TARTU ÜLIKOOL
Sotsiaal- ja haridusteaduskond
Riigiteaduste instituut
Rahvusvaheliste suhete õppetool

Kersti Oksaar

Küberjulgeolekustamine Kopenhaageni koolkonna teooria järgi Eesti Vabariigi diskursuse näitel

Magistritöö

Juhendajad: Anna-Maria Osula, MA
Maria Mälksoo, Ph.D

Tartu 2014

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

Olen nõus oma töö avaldamisega Tartu Ülikooli digitaalarhiivis DSpace.

……..

/Kersti Oksaar/

LÜHIKOKKUVÕTE

Käesoleva magistritöö eesmärkideks on uurida Kopenhaageni koolkonna esialgset ja edasiarendatud raamistikku küberjulgeoleku käsitlemiseks, ning analüüsida, kas ja kuidas on küberjulgeolekustamine aset leidnud reaalsuses. Töö uurimisküsimusteks on, kuidas toimub küberjulgeolekustamine Kopenhaageni koolkonna järgi ning kas Eestis on toimunud 2007. aastast alates küberjulgeolekustamine 2007. aasta küberrünnete tulemusel?

Töö teoreetiline raamistik keskendub Kopenhaageni koolkonna julgeolekustamise teooriale. Metodoloogiliseks aluseks võetakse Lene Hanseni poststrukturalistlik diskursusanalüüs kõneaktide uurimiseks. Empiirilises osas käsitletakse küberjulgeolekustamise teooria ja Hanseni poststrukturalistliku diskursusanalüüsi sünteesi abil Eesti riigi esindajate kõneakte ning uuritakse Eesti küberjulgeolekuga seotud arengukavasid ja kübervaldkonna teadvustamist riigi esindajate kõnedes.

Magistritöö tulemusena saab väita, et Kopenhaageni teooria põhjal on võimalik luua põhjalik küberjulgeolekustamise teooria ning küberjulgeolekustamine leidis aset Eesti Vabariigis 2007. aasta küberrünnete ajal ja järgselt.

Uurimistöö tulemusi on võimalik kasutada küberjulgeolekustamise analüüsimiseks teiste riikide ja metodoloogiate põhjal, sest magistritöös väljaarendatud teoreetiline raamistik pakub originaalse lähenemise Kopenhaageni koolkonna pinnalt loodud küberjulgeolekustamise teooriale.

Magistritöö autor tänab uurimistööga seotud osapooli nende panuse ja toetuse eest käesoleva töö valmimiseks.

Magistritöö märksõnad: küberjulgeolek, Kopenhaageni koolkond, küberjulgeolekustamine, Eesti, poststrukturalistlik diskursusanalüüs

SISUKORD

TÖÖS KASUTATUD LÜHENDID

Botnet – Robotivõrk (*robot network*)

CDA – Kriitiline diskursusanalüüs (*critical discourse analysis*)

CERT-EE – Riigi Infosüsteemi Ameti infoturbeintsidentide käsitlemise osakond (*Computer Emergency Response Team of Estonia*)

CI – Kriitiline infrastruktuur, KI (*critical infrastructure*)

CIS – Informatsiooni- ja kommunikatsioonisüsteemid (*communication and information systems*)

COPRI – Kopenhaageni Rahu-uuringute Instituut (*Copenhagen Peace Research Institute*)

CS – Kopenhaageni koolkond (*Copenhagen School*)

DDoS – Jagatud teenusetõkestamine (*distributed denial of service*)

EALL – Eesti Ajalehtede Liit (*Estonian Newspaper Association*)

EC³ – Küberkuritegevuse vastase võitluse Euroopa keskus (*European Cybercrime Center*)

EL – Euroopa Liit (*European Union*, EU)

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

EPL – Eesti Päevaleht

EWI – Ida-Lääne Instituut (*EastWest Institute*)

G20/G-20 – Kahekümne Rahandusministri ja Keskpangajuhi Grupp (*Group of Twenty Finance Ministers and Central Bank Governors/Group of 20*)

ICPO – Rahvusvaheline Kriminaalpolitsei Organisatsioon, Interpol (*International Criminal Police Organization*)

ICT – Informatsiooni- ja kommunikatsioonitehnoloogia, IKT (*information and communication technology*)

Infosec – Infoturve (*information security*)

ISO – Rahvusvaheline standardiorganisatsioon (*International Organization for Standardization*)

IT – infotehnoloogia (*information technology*)

ITU – Rahvusvaheline Telekommunikatsiooni Liit (*International Telecommunication Union*)

NATO – Põhja-Atlandi Lepingu Organisatsioon (*North Atlantic Treaty Organization*)

NATO CCD COE – NATO Kooperatiivne Küberkaitse Kompetentsikeskus ehk koodnimetusega K5 (*NATO Cooperative Cyber Defence Centre of Excellence*)

NGO – Mitteriiklik organisatsioon (*Non-Governmental Organization*)

PM – Postimees

RIA – Riigi Infosüsteemi Amet (*Estonian Information System's Authority*, EISA)/kuni 01.06.2011 Riigi Infosüsteemide Arenduskeskus (*Estonian Informatics Centre*, EIC)

SKO – Shanghai Koostööorganisatsioon (*Shanghai Cooperation Organisation*, SCO)

SMIT – Siseministeeriumi infotehnoloogia- ja arenduskeskus (*IT and Development Centre of the Ministry of the Interior*)

UNGA/GA – ÜRO Peaassamblee (*UN General Assembly*)

ÕL – Õhtuleht

1. SISSEJUHATUS

Küberjulgeolek on aina olulisemaks muutuv valdkond tänapäeva globaliseeruvas maailmas. Üha sagedasem teenuste Internetti kolimine ja nende kasutamine juhib tähelepanu informatsiooni- ja kommunikatsioonitehnoloogiate (IKT) haavatavustele. Kuna küberjulgeolek on muutunud rahvusvaheliste suhete tähtsaks osaks,[1] siis kerkib esile küsimus, kuidas julgeolekustatakse küberruumi ohustavaid küberohtusid. Uurimistöö teoreetiliseks sihiks on seega uurida Kopenhaageni koolkonna esialgset ja edasiarendatud raamistikku küberjulgeoleku analüüsimiseks julgeolekustamise teooria abil. Töö eesmärgiks on ka uurida, kas ja kuidas on küberjulgeolekustamine (*cyber securitization*) aset leidnud reaalsuses Eesti kaasuse näitel. Magistritöö uurimisküsimusteks on, kuidas toimub küberjulgeolekustamine Kopenhaageni koolkonna järgi ning kas Eestis on toimunud 2007. aastast alates küberjulgeolekustamine 2007. aasta küberrünnete tulemusel.

Magistritöö teoreetiline osa toetub Kopenhaageni koolkonnale, mille esialgsest raamistikust võetakse aluseks sektoriaalne käsitlus ja julgeolekustamise protsess. Teooriat arendatakse edasi Kopenhaageni koolkonna teise põlvkonna[2] käsitluste alusel, mille põhjalt uuritakse küberjulgeolekut kui eraldi julgeolekusektorit ja küberjulgeolekustamise teooriat. Kopenhaageni koolkonna analüüsimine on päevakajaline, sest Kopenhaageni koolkonnale on tekkinud niinimetatud teine põlvkond

[1] Näiteks on loodud mitmeid organisatsioone EL-i raames, näiteks ENISA 2004. aastal. ENISA koduleheküIg. http://www.enisa.europa.eu/ (kasutatud 03.03.2014). EL-i ametitest on küberjulgeolekuga veel seotud 2013. aastal Euroopa Komisjoni ettepanekul avatud EC³ Europoli koosseisus küberjulgeoleku ekspertide treenimiseks. Europoli koduleheküIg. https://www.europol.europa.eu/ec3 (kasutatud 03.03.2014). Küberjulgeolekuga tegelevad veel UNGA, ITU, G20, NATO, SKO ja Interpol. Küberjulgeolekuga on seotud ka regionaalsed organisatsioonid ja NGO-d, mis teeb küberjulgeoleku erinevate huvigruppide kaasamise (*multistakeholder*) lähenemiseks, kus iga asjakohaste teadmistega grupp (näiteks ettevõtted) või poliitilised autoriteedid (riigid) võivad osaleda küberjulgeoleku kujundamises. Bendiek, Annegret, and Andrew L. Porter. 2013. „European Cyber Security Policy within a Global Multistakeholder Structure." *European Foreign Affairs Review* 18 (2): 167. http://www.kluwerlawonline.com/abstract.php?area=Journals&id=EERR2013011 (kasutatud 29.12.2013) Eksisteerib ka suur arv riiklike küberjulgeoleku strateegiaid, mis näitab, et küberjulgeolek on riikide jaoks prioriteet. NATO CCD COE koduleheküljel on 24. aprilli 2014. aasta seisuga viidatud 40-le riiklikule küberjulgeoleku strateegiale. CCDCOE koduleheküIg. http://ccdcoe.org/328.html (kasutatud 24.04.2014)

[2] Julgeolekustamise akadeemilist diskursust on märkimisväärselt edasi arendatud teise põlvkonna teadlased (Juha A. Vuori, Thierry Balzacq, Holger Stritzel, Rita Floyd), kes on pakkunud detailseid teoreetilisi käsitlusi julgeolekustamise teooriale. Stritzel, Holger. 2011. „Security, the Translation." *Security Dialogue* 42 (4-5): 348. http://sdi.sagepub.com/content/42/4-5/343 (kasutatud 27.12.2013)

(näiteks Thierry Balzacq, Rita Floyd ja Holger Stritzel), kes täiendanud julgeolekustamise kontseptsiooni[3] ja rakendanud empiiriliselt edasiarendatud Kopenhaageni koolkonna teooriat. Ka Balzacq on tõdenud, et julgeolekustamise uurimine on populaarne ning viimase aastakümne jooksul on kirjutatud artikleid julgeolekustamise teoreetilise raamistiku arendamiseks. Sellest tulenevalt on julgeolekustamise uurijate peamiseks ülesandeks avada ja uuesti esitada teoreetilised argumendid sidusasse eelduste kogumikku, mille abil läbi viia empiirilist uuringut,[4] millest lähtutakse ka käesoleva magistritöö eesmärkides ja uurimisküsimustes.

Töö teoreetilisest raamistikust lähtuvalt koosneb küberjulgeolekustamise protsess julgeolekustavast liigutusest ja julgeolekupraktikast, mille käsitlemine võimaldab uurida, kas ja kuidas on küberjulgeolekustamise protsess aset leidnud. Uurimistöö metodoloogilises osas võetakse aluseks Lene Hanseni poststrukturalistlik diskursusanalüüs kõnede analüüsiks, uurimaks Eesti julgeolekustavate toimijate ehk julgeolekustajate kõneakte ettekannetes, (arvamus)artiklites ja intervjuudes, mille abil saab tuvastada julgeolekustavaid liigutusi julgeolekustajate kõnedes. Julgeolekupraktika analüüsimiseks uuritakse riigi poolt vastu võetud arengukavasid, milles määratletakse tegevuseesmärgid ja meetmed nende saavutamiseks.[5]

Poststrukturalistliku diskursusanalüüsiga saab riigijuhtide ametlike sõnavõttude kaudu analüüsida ja selgitada välja riigi esindajate avalikke seisukohti, sest nimetatud meetod keskendub ametlikule poliitilisele diskursusele. Välispoliitika mõjutajate sihiks on esitleda välispoliitikat, mis on legitiimne ja jõustatav relevantse auditooriumi jaoks. Sellest tulenevalt on poliitilise tegevuse keskmes kooskõlastatud sideme loomine poliitika ja identiteedi vahel,[6] mille analüüs võimaldab uurida auditooriumi veenmist ja nõusoleku saavutamist Kopenhaageni koolkonna julgeolekustamise teooriast lähtuvalt.

Küberjulgeolekut uuritakse Eesti näitel, sest küberründed Eesti poliitiliste institutsioonide ja erasektori vastu juhtisid tähelepanu vajadusele tõsta rahvusvahelist

[3] Donnelly, Faye. 2013. *Securitisation and the Iraq War: The Rules of Engagement in World Politics*. London: Routledge, 49-50.

[4] Balzacq, Thierry, ed. 2011. *Securitization Theory: How Security Problems Emerge and Dissolve*. New York: Routledge, xiii-xiv.

[5] Strateegiliste arengukavade liigid ning nende koostamise, täiendamise, elluviimise, hindamise ja aruandluse kord. 2005. Riigi Teataja I, 2005, 67, 522. https://www.riigiteataja.ee/akt/12790098 (kasutatud 28.04.2014)

[6] Hansen, Lene. 2007. *Security as Practice: Discourse Analysis and the Bosnian War*. London, New York: Routledge, 28, 66.

teadlikkust küberrünnetest.[7] Küberjulgeoleku teema ei ole Eesti kontekstis tähtis ainult sellepärast, et Eesti poliitikakujundajad on seda aktiivselt propageerinud, vaid olulised on ka vastavasisulised arutlused rahvusvaheliste suhete kontekstis. Lucas Kello on tõdenud, et kübervaldkonna integreerimine rahvusvahelistesse suhetesse on vajalik efektiivsete poliitikate arendamiseks ning IKT-de kiire levik võimaldab uut moodi koostööd riikide ja mitte-riiklike toimijate vahel.[8] Ka Nicholas Thomas on tõdenud, et küberohtudega silmitsi seistes on riikidel vaja arvesse võtta rahvusvahelisel areenil tegutsevate riikide ja organisatsioonide meetmeid,[9] millest tulenevalt on üha enam vaja tähelepanu pöörata küberjulgeoleku poliitikate arendamisele ja nende uurimisele.

Kello on nentinud, et kübervaldkond mõjutab rahvusvaheliste suhete teooriaid kolmel viisil. Esiteks, informatsiooniajastu[10] IKT-d laienevad kaugemale traditsioonilisest „sõja" kontseptsioonist ja esitavad uusi väljakutseid julgeolekule. Teiseks, teadlased peavad kasutama olemasolevaid teooriaid, et kujundada, selgitada ja võimalusel ennustada konkureerivaid küberjulgeoleku suhteid. Kolmandaks, kuna otsuse langetamise pinge tõttu ei ole praktiseerijatel (näiteks poliitikutel) aega küberjulgeoleku teoreetiliseks tõlgendamiseks, siis on teadlaste kohustus rakendada ja kohaldada eksisteerivaid teooriaid kübervaldkonna sündmuste empiirilisele hindamisele. Seeläbi saavad uurijad juhtida küberjulgeoleku poliitikate kujundamist, et luua vajalik stabiilsus praegu prevaleeriva kaootilisuse asemele kübervaldkonnas.[11]

Magistritöö uudsuse tagab tõik, et varem ei ole nii põhjalikult küberjulgeolekustamist Eesti näitel uuritud ning küberjulgeolekustamise teoreetilist raamistiku on ainult üldiselt kirjeldatud. Magistritöö on ajendatud soovist arendada edasi Helen Nissenbaumi ja Hanseni küberjulgeolekustamise artiklit „Digital Disaster, Cyber Security, and the Copenhagen School" (2009), kus on analüüsitud küberjulgeolekustamist Kopenhaageni

[7] Kaska, Kadri, Anna-Maria Talihärm, and Eneken Tikk. 2010. „Developments in the Legislative, Policy and Organisational Landscapes in Estonia since 2007." In *International Cyber Security. Legal & Policy Proceedings*, eds. Eneken Tikk and Anna-Maria Talihärm. Tallinn: CCD COE Publications, 40.

[8] Kello, Lucas. 2013. „The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 2 (38): 8, 37-38. http://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00138#.U2eg0xBpeAE (kasutatud 05.02.2014)

[9] Thomas, Nicholas. 2009. „Cyber Security in East Asia: Governing Anarchy." *Asian Security* 5 (1): 19. http://dx.doi.org/10.1080/14799850802611446 (kasutatud 02.02.2014)

[10] Informatsiooniajastu on periood, mis algab 1970. aastatega ning viitab informatsiooni laiahaardelisele avaldamisele, tarbimisele ja sellega manipuleerimisele, eelkõige arvutite ja arvutivõrkude kaudu. The Free Dictionary'i koduleheküIg. http://www.thefreedictionary.com/information+age (kasutatud 09.04.2014)

[11] Kello. „The Meaning of the Cyber Revolution," 38-39.

koolkonna teooria alusel Eesti näitel, kuid ei ole empiirilist analüüsi läbi viidud.[12] Samas on küberjulgeolekustamist tõestatud ka empiiriliselt, näiteks Myriam Dunn Cavelty oma teosega „Cyber-Security and Threat Politics: US efforts to Secure the Information Age" (2008), kuid Cavelty, kes toetub küll Kopenhaageni koolkonnale, keskendub USA analüüsile.[13] Samuti käsitleb Forrest Hare oma kirjutises „The Cyber Threat to National Security: Why Can't we Agree?" (2010) küberjulgeolekustamist, millele ta rakendab küll Barry Buzani („People, States, and Fear", 1991) esitletud ohtude raamistikku, kuid ei uuri süvitsi küberjulgeolekustamist.[14]

Küberjulgeolekustamise teooria kohta on kirjutatud mitmeid bakalaureuse- ja magistritöid, milles on teoreetiliseks baasiks küll võetud Kopenhaageni koolkond, kuid Eestit on analüüsitud vaid põgusalt või üldse mitte. Lundi Ülikooli üliõpilane Ola Hjalmarsson on uurinud küberruumi julgeolekustamist oma bakalaureusetöös „The Securitization of Cyberspace: How the Web Was Won" (2013), kuid ta keskendub julgeolekustamise ja kõneakti teooria uurimisele USA näitel,[15] mida on teinud ka Catherine Elizabeth Hart oma 2012. aastal avaldatud magistritöös „Securing Freedom: A Media Framing Analysis of Cybersecuritization".[16] Sofia Lisa Dinesen ja Heidi Bruvik Sæther on kirjutanud magistritöö „Cyber Security – Securitizing Cyber Threats in Denmark" (2013), milles nad uurivad küberohtude julgeolekustamist Taanis.[17]

Katarina Klingova on uurinud küberjulgeolekustamist oma magistritöös „Securitization of Cyber Space in the United States of America, the Russian Federation and Estonia"

[12] Hansen, Lene, and Helen Nissenbaum. 2009. „Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly* 53 (4): 1155-1175. doi: 10.1111/j.1468-2478.2009.00572.x (kasutatud 04.04.2013)

[13] Cavelty, Myriam Dunn. 2008. *Cyber-Security and Threat Politics: US efforts to Secure the Information Age*. London; New York: Routledge.

[14] Hare, Forrest. 2010. „The Cyber Threat to National Security: Why Can't We Agree?" In *Conference on Cyber Conflict. Proceedings 2010*, eds. Christian Czosseck and Karlis Podins. Tallinn: CCD COE Publications.

[15] Hjalmarsson, Ola. 2013. „The Securitization of Cyberspace: How the Web Was Won." Bachelor's thesis. Lund University. http://www.lunduniversity.lu.se/o.o.i.s?id=24965&postid=3357990 (kasutatud 28.10.2013)

[16] Hart, Catherine Elizabeth, 2012. „Securing Freedom: A Media Framing Analysis of Cybersecuritization." Master's thesis. Simon Fraser University. http://summit.sfu.ca/item/12560 (kasutatud 01.11.2013)

[17] Dinesen, Sofia Lisa, and Heidi Bruvik Sæther. 2013. „Cyber Security – Securitizing Cyber Threats in Denmark." Master's thesis. Copenhagen Business School. http://studenttheses.cbs.dk/handle/10417/3949 (kasutatud 11.11.2013)

(2013) Eesti, Ameerika Ühendriikide ja Venemaa näitel sisuanalüüsi[18] meetodi abil. Klingova analüüsib ainult Eesti „Küberjulgeoleku strateegiat 2008-2013" ning kõrvutab seda USA ja Venemaa küberstrateegiatega, kuid ei uuri süvitsi küberjulgeolekustamist Eesti näitel.[19] Dennis Halvordsson on kirjutanud bakalaureusetöö teemal „Securitizing the Virturality of the Real: A Gramscian Analysis of the Securitization of U.S. Cyberspace Governance" (2012), milles on aluseks võetud küll Kopenhaageni koolkond, kuid on analüüsitud USA küberruumi julgeolekustamist Antonio Gramsci teooria[20] ja kriitilise diskursusanalüüsi (CDA)[21] abil.[22] Kuigi küberjulgeolekustamisele on mitmetes kirjatöödes tähelepanu pööratud, siiski ei ole loodud põhjalikku küberjulgeolekustamise teoreetilist raamistikku.

Uurimistöö jaguneb kuueks peatükiks, millest esimene peatükk on sissejuhatus, kus kaardistatakse üldine töö ülesehitus, eesmärgid ja uurimisküsimused, peamised allikad, magistritöö aktuaalsus ja taust ning varasem teemaga seotud kirjandus. Töö teises peatükis käsitletakse kübervaldkonna termineid Eesti näitel küberjulgeolekustamise uurimiseks ning analüüsitakse mõistete vahelisi seoseid ja probleeme oskussõnade defineerimisel. Magistritöö kolmandas peatükis luuakse teoreetiline raamistik küberjulgeoleku analüüsimiseks. Uuritakse Kopenhaageni koolkonna julgeolekusektoreid, julgeolekustamise teooriat, kõneakti lähenemist, julgeolekustava liigutuse/katse ja julgeolekupraktika eristust ning rakendatakse Kopenhaageni koolkonna teoreetilist raamistikku küberjulgeolekule, et vastata uurimisküsimusele, kuidas toimub küberjulgeolekustamine Kopenhaageni koolkonna teooria järgi.

---

[18] Sisuanalüüsi kui uurimismeetodi eesmärgiks on leida märgusõnu, millele auditoorium reageeriks, seega uurija kodeerib sõnu, lauseid või teemasid kategooriate abil. Balzacq, Thierry, ed. 2011. „Enquiries into Methods." In *Securitization Theory*, 50-52.

[19] Klingova, Katarina. 2013. „Securitization of Cyber Space in the United States of America, the Russian Federation and Estonia." Master's thesis. Central European University. http://www.etd.ceu.hu/2013/klingova_katarina.pdf (kasutatud 27.10.2013)

[20] Itaalia poliitiline filosoof Antonio Gramsci (1891-1937) on seotud „hegemooniaga", mida tuleks mõista kui üldist nõusolekut domineeriva sotsiaalse ja alluvate jõudude vahel domineeriva jõu huvidega kooskõlas oleva kuulekuse saavutamiseks. McNally, Mark, and John Schwarzmantel, eds. 2009. *Gramsci and Global Politics: Hegemony and Resistance*. London; New York: Routledge, 164-165, 168.

[21] Kriitilise diskursusanalüüsiga uuritakse, kuidas ideoloogia ja võimusuhted kujundavad diskursust, mis avaldab mõju sotsiaalsetele suhetele, identiteetidele ja uskumustele. Fairclough, Norman. 1999. *Discourse and Social Change.* Cambridge: Polity Press, 1-12. Kriitilise diskursusanalüüsi eesmärgiks on analüüsida diskursuse osa võimu kehtestamisel, taastootmisel ja domineerimisele väljakutsete esitamisel. Van Dijk, Teun A. 1993. „Principles of Critical Discourse Analysis." *Discourse & Society*, 4 (2), 249-250. doi: 10.1177/0957926593004002006 (kasutatud 03.03.2014)

[22] Halvordsson, Dennis. 2012. „Securitizing the Virtuality of the Real: A Gramscian Analysis of the Securitization of U.S. Cyberspace Governance." Bachelor's thesis. Gothenburg University. https://gupea.ub.gu.se/handle/2077/32833 (kasutatud 31.10.2013)

Töö neljandas peatükis analüüsitakse metodoloogiliselt aluseks võetud Hanseni poststrukturalistlikku diskursusanalüüsi. Samuti antakse ülevaade 2007. aasta küberrünnetest ja kontekstist nendele ning tehakse valikuid Hanseni poststrukturalistlikus uurimiskavas tekstide piiritlemiseks empiirilise peatüki jaoks. Poststrukturalistliku diskursusanalüüsi metodoloogiliste juhiste ja uurimiskava ning küberjulgeolekustamise teooria alusel piiritletakse julgeolekustajate ring 2007. aasta küberrünnete ajal ministrite tasemele ning sellest lähtuvalt ka tekstide ja allikate valik. Meetodi kaasamine analüüsi võimaldab luua koos küberjulgeolekustamise teooriaga sidusa raamistiku Eesti kaasuse uurimiseks teooria tõestamiseks.

