar to disable Estonia. Veebilehel: http://www.guardian.co.uk/world/2007/may/17/topstories3.russia

Tiirmaa-Klaar, H. (2010). Rahvusvaheline koostöö küberjulgeoleku tagamisel. Diplomaatia, nr. 85, september.

Tiirumaa-Klaar,H (2019) Riigi Infosüsteemi Amet Küberturvalisus 2019, lk 43 Veebilehel: https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisus-2019.pdf

Tikk, E. (2010) Global Cyber Security – Thinking About The Niche for NATO. The SAIS Review of International Affairs, Sügis

Volker, Kurt 2009 „Julgeolekupoliitika - Pilk Peeglisse“ Veebilehel: https://vm.ee/et/julgeolekupoliitika-pilk-peeglisse-2009

Välisministeerium (2007) „Küberrünnakud Eesti vastu“ 58-71 Veebilehel: http://vm.ee/sites/default/files/content-editors/web-static/115/cyber_attacks.pdf

Välisministeerium (2013) „NATO on Eestile ja kogu siinsele piirkonnale suurim julgeolekugarantii“ Veebilehel: https://vm.ee/et/uudised/nato-eestile-ja-kogu-siinsele-piirkonnale-suurim-julgeolekugarantii

Välisministeerium, Gruusia partnerlus. veebilehel: https://vm.ee/et/riigid/gruusia?display=relations

Välisministeerium, Rahvusvahelised organisatsioonid, veebilehel https://vm.ee/et/tegevused-eesmargid/rahvusvahelised-organisatsioonid

Välisluureameti raport 2019: Eesti rahvusvahelises julgeoleku keskkonnas 2019 raport Veebilehel: https://www.valisluureamet.ee/pdf/raport-2019-EST-web.pdf

NATO CCD COE Tallin Manual 2.0 https://ccdcoe.org/research/tallinn-manual/

Ühtegi, R (2007) Postimees, 5. september „Kas Eesti pidas tänavu kevadel maha kübersõja?“ Veebilehel: http://arvamus.postimees.ee/1699321/riho-uhtegi-kas-eesti-pidas-tanavu-kevadel-maha-kubersoja

## Mõisted

**DDoS (denial of service attack) -** rünnak seisneb sihtmärgi päringutega nii ülekoormamises, et see muutub kättesaamatuks või kokku jookseb

**Botnet ehk robotvõrguks (robot network) -** nimetatakse küberkurjategijate poolt kontrollitavat arvutite kogumit, mis kasutajate teadmata pahatahtlikke taustategevusi teostavad

**CERT (Computer Emergency Response Team) -** Rahvusvahelise infoturbe kaitse spetsialistide võrgustik. Eesti riigi tasemel täidab CERTi ülesandeid Riigi infosüsteemide arenduskeskuse infoturbe-intsidentide käsitlemise osakond.

**Küberrelv -** Küberrelvaks nimetatakse pahavara eest vastutavat, mida kasutatakse sõjalisel eesmärgil rünnatava julgeoleku kahandamiseks.

**NATO CCD COE -** NATO Küberkaitsekoostöö Keskus

**EU-LISA -** Euroopa Liidu IT-amet

**SKP -** Sisemajanduse koguprodukt turuhindades

**PING käsk**- kasutatakse selleks, et kontrollida ühenduvust mingi muu arvutiga. Käsk saadab server võõrustajale voo ning esitab siis seejärel tulemuse.

## Summary

*An analyses of the Estonian foreign and security policy goals in the context of cyber security*

This bachelor's thesis study focuses on Estonia's foreign and security policy objectives advances in the context of cyber security issues as an example. In the first part of the empirical study which analyses Estonian Security policy views and niche positions. On the second half of the thesis, we concentrate on the Estonian cyber security. The focus is on the cyberattack conducted against Estonia in 2007, which can be referred as "history´s first cyberattack" which put different countries to think about information societies vulnerabilities. On the third part, we look at into the successful cooperation in organizations and how Estonia tries to succeed in his international status.

The main goal is to show how cyber security has affected Estonia´s foreign and security policy and what has manifested on that area. Thesis evaluates the 2007 cyberattack and how it has influenced Estonia´s cyber policy and thereafter given an overview of international cooperation overall and what is the Estonia´s role in that.

2007 cyberattack teaches us a lot, still there are lot of problems which need solving but we managed to emphasise how important is cyber security and how dangerous are the cyberattacks in world. It can be stated that Estonia has proved its willingness to shine with bigger states on the cyber arena. The cyber-attacks in 2007 against Estonia served as a wake-up call for NATO to engage into the issue more seriously. Today, NATO has actively taken measures in order to tackle the issue of cyber security, but still, there are many challenges ahead the sphere of cyber security.