Uurimistöö viies peatükk hõlmab empiirikat, milles analüüsitakse, kuidas rakendub väljatöötatud küberjulgeolekustamise teooria praktilisele juhtumile. Esmalt uuritakse diskursusanalüüsi valimit ning julgeolekustavat liigutust 2007. aasta küberrünnete ajal ministrite kõneaktides. Seejärel pööratakse tähelepanu julgeolekustava liigutuse sammu astunud julgeolekustajate julgeolekupraktikale. Analüüsi aluseks võetakse kübervaldkonnaga seotud Eesti valdkondlikud arengukavad, millega pannakse paika strateegilised eesmärgid, tegevusvaldkonnad ning meetmed nende saavutamiseks. Arengukavadest identifitseeritakse lubadust kaitsta referentobjekti ning ministrite julgeolekupraktikaid dokumentide koostamise ja vastuvõtmise kaudu. Küberjulgeolekuga seotud arengukavades määratletud meetmete täideviimist riigi poolt uuritakse reaalsuses ministrite kõneaktide (sõnavõtud, ettekanded ja arvamusartiklid) põhjal. Meetmete analüüs piiritletakse Eesti „Küberjulgeoleku strateegia 2008-2013" alusel küberjulgeoleku teadvustamisele. Töö viimases ehk kuuendas peatükis võetakse magistritöö olulisemad seisukohad kokku ning tehakse järeldusi ja ettepanekuid.

Olulisemad autorid, kelle põhjal kübervaldkonna terminoloogilist osa analüüsida, on Alexander Klimburg, Annegret Bendieko ja Andrew L. Porter. Kopenhaageni koolkonna teoreetilise baasi uurimiseks võetakse aluseks Buzani, Ole Wæveri, Jaap de Wilde'i, Hanseni ja John L. Austini teoreetiline käsitlus. Kopenhaageni koolkonna teooria edasiarenduse käsitlemiseks tuginetakse Stritzelile, Floydile ja Balzacqile. Küberjulgeolekustamise teoreetilise osa uurimiseks analüüsitakse Hare'i, Thomas'i, Nissenbaumi ja Hanseni käsitlusi ning metodoloogilises osas tuginetakse Balzacqile ja Hansenile. Empiirilise analüüsi läbiviimiseks toetutakse eelkõige Floydile, Hansenile ja Margaret Wetherellile ning Eesti „Küberjulgeoleku strateegiale 2008-2013".

2. KÜBERVALDKONNA MÕISTETE MÄÄRATLEMINE

Struktureerimise huvides analüüsitakse terminite peatükis ainult kübervaldkonna peamisi mõisteid ja nende omavahelised seoseid, mis on aluseks kogu magistritööle. Oskussõnad, mis ei ole otseselt seotud kübervaldkonnaga, määratletakse jooksvalt vastavas peatükis, kus nimetatud termin leiab põhjalikumat käsitlemist.

Kuigi kübervaldkond on muutunud tänapäeval üheks olulisemaks rahvusvaheliste suhete teemaks, ei ole siiani selgust kübervaldkonna oskussõnade osas. Informatsiooniajastul on saanud levinuks, et uusi termineid luuakse prefiksite „küber-", „arvuti-" või „informatsiooni-" lisamise abil. Küberjulgeoleku uudsuse tõttu on sellisel viisil loodud oskussõnadel nii palju tähendusi ja nüansse, et nad võivad muutuda segadusttekitavaks või kaotada oma tähenduse.[23] Kuigi kübervaldkonnas ei eksisteeri universaalseid definitsioone, esitab käesolev töö siiski määrangud, mis ühtlustatakse kogu ülejäänud magistritöö sõnakasutusega.

Definitsioonide määratlemiseks käsitletakse kitsamalt juhtumianalüüsi valiku tõttu Eesti määratlusi dokumendist „Küberjulgeoleku strateegia 2008-2013",[24] kuid samas tuleb silmas pidada, et 2014. aastal antakse välja „Küberjulgeoleku strateegia 2014–2017",[25] kus võivad olla täiendatud määrangud kübervaldkonnast. Laiemal tasandil kasutatakse defineeringute uurimiseks ja võrdlemiseks eelkõige Klimburgi toimetatud teost „National Cyber Security Framework Manual", mis annab põhjaliku ülevaate kübervaldkondade terminitest, kuid oluline on silmas pidada, et nimetatud raamat esindab ainult vastavate autorite arvamusi, mitte ei peegelda tingimata NATO CCD COE, NATO, mõne teise organisatsiooni või valitsuse arvamusi ja poliitikaid.[26]

Kübervaldkonna terminite analüüsimiseks kasutatakse ka Rahvusvahelise standardiorganisatsiooni (ISO) määratlusi, sest ISO standardid hõlmavad kõigile

[23] Cavelty, Myriam Dunn. 2008. „Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate." *Journal of Information Technology & Politics* 4 (1): 21. http://dx.doi.org/10.1300/J516v04n01_03 (kasutatud 24.12.2013)

[24] Küberjulgeoleku strateegia komisjon. 2008. *Küberjulgeoleku strateegia 2008-2013*. Tallinn: Kaitseministeerium. http://valitsus.ee/et/valitsus/arengukavad (kasutatud 31.10.2013)

[25] „Küberjulgeoleku strateegia 2014–2017" koostamise ettepaneku heakskiitmine. 2013. Riigi Teataja III, 2013, 9. https://www.riigiteataja.ee/akt/326032013009 (kasutatud 20.02.2014)

[26] Klimburg, Alexander, ed. 2012. *National Cyber Security Framework Manual*. Tallinn: NATO CCD COE Publications.

inimestele ühiselt mõistetavaid reegleid, määranguid ja tehnilisi spetsifikatsioone.[27] Definitsioonide peatükis tuginetakse ka ÜRO spetsialiseeritud allasutuse Rahvusvahelise Telekommunikatsiooni Liidu määratlustele, sest ITU on spetsialiseerunud IKT-dele,[28] mis on ka käesolevas magistritöös arutluse all. Küberrünnete klassifitseerimiseks võetakse eelkõige aluseks Bendieki ja Porteri käsitlus, sest nad esitavad väga argumenteeritud põhjenduse küberrünnete liigitamiseks.

2.1. Kübervaldkonna mõistele aluseks olevad terminid

Enne küberjulgeoleku, küberkaitse ja teiste kübervaldkonna oskussõnade määratlemist on oluline defineerida terminid „küberruum", „IKT" ja „informatsiooni- ja kommunikatsioonisüsteemid" (CIS), sest nimetatud definitsioonid esinevad erinevates kübervaldkonna kaitse ja julgeolekuga terminites.

Eesti küberjulgeoleku strateegia defineerib küberruumi arvutitel ja arvutisüsteemidel põhineva digitaalse ruumina, mis koosneb Interneti[29] tegevuskeskkondadest ja andmekogudest.[30] ITU aga määratleb küberruumi palju laiemalt, tõdedes, et küberrruum on Internetiga seotud IKT-d, millesse on süsteemid ja teenused ühendatud.[31] Lähtuvalt ITU definitsioonist on IKT-d audiovisuaalsed (raadio, televisioon jms) ja telefoni- ning arvutivõrgud,[32] seega küberruum ei ole seotud ainult arvutitega, vaid ka teiste tehnoloogiatega. ITU määratleb küberruumi osadena kasutajaid, võrke, vahendeid[33],

[27] ISO/IEC JTC 1/SC 27. 2012. „ISO/IEC 27032:2012. Information Technology – Security Techniques – Guidelines for Cybersecurity." https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en (kasutatud 05.01.2014)

[28] ITU. 2008. *Series X: Data Networks, Open System Communications and Security: Overview of Cybersecurity. Recommendation X.1205*. ITU-T Publications, ii. http://www.itu.int/rec/T-REC-X.1205-200804-I (kasutatud 21.04.2014)

[29] On oluline eristada Internetti (*the Internet*) internetist (*an internet*). ISO standardi järgi on Internet omavahel ühendatud võrkude globaalne süsteem avalikus domeenis ning internet on omavahel seotud võrkude kogu. ISO/IEC JTC 1/SC 27. „ISO/IEC 27032:2012. Information Technology." Autori märkus: Magistritöös kasutatakse läbivalt terminit „Internet".

[30] Küberjulgeoleku strateegia komisjon. *Küberjulgeoleku strateegia 2008-2013*, 41.

[31] Wamala, Frederick. 2011. *ITU National Cybersecurity Strategy Guide*. Geneva: ITU, 5. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf (kasutatud 05.02.2014)

[32] ITU kodulehekülg. http://www.itu.int/en/better-future/Pages/default.aspx (kasutatud 21.04.2014)

[33] Autori märkus: Vahendite all võib ITU definineeringute järgi mõista riistvara. Arvuti riistvara viitab arvuti füüsilistele osadele ja nendega seotud vahenditele. Sisemised riistvara vahendid on kõvakettad jms ning välised riistvara vahendid on monitorid, klaviatuurid, hiired, printerid ja skannerid. TechTerms.com kodulehekülg. http://www.techterms.com/definition/hardware (kasutatud 23.03.2014)

tarkvara[34], protsesse, informatsiooni, rakendusi, teenuseid ja süsteeme, mis on otseselt või kaudselt ühendatud võrkudesse.[35] Küberruumi sees olevad süsteemid on CIS, mis toetavad riigi kriitilise infrastruktuuri (KI) toimimist.[36]

ITU on tõdenud, et lisaks füüsilisele infrastruktuurile (ehitised, teed ja torud) toetavad nii küberruum, IKT-d kui ka CIS kriitilist infrastruktuuri, mis on peamised süsteemid, ja teenused, mille häirimine või hävitamine on nõrgestava mõjuga avalikkuse turvalisusele, tervisele, kaubandusele ja julgeolekule. Peamised KI sektorid on tervis, vesi, transport, kommunikatsioonid, valitsus, energia, toit, rahandus ja hädaabiteenused.[37] Nii CIS kui IKT-d on küberruumi osad ja toetavad KI toimimist.

Sarnaselt ITU määrangule tõdetakse ISO standardi küberruumi defineeringus, et küberruumile on omane inimeste koostoime,[38] mida tõstetakse esile ka teoses „National Cyber Security Framework Manual", kus lisaks inimeste rollile rõhutatakse ka kommunikatsiooni.[39] Ka Suurbritannia rõhutab suhtlust oma 2009. aasta strateegias „Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space", kus tõstetakse esile asjaolu, et küberruum hõlmab ka sisu ja tegevusi võrkudes.[40] Kui valitsus rõhutab sisu küberruumi defineeringus, siis saab täidesaatev võim ette võtte meetmeid inimeste vastuvõetamatute käitumisviisidega tegelemiseks, näiteks Internetile tsensuuri kehtestamise või kõne- ja väljendusvabaduse piiramise kaudu.[41] Sellest tulenevalt ei käsitleta uurimistöös küberruumi mõiste osana sisu, mille kaasamine defineeringusse loob võimaluse piirata infolevi küberruumis.

Kübervaldkonna kaitse ja julgeoleku definitsioonidele aluseks olevad terminid tähistavad küll erinevaid küberruumi osi või kogumeid, kui ei ole lõpuni selgepiirilised, sest võivad tihti ka omavahel kattuda. Sellest tulenevalt on oluline käesoleva uurimistöö kontekstiks omaks võtta kindel küberruumi defineering. Küberruumi osadeks on kasutajad, IKT-d (audiovisuaalsed, telefoni- ja arvutivõrgud), vahendid (riistvara),

[34] Tarkvara on toote osa, mis on arvutiprogrammid või nende kogu. ISO/IEC JTC 1/SC 7. 2004. „ISO/IEC 18019:2004. Software and System Engineering – Guidelines for the Design and Preparation of User Documentation for Application Software." https://www.iso.org/obp/ui/#iso:std:iso-iec:18019:ed-1:v1:en (kasutatud 23.03.2014)
[35] ITU. *Series X*, ii.
[36] Küberjulgeoleku strateegia komisjon. *Küberjulgeoleku strateegia 2008-2013*, 41.
[37] Wamala. *ITU National Cybersecurity*, 25.
[38] ISO/IEC JTC 1/SC 27. „ISO/IEC 27032:2012. Information Technology."
[39] Klimburg. *National Cyber Security*, 8.
[40] UK Cabinet Office. 2009. *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space*. Norwich: The Stationery Office, 7.
[41] Klimburg. *National Cyber Security*, 8-9.

tarkvara, protsessid, informatsioon, rakendused, teenused ja CIS, mis on ühendatud võrkudesse, kuid ei keskendu kommunikatsioonile ja sisule. Kriitilise infrastruktuuri toimimist toetavad nii küberruum kui ka selle sees olevad IKT-d ja CIS.

2.2. Julgeoleku ja kaitse terminid kübervaldkonnas

Küberjulgeolekust rääkides kasutatakse tihti vaheldumisi mõisteid „küberjulgeolek" (*cyber security*) ja „küberkaitse" (*cyber defence*)[42] ning „küberjulgeolek" ja „infoturve" (*information security*, infosec),[43] kuid neil terminitel tuleb vahet teha.

Selleks, et uurida küberjulgeolekut kui eraldi julgeolekusektorit ja analüüsida küberjulgeolekustamise protsessi, on vaja pöörata tähelepanu küberjulgeoleku terminile. Riigid defineerivad küberjulgeolekut erinevalt oma riiklikes strateegiadokumentides,[44] seega käesolevas töös käsitletakse Eesti määratlust küberjulgeolekust. „Küberjulgeoleku strateegia 2008-2013" järgi hõlmab küberjulgeoleku mõiste kõiki riigi julgeolekuga seotud elektroonilise teabe, teabekandjate ja -teenustega seotud toiminguid, eesmärgiga vähendada küberruumi haavatavust[45], ennetada küberründeid ning taastada rünnete korral võimalikult kiiresti süsteemide toimimine.[46]

Käesolevas magistritöös tuginetakse ITU määrangule, mis defineerib küberjulgeolekut märksa laiemalt kui Eesti küberjulgeoleku strateegia, määratledes küberjulgeolekut vahendite, poliitikate, julgeolekukontseptsioonide, juhiste, riskijuhtimise lähenemiste, meetmete, väljaõppe, praktikate ja tehnoloogiate kogumina küberruumi kaitseks.[47] ITU määrang sobib kokku töös Kopenhaageni koolkonna teoreetilise raamistikuga, mis keskendub meetmetele ja praktikatele, mida käsitletakse teooria peatükis.

Eesti küberjulgeoleku strateegia järgi on küberkaitse riigi kriitilise infrastruktuuri toimimist toetava CIS kaitse korraldamine, mis seisneb infotehnoloogiliste,

---

[42] Näiteks: Sulbi, Raul. 2011. „Ilves: Venemaa pole küberkaitse lepingutega ühinenud." *Postimees* 06. veebruar. http://www.postimees.ee/383820/ilves-venemaa-pole-kuberkaitse-lepingutega-uhinenud (kasutatud 10.02.2014); Kross, Eerik-Niiles. 2011. „Eerik-Niiles Kross: küünteta kübertiiger," *Postimees* 13. aprill. http://arvamus.postimees.ee/418624/eerik-niiles-kross-kuunteta-kubertiiger (kasutatud 10.02.2014)

[43] Küberjulgeoleku strateegia komisjon. *Küberjulgeoleku strateegia 2008-2013*, 5, 30.

[44] Klimburg. *National Cyber Security*, 12.

[45] ISO standardi järgi on haavatavus varade või juhtimissüsteemide nõrkus, mida võidakse ohuallika poolt ära kasutada. ISO/IEC JTC 1/SC 27. „ISO/IEC 27032:2012. Information Technology."

[46] Küberjulgeoleku strateegia komisjon. *Küberjulgeoleku strateegia 2008-2013*, 40.

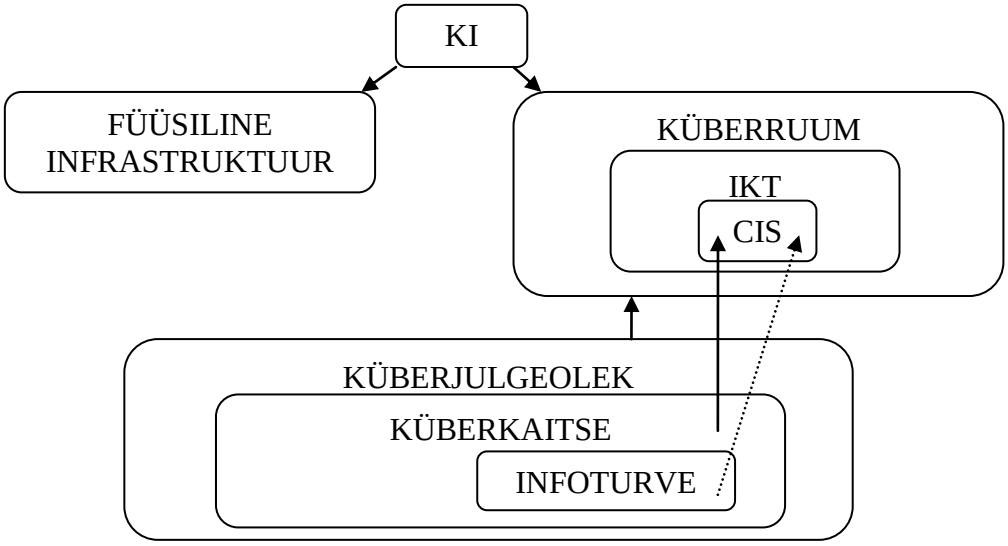
[47] ITU. *Series X*, ii.

organisatoorsete ja füüsiliste turvameetmete kasutuselevõtmises.[48] NATO defineerib küberkaitset võimena kaitsta teenuste kohaletoimetamist CIS-is, et reageerida küberruumist tulenevatele ohtudele,[49] lähtudes andmete konfidentsiaalsuse, terviklikkuse ja kättesaadavuse ning informatsiooni kaitsest.[50] Käesolevas magistritöös võetakse aluseks NATO määratlus, defineerides küberkaitset CIS kaitsena informatsiooni ja CIS terviklikkusest, konfidentsiaalsusest ja kättesaadavusest lähtuvalt. Küberjulgeolek on seega märksa laiem mõiste kui küberkaitse, sest ta ei sisalda endas ainult tehnilisi aspekte, vaid hõlmab ka muid teemasid, mis on kaetud riiklikes strateegiates.

Konfidentsiaalsuse, tervikluse ja käideldavusega on seotud ka termin „infoturve", mis on Eesti küberjulgeoleku strateegia järgi küberjulgeoleku tagamise aluseks, luues ja rakendades turvameetmeid.[51] Termin „küberjulgeolek" ulatub seega kaugemale infoturbest,[52] sest infoturve, mis teenib tarbijate vajadusi andmete konfidentsiaalsusest, käideldavusest ja terviklusest lähtuvalt, keskendub ainult informatsioonile ISO standardi määratluse järgi.[53] Infoturve on seega kitsam termin kui küberkaitse, sest infoturve keskendub ainult informatsioonile, kuid küberkaitse keskendub CIS-ile, mille sees informatsioon asetseb.

Joonis 1 annab ülevaate kübervaldkonna mõistete omavahelistest seostest ning illustreerib magistritöös omaksvõetud definitsioonide käsitlust. Mõistete peatükis käsitletud oskussõnadest on kõige laiem termin küberjulgeolek, sest küberjulgeolek tegeleb küberruumi kaitsega, mille osaks on ka CIS ja IKT-d. Küberkaitse keskendub ainult CIS-i ning infoturve ainult informatsiooni kaitsele, mistõttu on infoturve ainult osaliselt CIS-iga seotud.

[48] Küberjulgeoleku strateegia komisjon. *Küberjulgeoleku strateegia 2008-2013*, 41.
[49] Vázquez, Diego Fernández, Oscar Pastor Acosta, Christopher Spirito, Sarah Brown, and Emily Reid. 2012. „Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships." In *4th International Conference on Cyber Conflict. Proceedings 2012*, eds. Christian Czosseck, Rain Ottis and Katharina Ziolkowski. Tallinn: NATO CCD COE Publications, 430.
[50] Klimburg. *National Cyber Security*, 13; Hallingstad, Geir, and Luc Dandurand. 2010. *Cyber Defence Capability Framework – Revision 2. Reference Document RD-3060*. The Hague: NATO C3 Agency.
[51] Küberjulgeoleku strateegia komisjon. *Küberjulgeoleku strateegia 2008-2013*, 8; 39.
[52] Klimburg. *National Cyber Security*, 12.
[53] ISO/IEC JTC 1/SC 27. „ISO/IEC 27032:2012. Information Technology."



Joonis 1. Kübervaldkonna terminite omavahelised seosed

Küberkaitse on seega küberjulgeoleku osa, millest tulenevalt kasutatakse käesolevas magistritöös läbivalt küberjulgeoleku terminit ning ainult spetsiifilisematel juhtudel mõistet „küberkaitse".

2.3. Küberrünnete klassifikatsioon

Kübervaldkonna ohtude analüüsimiseks Kopenhaageni koolkonna teooria raames on oluline defineerida termin „küberrünne" ning esitleda küberrünnete klassifikatsioon, et rääkida eksistentsiaalsetest ohtudest küberjulgeolekule.

2.3.1. Küberründe definitsioon

Raamatus „National Cyber Security Framework Manual" on juhitud tähelepanu tõigale, et kui hakatakse arutama küberrünnete liike, siis on enne oluline selgitada, mida küberründe all mõeldakse. Termin „küberrünne" omandab erinevaid tähendusi lähtuvalt sellest, kuidas erinevad institutsioonid soovivad julgeolekuohtudele reageerida, seega on oluline konkreetses kontekstis ära määratleda küberrünnete tähendus. Sõdurid peavad ründeid jõu kasutamiseks, kuid õiguskaitseorganid (politsei ja prokurörid) kirjeldavad ründeid kuritegevusena. Tehnilised eksperdid kasutavad mõistet

„küberrünne" iga pahatahtliku katse kohta konfidentsiaalsuse või kättesaadavuse vastu.[54]

Eesti küberjulgeoleku strateegia järgi on küberrünne arvutisüsteemi vahendusel toime pandud rünne arvutisüsteemi või selles sisalduvate andmete vastu,[55] mida tõdeb ka Marie Harbo Dahle.[56] Samas on nimetatud määratlused on liiga kitsad lähtuvalt eelnevates alapeatükkides omaks võetud küberruumi ja küberjulgeoleku definitsioonidest, sest keskenduvad ainult arvutile, mitte teistele tehnoloogiatele. Märksa laiemalt on küberründeid määratlenud Uma ja Padmavathi, kes on defineerinud küberrünnet kui indiviidide ebaeetilist praktikat (näiteks luuramine, andmete varastamine) tehnoloogiate kasutamiseks teiste ekspluateerimiseks küberruumis, eesmärgiga omandada volitamata ligipääsu informatsioonile.[57] Sellest tulenevalt võetakse käesolevas uurimistöös aluseks Uma ja Padmavathi definitsioon küberründest. Ajakirjanduses, teadustöödes ja kõnedes võib näha terminite „küberrünne" ja „küberoht" sünonüümidena kasutamist, mis on õigustatud, sest küberrünne ja küberoht viitavad samadele asjadele,[58] seega kasutatakse käesolevas uurimistöid mõlemaid termineid eksistentsiaalsete ohtude tähenduses.

2.3.2. Küberrünnete liigid

Bendiek ja Porter on jaganud küberründed kolmeks liigiks: küberkuritegevus, küberspionaaž ja kübersõda, kuid nad rõhutavad, et tavaliselt eristatakse nelja kategooriat, kust on välja jäetud küberspionaaž, kuid on lisaks eristatud termineid „küberterrorism" ja „kübervandalism".[59] Käesolevas magistritöös võetakse aluseks

[54] Klimburg. *National Cyber Security*, 17.
[55] Küberjulgeoleku strateegia komisjon. *Küberjulgeoleku strateegia 2008-2013*, 41.
[56] Dahle, Marie Harbo. 2012. „Cyber-Attacks: A Short Guide." In *The Growing Cyber-Threat: What Role for the Transatlantic Alliance?* The Atlantic Treaty Association. *Atlantic Voices* 2 (5): 2. http://issuu.com/atlantic_treaty_association/docs/vol._2__no._5__may_2012_ (04.02.2014)
[57] Uma, M., and G. Padmavathi. 2013. „Survey on Various Cyber Attacks and their Classification". *International Journal of Network Security*, 15 (6): 391. http://ijns.femto.com.tw/contents/ijns-v15-n5/ijns-2013-v15-n5-p390-396.pdf (03.02.2014)
[58] Akcadag, Emine. 2012. „NATO and the Fight Against the Cyber-Threat." In *The Growing Cyber-Threat: What Role for the Transatlantic Alliance?* The Atlantic Treaty Association. *Atlantic Voices* 2 (5): 4. http://issuu.com/atlantic_treaty_association/docs/vol._2__no._5__may_2012_ (04.02.2014)
[59] Bendiek *et al*. „European Cyber Security Policy," 158.

nende kahe määratluse süntees ehk jagumine viieks kategooriaks: küberkuritegevus, -vandalism, -spionaaž, -sõda ja -terrorism.

Raamatus „National Cyber Security Framework Manual" konstateeritakse, et küberkuritegevuse definitsioonid erinevad piirkonniti, kuid küberruumis läbiviidud pettused, vargused ja teised varadega seotud ebaseaduslikud tegevused on üsna levinud komponendid küberkuritegevuse määratlustes.[60] Seda võib märgata ka Bendieki ja Porteri määratlusest, kus identifitseeritakse küberkuritegevusena intellektuaalse vara vargust, väljapressimist DDoS rünnete abil ja identiteedivarguse pettust küberruumis.[61] Jagatud teenusetõkestamise (DDoS) rünne on sissetungimine süsteemi, kavatsusega takistada volitatud kasutaja ligipääsu teenusele võrkude keelamisega.[62] Ka ISO standardi järgi on küberkuritegevus kriminaliseeritud teod (väär- ja kuriteod) küberruumis, kus küberruumi või selle teenuseid ja rakendusi kasutakse kuritegevuse vahendina või sihtmärgina,[63] et ekspluateerida kasutajaid materialistliku kasu saamiseks (näiteks krediitkaardi pettus).[64] Magistritöös defineeritakse küberkuritegevust kriminaliseeritud tegevusena küberruumis materiaalse kasu eesmärgil.

Lisaks küberkuritegevusele on küberrünnete liigiks ka küberterrorism. Uma and Padmavathi on tõdenud, et küberterrorism on küberruumi kasutamine suureulatusliku katkestuse või hävingu loomiseks elule ja varale (näiteks veevarude mürgitamine),[65] kuid Cavelty on täpsustanud küberterrorismi terminit, defineerides seda terroristide poolt läbiviidud ründena, millega sisestatakse hirmu või põhjustatakse märkimisväärset kahju poliitilistest, religioossetest või ideoloogilistest põhjustest lähtuvalt.[66] Ka Dorothy Denning on rõhutanud, et küberterrorismil on poliitiline motivatsioon, millest ajendatuna tahetakse põhjustada märkimisväärset kahju elu kaotuse või raske majanduslik kahju läbi (näiteks kahe lennuki kokkupõrke korraldamine).[67] Kuna Dorothy määratleb motivatsioone mõnevõrra kitsamalt kui Cavelty, siis võetakse uurimistöös võetakse omaks Cavelty definitsioon küberterrorismist, sest

[60] Klimburg. *National Cyber Security*, 15.
[61] Bendiek *et al*. „European Cyber Security Policy," 158.
[62] Uma *et al*. „Survey on Various Cyber Attacks," 396.
[63] ISO/IEC JTC 1/SC 27. *„ISO/IEC 27032:2012. Information Technology."*
[64] Uma *et al*. „Survey on Various Cyber Attacks," 396.
[65] Ibid., 396.
[66] Cavelty. „Cyber-Terror-Looming Threat or Phantom Menace,"19.
[67] Denning, Doroty E. 2001. „Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." In *Networks and Netwars: The Future of Terror, Crime, and Militancy*, eds. John Arquilla and David Ronfeldt. Rand Corporation, 241.

küberterrorismil peab olema religioosne, ideoloogiline või poliitiline motivatsioon märkimisväärse kahju tekitamiseks.

Küberründe üheks liigiks on küberspionaaž, mis on sissemurdmised või volitamata ligipääs infole või CIS-ile,[68] eesmärgiga teha väljavõte tundlikust või kaitstud informatsioonist[69] kasusaamise eesmärgil.[70] Küberründeks on ka kübervandalism, mis on „skriptijuntsu" (*script kiddies*) poolne veebilehekülgede moonutamine lõbu eesmärgil, keda võib seetõttu pidada vandaaliks.[71] „Skriptijuntsud" on seega mitte-tõsiseltvõetavad häkkerid[72], kes hülgavad eetilised printsiibid (teadmise ja oskuste omandamise soov), mida järgivad professionaalsed häkkerid ning kasutavad tihti häkkerite kirjutatud programme oskuste puuduse tõttu.[73]

2007. aasta küberrünnetega Eesti vastu tõusis meedias esile termin „kübersõda",[74] mistõttu tuleks kübersõja termin enne kasutamist ära defineerida. Oskussõna „kübersõda" kasutamisel tuleb olla ettevaatlik ja täpne mitmete põhjuste tõttu. Esiteks on raske määratleda, mis tegevused moodustavad kübersõja küberrünnete uudsuse tõttu.[75] Teiseks, termin „kübersõda", mis keskendub riikidevahelistele konfliktidele küberruumi sees ja kaudu, on ambivalentne ja vastuoluline termin. Sellest tulenevalt ei eksisteeri üldiselt aktsepteeritud kübersõja definitsiooni, mistõttu terminit „kübersõda" ei kasutata ametlikes dokumentides.[76]

Thomas Rid on tõdenud, et siiani ei ole ühtegi kübersõda toimunud, ei leia aset ka olevikus ning tõenäoliselt ei ilmne ka tulevikus, kui järelliide „-sõda" on korrektselt defineeritud. Sõja määratlusest lähtuvalt võib kübersõda defineerida surmava ehk vägivaldse vahendi ehk instrumendina ning poliitilise jõuaktina, mis viiakse läbi

---

[68] Klimburg. *National Cyber Security*, 16.

[69] Rid, Thomas. 2012. „Cyber War will not take Place." *Journal of Strategic Studies* 35 (1): 20. http://dx.doi.org/10.1080/01402390.2011.608939 (kasutatud 15.04.2013)

[70] Uma *et al*. „Survey on Various Cyber Attacks," 396.

[70] Küberjulgeoleku strateegia komisjon. *Küberjulgeoleku strateegia 2008-2013*, 41.

[71] Bendiek *et al*. „European Cyber Security Policy," 158.

[72] ISO standardi järgi tegelevad häkkimisega häkkerid, et omandada tahtlikult ligipääsu süsteemidele ilma kasutaja või omaniku loata. ISO/IEC JTC 1/SC 27. *„ISO/IEC 27032:2012. Information Technology."*

[73] Technopedia.com kodulehekülg. http://www.techopedia.com/definition/4090/script-kiddie (kasutatud 14.03.2014)

[74] Näiteks Ellam, Haldi. 2007. „Ansip: Eestis katsetati kübersõda." *Eesti Päevaleht* 30. mai. http://www.epl.ee/news/eesti/ansip-eestis-katsetati-kubersoda.d?id=51088956 (kasutatud 29.12.2013)

[75] Mahnken, Thomas G. 2011. „Cyber War and Cyber Warfare." In *America's Cyber Future: Security and Prosperity in the Information Age*, eds. Kristin M. Lord and Travis Sharp. Washington, D.C.: Center for a New American Security, 58, 60.

[76] Klimburg. *National Cyber Security*, 17.

küberruumis.[77] Sõda võib seega mõista kui riikidele antud monopoli kasutada legitiimselt vägivalda, kuid küberruumis ei ole vägivalda samal viisil nagu füüsilises konfliktis.[78] Ka Bendiek ja Porter on tõdenud, et kübersõda on riigi püüe rünnata teist riiki võrkude läbi,[79] kuid autorid määratlevad keskkonnana ainult võrgud, mitte küberruumi tervikuna. Magistritöös võetakse osaliselt omaks raamatu „National Cyber Security Framework Manual" määratlus, mida põimitakse Ridi defineeringuga kübersõjast, et rõhutada vägivalla, instrumentaalsuse ja poliitilisuse komponenti.

2.4. Takistused kübervaldkonna terminite defineerimisel

Nagu eespool mainitud, siis kübervaldkonna definitsioonide osas valitseb siiani segadus ning ei eksiteeri universaalseid määratlusi. On mitmeid põhjuseid, mis riigid ei suuda kokku leppida kõikehõlmavates definitsioonides. Näiteks USA, Suurbritannia ja mitmed teised riigid on näidanud suurenenud tahet pühenduda koos Venemaa ja Hiinaga küberjulgeoleku probleemidele, kuid seda on väga raske saavutada kuna puuduvad ühiselt kokkulepitud määratlused küberjulgeoleku kohta. Peamiste toimijate (USA, Suurbritannia, Venemaa ja Hiina) defineeringud „kübersõjast", „küberrünnetest" ja teiste kübervaldkonna terminitest ei ühti, isegi kui ametlikud või üldiselt tunnustatud määrangud eksisteerivad vastavates keeltes.[80]

Kui rääkida küberjulgeoleku definitsioonist, siis üheks takistuseks küberjulgeoleku määratlemisel on tõik, et küberjulgeolek sisaldab väga erinevaid tehnoloogiaid, strateegiaid ja sektoreid.[81] Küberjulgeolekut on väga raske universaalselt defineerida, sest küberjulgeolek on seotud nii paljude erinevate aspektidega, mida on juba algselt raske kõikehõlmavalt määratleda. Näiteks on keeruline defineerida küberjulgeolekule aluseks olevat terminit „küberruum", sest see on inimeste poolt loodud ja pidevalt

[77] Rid. „Cyber War," 5, 15.
[78] Barnard-Wills, David. 2011. „This is not a Cyber War, its a…? Wikileaks, Anonymous and the Politics of Hegemony." In *Proceedings of the 10th European Conference on Information Warfare and Security*, ed. Rain Ottis. Tallinn: Tallinn University of Technology, 20.
[79] Bendiek *et al*. „European Cyber Security Policy," 158.
[80] Giles, Keir, and William Hagestad II. 2013. „Divided by a Common Language: Cyber Definitions in Chinese, Russian and English." In *5th International Conference on Cyber Conflict. Proceedings 2013*, eds. Karlis Podins, Jan Stinissen and Markus Maybaum. Tallinn: NATO CCD COE Publications.
[81] Carleton, Jarad. 2012. *Cybersecurity: A Global Economic Security Crisis*. Frost & Sullivan, 4. http://www.frost.com/reg/file-get.do?id=2958781&file=1 (kasutatud 03.03.2014)

laienev keskkond, seega muutuvad ka küberruumi definitsioonid,[82] mis süvendab veelgi terminite määratlemise probleeme. Ühiste defineeringute leidmist takistab ka asjaolu, et küberjulgeoleku tarnijatel ja teenusepakkujatel on erinevad küberjulgeoleku definitsioonid.[83] Ka teoses „Cyber Security Policy Guidebook" on nenditud, et isegi neil, kes töötavad julgeoleku ametikohtadel, on erinevad küberjulgeoleku määratlused, mis sõltub nende tööga seotud küberruumi komponendist.[84]

Samuti ei ole kübersõjal siiani kindlat defineeringut, sest riikidel puudub tahe kokku leppida ühises määrangus, mis võiks vähendada nende võimekust tegutseda kübervaldkonnas või nõuda neil soovimatute meetmete ettevõtmist.[85] Näiteks Venemaa ja Hiina doktriinid rõhutavad väga erinevaid julgeoleku ohtusid Suurbritannia ja USA omadest,[86] mis mõjutab nende suhtumist, sest riigid tajuvad endale suunatud ohte erinevalt.

Lisaks põhjustab raskusi spetsiifiliste terminite otsetõlked vene ja hiina keelest, mis sarnanevad ingliskeelsetele terminitele ning vastupidi. See võib aga anda väära arusaama vastastikkusest arusaamisest, kuid tegelikult viidatakse erinevatele kontseptsioonidele.[87] Kokkuleppe saavutamist riikide vahel takistavad ka filoloogilised probleemid, sest tõlkeid ühest keelest teise ei saa teha vahetult, vaid tuleb arvesse võtta keelelisi eripärasid. Näiteks 2011. aastal tehti Ida-Lääne Instituudi (EWI)[88] poolt algatus otsida konsensust Venemaa ja Ameerika terminoloogias, kuid EWI püüe osutus illusiooniks kuna kokkulepitud definitsioonid erinevates keeltes ei sobinud üksteisega kokku.[89] Kuigi riigid on püüdnud maha istuda, et saavutada kokkulepe kübervaldkonna definitsioonide osas, on siiski olnud takistuseks keelelised probleemid.

Riigid tajuvad, et kübervaldkond on üha olulisem aspekt rahvusvahelistes suhetes, mistõttu on oluline selles valdkonnas koostööd teha. Samas osutub koostöö keeruliseks, kui ei ole paika pandud terminoloogiat, mis on aluseks lepingutele, kokkulepetele,

[82] Klimburg. *National Cyber Security*, 9.
[83] Carleton. *Cybersecurity*, 5.
[84] Bayuk, Jennifer L. *et al*. 2012. *Cyber Security Policy Guidebook*. Hoboken: Wiley, 1.
[85] Barnard-Wills. „This is not a Cyber War," 19.
[86] Giles *et al*. „Divided by a Common Language."
[87] Ibid.
[88] 1980. aastal asutatud Ida-Lääne Instituut, mille kontorid asuvad New Yorgis, Brüsselis, Moskvas ja Washingtonis, on rahvusvaheline erapooletu organisatsioon, mille eesmärgiks on tegeleda regionaalset ja globaalset stabiilsust häirivate probleemidega. EastWest Institute'i koduleheküIg. http://www.ewi.info/ (kasutatud 03.03.2014)
[89] Giles *et al*. „Divided by a Common Language."

dokumentidele ja kohtumistele. Ka käesoleva magistritöö kontekstis on tähtis omaks võtta kindlad määratlused, millele pööratakse tähelepanu järgnevas alapeatükis.

2.5. Magistritöös aluseks võetud terminoloogiline baas

Tabelis 1 on toodud kübervaldkonna põhiterminid ning uurimistöös omaksvõetud määrangud, millele tugineb kogu edaspidine analüüs.

Tabel 1. Kübervaldkonna põhiterminite kasutatavad defineeringud magistritöös

Termin	Uurimistöös kasutusel olevad määratlused
Küberruum	Küberruumi osad on kasutajad, IKT-d (audiovisuaalsed, telefoni- ja arvutivõrgud), vahendid (riistvara), tarkvara, protsessid, info, rakendused, teenused ja CIS, mis on otseselt või kaudselt ühendatud võrkudesse.
IKT	Audiovisuaalsed, telefoni- ja arvutivõrgud, mis on aluseks küberruumile.
Küber-julgeolek	Vahendite, poliitikate, julgeolekukontseptsioonide, juhiste, riskijuhtimise lähenemiste, meetmete, väljaõppe, praktikate ja tehnoloogiate kogum küberruumi kaitseks.
Küberkaitse	CIS ja kitsamalt informatsiooni kaitse terviklikkusest, konfidentsiaalsusest ja käideldavusest lähtuvalt.
Küberrünne	Tehnoloogia abil teiste ekspluateerimine (andmete ja info tervikluse ja autentsuse häirimine), eesmärgiga omandada ligipääsu volitamata infole.
Küberkuri-tegevus	Kriminaliseeritud teod küberruumis materiaalsest kasust lähtuvalt, näiteks intellektuaalse vara vargus, DDoS ründed, idenditeedivargus.
Küber-terrorism	Terroristlikud aktid küberruumis märkimisväärse kahju tekitamiseks religioossetest, ideoloogilistest või poliitilistest sihtidest lähtuvalt.
Küber-vandalism	„Skriptijuntsude" poolne veebilehekülgede moonutamine lõbu eesmärgil.
Kübersõda	Riikidevaheline surmav, instrumentaalne ja poliitiline sõda küberruumis.

Tabelis 1 olevatest mõistetest kasutatakse magistritöös eelkõige oskussõnu „küberruum", „-julgeolek" ja „-rünne" ning küberrünnete liike. Terminoloogiline osa on käesoleva töö uurimisküsimustest lähtuvalt oluline küberjulgeolekustamise protsessi analüüsimiseks, kus on vaja määratleda küberruumis eksisteerivad eksistentsiaalsed ohud jne. Definitsioonide peatükis analüüsitud terminid on aluseks eelkõige teoreetilisele ja ka empiirilisele peatükile, et analüüsida Eestis toimunud küberründeid.

3. TEOREETILINE RAAMISTIK

Teooria peatüki eesmärgiks on uurida Kopenhaageni koolkonna[90] julgeolekusektoreid, julgeolekustamise teooriat[91], kõneakti käsitlust ning julgeolekustava liigutuse ja julgeolekupraktika eristust kübervaldkonna analüüsiks. Selle abil on võimalik vastata magistritöö uurimisküsimusele, kuidas toimub teoreetilises plaanis küberjulgeolekustamine Kopenhaageni koolkonna teooria järgi.

3.1. Julgeolekusektorid Kopenhaageni koolkonna järgi

Küberjulgeoleku uurimiseks eraldi julgeolekusektorina[92] tuleb analüüsida Kopenhaageni koolkonna sektoriaalset jaotust sõjaliseks, poliitiliseks, majanduslikuks, sotsiaalseks ja keskkonnasektoriks,[93] mille pinnalt on võimalik analüüsida ka küberjulgeolekut eraldi sektorina. Kopenhaageni kookond on eristanud just need viis sektorit julgeoleku-diskursuse olemasoleva kasutuse tõttu, kuid Kopenhaageni koolkonna esindajate sõnastus viitab võimalusele ka rohkemate sektorite eksisteerimisele. Samas ei ole Kopenhaageni koolkond määratlenud, kui palju veel võiks sektoreid olla, sest nad ei ole defineerinud „tervikut",[94] kuigi nad peavad sektoreid kompleksse terviku osadeks.[95] Buzan, Waever ja de Wilde on tõdenud, et need

[90] Kopenhaageni koolkonna nimetuse vermis Bill McSweeney 1996. aastal, et viidata inimeste grupile, kes on kirjutanud koos Barry Buzani ja Ole Wæveriga alates 1988. aastast COPRI all. Buzan, Barry. 1997. „Rethinking Security after the Cold War." *Cooperation and Conflict* 32 (1): 13. http://cac.sagepub.com/content/32/1/5 (kasutatud 03.04.2013)

[91] Julgeolekustamise kontseptsiooni vermis esialgselt pangasüsteem, kuid selle võttis rahvusvahelistesse suhetesse üle Ole Wæver 1989. aastal. Balzacq. *Securitization Theory*, xiv.

[92] Julgeolekusektorit võib defineerida kui tegevusala või areeni, millele on omased konkreetsed koostöövormid ja referentobjektid. McDonald, Matt. 2012. „Constructivisms." In *Security Studies: An Introduction*, 2nd ed, ed. Paul D. Williams. London; N.Y.: Routledge.

[93] Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. London: Lynne Rienner Publishers, 22-23; Buzan, Barry. 1991. *People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era*. 2nd ed. Harlow: Longman, 133. Märkus: Algselt eristas Barry Buzan neli sektorit (sõjaline, poliitiline, majanduslik ja ökoloogiline sfäär). Buzan, Barry. 1983. *People, States, and Fear: The National Security Problem in International Relations*. Brighton: Wheatsheaf Books, 75.

[94] Albert, Mathias, and Barry Buzan. 2011. „Securitization, Sectors and Functional Differentiation." *Security Dialogue* 42 (4-5): 415. http://sdi.sagepub.com/content/42/4-5/413 (kasutatud 02.01.2014)

[95] Buzan *et al*. *Security: A New Framework*, 8.

viis sektorit on põhilised valdkonnad, mis hõlmavad rahvusvaheliste suhete uuringuid.[96] Ka Buzan ja Richard Little on eristanud need samad viis sektorit, kuid nad ei identifitseeri neid kui peamisi valdkondi, vaid kirjeldavad neid kui üldiselt kasutatuid sektoreid maailma analüüsimiseks.[97]

Alates viie sektori eristamisest on käinud arutelud, kas sektorite nimistut tuleks laiendada, kuid Kopenhaageni koolkond ei ole esitanud kriteeriume, mille alusel määratleda uusi sektoreid.[98] Käesoleva magistritöö eesmärgiks on eristada küberjulgeolekut eraldina sektorina, kuid diferentseerimise aluseks võetakse küberjulgeolekustamise protsessis osalevad üksused, mille pinnalt arendatakse välja käsitlus, mis hõlmab küberjulgeoleku sfääri ja küberjulgeolekustamise teooriat.

3.2. Julgeolekustamine ja selles protsessis osalevad üksused

Mõiste „küberjulgeolekustamine" käsitlemiseks ja küberjulgeoleku uurimiseks eraldi valdkonnana on oluline analüüsida „julgeolekustamise" protsessi ja selles osalejaid. Buzan, Wæver ja de Wilde, kes on defineerinud julgeolekustamist kõneaktina, on tõdenud, et julgeolekuprobleemiks saab teemat lugeda alles siis, kui on olemas eksistentsiaalsed ohud referentobjektidele, mida julgeolekustatakse julgeolekustaja poolt hädaolukorra meetmetele toetuse saamiseks. Kirjeldatud etapp on „julgeolekustav liigutus", kuid probleem on julgeolekustatud ainult siis, kui auditoorium annab sellele nõusoleku.[99] Julgeolekustamise protsessi etappidele pööratakse süvitsi tähelepanu julgeolekustava liigutuse ja julgeolekupraktika alapeatükis.

Uurimistöö raames on oluline analüüsida julgeolekustamise protsessis osalevaid üksusi küberjulgeolekustamise teooria loomiseks. Jef Huysman on tõdenud, et Kopenhaageni koolkond on eeldanud, et üks spetsiifiline üksus (näiteks riik) on peamine toimija ja referentobjekt kõikides julgeolekusektorites, kuid see tekitab raskusi üksuste

[96] Buzan *et al*. *Security: A New Framework*, 19.
[97] Buzan, Barry, and Richard Little. 2000. *International Systems in World History: Remaking the Study of International Relations.* New York: Oxford University Press, 73.
[98] Albert *et al*. „Securitization," 413-415.
[99] Buzan *et al*. *Security: A New Framework*, 5, 24-25.

identifitseerimisel konkreetsetes sektorites.[100] Ka Barry Buzan on tõdenud, et kuna igat sektorit nähakse Kopenhaageni koolkonna poolt terviku osana, siis põimub ja kattub sektorite sisu üksteisega,[101] näiteks riik on nii majanduslik kui ka poliitiline toimija sõjalises ja keskkonnasektoris.[102] Uurimistöö eesmärgiks ei ole analüüsida süvitsi julgolekustamise protsessis osalevaid üksusi igas Kopenhaageni koolkonna poolt eristatud sektoris, vaid pöörata sellele tähelepanu üldises plaanis, mille pinnalt on võimalik põhjalikult uurida julgeolekustamise protsessi üksusi kübervaldkonnas.

Küberjulgeolekut analüüsides tuleb Kopenhaageni koolkonnale sarnaselt küsida, millised on julgeolekustamise protsessi kaasatud referentobjektid ja -subjektid, julgeolekustajad, auditoorium ja eksistentsiaalsed ohud. Kübervaldkond hägustab reaalset ja virtuaalset ning tsiviil- ja militaarsfääri, mis on teinud raskeks määratleda „mida" või „keda" peaks kaitsma „kelle" poolt,[103] kuid magistritöö sihiks on luua selgust küberjulgeoleku protsessis osalevate üksuste osas, millele on siiani varasemates uurimustes ainult põgusalt tähelepanu pööratud.

3.2.1. Referentobjekt, eksistentsiaalne oht ja referentsubjekt

Käesoleva alapeatüki eesmärgiks on analüüsida eksistentsiaalset ohtu ning referentobjekti ja -subjekti küberjulgeolekustamise teooriale aluse loomiseks. Eksistentsiaalsed ohud referentobjektidele on kindlad probleemid, isikud või üksused,[104] kuid Balzacq nimetab referentobjekti ohustajat referentsubjektiks,[105] seega võib eksistentsiaalseks ohuks nimetada ohtu kui sellist ning selle ohu tekitajat referentsubjektiks. Buzan, Wæver ja de Wilde on tõdenud, et referentobjekte nähakse eksistentsiaalselt ohustatuna, millest tulenevalt on neil legitiimne õigus ellujäämisele.

[100] Huysmans, Jef. 2007. „Revisiting Copenhagen: Or, on the Creative Development of a Security Studies Agenda in Europe." In *International Security. Volume IV: Debating Security and Strategy and the Impact of 9-11*, eds. Barry Buzan and Lene Hansen. London: SAGE, 53.
[101] Buzan *et al*. *International Systems in World History*, 75.
[102] Albert *et al*. „Securitization,"416.
[103] Davì, Marco. 2010. *ESDF Workshop 4: Cyber Security: European Strategies and Prospects for Global Cooperation.* London: Cratham House, 7. http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/1110esdf_davi.pdf (kasutatud 12.11.2013)
[104] Emmers, Ralf. 2007. „Securitization." In *Contemporary Security Studies*, ed. Alan Collins. Oxford: Oxford University Press, 112.
[105] Balzacq. „Enquiries into Methods," 36.

Põhimõtteliselt saab referentobjektina käsitleda mida iganes, kuid Kopenhaageni koolkond eristanud siiski kõigis sektorites peamisi referentobjekte.[106]

Sõjalise sektori referentobjektiks on tavaliselt riik (riigivõim, valitsus) ja teist tüüpi poliitiline üksus (näiteks sõjajõud), mida ohustab sõjalise jõu kasutamine,[107] näiteks pommitamine.[108] Poliitilise sektori referentobjektideks on riiklik suveräänsus ja ideoloogia, riigiülesed referentobjektid (näiteks EL), ning rahvusvahelised režiimid ja ühiskond,[109] ning ka laiemalt riik ja tema institutsioonid, mida võivad ohustada valitsuse kukutamine ja riigi poliitilise struktuuri nõrgendamine.[110] EL-i võivad ohustada integratsiooniprotsessi katkestavad sündmused ning rahvusvahelistele režiimidele ja ühiskonnale on ohuks normide, institutsioonide ja reeglite õõnestamine.[111]

Majandussektori referentobjektideks on ettevõtted ja riiklikud majandused, mida ohustavad pankrot ja seaduste muudatused. Sotsiaalse sektori refentobjektid on kollektiivsed identiteedid (rahvused ja religioonid), mis muutuvad sisemiste ja väliste arengute tulemusena (näiteks identiteetide rivaalitsemine). Keskkonnasektori referentobjektid on liigid (tiigrid, inimkond jne) ja nende elukohatüübid (vihmametsad, järved jms) ning kliima ja tsivilisatsioon, millele on ohuks liikide ellujäämine.[112]

Hare on tõdenud, et Kopenhaageni koolkonna julgeolekustamise teooria tähenduses võivad ka küberründed olla eksistentsiaalseteks ohtudeks referentobjektidele,[113] millest tulenevalt saab näha julgeolekustajate liigutusi küberjulgeolekustamiseks.[114] Eksistentsiaalseteks ohtudeks küberruumile on mõistete peatükis eristatud küberründed – küberkuritegevus, küberterrorism, kübersõda, küberspionaaž ning kübervandalism –, seega referentsubjektideks võivad olla kriminaalid, terroristid, rahvusriigid,[115] luureteenistused[116] ja „skriptijuntsud". Kübervaldkonnas on julgeolekuohud jäänud oma

[106] Buzan *et al*. *Security: A New Framework*, 36.
[107] Ibid., 22.
[108] Buzan. *People, States, and Fear: An Agenda*, 116-118.
[109] Buzan *et al*. *Security: A New Framework*, 22.
[110] Buzan. *People, States, and Fear: An Agenda*, 119.
[111] Buzan *et al*. *Security: A New Framework*, 22.
[112] Ibid., 22-23.
[113] Hare. „The Cyber Threat," 213-214.
[114] Nissenbaum, Helen. 2005. „Where Computer Security Meets National Security." *Ethics and Information Technology* 7 (2): 67. DOI 10.1007/s10676-005-4582-3 (kasutatud 06.06.2013)
[115] Hare. „The Cyber Threat," 213.
[116] NATO Heads of State and Government. 2010. *Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*. Lisbon, 11. http://www.nato.int/cps/en/natolive/official_texts_68580.htm (kasutatud 03.01.2014)

olemuselt samaks, kuid küberruum võimaldab uut kohaletoimetamise viisi,[117] näiteks terrorismi- ja sõjaoht võivad tuleneda küberruumi kaudu. Poliitilise sektori referentobjekti ehk suveräänsust võib valitseva võimu kahtluse alla seadmise läbi eksistentsiaalselt ohustada ka küberruumi kaudu.

Küberjulgeoleku referentobjektideks on laiemalt Kopenhaageni koolkonna neli sektorit (sõjaline, poliitiline, majanduslik ja sotsiaalne sfäär) ning osaliselt ka keskkonnasektor, sest küberründed võivad olla suunatud inimeste kui keskkonnas elavate liikide vastu. Kitsamalt on referentobjektideks nende sektorite sees olevad referentobjektid. Hansen ja Nissenbaum on eristanud kollektiivsete referentobjektidena riiki, ühiskonda, rahvust ja majandust, mis on ühenduses võrgu ja indiviididest kodanikega,[118] kuid tegelikult tuleb põhjalikumalt eristada referentobjekte erinevate sektorite sees ja esitada struktureeritud lähenemine referentobjektide klassifikatsioonile kübervaldkonnas.

Esiteks võib küberrünne olla suunatud sõjalise sektori ning seeläbi riigi, valitsuse ja sõjajõudude vastu. Küberrünnete sihtmärkideks on valitsus (ministeeriumid) ning sõja- ja kaitseorganid (riigikaitsesüsteemid),[119] mida võivad ohustada küberkuritegevus, -vandalism, -spionaaž ja -terrorism. Riigile võib ohuks olla kübersõda, kuid küberründed riikide vastu ei ole lihtne tehniliselt, poliitiliselt ja juriidiliselt tõestada.

Teiseks, küberründed võivad olla suunatud ka poliitilise sektori, kitsamalt riigi ja tema institutsioonide (poliitikute), suveräänsuse ja ideoloogia ning rahvusvaheliste organisatsioonide vastu. Küberrünnete ohvriks võivad olla riigiinstitutsioonid (president, ministeeriumid, parlamendid, õigusorganid, keskpank),[120] mida võivad ohustada küberkuritegevus, -vandalism, -terrorism ja -spionaaž, mis võivad olla suunatud ka organisatsioonide vastu.[121] Organisatsioonideks võivad olla nii valitsuslikud kui ka mitte-valitsuslikud ning rahvusvahelised organisatsioonid (näiteks Euroopa Liit), mille korral on referentobjektideks vastav sektor (näiteks poliitiline sektor), organisatsioon ning sellesse kuuluvad indiviidid ja riigid.

---

[117] Geers, Kenneth. 2010. „A Brief Introduction to Cyber Warfare." *Common Defense Quarterly*, 16-18. http://commondefensequarterly.com/archives/CDQ5/index.html (kasutatud 13.11.2013)

[118] Hansen *et al*. „Digital Disaster," 1155-1157.

[119] Goderdzishvili, Nata. 2010. *Legal Assessment of Cyber Attacks on Georgia*. Tbilisi, Georgia: Data Exchange Agency, Ministry of Justice of Georgia. http://www.e-government.ge/uploads/library/2.%20Nov.9_FINAL_Nata's%20Presentation.pdf (kasutatud 03.01.2014)

[120] Ibid.

[121] Uma *et al*. „Survey on Various Cyber Attacks," 391.

Kolmandaks, küberründed (küberkuritegevus, -vandalism, -terrorism ja -spionaaž) on ohuks majanduslikule sektorile ja seeläbi riiklikule majandusele ja ettevõtetele. Küberrünnete sihtmärkideks on ka finantsinstitutsioonid ja meedia,[122] millest viimase võib samuti paigutada Kopenhaageni koolkonna sektoriaalse jaotuse põhjal majanduse alla. Küberründed võivad olla suunatud ka transpordile ja võrkudele,[123] millest esimese võib liigitada majandussektori alla, kuid võrgud on kasutusel erinevates sektorites. Ettevõttesse kuuluvate inimeste identiteetide vargus või spioneerimine muudab ka indiviidid ohvriteks[124] ja seeläbi referentobjektideks. Küberründe toimumist saab õigesti hinnata alles pärast ründe aset leidmist kuna rünnete ohvriks ei ole alati inimesed, vaid näiteks ka pangakontod,[125] kuid tegelikult omab indiviid pangakontot, mille kaudu on ikkagi referentobjektiks inimene.

Neljandaks, küberründed (küberkuritegevus, -vandalism, -terrorism ja -spionaaž) võivad ohustada osaliselt ka sotsiaalset sektorit (rahvust) ja viiendaks ka keskkonnasektorit (inimesi), kuid mitte täies ulatuses, sest näiteks küberründeid loomade elupaikade või religiooni vastu on keeruline tõestada.

Küberjulgeoleku referentobjektideks on seega laiemal tasandil sektorid (majanduslik, sotsiaalne, poliitiline ja sõjaline sektor) ning vähesel määral ka keskkonnasektor. Kitsamalt on referentobjektideks nende sektorite sees olevas referentobjektid (näiteks riik, ettevõtted, rahvus jne). Lisaks esialgsele Kopenhaageni koolkonnale võib referentobjektina tuvastada ka meedia, finantsinstitutsioonid, transpordi ja võrgud. Eksistentsiaalseteks ohtudeks on laiemalt küberründed ja kitsamalt küberrünnete liigid ning referentsubjektideks on nende küberrünnete läbiviijad ehk kriminaalid, terroristid, rahvusriigid, luureteenistused ja „skriptijuntsud".

3.2.2. Julgeolekustaja

Kui referentobjetile eksisteerib referentsubjekti poolt eksistentsiaalne oht, siis on julgeolekustaja see, kes annab tõuke julgeolekustamise protsessi algusele. Buzani, Wæveri ja de Wilde sõnul on julgeolekustav toimija isik või grupp (tavaliselt poliitilised

[122] Goderdzishvili. *Legal Assessment*.
[123] NATO Heads of State and Government. *Active Engagement*, 11.
[124] Hare. „The Cyber Threat," 213.
[125] Thomas. „Cyber Security in East Asia," 7.

liidrid, valitsused, lobistid ja survegrupid), kes julgeolekustab probleeme läbi kõneakti, kuulutades, et referentobjekt on eksistentsiaalselt ohustatud.[126]

Thomas on tõdenud, et ka küberruumis on mitmeid julgeolekustajaid lisaks valitsusele. Nendeks on suuremad üksused (riigid, rahvusvahelised organisatsioonid, korporatsioonid) ja väiksemad osad (kodanikuühiskonna organisatsioonid, küberjulgeoleku spetsialistid, arvutiprogrammeerijad). Indiviididel või gruppidel, kellel ei ole esinduslikku legitiimsust, on palju raskem julgeolekustada ohtu.[127] Lisaks avalikule sektorile võivad julgeolekustajad olla ka eraorganisatsioonid ja -ettevõtted,[128] näiteks pangad, kuid samas tuleb arvestada ka seda, et kübersektori julgeolekustajad võivad ka ise olla referentobjektideks või auditooriumiks.

Küberjulgeoleku julgeolekustavad toimijad kattuvad suuresti ka Kopenhaageni koolkonna poolt nimetatud julgeolekustajatega. Kübervaldkonnas võivad olla julgeolekustajateks suuremad üksused nagu riik, rahvusvahelised organisatsioonid ja korporatsioonid, kuid kitsamalt ka nende suurte osade sees olevad toimijad (kodanikuühiskonna organisatsioonid, näiteks ametiühingud ja rahvaliikumised; eraettevõtted, näiteks pangad; indiviidid, näiteks küberjulgeoleku spetsialistid ja arvutiprogrammeerijad).

3.2.3. Auditoorium

(Küber)julgeolekustamise protsessis osalevaks üksuseks on ka auditoorium. Buzan, Wæver ja de Wilde on tõdenud, et probleem on julgeolekustatud ainult siis, kui auditoorium aktsepteerib seda sellisena.[129] Kuigi Michael C. Williams peab positiivseks seda, et julgeolekustamine nõuab auditooriumi heakskiitu, nendib ta siiski, et just auditooriumi osa julgeolekustamises on jäänud peaaegu täielikult välja arendamata.[130] Näiteks Wæver ei räägi oma varastes töödes palju auditooriumist, vaid väidab, et miski

[126] Buzan *et al*. *Security: A New Framework*, 36, 40.
[127] Thomas. „Cyber Security in East Asia," 7-8.
[128] Hansen *et al*. „Digital Disaster," 1165.
[129] Buzan *et al*. *Security: A New Framework*, 25.
[130] Williams, Michael C. 2003. „Words, Images, Enemies: Securitization and International Politics." *International Studies Quarterly* 47 (4): 526. http://www.samorzad.pwsz.krosno.pl/gfx/pwszkrosno/pl/defaultaktualnosci/675/5/1/s08b_rm_williams.pdf (kasutatud 03.03.2013)

on julgeoleku probleem, kui eliidid kuulutavad seda sellisena.[131] Kopenhaageni koolkond keskendub suuresti vaid ohtude diskursiivsele esitamisele, mitte auditooriumile, kellele omistatakse suur roll. Balzacq on tõdenud, et Kopenhaageni koolkonna läbikukkumine auditooriumi korrapärases kaasamises muudab raskeks julgeolekustamise teooria kasutamise,[132] mistõttu on käesoleva alapeatüki eesmärk edasi arendada auditooriumi käsitlust julgeolekustamise teoorias.

Sarah Léonard ja Christian Kaunert on võtnud omaks John W. Kingdoni „kolme voo mudeli" (*three streams model*) 1984. aasta raamatust „Agendas, Alternatives and Public Policy", milles eristatakse poliitika (*politics stream*), strateegia (*policy stream*) ja probleemi (*problem stream*) vooge,[133] kuid Léonard ja Kaunert täiendavad seda käsitlust omalt poolt detailse auditooriumi analüüsiga, mis aitab edasi arendada auditooriumi teoretiseerimist. Probleemi voos konstrueerib julgeolekustav toimija poliitika probleemi (näiteks vaesust) poliitikategijate tähelepanu püüdmiseks, mis võib enamasti aset leida dramaatiliste sündmuste või kriiside ajal.[134] Sellisel juhul on auditooriumiks peamiselt teised poliitikategijad, kes on hõlmatud poliitika tegemise protsessi ja keda tuleb veenda probleemi eksisteerimises.[135] Strateegia voog on seotud poliitika loomise protsessi ehk alternatiivide ja ettepanekute ettevalmistamisega poliitikaringkondades, mis moodustatakse konkreetse valdkonna (näiteks täidesaatva võimu ja akadeemia) spetsialistidest.[136] Strateegia voos on auditooriumiks spetsialistid ja tehnokraadid, mitte üldine avalikkus või otsusetegijad.[137]

Poliitika voog hõlmab avalikku meelsust, huvigruppide kampaaniaid, valimistulemusi, ja muutusi administratsioonides, mis võivad mõjutada poliitikaettepanekute heaks kiitmist. Poliitika voogu iseloomustab veenmine ja läbirääkimised, näiteks parlamendis seaduseandjate poolt koalitsioonide loomiseks,[138] seega auditooriumiks on otsustamise

[131] Wæver, Ole. 1995. „Securitization and Desecuritization." In *On Security*, ed. Robert D. Lipschutz. New York: Columbia University Press, 54-55.
[132] Balzacq, Thierry. 2005. „The Three Faces of Securitization: Political Agency, Audience and Context." *European Journal of International Relations*, 11 (2): 178. doi: 10.1177/1354066105052960 (kasutatud 14.04.2013)
[133] Léonard, Sarah, and Christian Kaunert. 2011. „Reconceptualizing the Audience in Securitzation Theory." In *Securitization Theory*, 63.
[134] Léonard, and Kaunert. „Reconceptualizing the Audience," 65; Kingdon, John W. 1984. *Agendas, Alternatives, and Public Policies*. Boston: Little, Brown & Co., 91, 109.
[135] Léonard *et al*. „Reconceptualizing the Audience," 66.
[136] Léonard *et al*. „Reconceptualizing the Audience," 66-67; Kingdon. *Agendas*, 116-117.
[137] Léonard *et al*. „Reconceptualizing the Audience," 67.
[138] Léonard *et al*. „Reconceptualizing the Audience," 67; Kingdon. *Agendas*, 152-157, 160.

protsessi kaasatud otsuselangetajad (näiteks ametkonnad ja parlamendiliikmed) ja üldine avalikkus.[139] Ka küberjulgeolekustamise puhul võib pidada auditooriumiks üldist avalikkust, insitutsionaalseid organeid ning tehnokraate ja spetsialiste, seega käesolevas magistritöös võetakse omaks Kingdoni „kolme voo mudeli" käsitlus.

Floyd on tõdenud, et poliitilistel esindajatel valitsuses on legitiimsust rääkida julgeolekust, mis omandatakse liberaaldemokraatlikes riikides tavaliselt valimiste kaudu, seega auditooriumi võib võrdsustada valijaskonnaga.[140] Kodanikke (valijaid) ning nende isikute ühendusi ja organisatsioone võib pidada ka avalikkuseks ehk üldsuseks (avalikuks arvamuseks). Kui riigile ja tema institutsioonidele (referentobjektidele) on eksistentsiaalseks ohuks režiimi kukutamine läbi küberruumi, siis eksisteerib eksistentsiaalne oht ka indiviididest kodanikele, millest tulenevalt on poliitikutel motivatsiooni julgeolekustada ohtusid valijate huvidest lähtuvalt.[141] Julgeolekustajal on vaja piisavalt sotsiaalset ja poliitilist kapitali, et veenda auditooriumi eksistentsiaalse ohu olemasolus,[142] kuid nagu Paul Roe on tõdenud, siis julgeolekustamise protsessis on julgeolekustajatel (eriti valitsustel ja teistel poliitilistel institutsioonidel) julgeolekust rääkimiseks vajalik hulk legitiimsust juba olemas üldise avalikkuse poolt.[143] Kuna julgeolekustamise kontseptsioonist tulenevalt on julgeolekustamise protsessis suur roll auditooriumi nõusolekul, siis võib tõdeda, et julgeolekustajatel on vajalik legitiimsus juba olemas valijatelt.

Balzacq on öelnud, et julgeolekustaja väljakutseks on veenda auditooriumi (näiteks rahvust ja avalikkust), et ta tunnistaks sümboolse referentobjekti loomust, milleks peab julgeolekustaja kooskõlastama oma keele auditooriumi tunnete ja huvidega.[144] Balzacq on nimetanud auditooriumi „volitavaks auditooriumiks", sest auditooriumil peab olema kaks tingimust täidetud. Auditooriumil peab olema otsene põhjuslik seotus probleemiga ning ta peab volitama julgeolekustajat omaks võtma meetmeid ohuga võitlemiseks.[145] Küberjulgeolekuga seoses peab auditooriumil olema otsene põhjuslik seotus

[139] Léonard *et al*. „Reconceptualizing the Audience," 68.
[140] Floyd, Rita. 2010. *Security and the Environment: Securitisation Theory and US Environmental Security Policy*. Cambridge: Cambridge University Press, 51.
[141] Hare. „The Cyber Threat," 213.
[142] Barnard-Wills. „This is not a Cyber War," 20.
[143] Roe, Paul. 2008. „Actor, Audience(s) and Emergency Measures: Securitization and the UK's Decision To Invade Iraq." *Security Dialogue* 39 (6): 632. http://sdi.sagepub.com/content/39/6/615 (03.04.2013)
[144] Balzacq. „The Three Faces of Securitization," 184.
[145] Balzacq. „Enquiries into Methods," 34.

probleemiga, mis on nii avalikkusel, tehnokraatidel, spetsialistidel kui ka institutsionaalsetel organitel küberohtudega seoses olemas, kui ka neid on tabanud küberründed. Samuti peab julgeolekustaja samastuma auditooriumi tunnetega, mida on küberohtude puhul kergesti võimalik teha, sest küberründed võivad mõjutada nii julgeolekustajaid, referentobjekte kui ka auditooriumi.
Kübervaldkonnas eksisteerivad seega kolm suuremat auditooriumi: institutsionaalsed organid, avalikkus (avalik arvamus) ning tehnokraadid ja spetsialistid, kuid kitsamalt võivad auditooriumiks olla poliitikud riigiinstitutsioonide sees ning valijaskond, rahvuse indiviidid ja kodanikud, kellel on põhjuslik seotus probleemiga ning kes saavad volitada julgeolekustajat ette võtma hädaolukorrameetmeid küberrünnetega võitlemiseks.

3.3. Kõneakti teooria ja julgeolekustamise protsessi etapid

On oluline uurida kõneakti teooriat julgeolekustamise protsessi osana kuna käesolevas magistritöös analüüsitakse kõnesid. Kõneakti teooriat analüüsitakse Austini käsitluse põhjal ning täiendatakse seda Kopenhaageni koolkonna teise põlvkonna teooria abil. Uurimistöö kontekstis on tähtis vahet teha ka julgeolekustaval liigutusel ja julgeolekupraktikal, et analüüsida, millal saab julgeolekustavast liigutusest (kõneaktist) praktikas eksisteeriv olukord.

3.3.1. Kõneakt

Kõneakti teooria alapeatüki eesmärgiks on analüüsida kõneakti tüüpe, mille abil on võimalik uurida julgeolekustava liigutuse ja julgeolekupraktika eristust, mille pinnalt saab omakorda välja arendada küberjulgeolekustamise teooria. Buzan, Wæver ja de Wilde on tõdenud, et julgeolekustamise protsess on see, mida kõneteoorias kutsutakse kõneaktiks, seega julgeolek on enesele-viitav diskursiivne praktika, mis tähendab, et probleem muutub eksistentsiaalseks ohuks selle esitamisel ohuna,[146] seega kui ei kõnelda ohust julgeolekule, siis ei teata, et eksisteerib julgeolekuprobleem. Kõneakti teooria loojaks võib pidada Inglise filosoofi Austinit, kes on tõdenud oma teoses „How

[146] Buzan *et al*. *Security: A New Framework*, 24, 26.

to do Things with Words", et kõne ei ole oluline ainult tegelikkuse kirjeldamiseks, vaid selleks, et ütlused kutsuvad esile mingi teo.[147]

Austin eristab lausetes esinevaid kõneakti tüüpe: lokutiivne, illokutiivne ja perlokutiivne akt,[148] mille analüüsimine aitab vahet teha julgeolekustamise protsessi etappidel. Kahjuks ei ole Kopenhaageni koolkonna liikmed kirjeldanud detailselt, kuidas on julgeolekustamise kontseptsioon seotud nende kolme kõneakti dimensiooniga, mille abil muutub julgeolekustav liigutus täielikuks julgeolekustamiseks.[149]

Austin on tõdenud, et lokutiivne akt tähendab kõneleja poolset ütluse formuleerimist vastavalt keelele,[150] mis on konventsionaalne arusaam rääkimisest ehk rääkija toob kuuldavale hääle, mis väljendab mõtet ja annab vihje konkreetsele sõnavarale ja grammatikale.[151] Lokutiivne akt on seega kõneakti see osa, kus öeldakse midagi.

Austin on öelnud, et illokutiivne akt on lokutiivse produktsiooni väljalausumine keele abil spetsiifilise jõuga (näiteks väitmine, küsimine, palve esitamine),[152] seega akt on elluviidud niipea, kui lause on välja öeldud. Kui öeldakse „julgeolek", siis riigi esindajad kuulutavad hädaolukorraseisundi välja.[153] Eesti hädaolukorra seaduse järgi on hädaolukord sündmus(ed), mis ohustavad paljude inimeste tervist ja elu või põhjustavad suure varalise või keskkonnakahju ja ulatuslikke häireid elutähtsate teenuste toimepidevuses.[154] Lokutiivse aktiga seotud illokutiivne akt on kõneakti see osa, kui julgeolekustaja ütleb välja, et eksisteerib eksistentsiaalne oht referentobjektile, et õigustada erakorralisi meetmeid.

Austini kõneakti teooria järgi on perlokutiivne akt illokutiivse akti tagajärjed ja mõju (näiteks auditooriumi uskuma saamine või auditooriumi tegutsema saamine kõneakti tegija palvel),[155] seega auditooriumi on veendud rääkija poolt tegema midagi.[156] Balzacq on tõdenud, et auditooriumilt tugevama mõjujõu saavutamiseks kasutatakse kõnedes

[147] Longworth, Guy. 2012. „John Langshaw Austin." *The Stanford Encyclopedia of Philosophy*. http://plato.stanford.edu/entries/austin-jl/ (kasutatud 29.12.2013)
[148] Austin, John L. 1975. *How to Do Things with Words*. 2nd ed. Oxford: Oxford University Press, 98.
[149] Stritzel. „Security," 349.
[150] Austin. *How to Do Things*, 98.
[151] Stritzel. „Security," 349.
[152] Austin. *How to Do Things*, 98.
[153] Stritzel. „Security," 349.
[154] Hädaolukorra seadus. 2009. Riigi Teataja I, 2014, 25. https://www.riigiteataja.ee/akt/HOS (23.04.2014)
[155] Austin. *How to Do Things*, 98.
[156] Stritzel. „Security," 349.

emotsioone, metafoore, stereotüüpe, žeste ja valesid,[157] näiteks võib küberohtusid toetada meditsiinist pärit metafooridega („viirused" ja „nakatunud arvutid").[158]

Kopenhaageni koolkonna poolne julgeolekustamise väljendamine kõneakti, illokutiivse akti või auditooriumi nõusoleku tähenduses on põhjustanud segadust, sest nad võivad väljendada erinevaid arusaamu sellest, mis moodustab julgeolekustamise. Mida rohkem tõstetakse esile illokutiivset akti kui julgeolekustamist, seda vähem tähtsamaks muutub auditoorium. Mida enam rõhutatakse auditooriumi, seda rohkem on julgeolekustamine perlokutiivne akt.[159] Sellest tulenevalt on Floyd väitnud, et julgeolekustamine ei saa samal ajal olla illokutiivne akt ja sõltuda auditooriumi nõusolekust, sest illokutiivne akt eitab auditooriumi rolli,[160] seega on julgeolekustava liigutuse ja julgeolekupraktika alapeatüki eesmärgiks uurida illokutiivse ja perlokutiivse akti rolli julgeolekustamises ning panna paika nende asetsemine julgeolekustamise protsessis, et rakendada aluseks võetud käsitlust küberjulgeolekustamisele.

3.3.2. Julgeolekustav liigutus ja julgeolekupraktika

Mark B. Salter ja Can E. Mutlu on tõdenud, et on oluline vahet teha julgeolekustaval liigutusel ja praktikal, et analüüsida kuna julgeolekustamise protsess on praktikas aset leidnud. Selleks tuleb eristada julgeolekumeetmeid ja julgeolekustavaid liigutusi. Kui meetmed viitavad konkreetsetele praktikatele, siis julgeolekustav liigutus (diskursused) on püüe nimetada probleemide valdkond.[161] Julgeolekustava liigutuse ja julgeolekupraktika eristuse analüüsimine aitab arendada välja küberjulgeolekustamise teooria ning analüüsida selle pinnalt empiirilisi näiteid.

Balzacq on nentinud, et Kopenhaageni koolkonna tõdemus julgeolekustamisest kui illokutiivsest aktist esitab suure väljakutse julgeolekustamise protsessile,[162] sest tegelikult on illokutiivne akt ainult julgeolekustav liigutus,[163] seega tuleb defineerida,

[157] Balzacq. *Securitization Theory*, 2.
[158] Hansen *et al*. „Digital Disaster," 1166.
[159] Stritzel. „Security," 349.
[160] Floyd. *Security and the Environment*, 52.
[161] Salter, Mark. B, and Can E. Mutlu. 2013. „Securitisation and Diego Garcia." *Review of International Studies* 39(4): 816. http://dx.doi.org/10.1017/S0260210512000587 (kasutatud 03.02.2014)
[162] Balzacq. „The Three Faces of Securitization," 177.
[163] McDonald. „Constructivisms."

mida tegelikult tähendab julgeolekupraktika. Ka Floyd on tõdenud, et idee, et julgeolekustamine toimib nagu illokutiivne kõneakt, on konfliktis eristusega, mille on Kopenhaageni koolkonna liikmed teinud julgeolekustava liigutuse ja täieliku julgeolekustamise vahel. Kui ütlus iseenesest on akt, siis kõneakt on võrdne täieliku julgeolekustamisega ja vastupidi.[164] Samas ei saa nii lihtsustatult julgeolekustamise protsessile läheneda, vaid tuleb kõneakti tüüpide abil eristada kindlate piiridega julgeolekustava liigutuse ja julgeolekupraktika etappe.

Balzacq on arvanud, et ainult perlokutiivse kõneakti kasutamine võib seletust anda auditooriumi rollile julgeolekustamise teoorias, sest perlokutiivne akt püüab paremini julgeolekustamise loogikat kui illokutiivne akt,[165] kuid Floyd väidab, et julgeolekustamise ideed ei püüa ka perlokutiivne kõneakt. Sellest tulenevalt on Floyd tõdenud, et kõneakti teooriat ei peaks täielikult hülgama, vaid illokutiivset akti peaks seostama ainult julgeolekustava liigutuse, mitte täieliku julgeolekustamisega. Floyd on lisanud, et samal ajal tuleb hoiduda auditooriumi rolli teoretiseerimisest julgeolekustamise protsessis.[166] Seega on Floyd erinevalt Balzacqist tõdenud, et ei tohiks kõrvale lükata illokutiivset akti, vaid see tuleks seostada julgeolekustava liigutusega julgeolekustamise asemel.

Floydi väljaarendatud täiendatud julgeolekustamise teoreetiline raamistik näeb ette, et julgeolekustamine koosneb kahest sündmusest: julgeolekustavast liigutusest ja julgeolekupraktikast. Esimene samm on julgeolekustava toimija poolt kõneaktis tehtud hoiatus ohuallikale või antud lubadus kaitsta referentobjekti. Hoiatusega või lubadusega põhjendatakse eksistentsiaalse ohu eksisteerimine, kuid see ei ole julgeolekustamine.[167]

Täielik julgeolekustamine eksisteerib ainult siis, kui julgeolekustav liigutus on täiendatud samm kahe ehk julgeolekupraktika poolt. Julgolekupraktika on muutus relevantse julgeolekustaja asjakohases käitumises (näiteks muutus juhtimises ja eelarves või uute poliitika ja institutsioonide loomine), mis on õigustatud selle toimija poolt viitega väljakuulutatud ohule ja vajadusele tegeleda julgeolekuprobleemiga.[168]

Reageerimine eksistentsiaalsetele ohtudele ehk julgeolekupraktika peab vastama kahele nõudmisele Flodyi järgi. Esiteks, peab reageerimise ulatus olema mõõdetav ohuga ehk

[164] Floyd. *Security and the Environment*, 52.
[165] Balzacq. „The Three Faces of Securitization," 175.
[166] Floyd. *Security and the Environment*, 52-53.
[167] Ibid., 53.
[168] Floyd. *Security and the Environment*, 53, 117.

julgeolekustaja peab arvesse võtma agressori võimekusi, millest tulenevalt võib julgeolekustaja poolne meetmete kasutamine olla vähem või rohkem tõsisem kui esialgne rünne või oht.[169] Küberjulgeoleku valdkonnas on riigi esindajatel erinevalt IT-spetsialistidest raske mõõta esialgse ründe ulatust, seega ei tuleks küberjulgeolekustamise teoorias tähelepanu pöörata sellele nõudmisele, kui analüüsitakse riigi esindajaid julgeolekustajatena.

Teine tingimus on see, et julgeolekustaja reageering peab olema siiralt ohule reageerimise eesmärgiga ehk sihiks peab olema referentobjekti julgeoleku kaitsmine ja olukorra turvaliseks muutmine. Julgeolekustaja kavatsusi saab testida läbi võrdlemise, kas julgeolekustaja kõneakti retoorika ja julgeolekustaja mõtted (julgeolekustav liigutus) on kooskõlas julgeolekupraktikaga (meetmed ohule reageerimiseks). Julgeolekustaja on ainult siis siiras, kui reageerimine sobib kokku julgeolekustava katsega.[170] Küberjulgeolekustamise puhul keskendutakse eelkõige teisele tingimusele ehk julgeolekustaja meetmetele referentobjekti olukorra paremaks muutmiseks.

Tabelis 2 on erinevad lähenemised julgeolekustamise protsessi etappidele. Kopenhaageni koolkond defineerib julgeolekustamist kui illokutiivset kõneakti, mis seisneb selles, et julgeolekustaja ütleb välja konkreetse jõuga, et eksisteerib eksistentsiaalne oht referentobjektile, mida julgeolekustatakse auditooriumi nõusolekul. Kuna ütlus iseenesest on kõneakt, siis on julgeolekustav liigutus täielik julgolekustamine ja vastupidi. Balzacq ei käsitle julgeolekustamist kui illokutiivset akti, vaid tõdeb, et julgeolekustavast liigutusest saab julgeolekupraktika perlokutiivse aktiga. Floyd määratleb julgeolekustava liigutuse illokutiivse aktina, kuid rõhutab, et julgeolekupraktika eksisteerimiseks peab toimuma muutus julgeolekustaja käitumises ehk tema meetmed ohule reageerimiseks peavad olema vastavuses kõneaktis (julgeolekustavas liigutuses) väljaöelduga. Magistritöös võetakse aluseks Floydi ja Balzacqi käsitluste süntees, sest Floyd tõdeb, et auditooriumi osa ei tuleks teoretiseerida, kuid tegelikult on auditooriumil (perlokutiivsel aktil) julgeolekustamises oluline roll.

[169] Floyd, Rita. 2011. „Can Securitization Theory be used in Normative Analysis? Towards a Just Securitization Theory." *Security Dialogue* 42 (4-5): 433. http://sdi.sagepub.com/content/42/4-5/427 (kasutatud 05.02.2014)
[170] Ibid., 429, 433.

Tabel 2. Erinevad lähenemised julgeolekustamise protsessi etappidele

	CS	*Balzacq*	*Floyd*	*Magistritöö käsitlus*
Julgeolekustav liigutus	Illokutiivne akt (julgeolekustav liigutus)	Julgeolekustav liigutus	Illokutiivne akt	Illokutiivne akt + perlokutiivne akt
Julgeolekupraktika	Illokutiivne akt (auditoorium)	Perlokutiivne akt	Julgeolekustaja meetmed	Perlokutiivne akt + julgeolekustaja meetmed

Uurimistöös pannakse kokku Floydi ja Balzacqi käsitlus ehk julgeolekustamine koosneb kahest etapist, millest esimeseks etapiks on julgeolekustav liigutus (illokutiivne akt + perlokutiivne akt) ning teiseks sammuks on julgeolekupraktika (perlokutiivne akt + julgeolekustaja meetmed). Julgeolekustamise esimesele etapile võib erinevalt Kopenhaageni koolkonnast ja Balzacqist omistada auditooriumi rolli, sest julgeolekustaja hakkab juba julgeolekustava liigutuse etapis kõnetama relevantset auditooriumi veenmise eesmärgil.

3.4. Küberjulgeolek julgeolekusektorina ja küberjjulgeolekustamine

Eelneva teoreetilise analüüsi põhjal on võimalik analüüsida kübervaldkonda ja küberjulgeolekustamise protsessi, mille abil saab vastata uurimisküsimusele, kuidas toimub küberjulgeolekustamine Kopenhaageni koolkonna teooria järgi ning võimaldab rakendada teoreetilist raamistikku praktikas asetleidnud juhtumitele.

Johan Eriksson, kes on esitanud oma debatiga „Observers or Advocates? On the Political Role of Security Analysts" kriitika Kopenhaageni koolkonnale, on tõstatanud küsimused, millisesse sektorisse kuulub infotehnoloogia (IT)[171] ja kas uute probleemide julgeolekustamine nõuab uute sektorite loomist.[172] Eriksson on esitanud just need küsimused, mis on seotud ka küberjulgeolekuga, sest Kopenhaageni koolkond ei ole palju tähelepanu pööranud sellele, mis saab siis, kui kerkivad esile uued ohud, näiteks ohud küberründed. Kopenhaageni koolkond kujundas oma seisukohad enamasti 20.

[171] „Infotehnoloogia" (IT) on sarnane IKT-dele, kuid IT viitab kõigele, mis on seotud arvutitehnoloogiatega (riistvara, tarkvara, Internet jms) ning IKT-d on seotud laiemalt kommunikatsioonitehnoloogiatega. TechTerms.com kodulehekülg. http://www.techterms.com/definition/it (kasutatud 26.02.2014) Autori märkus: Käesolevas magistritöös kasutatakse läbivalt terminit „IKT".

[172] Eriksson, Johan. 1999. „Observers or Advocates? On the Political Role of Security Analysts." *Cooperation and Conflict* 34 (3): 317. http://cac.sagepub.com/content/34/3/311 (kasutatud 06.04.2013)

sajandi lõpus, kuid nüüd eksisteerivad ohud ka küberruumile, seega tuleks eristada küberjulgeolekut eraldi sfäärina.

Stephen Walt on konstateerinud, et julgeoleku-uuringute peamine fookus on sõja fenomenil, kuid mõned autorid (näiteks Barry Buzan) on soovitanud julgeoleku mõiste laiendamist mittesõjaliste tegurite kaasamiseks, kuid sellega seoses tekib risk, et julgeoleku-uuringuid laiendatakse ülemääraselt, mis võib hävitada valdkonna koherentsuse.[173] Hare on öelnud, et „küberjulgeolek kui riikliku julgeoleku osa" on ambivalentse loomusega tõdemus, mis on saanud oma koha julgeoleku mõiste laiendamise debatis. Neorealistid (näiteks Walt) ei soovita laiendada julgeoleku-uuringute ulatust, millest tulenevalt ei erista nad küberjulgeolekut eraldi sektorina kuna siiani käib debatt küberrünnete tõeliste mõjude üle riiklikule julgeolekule.[174] Kuigi Walti käsitluse järgi ei tohiks küberjulgeolekut eristada eraldi sektorina, on siiski käesoleva töö sihiks analüüsida küberjulgeolekut diferentseeritud sektorina julgeolekustamise teooria raames.

Hare on nentinud, et kuna küberohte võib käsitleda riiklike julgeolekuprobleemidena, siis võib julgeoleku-uuringute teooriaid (eriti Buzani ohtude raamistikku) rakendada küberjulgeoleku uurimisele.[175] Ka Ronald Deibert on juhtinud tähelepanu asjaolule, et küberruum on muutunud riikliku julgeoleku osaks,[176] kuigi neorealistid (ka Buzan ja Wæver) ei nõustu sellega. Siiski on selge, et riigid on otsustanud, et riikliku julgeoleku komponendiks on küberjulgeolek. Nii kaua, kui riigi esindajad jätkavad küberohtude julgeolekustamist oma kõnedes, ettepanekutes ja riiklikes strateegiates, peab küberjulgeolekut arvesse võtma riiklikus julgeolekus.[177]

Samas on David Barnard-Wills ja Debi Ashenden arvanud, et mitmed valitsused (näiteks Suurbritannia ja USA), kes on püüdnud poliitilise tegevuse kaudu julgeolekustada küberruumi riikliku julgeoleku osana ja luua küberjulgeolekut, on loonud võimaluse, et julgeolekupraktikaid hakatakse kohandama teistest keskkondadest

[173] Walt, Stephen. 1991. „The Renaissance of Security Studies." *International Studies Quarterly* 35 (2): 212-213. http://www.jstor.org/stable/2600471 (kasutatud 06.04.2013)
[174] Hare. „The Cyber Threat," 214.
[175] Ibid., 213.
[176] Deibert, Ronald. 2012. „Cybersecurity: The New Frontier." *Foreign Policy Association Great Decisions*, 45. http://www.fpa.org/ckfinder/userfiles/files/Cybersecurity%20Intro.pdf (kasutatud 15.04.2013)
[177] Hare. „The Cyber Threat," 214.

(näiteks sõjalisest sektorist), mis võib põhjustada küberruumi militariseerimist.[178] Lisaks on Thomas nentinud, et küberjulgeoleku juhtumiuuringute puhul ei ole võimalik jääda Kopenhaageni koolkonna loodud riigikeskse raamistiku piiridesse,[179] kuid siiski tuleb silmas pidada, et on hea aluseks võtta Kopenhaageni koolkonna põhiseisukohad, mille pinnalt edasi arendada küberjulgeolekustamise teooriat.

Kübervaldkond on keeruline sfäär, sest küberjulgeolek seob sõjalist, majanduslikku, poliitilist ja sotsiaalset dimensiooni.[180] Rachel E. Yould on konstateerinud, et IT on tänapäeval ühel või teisel viisil kõikide julgeoleku sektorite ühiseks nimetajaks,[181] mida võib tõdeda ka küberjulgeoleku kohta, sest küberjulgeolek hõlmab referentobjekte, julgeolekustajaid, eksistentsiaalseid ohtusid ja auditooriume ka teistest sektoritest. Diana Saco on toonud välja, et küberjulgeolekut iseloomustab erinevate valdkondade omavaheline võistlemine,[182] mida on arvanud ka Ronald Deibert.[183] Samas on Hansen ja Nissebaum öelnud, et kuigi võib tunduda, et kübervaldkond on killustunud sektor (referentobjektide rikkus, võistlevad julgeolekustajad ja arvukad ohud), siis tegelikult on võimalik luua ühtne teoreetiline raamistik küberohtude esitamiseks julgeolekuprobleemidena.[184] Kübervaldkonnas võivad olla julgeolekustajad nii avalikust kui ka erasektorist, referentobjektide iseloomustab kollektiivsete objektide seotus indiviidi ja võrgustiku julgeolekuga ning eksisteerib mitmeid ohte referentobjektidele, kuid need on kõik omavahel seotud. Seetõttu tuleks küberjulgeolekut vaadata eraldi sektorina, mis hõlmab julgeolekustamise üksusi ka teistest sektoritest.

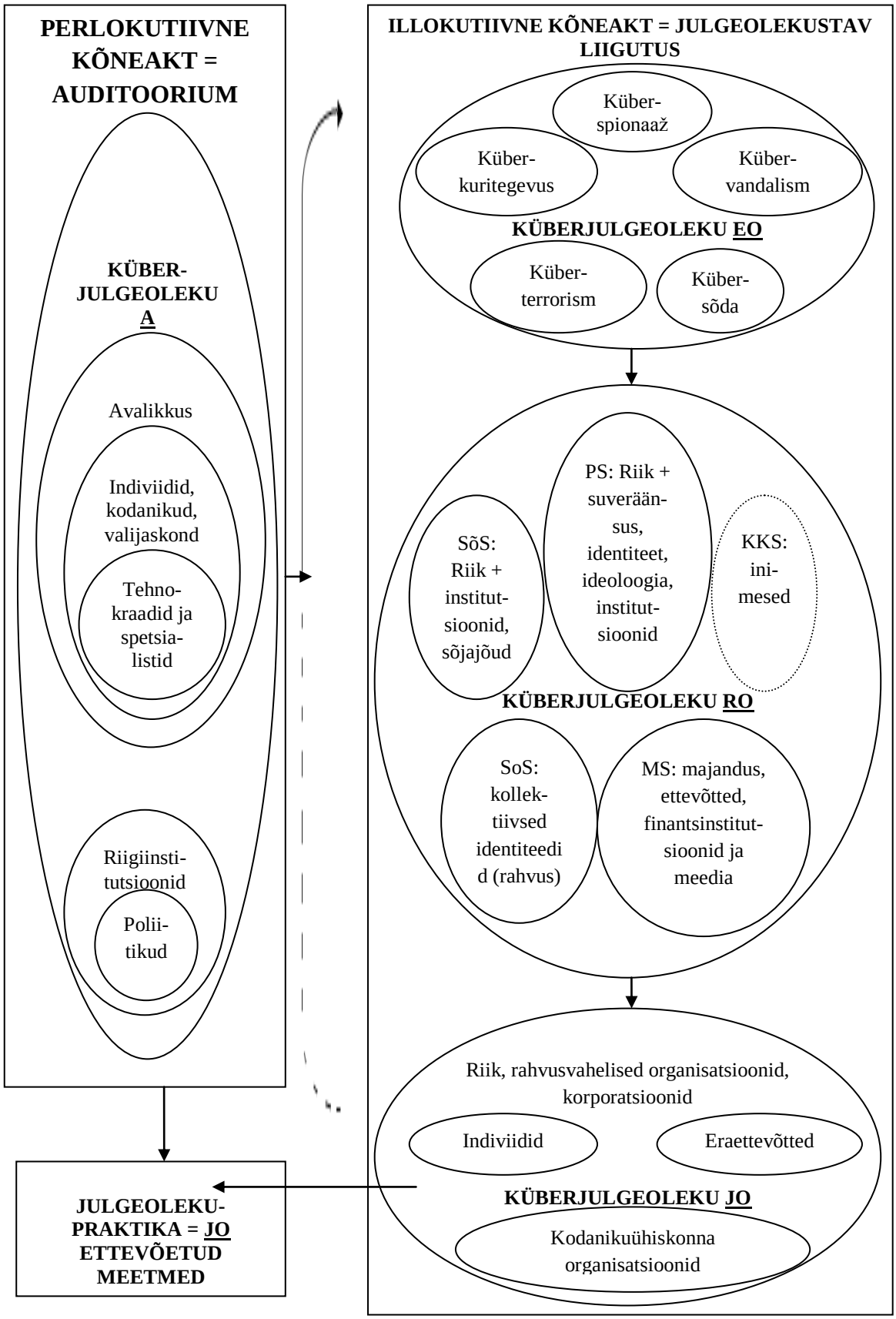
Joonisel 2 on illustreerivalt kujutatud vastus töö uurimisküsimusele, kuidas toimub küberjulgeolekustamine Kopenhaageni koolkonna järgi. Küberjulgeolekustamist võib teoreetilise analüüsi põhjal defineerida kui eesliitest „küber-" ja terminist

[178] Barnard-Wills, David, and Debi Ashenden. 2012. „Securing Virtual Space: Cyber War, Cyber Terror, and Risk." *Space and Culture* XX(X): 3, 11. http://sac.sagepub.com/content/15/2/110 (kasutatud 02.02.2014)
[179] Thomas. „Cyber Security in East Asia," 19.
[180] Davì. *ESDF Workshop 4*, 1.
[181] Yould, Rachel E. 2003. „Beyond the American Fortress: Understanding Homeland Security in the Information Age." In *Bombs and Bandwidth: The Emerging Relationship between Information Technology and Security*, ed. Robert Latham. New York: The New Press, 8.
[182] Saco, Diana. 1999. „Colonising Cyberspace: National Security and the Internet." In *Cultures of Insecurity: States, Communities, and the Production of Danger*, ed. Jutta Weldes. Minneapolis, MN: University of Minnesota Press, 274.
[183] Deibert, Ronald. 2002. „Circuits of Power: Security in the Internet Environment." In *Information Technologies and Global Politics: The Changing Scope of Power and Governance*, eds. James N. Rosenau, and J. P. Singh. Albany: State University of New York Press, 118-135.
[184] Hansen *et al*. „Digital Disaster," 1163.

„julgeolekustamine" koosnevat kontseptsiooni. Küberjulgeolekustamine koosneb kahest etapist, milleks on julgeolekustav liigutus ja julgeolekupraktika. Julgeolekustava liigutuse staadiumis julgeolekustab julgeolekustaja eksistentsiaalseid ohtusid referentobjektide nimel, lubades kaitsta referentobjekti või hoiatades agressorit (illokutiivne akt) ja püüdes veenda auditooriumi (perlokutiivne akt).

Julgeolekustavale katsele järgneb julgeolekupraktika, mis leiab aset ainult siis, kui julgeolekustaja võtab auditooriumi nõusolekul (perlokutiivne kõneakt) ette meetmeid referentobjekti olukorra parandamiseks viitega eksisteerivale/toimunud ohule. Kuigi Kopenhaageni koolkond omistab auditooriumi nõusoleku julgeolekustamise teisele etapile, võib siiski auditooriumi rolli omistada ka julgeolekustavale liigutusele, sest julgeolekustaja püüab auditooriumi veenda juba oma kõneaktiga. Teises staadiumis on vaja auditooriumi nõusolekut meetmete ettevõtmiseks.

Joonisel 2 on kujutatud ka küberjulgeolekustamise protsessis osalevad üksused. Skeemi lihtsustamiseks on kasutatud järgnevaid tähiseid: EO (eksistentsiaalne oht), RO (referentobjekt), JO (julgeolekustaja) ja A (auditoorium). Küberjulgeoleku EO on eksistentsiaalne oht ehk küberrünne (küberkuritegevus, kübervandalism, küberterrorism, küberspionaaž ja kübersõda) referentobjektile ehk kübervaldkonna RO-le. Referentobjektideks on kübervaldkonnas laiemalt Kopenhaageni koolkonna teooria viis sektorit ning kitsamalt sektorites sisalduvad üksused. Joonisel 2 on sõjalisel sektoril tähiseks SõS, poliitilisel sektoril PS, majanduslikul sektoril MS, sotsiaalsel sektoril SoS ning keskkonnasektoril KKS, millest viimane on katkendliku joonega, sest keskkonnasektorist on ainult inimene küberjulgeoleku referentobjektiks. Kübervaldkonna julgeolekustaja (JO) on laiemalt riik, rahvusvahelised organisatsioonid ja korporatsioonid ning kitsamalt indiviidid, eraettevõtted ja kodanikuühiskonna organisatsioonid). Küberjulgeoleku auditooriumiks (A) on riigiinstitutsioonid (poliitikategijad), avalikkus (indiviidid/kodanikud/valijaskond) ning kitsamalt tehnokraadid ja spetsialistid.



Joonis 2. Küberjulgeolekustamise protsess ja selles osalevad üksused

Küberjulgeolekut kui uut eraldiseisvat sektorit on uurinud ka Hansen ja Nissenbaum, kes on tõdenud, et Kopenhaageni koolkonnal ei olnud vajadust oma raamatus „Security: A New Framework for Analysis" eraldi teoretiseerida küberjulgeolekut poliitilise, sõjalise, sotsiaalse, majandusliku ja keskkonnasektori kõrval, kuid väga palju on muutunud sellest asjast, kui Kopenhaageni koolkond avaldas oma seisukohad. Nüüdseks on küberjulgeolek julgeolekustatud ning hõlmab unikaalset sektorit julgeoleku-uuringutes.[185] Hansen ja Nissenbaum on väitnud ennatlikult, et küberjulgeolek on julgeolekustatud, kuigi nad ei ole seda enda artiklis empiiriliselt analüüsinud ja tõestanud, mis ongi käesoleva uurimistöö edasiseks sihiks.

Magistritöö teoreetilise peatüki analüüsi tulemusel võib tõdedada, et küberjulgeolekut kui eraldi julgeolekusektorit saab analüüsida Kopenhaageni koolkonna teooria järgi ning seega on teoreetilises peatükis vastatud ka uurimisküsimusele, kuidas toimub küberjulgeolekustamine Kopenhaageni koolkonna teooria järgi. Töö järgnevaks eesmärgiks on analüüsida, et kas (ja kuidas) on küberründed julgeolekustatud Eestis, et hinnata, kuidas on praktilise näite põhjal kübervaldkonda julgeolekustatud.

[185] Hansen *et al*. „Digital Disaster," 1156-1157.

4. Metodoloogia

Meetodi peatüki eesmärgiks on luua metodoloogiline raamistik toetuseks küberjulgeolekustamise teooriale empiirilise analüüsi läbiviimiseks Eesti näitel. Meetodi osa tugineb poststrukturalistlikule diskursusanalüüsile, millega analüüsitakse küberjulgeolekustamise esimest etappi ehk julgeolekustavast liigutust kõneaktides, mille pinnalt saab edasi uurida julgeolekupraktika vastavust julgeolekustava liigutuse sammule.

Metodoloogilise raamistiku ja teoreetilise osaga vastatakse empiirilises peatükis uurimisküsimusele, kas Eestis on leidnud 2007. aasta küberrünnete ajal ja järgselt aset küberjulgeolekustamine. Meetodi peatükis analüüsitakse esmalt diskursuse sisu ja poststrukturalistlikku diskursusanalüüsi. Seejärel käsitletakse konteksti kui olulist diskursusanalüüsi osa, milles antakse ülevaade 2007. aasta küberrünnetest Eestis ja taustast nendele sündmustele, mille analüüsimine võimaldab uurida magistritöö tekstide valikut Hanseni uurimiskavast lähtuvalt.

4.1. Hanseni poststrukturalistlik diskursusanalüüs

Diskursusanalüüsi alapeatükis käsitletakse erinevaid diskursuste piiritlemise võimalusi ja poststrukturalistlikku diskursusanalüüsi, ning põhjendatakse, miks on diskursusanalüüs sobiv metodoloogia käesoleva magistritöö jaoks.

Julgeolekustamise teooriale toetuvad küberjulgeoleku diskursust uurivad teadlased (Eriksson, Cavelty, Hansen, Nissenbaum) on toonud välja, et julgeolekuohud ei ole loomulikud ja antud, vaid nad tuleb konstrueerida läbi poliitilise diskursuse.[186] Ka Balzacq on nentinud, et ohukuvandite kujutamist saab uurida läbi diskursusanalüüsi, mida toob välja ka Kopenhaageni koolkond, kuid kahjuks piirab Kopenhaageni koolkonna poolt propageeritud meetod diskursusanalüüsi suulistele või kirjalikele sõnavõttudele. Diskursusanalüüsiga tegeledes tuleb seega alguses ära määratleda diskursuse piirid, sest diskursust defineeritakse erinevalt. Balzacqi jaoks on diskursus

[186] Lawson, Sean. 2013. „Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats." *Journal of Information Technology & Politics*, 10 (1): 87-88. http://dx.doi.org/10.1080/19331681.2012.759059 (03.03.2014)

vahend, mis aitab kaardistada hädaolukorda ja ohukuvandite loomist.[187] Cynthia Hardy, Bill Harley ja Nelson Philipps on öelnud, et diskursused on tekstide kogumid ja praktikad, mis toovad ideed ja objektid eksisteerimisse. Tavaliselt luuakse, toetatakse ja vaidlustatakse diskursusi läbi tekstide tootmise, levitamise ning tarbimise.[188] Balzacq täpsustab, et tekstid ei tähenda ainult kirjutatud või räägitud sõnu, vaid tekst viitab ka sümbolitele, piltidele ja muusikale.[189] Uurimistöös omaksvõetud diskursuse piirid määratletakse ära metodoloogilise peatüki tekstiliste valikute osas.

Uurimistöö eesmärgiks on analüüsida empiirilises peatükis Eesti näitel, kas (ja kuidas) on Eestis küberjulgeolekustamine aset leidnud. Magistritöös sobib seega aluseks võtta diskursusanalüüs, mis kvalitatiivse uurimismeetodina keskendub sellele, kas ja kuidas on julgeolekustamine aset leidnud, mitte sellele, miks ja millal teatud julgeolekustavad liigutused on edukad. Diskursusanalüüsi põhjal on võimalik teha järeldusi tekstide põhjal ja pöörata tähelepanu teksti asetsemisele laiemas kontekstis, millest tulenevalt on diskursusanalüüsi jaoks oluline reaktsioon, mille tekst kutsub esile konkreetses auditooriumis.[190] Kopenhaageni koolkonna järgi on julgeolekustamise protsessi oluliseks osaks auditooriumi nõusolek, mille saavutamiseks astutud samme on võimalik analüüsida läbi diskursusanalüüsi. Floyd on tõdenud, et algne Kopenhaageni koolkonna julgeolekustamise teooria on tervenisti seotud diskursusanalüüsiga, mis tuleks piirata tegelikult ainult julgeolekustava liigutuse uurimisele,[191] mida tehakse ka käesolevas töös. Julgeolekupraktika tasandit uuritakse vastavalt julgeolekustava liigutuse analüüsi tulemustele julgeolekustajate ettevõetud meetmete kaudu.

Uurimistöös võetakse aluseks Hanseni poststrukturalistlik diskursusanalüüs julgeolekustava liigutuse uurimiseks. Diskursusanalüüs toodi 1980. aastatel rahvusvaheliste suhete uuringutesse poststrukturalistlike teadlaste (Richard Ashley, James Der Derian, R. B. J. Walker ja Michael J. Shapiro) poolt, kes kasutasid keele võimule keskendunud poststrukturalistlike filosoofide (Michel Foucault ja Jacques Derrida) teooriaid. Poststrukturalistid näevad keelt vahendina, mille kaudu luuakse

[187] Balzacq. „Enquiries into Methods," 39.
[188] Hardy, Cynthia, Bill Harley, and Nelson Phillips. 2004. „Discourse Analysis and Content Analysis: Two Solitudes?" *Qualitative Methods*, 2 (1): 19-22. https://www.maxwell.syr.edu/uploadedFiles/moynihan/cqrm/Newsletter2.1.pdf (kasutatud 07.03.2014)
[189] Balzacq. „Enquiries into Methods," 39.
[190] Ibid. 47, 51.
[191] Floyd. „Can Securitization Theory," 438.

tähendus[192] ning varustatakse riigid, elusolendid ja materiaalsed objektid identiteediga.[193] Keele rolli rõhutamine seob poststrukturalistliku diskursusanalüüsi Kopenhaageni koolkonnaga. Riikidele ja võimule keskenduv poststrukturalistlik teooria väidab, et riigid ja teised poliitilised üksused püüavad hoida kindlat visiooni endast läbi poliitilise diskursuse. Välispoliitika mängib olulist rolli nende nägemuste loomises kuna ta tõmbab piiri riigi ja tema identiteedi („mina") ning riigist erineva „teise" vahele. Välispoliitikad on sõltuvad konkreetsete riikide, kohtade ja inimeste esitlemisest eemaletõukavate ehk „teisena" ning „mina" representeerimisest.[194]

Välispoliitika diskursuses on „mina" Kopenhaageni koolkonna tähenduses referentobjekt, keda ohustab eksistentsiaalne oht. „Teine" on Kopenhaageni koolkonna teooria järgi referentsubjekt (ohu põhjustaja). Metodoloogiliselt tuleb tekstidest identifitseerida selliseid termineid, mis viitavad selgele „teise" (näiteks „õel", „diktaator", „mõrvar", „terrorist") või „mina" (näiteks „hea", „tsiviliseeritud", „õigustatud" või „rünnatud") loomisele. Poliitikud koondavad seeläbi toetust oma meetmetele identiteedi ja välispoliitika vahelise suhte loomisega, milles välispoliitika toetub identiteeti esitlemisele ja välispoliitika kaudu luuakse identiteeti.[195]

Kuigi poststrukturalistid toetuvad „mina-teine" eristusele, siis Hansen ja Wæver on tõdenud, kui analüüsida diskursuses riiki, rahvust, inimesi ja Euroopat „meiena", siis see võib paremini selgitada välispoliitikaid,[196] seega pööratakse magistritöös tähelepanu nii „mina-teine" kui ka „meie" representatsioonidele. „Meie" on uurimistöös kasutusel lisaks referentobjektile ka julgeolekustaja kohta, sest kui „meiena" identifitseeritakse näiteks rahvust või riiki, siis kuulub ka julgeolekustaja „meie" alla.

Lisaks on Hansen ja Nissenbaum rõhutanud vajadust eristada „sina" (auditoorium), kes luuakse diskursuses ja kes peab heaks kiitma avaliku julgeoleku diskursuse.[197] „Sinu" all mõeldakse käesolevas töös auditooriumi, kes annab julgeolekustajale heakskiidu hädaolukorrumeetmete kasutamiseks. Näiteks poliitikud pöörduvad poliitilise

[192] Hansen, Lene. 2012. „Discourse Analysis, Post-Structuralism, and Foreign Policy." In *Foreign Policy: Theories, Actors, Cases*. 2nd ed. Steve Smith, Amelia Hadfield, and Tim Dunne, eds. Oxford: Oxford University Press, 94, 101.
[193] Hansen. *Security as Practice*, 18.
[194] Hansen. „Discourse Analysis," 94-95.
[195] Hansen. *Security as Practice*, 1, 42.
[196] Wæver, Ole. 2003. „Identity, Communities and Foreign Policy: Discourse Analysis as Foreign Policy Theory." In *European Integration and National Identity: The Challenge of the Nordic States*. Lene Hansen, and Ole Waever, eds. Taylor & Francis e-Library, 20-49.
[197] Hansen *et al*. „Digital Disaster," 1165.

opositsiooni ja laiema avaliku sfääri poole püüdega saada toetust oma arusaamadele identiteetidest ja poliitika valikuvõimalustest.[198]

Poststrukturalistliku diskursusanalüüsi abil saab kõnede kaudu selgitada välja riigi esindajate ametlikud arvamused, ning uurida, kuidas julgeolekustaja loob läbi identiteedi auditooriumile aktsepteeritavat välispoliitikat. Poststrukturalistliku disursusanalüüsi ja Kopenhaageni koolkonna teooria sünteesi põhjal on võimalik empiirika osas tuvastada kõnedest referentobjekte („mina"), referentsubjekte („teine"), auditooriume („sina") ning julgeolekustajaid ja referentobjekte („meie").

4.2. Kontekst

Enne tekstide uurimist on oluline analüüsida konteksti 2007. aasta küberrünnetele, mille alusel saab põhjendada tekstilisi valikuid. Balzacq on tõdenud, et Kopenhaageni koolkond püüab edendada diskursusanalüüsi kui uut meetodit, kuid ei võta arvesse konteksti, mille abil saab uurida kõne mõjusust,[199] seega konteksti kaasamine diskursusanalüüsi aitab paremini mõista kõne tausta ja selle jõudmist auditooriumini. Ka Hansen on nentinud, et välispoliitika ei ole suletud süsteem, vaid välispoliitikat ja seeläbi ka poliitika-identiteedi suhet luuakse sotsiaalse ja poliitilise ruumi sees.[200] Sellest tulenevalt võib väita, et ohud tekkivad läbi spetsiifiliste kontekstide,[201] mistõttu tuleb avada kõigepealt kõneakti asetsemine laiemas kontekstis.

Balzacq on omaks võtnud Margaret Wetherelli kontekstide eristuse, mis valitakse ka magistritöös aluseks. Esmalt võib identifitseerida vahetut konteksti, mis hõlmab koostoimist sündmuse ajal (näiteks kokkusaamine, intervjuu, tippkohtumine). Vahetu kontekst on omakorda hõlmatud distaalse konteksti sisse, mis keskendub teksti sotsiaalkultuurilisele paigutusele ning viitab sündmusel osalejate etnilisele koosseisule, diskursuse toimumise kohtadele (ökoloogilised, regionaalsed või kultuurilised keskkonnad) või institutsioonidele.[202] Konteksti alapeatükis analüüsitakse vahetut

[198] Hansen. *Security as Practice*, 1.
[199] Balzacq. „The Three Faces of Securitization," 176.
[200] Hansen. *Security as Practice*, 29.
[201] Balzacq. „Enquiries into Methods," 36-37.
[202] Balzacq. „Enquiries into Methods," 36-37; Wetherell, Margaret. 2001. „Debates in Discourse Research." In *Discourse Theory and Practice: A Reader*, eds. Margaret Wetherell, Stephanie Taylor, and Simeon J. Yates. Thousand Oaks, CA: Sage, 380-399.

konteksti Eestis 2007. aastal toimunud küberrünnetele. Distaalset ning spetsiifilist vahetut konteksti analüüsitakse empiirilises osas iga kõneakti juures eraldi.

Eestis puhkesid küberründed 27. aprillil 2007. aastal. Alguses kasutasid ründajad DDoS ründeid, kuid 30. aprillil võeti appi robotivõrgud (botnet)[203]. Lisaks kasutati e-mailidele rämpsposti saatmist ja Eesti Reformierakonna koduleheküIje moonutamist.[204] Robotivõrke kasutati peamiselt pankade (Hansapank[205], SEB Eesti Ühispank[206] ja Krediidipank) majandustegevuse halvamiseks, meediaväljaannete infoleviku tõkestamiseks ja väikefirmade äritegevuse häirimiseks.[207] Rünnati ka Eesti riigi ametlikke koduleheküIgi (www.riik.ee, www.president.ee, www.peaminister.ee), ning sihtmärgiks oli ka tuvasta.pol.ee, kuhu olid riputatud fotod vara lõhkujatest.[208] Eesti valitsus, ärid ja ühiskond kogesid kõigi aegade kõige hullemaid DDoS ründeid, mis tulid suurest hulgast (kuni 85 000) „ärandatud" arvutitest. Rünnete mastaapsust suurendab ka see, et küberründed, mis lõppesid 19. mail 2007. aastal, kestsid ebatavaliselt pikka aega (3 nädalat).[209]

Bendiek ja Porter on tõdenud, et kübersõda viiakse tänapäeval läbi ussviiruste[210] ja robotivõrkudega, näiteks Eestis 2007. aastal,[211] kuid kübersõja võrdsustamine robotivõrkude või ussviirustega on liiga lihtsustatud käsitlus ning teisendab „sõja" tähendust. Küberrünnete uudsus oli põhjuseks, miks Eestis toimunud küberründeid ümbritses sõja retoorika,[212] näiteks Eesti meedias,[213] kuid küberründed Eestis olid robotivõrgud ja DDoS ründed, mis liigituvad küberkuritegevuse alla.

---

[203] Robotivõrk on ühest allikast korraga mitmete pahatahtliku tarkvaraga nakatunud arvutite kontrollimine. Techterms.com koduleheküIg. http://www.techterms.com/definition/botnet (kasutatud 22.03.2014)

[204] Rid. „Cyber War," 11-12.

[205] AS Hansapank on Swedbank AS 2009. aastast. Swedbanki koduleheküIg. https://www.swedbank.ee/private (kasutatud 07.04.2014)

[206] Alates 2008. aastast on SEB Eesti Ühispank uueks nimeks AS SEB Pank. Intress.ee koduleheküIg. http://seb.intress.ee/ (kasutatud 07.04.2014)

[207] Randel, Tarmo. 2007. *CERT Eesti tegevuse aastakokkuvõte 2007*. https://www.ria.ee/public/CERT/CERT_2007_aastakokkuv6te.pdf (kasutatud 23.03.2014)

[208] Ibid.

[209] Rid. „Cyber War," 12.

[210] Ussviirus on süsteemide vahel liikuv arvutiviirus, mis „uuristab käigu" läbi arvutimälu ja kõvaketta, ning kopeerib iseennast, kuid ei muuda arvutis olevaid faile. Techterms.com koduleheküIg. http://www.techterms.com/definition/botnet (kasutatud 22.03.2014)

[211] Bendiek *et al*. „European Cyber Security Policy," 158.

[212] Rid. „Cyber War," 14.

[213] Kaska *et al*. „Developments in the Legislative," 45-46.

Küberrünnete ajal oli rünnetele reageerimise koordineerivaks organiks eelkõige Riigi Infosüsteemide Arenduskeskuse (alates 2011. aastast Riigi Infosüsteemi Ameti, RIA)[214] infoturbeintsidentide käsitlemise osakond (CERT-EE), mis koosnes vabatahtlikest kohalikest teenusepakkujatest ja IT-spetsialistidest nii era- kui ka avalikust sektorist Eestist ja välismaalt. CERT-EE analüüsis intsidendi tõsidust ning edendas infovahetust rünnatud organisatsioonide ja Internetiteenuse pakkujate vahel.[215] CERT organisatsioonid on loodud üle maailma küberrünnete lahendamiseks ja ärahoidmiseks ning Eestis täidab neid eesmärke alates 2006. aastast RIA CERT-EE,[216] mille peamine ülesanne oli 2007. aastal tõkestada küberründeid ja tagada infokanalite kättesaadavus Eestis ja välismaal koos Soome CERT meeskonnaga, kelle kaasabil tehti koostööd teiste riikide CERT meeskondadega.[217] RIA põhimäärusest tulenevalt on CERT-EE eesmärgiks täita Eesti riigi tasemel CERT ülesandeid, tegeleda Eesti arvutivõrkudes toimuvate intsidentide käsitlemise ning kasutajate teadlikkuse tõstmisega.[218]

Kuigi meetmeid küberrünnetele reageerimiseks analüüsitakse alles empiirilises osas, siiski uuritakse konteksti alapeatükis vahetuid meetmeid RIA-CERT poolt küberrünnete likvideerimiseks, sest uurimistöös analüüsitakse julgeolekustajatena riigi esindajaid, mistõttu käsitletakse nende tarvitusele võetud meetmeid eelkõige 2007. aasta küberrünnete järgselt, sest meetmete elluviimine võtab aega. Kuna küberohud on üsna uued, siis ei saa koheselt öelda, et nad on julgeolekustatud kuna uued meetmed tuleb eraldada küberrünnetele reageerimiseks.[219]

Kõige olulisemaks vahetuks kontekstiks 2007. aasta küberrünnetele Eestis oli pronkssõduri julgeolekustamine. 1947. aastal avati Eestis pronkssõduri mälestusmärk

---

[214] Kuni 1. juunini 2011 oli Riigi Infosüsteemi Ameti (RIA) eelkäijaks Riigi Infosüsteemide Arenduskeskus (RIA), mis moodustati 2003. aastal, seega 2007. aastal kuulus CERT-EE Riigi Infosüsteemide Arenduskeskuse alla. Vaks, Toomas. 2012. „Riigi Infosüsteemi Ameti roll Eesti küberturvalisuse tagamisel." *Eesti infoühiskonna aastaraamat 2011/2012*. http://www.riso.ee/et/content/riigi-infos%C3%BCsteemi-ameti-roll-eesti-k%C3%BCberturvalisuse-tagamisel#.UzBU7X8XjyU (kasutatud 24.03.2014)

[215] Evron, Gadi. 2008. „Battling Botnets and Online Mobs. Estonia's Defence Efforts during the Internet War." *Georgetown Journal of International Affairs* Winter/Spring: 123. http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/geojaf9&section=19 (kasutatud 07.03.2014)

[216] Riigi Infosüsteemide Amet. 2007. „CERT Eesti: Varahommikul kordistati ründeid Eesti küberruumi vastu." *Riigi Infosüsteemide Amet* 01. mai. https://www.ria.ee/cert-eesti-varahommikul-kordistati-runnakuid-eesti-kuberruumi-vastu/ (kasutatud 01.03.2014)

[217] Randel. *CERT Eesti tegevuse aastakokkuvõte*.

[218] Riigi Infosüsteemi Ameti põhimäärus. 2011. Riigi Teataja I, 2011, 1. https://www.riigiteataja.ee/akt/128042011001 (kasutatud 09.03.2014)

[219] Thomas. „Cyber Security in East Asia," 7.

Tallinna vabastajatele ehk punaarmee sõduritele, mis legitimeeris Nõukogude ajal NSV Liidu võimu, kuid eestlaste jaoks sümboliseerib pronkssõdur rahvuslikku tragöödiat. Sellest tulenevalt hakkasid Eesti võimud kujundama seadusandlust pronkssõduri ümberpaigutamiseks. 2007. aasta alguses jõustus sõjahaudade kaitse seadus, millele tuginedes andis Eesti kaitseminister Jaak Aaviksoo (ametis 05.04.2007-06.04.2011) aprillis käsu hakata hauast välja kaevama pronkssõduri alla maetud sõdureid, mis tõi kaasa vägivaldse protesti. Valitsus otsustas teisaldada monumendi Tõnismäelt, et vältida edasisi rahuhäirimisi. 30. aprillil püstitati pronkssõdur ja maeti sõdurite säilmed ümber Kaitseväe kalmistule.[220] Venemaa Teise maailmasõja mälestusmonumendi „Tundmatu sõdur" ümberteiseldamine põhjustas hämmingut Eesti venekeelse rahvastiku seas ja Venemaal, mis kutsus esile 26.-27. aprillil Tallinnas vägivaldseid tänavaproteste, mille käigus arreteeriti 1300 inimest, 100 inimest said vigastada ja 1 surma.[221]

Ka pronkssõdurit julgeolekustasid Eesti julgeolekustajad. Eksistentsiaalseks ohuks peeti Venemaa poolset väljakutsete esitamist Eesti riigi mineviku domineerivatele tõlgendustele, seega Venemaad käsitleti vaenlasena.[222] Venemaa kui „teine" põhjustas pronkssõduriga Eesti Vabariigi ajaloolisele käsitlusele eksistentsiaalset ohtu, mistõttu Eesti täidesaatva võimu esindajad (eelkõige Aaviksoo) julgeolekustasid pronkssõdurit. Pronksikriisi võib seega pidada Vabariigi Valitsuse poolseks julgeolekustamise kaasuseks: kiirendatud korras suruti läbi konkreetne seadusandlus, et anda näiliselt jõuline raam julgeolekustavale liigutusele. Samuti kasutati erakorralisi meetmeid, mille raames teisaldati pronkssõdur kui ohuallikas referentobjektile ehk Eesti riigile.

Käesolevas magistritöös ei analüüsita süvitsi pronkssõduriga seotud julgeolekustamise juhtumit, kuid pronkssõduri julgeolekustamisega seoses tekib küsimus, et kuivõrd pronkssõduri julgeolekustamisele järgnenud küberrünnete rõhutamine näitas Eesti julgeolekustajate soovi saada toetust esialgsele julgeolekustamise protsessile ja tuua pronkssõduri julgeolekustamisega seoses tekkinud küsitavaid aspekte rahvusvahelise tähelepanu alt välja. Küberründed toimusid kriisiolukorras ja said alguse koos

[220] Lehti, Marko, Matti Jutila, and Markku Jokisipilä. 2008. „Never-Ending Second World War: Public Performances of National Dignity and the Drama of the Bronze Soldier." *Journal of Baltic Studies* 39 (4): 397-399. http://estudijas.lu.lv/pluginfile.php/158478/mod_resource/content/0/Bronzas_karav.pdf (kasutatud 07.04.2013)
[221] Rid. „Cyber War," 11.
[222] Lehti *et al*. „Never-Ending Second World War," 394.

pronkssõduri julgeolekustamisega, seega tuleb arvesse võtta konteksti, milles Eesti täidesaatva võimu esindajad pidid oma avaldusi tegema.

Paralleelselt küberrünnete ja pronkssõduri julgeolekustamisega korraldasid mitmed noorteorganisatsioonid (näiteks Naši ehk „Meie omad") protestina pronkssõduri teisaldamisele Eesti Moskvas asuva saatkonna piiramise ajavahemikus 27.04-05.05.2007. Häiriti saatkonna rahu, saatkonda sisenemist ja lahkumist ning rünnati füüsiliselt saadikut Marina Kaljuranda.[223] Sarnaselt pronkssõduri teisaldamisele mõjutas ka Eesti Moskva saatkonna piiramine vahetult Eesti julgeolekustajate kõneaktide sisu, sest küberrünnetega samal ajal juhtus mitu pingeliselt sündmust Eestis.

Konteksti alapeatükis pöörati tähelepanu vahetule kontekstile (pronkssõduri teisaldamine ja saatkonna piiramine), kuid konteksti puhul on oluline ka see, kes on kõne vastuvõtjaks ehk auditooriumiks ning distaalne ja spetsiifiline vahetu kontekst, mida käsitletakse iga kõneakti juures eraldi. Samuti on tähtsad iga inimese isiklikud arusaamad maailmast, mis võib mõjutada kõneakti sisu ja identiteetide konstrueerimist. Uurimistöös ei keskenduta iga kõneakti juures isikliku suhtumise analüüsile, sest see võib tihti subjektiivne olla, kuid diskursusanalüüsi läbi viies tuleb alati arvestada ka seda, et inimeste arusaamad võivad kõneakti sisu mõjutada. Riigi esindaja võib isiklike veendumuste alusel olla mõne riigi või organisatsiooni vastane või pooldaja, mis võib mõjutada „teise" identifitseerimist ja võib aidata paremini auditooriumini jõuda.

4.3. Tekstide valik julgeolekustava liigutuse analüüsimiseks

Välispoliitika mõistmiseks diskursusena tuleb metodoloogiliselt kasutada tekstide analüüsi,[224] seega on oluline empiirilise uurimuse läbiviimiseks põhjendada tekstide valikut teooriast ja meetodist lähtuvalt. Käesolevas alapeatükis piiritletakse diskursusanalüüsile aluseks olevaid tekste, mille pinnalt on võimalik empiirika peatükis analüüsida, kas Eesti julgeolekustajate kõnedes leidis aset julgeolekustav liigutus.

Magistritöös keskendutakse riiklikule poliitilisele tasandile, sest 2007. aasta küberründed nõudsid riiklikul tasemel reageerimist. Uurimistöös sõltub tekstide valik

[223] Värk, René. 2008. „The Siege of the Estonian Embassy in Moscow: Protection of a Diplomatic Mission and Its Staff in the Receiving State." *Juridica International* 13: 145, 148, 150. http://www.juridicainternational.eu/public/pdf/ji_2008_2_144.pdf (kasutatud 04.04.2014)
[224] Hansen. „Discourse Analysis," 94.

julgeolekustajate ringist, mida piiritletakse vastavalt teoreetilise peatüki tõdemusele, et teatud julgeolekustajatel on rohkem legitiimsust ja võimu julgeolekust rääkida.

4.3.1. 2007. aasta küberrünnetega seotud julgeolekustajad

Tekstide valiku piiritlemiseks on esiteks vaja analüüsida julgeolekustajaid 2007. aasta küberrünnete ajal. Kuna julgeolekustajatel, kellel on rohkem autoriteeti ja mõjuvõimu, on rohkem võimalusi julgeolekust rääkida, siis analüüsitakse käesolevas alapeatükis ainult Eesti võimude esindajaid ning valitakse nende hulgast analüüsi aluseks olevad julgeolekustajad, mis võimaldab järgmises alapeatükis piiritleda valitud julgeolekustajate kõneaktide allikaid.

Eestis on kolme sorti võimu: seadusandlik (Riigikogu), täidesaatev (Vabariigi Valitsus) ning kohtuvõim (kohtud). Riigikogu tegeleb seadusandlusega, kohtud õigusemõistmisega ning valitsus seaduste rakendamisega.[225] Uurimistöös soovitakse analüüsida poliitilisi meetmeid referentobjekti olukorra paremaks muutmiseks, mistõttu keskendutakse täidesaatvale võimule, kellel on oma pädevusest tulenevalt võimalik pingelise sündmuse ajal eriolukord riigis välja kuulutada. Eesti Vabariigi põhiseaduse § 86 tulenevalt kuulub täidesaatev võim Vabariigi Valitsusele, kes viib ellu riigi sise- ja välispoliitikat, koordineerib valitsusasutuste tegevust, korraldab seaduste, Riigikogu otsuste ja presidendi aktide täitmist, annab täitmiseks määrusi ja korraldusi ning kuulutab loodusõnnetuse ja katastroofi korral välja eriolukorra riigis.[226]

Käesolevas magistritöös analüüsitakse julgeolekustajatena seega Vabariigi Valitsuse liikmeid, kelleks on ministrid, kes korraldavad vastava ministeeriumi juhina ministeeriumi valitsemisalasse kuuluvaid küsimusi,[227] annavad seaduse alusel ja täitmiseks määrusi ja käskkirju.[228] Ka Eesti „Küberjulgeoleku strateegia 2008-2013" järgi on just Vabariigi Valitsus ja ministeeriumid vastutavad küberjulgeoleku alaste meetmete elluviimise eest,[229] seega käesolevas magistritöös analüüsitakse Vabariigi

[225] Eesti Vabariigi põhiseadus. 1992. Riigi Teataja 1992, 26, 349. https://www.riigiteataja.ee/akt/633949 (26.03.2014)
[226] Ibid.
[227] Vabariigi Valitsuse seadus. 1995. Riigi Teataja I, 1995, 94, 1628. https://www.riigiteataja.ee/akt/1011049?leiaKehtiv (kasutatud 26.03.2014)
[228] Eesti Vabariigi põhiseadus.
[229] Küberjulgeoleku strateegia komisjon. *Küberjulgeoleku strateegia 2008-2013*, 27-35.

Valitsuse liikmete ehk ministrite kõneakte, kes saavad riiklikul tasemel astuda meetmeid täidesaatva võimu kaudu.

Selleks, et analüüsida, kas Eestis on aset leidnud küberjulgeolekustamine, uuritakse ministrite kõnesid ning vastavate ministeeriumite koostatud või elluviidud dokumente. Ka Marco Davi on tõdenud, et küberjulgeolekustamist iseloomustavad valitsuse liikmete teostatud mitmed julgeolekustavad liigutused, mille jälgi võib leida strateegilistest dokumentidest, täidesaatvatest korraldustest ja avalikest pöördumistest,[230] mida ei piiritleta käesolevas magistritöös ainult julgeolekustava liigutuse etapiga, vaid ka julgeolekupraktikaga, sest läbi kõnede ja dokumentide on võimalik analüüsida, kas julgeolekustav liigutus on vastavuses julgeolekupraktikaga. Kõneaktide piiritlemist analüüsitakse käesolevas alapeatükis, kuid dokumentide valikut põhjendatakse empiirilises peatükis julgeolekupraktikaga seoses.

Magistritöö keskendub ainult nendele ministritele, kelle ministeerium on seotud küberjulgeolekuga. Ministeeriumite struktuuri uurimiseks analüüsitakse ministeeriumite kodulehekülgede abil läbi kõikide Eesti ministeeriumite tööülesanded. Eestis on kokku üksteist ministeeriumi: Justiits-, Haridus- ja Teadus-, Kaitse-, Keskkonna-, Kultuuri-, Majandus- ja Kommunikatsiooni-, Põllumajandus-, Rahandus-, Sise-, Sotsiaal- ja Välisministeerium.[231] Ministeeriumite ülesannete uurimiseks analüüsitakse kübervaldkonnaga seotud olulisemaid arengukavasid, ministeeriumi valitsemisalasse kuuluvaid asutusi ja ministeeriumi struktuuri kuuluvaid üksusi. Arengukavasid mainitakse tekstide valiku alapeatükis ainult põgusalt ministeeriumite ja ministrite väljaselgitamiseks, kuid arengukavadele pööratakse rohkem tähelepanu empiirika osas, kui põhjendatakse dokumentide piiritlemist arengukavade tasandile.

Eesti küberjulgeoleku strateegia järgi on küberjulgeolekuga seotud Vabariigi Valitsus ning Justiits-, Kaitse-, Majandus- ja Kommunikatsiooni-, Haridus- ja Teadus-, Sise- ning Välisministeerium,[232] mis leidis kinnitust ka käesolevas töös ministeeriumite tööülesannete analüüsi tulemusel. Esmalt analüüsitakse julgeolekustajana peaministrit kui valitsuse liiget, sest valitsus koordineerib ministeeriumite tööd. Vabariigi Valitsuse seaduse § 36 alusel on peaministri pädevuseks esindada valitsust ja juhtida selle tegevust. Peaministri ülesandeks on anda ka korraldusi üksikküsimuste

[230] Davì. *ESDF Workshop 4*, 7.
[231] Vabariigi Valitsuse kodulehekülg. http://valitsus.ee/et/valitsus/ministeeriumid (kasutatud 25.04.2014)
[232] Küberjulgeoleku strateegia komisjon. *Küberjulgeoleku strateegia 2008-2013*.

otsustamiseks,[233] seega valitsus (eesotsas peaministriga) saab heaks kiita korraldusi, millega saab valitsus anda ministeeriumitele ülesande moodustada komisjone arengukavade koostamiseks või kiita heaks dokumente. Peaminister esindab valitsusjuhina ka valitsust ja edastab auditooriumitele valitsuse seisukohtasid.

Lisaks peaministrile võetakse vaatluse alla kaitseminister, sest Kaitseministeerium kui riigikaitsega tegelev asutus koordineeris Eesti „Küberjulgeoleku strateegia 2008-2013" koostamist 2008. aastal.[234] 2014. aasta veebruarist alustas Kaitseministeeriumi juures tööd küberpoliitika osakond, mis kujundab ja viib ellu küberjulgeolekut, analüüsib küberjulgeoleku arenguid ning esindab Eestit NATO-s ja EL-is küberjulgeoleku aruteludes.[235] Ka Välisministeerium on kübervaldkonnaga seotud, sest Välisministeeriumi juhtimisel koostati „Julgeolekupoliitika alused" (2010), milles pööratakse tähelepanu ka küberjulgeolekule.[236] Lisaks kuulub Välisministeeriumi struktuuri poliitikaosakond, mille julgeolekupoliitika ja relvastuskontrolli büroo tegeleb Eesti julgeoleku,[237] seega ka küberjulgeolekuga, kuigi poliitikaosakonna põhimääruses ei ole seda otseselt kirjas.

Ka Justiitsministeerium on seotud küberjulgeolekuga, sest kriminaalpoliitika valdkonnas on Justiitsministeeriumi prioriteediks võitlus kuritegudega küberruumis.[238] Justiitsministeerium viib ellu kriminaalpoliitikat lähtuvalt arengukavale „Kriminaalpoliitika arengusuunad aastani 2018" (2010), milles tõdetakse, et ühiskonnale tekitavad kahju küberkuriteod, mistõttu tuleb pöörata kõrgendatud tähelepanu küberrünnete ennetamisele ja neile reageerimisele.[239] Ka Haridus- ja Teadusministeerium on seotud kübervaldkonnaga, sest ta on üks vastutavatest ministeeriumitest Eesti teadus- ja arendustegevuse ning innovatsiooni strateegia 2014-

[233] Vabariigi Valitsuse seadus.
[234] Küberjulgeoleku strateegia komisjon. *Küberjulgeoleku strateegia 2008-2013*, 8.
[235] Loonet, Teelemari. 2014. „Kaitseministeeriumis alustas tööd küberpoliitika osakond." *Postimees* 04. veebruar. http://www.postimees.ee/2684832/kaitseministeeriumis-alustas-tood-kuberpoliitika-osakond (kasutatud 29.03.2014)
[236] Julgeolekupoliitika aluste töörühm. 2010, 6. *Eesti julgeolekupoliitika alused*. Tallinn. http://www.vm.ee/?q=node/9180 (kasutatud 01.03.2014)
[237] Poliitikaosakonna põhimäärus. 2012. Välisministeeriumi koduleheküg. http://www.vm.ee/?q=node/9220 (kasutatud 08.04.2014)
[238] Justiitsministeeriumi koduleheküg. http://www.just.ee/26990 (kasutatud 06.04.2014)
[239] Kriminaalpoliitika arengusuunad aastani 2018 heakskiitmine. 2010. Riigi Teataja III, 2010, 26, 51. https://www.riigiteataja.ee/akt/13329831 (kasutatud 07.04.2014)

2020 „Teadmistepõhine Eesti" elluviimisest eest, mis rõhutab vajadust teadus- ja arengustegevuse edendamiseks arendada IKT-sid ja küberturvalisust.[240]

Majandus- ja Kommunikatsiooniministeeriumis, mis koordineerib uut Eesti „Küberjulgeoleku strateegia 2014–2017" koostamist,[241] on side ja riigi infosüsteemide asekantsler, kellele alluvad sideosakond, infoühiskonna ja infotehnoloogia arhitektuuri talitus ning riigi infosüsteemide ja infoühiskonna teenuste arendamise osakond,[242] mis on seotud infotehnoloogiaga. Majandus- ja Kommunikatsiooniministeeriumi haldusalasse kuulub ka RIA, mis koordineerib riigi infosüsteemide arendamist ja korraldab infoturbega seotud tegevusi.[243] Majandus- ja Kommunikatsiooniministeerium koostas arengukava „Eesti infoühiskonna arengukava 2020" (2013) ja on üldvastutav kõikide meetmete elluviimise ees selle dokumendi raames.[244]

Siseministeerium, mis tegeleb riigi sisejulgeoleku tagamisega,[245] on ka seotud küberjulgeolekuga. Siseministeeriumi haldusalasse kuulub 2008. aastast tegevust alustanud infotehnoloogia- ja arenduskeskus (SMIT), mis tegeleb infoturbe standardite rakendamise ja soovituste väljatöötamisega.[246] Siseministeerium valmistas ette ja vastutab ka küberjulgeoleku alast võimekust rõhutava arengukava „Eesti turvalisuspoliitika põhisuunad aastani 2015" elluviimise eest.[247]

Magistritöö piiritlemise huvides käsitletakse empiirilises peatükis ainult peaministri ja nende ministeeriumite ministrite kõneakte, mis on küberjulgeolekuga seotud. Nendeks ministeeriumiteks on Justiits-, Kaitse-, Majandus- ja Kommunikatsiooni-, Haridus- ja Teadus-, Sise- ja Välisministeerium ning vastavateks ministriteks on justiits-, kaitse-,

[240] Eesti teadus- ja arendustegevuse ning innovatsiooni strateegia 2014–2020 „Teadmistepõhine Eesti" heakskiitmine. 2014. Riigi Teataja III, 2014, 2. https://www.riigiteataja.ee/akt/329012014002 (kasutatud 26.04.2014)

[241] „Küberjulgeoleku strateegia 2014–2017" koostamise ettepaneku heakskiitmine.

[242] Majandus- ja Kommunikatsiooministeeriumi koduleheküIg. http://www.mkm.ee/326177/ (kasutatud 29.03.2014)

[243] Riigi Infosüsteemi Ameti koduleheküIg. https://www.ria.ee/ria/ (kasutatud 07.04.2014)

[244] Majandus- ja Kommunikatsiooniministeerium. 2013. *Infoühiskonna arengukava 2020*, 4, 19. http://valitsus.ee/et/valitsus/arengukavad (kasutatud 28.04.2014)

[245] Siseministeeriumi põhimäärus. 2012. Riigi Teataja I, 2012, 4. https://www.riigiteataja.ee/akt/128012014003 (kasutatud 06.04.2014)

[246] Siseministeeriumi infotehnoloogia- ja arenduskeskuse põhimäärus. 2013. SMIT-i koduleheküIg. http://www.smit.ee/pohimaarus.html (kasutatud 06.04.2014)

[247] Eesti turvalisuspoliitika põhisuundade aastani 2015 heakskiitmine. 2008. Riigi Teataja I, 2008, 25, 165. https://www.riigiteataja.ee/akt/12979629 (kasutatud 26.04.2014)

majandus- ja kommunikatsiooni-[248], haridus- ja teadus-, sise- ning välisminister. Oluline on analüüsida nendes ministrite ametites olnud isikuid 2007. aasta küberrünnete ajal, et uurida, kas nad astusid julgeolekustava liigutuse, mille pinnalt on võimalik analüüsida julgeolekustava katse vastavust julgeolekupraktikale.

2007. aasta küberrünnete ajal oli Eesti peaministriks Andrus Ansip (13.04.2005-26.03.2014), justiitsministriks Rein Lang (13.04.2005-06.04.2011), kaitseministriks Jaak Aaviksoo (05.04.2007-06.04.2011), majandus- ja kommunikatsiooniministriks Juhan Parts (05.04.2007-26.03.2014), haridus- ja teadusministriks Tõnis Lukas (05.04.2007-06.04.2011), siseministriks Jüri Pihl (05.04.2007-21.05.2009) ja välisministriks Urmas Paet (13.04.2005-...).[249] Nimetatud julgeolekustajate ringi põhjal on võimalik analüüsida kõneaktide valikut empiirilise analüüsi läbiviimiseks.

4.3.2. Julgeolekustajate kõneaktide valiku määratlemine

Selleks, et analüüsida, kas justiits-, kaitse-, majandus- ja kommunikatsiooni-, haridus- ja teadus-, sise- ning välisminister tegid 2007. aasta küberrünnete ajal julgeolekustava liigutuse, on vaja ära piiritleda tekstide valik, mille alusel valitakse empiirika peatükis valim, mida analüüsitakse süvitsi metodoloogia ja teooria abil.

Magistritöö toetub Hanseni poststrukturalistlikule uurimiskavale, mille põhjal on võimalik teha tekstilisi valikuid, piiritleda ajalist raami ning valida analüüsi aluseks olevaid sündmusi ja nendega seotud „mina(sid)". Uurimiskavas tuleb teha valikud nelja dimensiooni vahel, milleks on intertekstuaalne mudel, ajaline perspektiiv, „mina(de)" ja sündmuste arv. Tuleb valida, kas uurida ametlikku välispoliitilist diskursust või laiendada ulatust ka poliitilise opositsiooni, meedia ja marginaalsete diskursuste juurde. Samuti on vaja selgust saada, kas uurida ühte või mitut „mina", konkreetset olukorda või pikemat ajaloolist arengut ning ühte pingelist või arvukaid sündmusi (joonis 3).[250]

[248] Alates 2014. aastast on Majandus- ja Kommunikatsiooniministeeriumil kaks ministrit, kelleks on majandus- ja kommunikatsiooniminister ning väliskaubanduse- ja ettevõtlusminister. Majandus- ja Kommunikatsiooniministeeriumi koduleheküIg. http://www.mkm.ee/326176/ (kasutatud 26.04.2014)

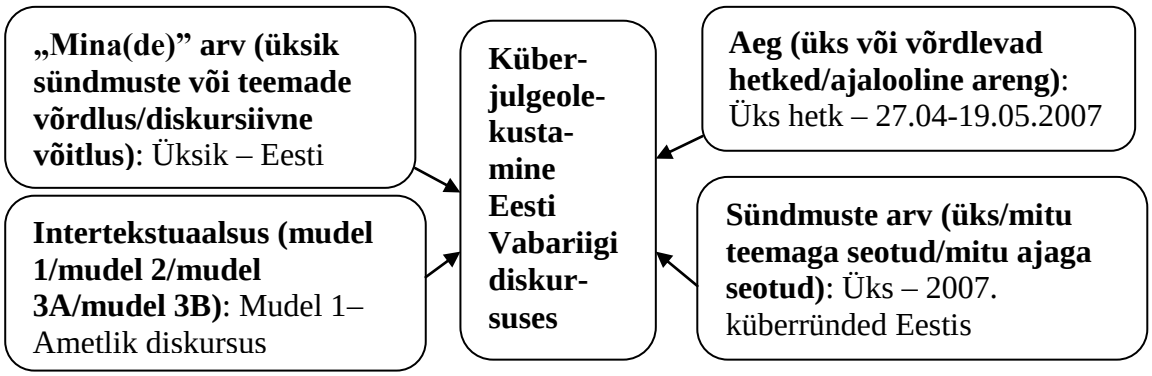
[249] Vabariigi Valitsuse koduleheküIg. http://valitsus.ee/et/valitsus/varasemad-valitsused/ministrid (kasutatud 26.04.2014)

[250] Hansen. *Security as Practice*, 12-13,73.

Välispoliitika diskursused on intertekstuaalselt seotud, mis tähendab, et tekstid ehitavad oma argumendid ja võimu üles läbi otseste viitamiste teistele tekstidele või peamiste kontseptsioonide omaksvõtu kaudu,[251] seega Hanseni poststrukturalistliku diskursusanalüüsi metodoloogiliste juhiste järgi tuleb analüüsi aluseks valida ka intertekstuaalsuse mudel, mis võimaldab piiritleda tekstide valikut.

Hansen on tõdenud, et on kolm intertekstuaalset mudelit, mis struktureerivad ametlikke välispoliitika diskursusi. Mudel üks on ametlik diskursus, mis on seotud poliitikute loodud tekstidega (kõned, poliitilised debatid, intervjuud, artiklid, raamatud ja intertekstuaalsuse kaudu seotud tekstid). Mudel kaks on laiem poliitiline debatt, millele on omased meedia ja poliitiliste opositsiooniparteide poolt loodud parlamendidebatid ja meediatekstid, millest viimaseid võib kategoriseerida toimetajate juhtkirjadeks/ametlikeks seisukohavõttudeks, reportaažideks ning suulisteks/kirjalikeks debattideks. Mudel kolm on ametliku poliitilise diskursuse taasloomine või sellele väljakutse esitamine. Mudel 3A on popkultuur (filmid, televisioon, arvutimängud, fotograafia, koomiksid, ilukirjandus, muusika, luule, joonistused, arhitektuur, reisikirjeldused ja autobiograafiad) ja mudel 3B on kriitiline poliitiline diskursus (ajalehed, koduleheküljed, raamatud, brošüürid ja akadeemilised analüüsid).[252]

Jooniselt 3, millel on kujutatud uurimiskava Eesti põhjal diskursusanalüüsi läbi viimiseks, on näha, et intertekstuaalsuse mudelite hulgast valitakse esimene mudel (ametlik diskursus), sest julgeolekustajateks valiti Eesti ministrid. „Minade" alt võetakse aluseks üksik „mina" ehk Eesti riik, ajaliseks perspektiiviks üks hetk (27.04-19.05.2007) ja sündmuste arvuks üksik sündmus (2007. aasta küberründed Eestis).



Joonis 3. Diskursusanalüüsi uurimiskava küberjulgeolekustamise uurimiseks Eesti näitel
Allikas: Koostatud Hanseni diskursusanalüüsi uurimiskava põhjal (Hansen. *Security as Practice*, 81)

[251] Hansen. *Security as Practice*, 8.
[252] Ibid., 53-55, 75.

Diskursusanalüüsi analüüsiobjektiks valimiseks peab vastavate ministeeriumite ja valitsuse koduleheküljedel või Eesti suurimates päevalehtedes – Postimees (PM), Eesti Päevaleht (EPL), Õhtuleht (ÕL) – ajavahemikus 27.04.2007-19.05.2007 avaldatud ministri kõneaktis sisalduma viide Eestis toimunud küberrünnetele. Ajalehtede valiku aluseks on asjaolu, et nimetatud ajalehed ilmuvad kuus korda nädalas ja on Eesti Ajalehtede Liidu (EALL) andmetel suurima tiraažiga üleriiklikud päevalehed 2014. aasta märtsi seisuga,[253] ning mis ei ole erialased ajalehed, vaid üldloetavad ajalehed, milles on seetõttu suurem potentsiaal käsitleda küberjulgeolekut. Magistritöös analüüsitakse ainult eestikeelseid ajalehti, sest oluline on tuvastada julgeolekustajate kõneaktid, kus Eesti ministrid rääkisid Eestis toimunud küberrünnetest, mitte kõned, intervjuud ja artiklid, kus on välismaiste ajalehtede nägemus või kajastus Eesti ajalehtedest. Lisaks tuleb silmas pidada Hanseni tõdemust poststrukturalistliku diskursusanalüüsi jaoks tekstide valimisel, et tõlked võivad mõnikord olla väärtuslikud alternatiivid originaaltekstidele, kuid siiski tuleb ettevaatlik olla tõlgete suhtes,[254] mis viitab sellele, et eesti keelest teistesse keeltesse tõlgitud ajalehe artiklid võivad esitada oma nägemuse algallikast pärit teksti kohta.

Poststrukturalistlik diskursusanalüüs rõhutab esmaste allikate (näiteks kõned, intervjuud, parlamentaarsed debatid, reportaažid ja juhtkirjad) tähtsust, kuid see ei tähenda, et teisastel allikatel ei ole kohta poststrukturalistlikus diskursusanalüüsis.[255] Sellest lähtuvalt on käesoleva uurimistöö põhiline rõhk esmaste allikate (ministrite suulised ja kirjalikud kõned, intervjuud, ministri arvamusartiklid ning ministri kirjutatud artiklid) peal, kuid uuritakse ka intertekstuaalsuse kaudu kõneaktide avaldamist Eesti kolme suurima päevalehe vahendusel (ministrite tsitaatidele viitavad artiklid), sest ministeeriumid ja valitsus edastavad oma kõnesid väljaannetele.

Julgeolekustava liigutuse analüüsiühikuks on seega laiemalt tekst ning kitsamalt ministeeriumite ja valitsuse koduleheküljedel ning Eesti kolmes suurimas päevalehes avaldatud kõned, (arvamus)artiklid ja intervjuud, ning artiklid, milles on tsiteeritud ministrit. Kuigi käesolevas magistritöös on analüüsiobjektideks koduleheküljed (Hanseni järgi mudel 3B) ja meediatekstid (Hanseni mudel kaks), siiski kuuluvad ka

[253] Eesti Ajalehtede Liidu koduleheküljg. http://www.eall.ee/tiraazhid/ (kasutatud 26.04.2014)
[254] Hansen. *Security as Practice*, 83.
[255] Ibid., 82-83.

need mudel üks alla, mis keskendub poliitikute poolt loodud tekstidele. Hanseni liigitab koduleheküljed mudel 3B alla selles tähenduses, et koduleheküljed haldajad tõlgendavad juba poliitikute poolt öeldud sõnu/kirjutatud tekste. Meediatekstid on mudel kaks all, sest neis käsitletakse ka meedia ja opositsiooniliste parteide arvamust, kuid magistritöös uuritakse ministrite loodud tekste.

Tabelis 3 on pea-, justiits-, kaitse-, majandus- ja kommunikatsiooni-, haridus- ja teadus-, sise- ning välisministri ministeeriumi ja valitsuse koduleheküljel, Postimehes, Eesti Päevalehes ja Õhtulehes ilmunud kõneaktid ajavahemikus 27.04.2007-19.05.2007. Tabelis olevad numbrid viitavad 2007. aasta küberrünnetega seotud kõneaktide arvule suhestuna vastava ministri kõikide kõneaktide arvuga nimetatud perioodil.

Valikusse valitakse ainult need kõneaktid, kus on tsiteeritud või otse kajastatud vastavat ministrit, tema ettekandeid, intervjuud ministriga ja tema arvamusartikleid. Intertekstuaalsus aitab analüüsida, kas Eestis toimus ja toimub küberjulgeolekustamine 2007. aastal ja selle järgselt ehk kas rõhutatakse küberjulgeoleku olulisust allikatest allikatesse. Tabelis 3 on seega ka intertekstuaalsuse kaudu seotud tekste, mida analüüsitakse pikemalt empiirilises peatükis, kuid oluline on kõnede allikaks lisaks ministeeriumite ja valitsuse kodulehtedele võtta ka Eesti suurimad päevalehed, sest kõiki ministrite kõneakte ei pruugita ministeeriumi ja valitsuse kodulehel avaldada. Diskursusanalüüsi valikusse ei kuulu need kõneaktid, kus minister mainib küll kübervaldkonda, kuid ei räägi 2007. aastal aset leidnud küberrünnetest.

Kogu kõneaktide arv viitab kõnedele, mis analüüsiti läbi selleks, et tuvastada nendest ministri viiteid 2007. aasta küberrünnetele (tabel 3). Tabelis on märgitud miinusmärgiga lahtrid, kui vastava allika arhiivis ei ole nimetatud perioodi kohta kõneakte (Majandus- ja Kommunikatsiooniministeeriumi koduleheküg ja Õhtuleht). Ministri kogu kõnearv valitsusasutuse koduleheküljel koosneb koduleheküljel avaldatud kõneaktidest, mida analüüsitakse nii ettekannete kui uudiste põhjal, seega võib kõnede allikaks olla mitu Internetiaadressi, mille põhjal on kõneaktide arv kokkuliidetud arv. Ajalehtede (Postimees, Õhtuleht ja Eesti Päevaleht) kogu kõneaktide arv viitab arhiivi otsingumootori abil leitud kõnedele, mis on nimetatud perioodil seotud vastava ministri nime (Ansip, Lang, Aaviksoo, Parts, Pihl, Paet, Lukas) või ametiga (pea-, justiits-, kaitse-, majandus- ja kommunikatsiooni-, haridus- ja teadus-, sise- ja välisminister).

Tabel 3. Eesti küberründeid käsitlevad ministrite kõneaktid 2007. aasta küberrünnete ajal suhestuna kõikide kõneaktide arvuga nimetatud perioodil

	Ansip	**Lang**	**Aaviksoo**	**Parts**	**Pihl**	**Paet**	**Lukas**
Valitsusasutus	1/36	0/4	0/24	-	0/2	2/57	0/20
PM	3/74	0/9	1/41	0/16	0/19	1/57	0/14
EPL	1/77	0/16	1/30	0/9	0/20	2/57	0/12
ÕL	-	-	-	-	-	-	-

Allikas: Tabel on koostatud järgnevate allikate põhjal: Haridus- ja Teadusministeeriumi kodulehekülg. http://www.hm.ee/index.php?03295&aasta=2007; Vabariigi Valitsuse kodulehekülg. http://valitsus.ee/et/valitsus/Valitsuse-liikmed/peaminister/Peaministri-koned; http://valitsus.ee/et/uudised/pressiteated; Justiitsministeeriumi kodulehekülg. http://www.just.ee/32927; Kaitseministeeriumi kodulehekülg. http://www.kmin.ee/et/uudised, Majandus- ja Kommunikatsiooniministeeriumi kodulehekülg. http://www.mkm.ee/pressiteated/?op=archive; Siseministeeriumi kodulehekülg. https://www.siseministeerium.ee/2716/?id=2716&op=newsarchive; https://www.siseministeerium.ee/17601/?id=17601&op=newsarchive, Välisministeeriumi kodulehekülg. http://www.vm.ee/?q=taxonomy/term/28; http://www.vm.ee/?q=taxonomy/term/27; Postimehe kodulehekülg. http://www.postimees.ee/otsi/arhiiv; Eesti Päevalehe kodulehekülg. http://epl.delfi.ee/archive/; Õhtulehe kodulehekülg. http://www.ohtuleht.ee/arhiiv (kasutatud 06.04.2014)

Meetodi peatüki eesmärgiks oli analüüsida Hanseni poststrukturalistlikku diskursusanalüüsi meetodit, mille alusel analüüsitakse ministrite kõneakte sünteesituna küberjulgeolekustamise teooriaga. Metodoloogiline raamistik tugevdab julgeolekustamise teooriat selles tähenduses, et identiteedi tuvastamine ministrite kõnedest võimaldab analüüsida ministrite kõneakte auditooriumi veenmisest lähtuvalt. Metodoloogia peatükis kuuluvad poststrukturalistliku uurimiskava alusel tekstide valikusse Ansipi viis, Aaviksoo kaks ja Paeti viis kõneakti, sest nimetatud ministrid võtsid 2007. aasta küberrünnete ajal sõna Eestis toimunud küberrünnete teemal.

Sellest tulenevalt on empiirilise peatüki esimeseks eesmärgiks analüüsida kokku kahteteist kõneakti tabeli 3 põhjal, et tuvastada, kas nad astusid julgeolekustava liigutuse. Kui nimetatud minister astus julgeolekustava liigutuse, siis analüüsitakse süvitsi tema vastavat kõneakti küberjulgeolekustamise teooria, Hanseni poststrukturalistliku diskursusanalüüsi ning Wetherelli vahetu konteksti alusel.

5. EMPIIRILINE ANALÜÜS

Empiirika osa eesmärgiks on analüüsida küberjulgeolekustamist Eesti Vabariigi kaasuse näitel, et vastata uurimisküsimusele, kas ja kuidas on küberjulgeolekustamine reaalsuses aset leidnud vastavalt käesolevas töös loodud küberjulgeolekustamise teooriale. Sellest tulenevalt uuritakse empiirilises peatükis, milliste ministrite kõneaktid kuuluvad valimisse, kuidas avaldub julgeolekustav liigutus valimisse võetud ministrite kõnedes ning kas (ja kuidas) on ministrite kõneaktid kooskõlas julgeolekupraktikaga.

Empiiriline analüüs koosneb neljast etapist. Esiteks uuritakse magistritöö metodoloogilisest peatükist lähtuvalt pea-, kaitse- ja välisministri kõneakte, kes olid ministriametis 2007. aasta küberrünnete ajal (27.04-19.05.2007) ja võtsid Eestis toimunud küberrünnete teemal sõna küberrünnete ajal. Kui nimetatud ministri kõnest, mis tuvastati metodoloogilises peatükis, ei ole võimalik identifitseerida lubadust kaitsta referentobjekti või hoiatust agressorile, siis jäetakse see kõneakt valimi alt välja, sest lubaduse või hoiatuseta ei ole minister astunud julgeolekustavast liigutust. Teiseks, valimisse võetud kõneakte käsitletakse küberjulgeolekustamise teooria, Hanseni poststrukturalistliku diskursusanalüüsi ja Wetherelli vahetu konteksti alusel, et tuvastada, kuidas on julgeolekustav liigutus küberjulgeolekustamise protsessis kuju võtnud.

Kolmandaks, julgeolekupraktika alapeatükis uuritakse Eesti riigi poolt vastu võetud arengukavasid, et selgitada välja küberjulgeolekuga seotud dokumendid. Strateegiate analüüs võimaldab tuvastada ministrite julgeolekupraktikaid küberjulgeolekustamise protsessis arengukavade loomise kaudu. Arengukavadest tuvastatakse lubadust kaitsta referentobjekti, et tugevdada kõneaktides antud lubadust, ning lisaks identifitseeritakse meetmeid lubaduse täitmiseks. Neljandaks, ministrite elluviidud meedet/meetmeid analüüsitakse ministeeriumite ja valitsuse koduleheküljegedel avaldatud ettekannete, arvamusartiklite ja intervjuude põhjal. Ministrite kõneaktide arvu uurimine piiritletakse Ansipi, Aaviksoo ja Paeti ametiajaga. Ministri kogu kõnede arvu kõrvutatakse küberjulgeolekuga seotud tekstide arvuga, mida võrreldakse omakorda teiste ministrite kõneaktide arvuga. Kübervaldkonna esinemine ministriga seotud tekstides võimaldab vastata uurimisküsimusele, kuidas on küberjulgeolekustamine praktikas aset leidnud.

5.1. Diskursusanalüüsi valim ja julgeolekustav liigutus

Käesoleva alapeatüki eesmärgiks on analüüsida meetodi peatükis tekstide hulka valitud pea-, kaitse- ja välisministri kõnesid, arvamusartikleid, intervjuusid ja ministrite tsitaate kasutavaid artikleid, et tuvastada, kas nendes analüüsiobjektides antakse lubadus kaitsta referentobjekti või hoiatus referentsubjektile. Käesolevas alapeatükis analüüsitakse viite Andrus Ansipi, kahte Jaak Aaviksoo ning viite Urmas Paeti kõneakti, seega kokku kahteteist kõneakti. Valimisse ei kaasata neid kõneakte, mis on intertekstuaalsuse kaudu seotud valimisse võetud kõnedega, vaid neile viidatakse intertekstuaalsuse tähenduses.

Esmalt analüüsitakse peaminister Ansipi viite kõneakti. Valimisse kuulub 2. mail 2007. aastal Riigikogu ees peetud kõne „Peaminister Andrus Ansipi kõne Riigikogu ees",[256] sest selles anti lubadus referentobjekti kaitsta. Valimisse ei kuulu Ansipi Riigikogu ees peetud kõnega seotud artikkel „Ansip: meie suveräänne riik on tugeva rünnaku all"[257] ja arvamuslugu „Andrus Ansipi poliitiline avaldus riigikogu ees"[258], sest neile viidatakse intertekstuaalsuse tähenduses. Valimisse ei kuulu ka Ansipi TV3-le „Seitsmestele uudistele" antud otseintervjuud tsiteerivad Postimehe „Ansip: juhtunu oli šokk terve maailma jaoks"[259] ja Eesti Päevalehe artikkel „Ansip: mis juhtus, oli šokk kogu maailma jaoks",[260] sest nendes ei anta lubadust ega hoiatust.

Teisena analüüsitakse kaitseminister Aaviksooga seotud kahte kõneakti. Valimisse kuuluvad 11. mail nii Eesti Päevalehes kui ka Postimehes ilmunud artiklid, mis viitasid Jaak Aaviksoo suulisele ettekandele valitsuse pressikonverentsil „Visioonist lahenduseni", sest neis antakse lubadus referentobjekti kaitsta. Nende artikliteks on

[256] Ansip, Andrus. 2007. „Peaminister Andrus Ansipi kõne Riigikogu ees." *Valitsuse kommunikatsioonibüroo* 02. mai. http://www.valitsus.ee/et/valitsus/Valitsuse-liikmed/peaminister/Peaministri-koned/51/peaminister-andrus-ansipi-k%C3%B5ne-riigikogu-ees (kasutatud 06.04.2014)

[257] Postimees.ee. 2007. „Ansip: meie suveräänne riik on tugeva rünnaku all." *Postimees* 02. mai. http://www.postimees.ee/1656303/ansip-meie-suveraanne-riik-on-tugeva-runnaku-all (kasutatud 06.04.2014)

[258] Ansip, Andrus. 2007. „Andrus Ansipi poliitiline avaldus riigikogu ees," *Postimees* 02. mai. http://arvamus.postimees.ee/1656331/andrus-ansipi-poliitiline-avaldus-riigikogu-ees (kasutatud 06.04.2014)

[259] Tiks, Oliver. 2007. „Ansip: juhtunu oli šokk terve maailma jaoks." *Postimees* 10. mai. http://www.postimees.ee/1659579/ansip-juhtunu-oli-okk-terve-maailma-jaoks (kasutatud 22.03.2014)

[260] Rannajõe, Maria-Elisa. 2007. „Ansip: mis juhtus, oli šokk kogu maailma jaoks." *Eesti Päevaleht* 10. mai. http://epl.delfi.ee/news/eesti/ansip-mis-juhtus-oli-sokk-kogu-maailma-jaoks.d?id=51086560 (kasutatud 22.03.2014)

„Rünnak Eestile hoogustab kübersõja arutelu NATO-s"[261] ja „Eesti-vastane kübersõda kerkis ühtlasi NATO väljakutseks".[262]

Viimaks analüüsitakse välisminister Paeti viite kõneakti. Valimisse võetakse 1. mail Välisministeerium poolt avaldatud „Välisministri avaldus",[263] millest võib identifitseerida lubaduse kaitsta referentobjekti. Valimisse ei valita Eesti Päevalehes 1. mail avaldatud artiklit „Venemaa ründab Eesti kaudu Euroopa Liitu",[264] sest see on intertekstuaalsuse kaudu seotud Välisministeeriumi poolt avaldatud Paeti kõnega.

Valimisse võetakse ka Postimehes 4. mail 2007. aastal avaldatud refereering „Paet: Vene karu jätkab vana joont" Urmas Paeti arvamusloost Rootsi päevalehes Svenska Dagbladet, milles mainib Paet ainult ühe korra eesliitega „küber-" seotud terminit „kübertasand" koos teiste Eestis aset leidnud sündmustega,[265] kuid Paeti kõnest on võimalik tuvastada lubaduse kaitsta referentobjekti. Valimisse ei valita Eesti Päevalehes 5. mail ilmunud artiklit „Paet: hoopis Venemaal on põhjust Eesti ees vabandada", sest sellest ei ole lubadust ega hoiatust.[266] Valimisse võetakse ka Välisministeeriumi koduleheküljel ilmunud artikkel „Välisminister kõneles Euroopa Nõukogus",[267] milles on antud lubadus referentobjekti kaitsta.

Lisaks Eesti-siseselt intertekstuaalsuse kaudu seotud tekstidele analüüsitakse ka välismaa meedias avaldatud artikleid. Selleks kasutatakse Google'i otsingumootorit, kuhu sisestatakse otsingusõnadeks vastava ministri nimi, eesliide „cyber-" ja 2007. Valimisse võetud välismaal avaldatud artikleid mainitakse vastava ministri kõneakti juures, kui uuritakse intertekstuaalsust.

---

[261] Anvelt, Kärt, ja Mirko Ojakivi. 2007. „Rünnak Eestile hoogustab kübersõja arutelu NATO-s." *Eesti Päevaleht* 11. mai. http://epl.delfi.ee/news/eesti/runnak-eestile-hoogustab-kubersoja-arutelu-nato-s.d?id=51086579 (kasutatud 21.03.2014)

[262] Kalamees, Kai. 2007. „Eesti-vastane kübersõda kerkis ühtlasi NATO väljakutseks." *Postimees* 11. mai. http://www.postimees.ee/1659637/eesti-vastane-kubersoda-kerkis-uhtlasi-nato-valjakutseks (kasutatud 21.03.2014)

[263] Välisministeerium. 2007 „Välisministri avaldus." *Välisministeeriumi koduleheküg* 01. mai. http://www.vm.ee/?q=node/2874 (kasutatud 21.03.2014)

[264] Rand, Erik, ja Aivar Pau. 2007. „Paet: Venemaa ründab Eesti kaudu Euroopa Liitu." *Eesti Päevaleht* 01. mai. http://epl.delfi.ee/news/eesti/paet-venemaa-rundab-eesti-kaudu-euroopa-liitu.d?id=51085322 (kasutatud 26.03.2014)

[265] Postimees.ee. 2007. „Paet: Vene karu jätkab vana joont." *Postimees* 04. mai. http://www.postimees.ee/1657319/paet-vene-karu-jatkab-vana-joont (kasutatud 21.03.2014)

[266] Kaldoja, Kerttu. 2007. „Paet: hoopis Venemaal on põhjust Eesti ees vabandada." *Eesti Päevaleht* 05. mai. http://epl.delfi.ee/news/eesti/paet-hoopis-venemaal-on-pohjust-eesti-ees-vabandada.d?id=51085903 (kasutatud 22.03.2014)

[267] Välisministeerium. 2007. „Välisminister kõneles Euroopa Nõukogus." *Välisministeeriumi koduleheküg* 11. mai. http://www.vm.ee/?q=node/2892 (kasutatud 22.03.2014)

Diskursusanalüüsi valimisse kuulub seega üks Ansipi, kolm Paeti ning kaks Aaviksoo kõneakti, seega kokku kuus kõne. Tabelis 4 määratletakse iga valimisse võetud kõneakti puhul julgeolekustaja (SA), referentobjekt (RO = „mina"), eksistentsiaalne oht (ET), referentsubjekt („teine"), võimalusel „meie" (RO + SA), auditoorium („sina"), kontekst, lubadus RO-d kaitsta ning intertekstuaalsus. Tabelis 4 kasutatakse ministrite kõneaktide puhul initsiaalidest ja järjekorranumbrist moodustuvat tähist, kui analüüsitakse rohkemat kui ühte ministri kõneakti. Paeti kõned on tähistatud järgnevalt: „Välisministri avaldus" (UP1), „Paet: Vene karu jätkab vana joont" (UP2) ja „Välisminister kõneles Euroopa Nõukogus" (UP3). Aaviksoo kõnede tähisteks on JA1 („Rünnak Eestile hoogustab kübersõja arutelu NATO-s") ja JA2 („Eesti-vastane kübersõda kerkis ühtlasi NATO väljakutseks"). Ansipi kõnega intertekstuaalsuse kaudu seotud kõneaktid on tähistatud AA1 („Ansip: meie suveräänne riik on tugeva rünnaku all") ning AA2 („Andrus Ansipi poliitiline avaldus riigikogu ees").

Tabel 4. Julgeolekustav liigutus pea-, kaitse- ja välisministri kõneaktides

SA	**Ansip**	**Aaviksoo**	**Paet**
RO = mina	Suveräänne Eesti riik = perekond, EL, väärikas, rahumeelne, kristlik, euroopalik, armas ja väärikas; EL	**JA1 ja JA2**: Eesti riik kui tervik; riigi infokanalid ja suhtlusportaalid = rünnak sadamate ja õhuruumi vastu	**UP1**: Eesti valitsusasutuste ja presidendi kantselei; Eesti = EL **UP2**: Eesti = ELi ja NATO osa, diplomaatiliste ja poliitilistest tavadest kinni pidaja, endine liiduvabariik, Venemaa naaberriik, koostööaldis, heade suhete otsija, Baltimaade osa **UP3**: Eesti riigiasutused ja infrastruktuur; kaudselt ka Euroopa Nõukogu liikmesriigid; Eesti = pragmaatilisuse ja heanaaberlike suhete otsija
ET	Küber-rünnakud	**JA1 ja JA2**: Küberrünnakud = huligaansus	**UP1**: Küberterrorism **UP2**: Rünnakud kübertasandil **UP3**: Küberrünnakud
Referent-subjekt = teine	Venemaa = barbaarsus, vägivald, vaenulikkus	**JA1 ja JA2**: Vaenulikud jõud	**UP1**: Venemaa **UP2**: Venemaa, Vene valitsus = Vene jõud, vene karu, propagandasõja läbiviija **UP3**: Venemaa = siseasjadesse sekkuja, vaenulikkus; Venemaa avalikkus = agressiivsus, küberkurijategijad
Meie = RO + SA	Meie = Eesti rahvas	**JA1**: Meie = Eesti, EL ja NATO	**UP3**: Meie = Euroopa Nõukogu liikmesriigid
Auditooriu	Riigikogu liikmed	**JA1 ja JA2**: Ajakirjanikud ja	**UP1**: Eesti avalikkus **UP2**: Rootsi, Soome, Läti, Leedu, EL-i

m = sina		seeläbi Eesti avalikkus	eesistujamaa Saksamaa, Euroopa komisjon (EL), NATO peasekretär (NATO), USA **UP3**: Euroopa Nõukogu liikmesriigid
Kontekst	Vahetu: Riigikogu: distaalne: Eesti	**JA1 ja JA2**: Vahetu: Valitsuse pressikonverents; distaalne: Eesti	**UP1**: Vahetu: Välisministeeriumi kodulehekülg; distaalne: Eesti **UP3**: Vahetu: Postimees.ee: distaalne: Rootsi päevaleht Svenska Dagbladet **UP3**: Vahetu: Euroopa Nõukogu Ministrite Nõukogu istung; distaalne: Strasbourg
Lubadus	Valitsus on pöördunud ELi poole ja on palunud neil reageerida koheselt.	**JA1 ja JA2**: NATOs peab saama vastuse küsimus, kas küberrünnak langeb Põhja-Atlandi lepingu alla.	**UP1**: Välisministeerium teeb ettepaneku valitsusele, milliseid meetmeid peaks EL Venemaa suhtes kehtestama (näiteks EL-Venemaa tippkohtumise edasilükkamine) küberrünnakute lõpetamiseks. **UP2**: Paet tõdes, et ta loodab asuda dialoogi ja leida olukorrale lahenduse. **UP3**: Paet lubas pöörduda Vene võimude poole üleskutsega võtta tarvitusele meetmed Venemaal tegutsevate küberkurjategijate vastu.
Interteks-tuaalsus	**AA1** ja **AA2** (Eesti)	**JA1 ja JA2**: „Visioonist lahendusteni" (Eesti); „Digital Fears Emerge After Data Siege in Estonia" (välismaa)	**UP1**: „Russia Accused of 'Attack on EU'", Eesti meedia: „Venemaa ründab Eesti kaudu Euroopa Liitu" (välismaa)

Allikas: Koostatud järgmiste allikate põhjal: Ansip. „Peaminister Andrus Ansipi kõne Riigikogu ees"; Postimees.ee. „Ansip: meie suveräänne riik on tugeva rünnaku all"; Ansip. „Andrus Ansipi poliitiline avaldus riigikogu ees"; *Välisministeerium*. „Välisministri avaldus"; *BBC News*. 2007. „Russia Accused of 'Attack on EU'." *BBC kodulehekülg* 02. mai. http://news.bbc.co.uk/2/hi/europe/6614273.stm; „Venemaa ründab Eesti kaudu Euroopa Liitu," *Eesti Päevaleht*; „Välisminister kõneles Euroopa Nõukogus," *Välisministeerium*; „Paet: Vene karu jätkab vana joont," *Postimees*; Anvelt, ja Ojakivi, „Rünnak Eestile hoogustab kübersõja arutelu NATO-s"; Kalamees, „Eesti-vastane kübersõda kerkis ühtlasi NATO väljakutseks"; Aaviksoo, Jaak. 2007. „Eesti küberjulgeolek: küberkaitse ja NATO küberkaitse." *Konverentsil Visioonist lahendusteni*. https://www.youtube.com/watch?v=113XjfYDPYs; Landler, Mark, and John Markoff. 2007. „Digital Fears Emerge After Data Siege in Estonia." *The New York Times* 29. mai. http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (kasutatud 13.12.2013)

Nii Paet kui ka Ansipi kõnest võib tuvastada referentobjekti ehk „minana" Eesti ja Euroopa Liidu. „Mina" ehk Eestit identifitseeritakse ELi, väärika, rahumeelse, kristliku, armsa, koostööalti, NATO, diplomaatilisest tavadest kinni pidaja, heade suhete otsijana, Baltimaade osa, endise liiduvabariigi ja Venemaa naaberriigina. Ansip tuvastab „meiena" Eesti rahva, Aaviksoo Eesti koos partneritega EL-is ja NATO-s ning Paet Euroopa Nõukogu liikmesriigid, et mõjuda veenvamana auditooriumi jaoks.

Ansipi kõne toimus päev aega hiljem kui Paeti kõne „Välisministri avaldus", seega võib leida nende kõnede vahel intertekstuaalsuse, sest 1. mail 2007. aastal ütles Paet, et Välisministeerium teeb ettepaneku valitsusele, mis meetmeid peaks EL kasutama (UP1) ning 2. mail ütles Ansip, et valitsus on pöördunud EL-i poole, seega võib leida nii Paeti kui ka Ansipi kõnest selge lubaduse kaitsta referentobjekti. Paet andis ka teistes kõneaktides lubaduse. Paet rõhutas vajadust dialoogi astuda küberrünnete teemal ja leida olukorrale lahendus (UP2) ning Paet lubas pöörduda Venemaa poole võtta tarvitusele meetmed küberkurjategijate vastu (UP3). Samuti võib Aaviksoo mõlemast kõnest leida lubaduse referentobjekti kaitsta, sest Aaviksoo sõnas, et NATO tasandil tuleb leida kokkulepe, kas küberrünne käib Põhja-Atlandi lepingu alla.

Pea-, välis- ja kaitseminister kuulutasid, et küberründed on suunatud suveräänse riigi kui terviku vastu, kuid tegelikult kui viidatakse, et ohud eksisteerivad riigile, siis võib 2007. aasta küberrünnete ajal referentobjektideks pidada kitsamalt ka valitsust, ühiskonda, riiklikku suveräänsust, majandust, indiviide, võrke, rahvust, riigiinstitutsioone (president, ministeeriumid, parlament), finantsinstitutsioone (pangad), meediat (ajalehed, uus meedia jne) ja ettevõtteid (ettevõtjaid), sest küberründeid riigi vastu ei ole kerge tõestada. Tavaliselt on julgeolekustajal raske julgeolekustada eksistentsiaalseid ohtusid iseenda vastu, kuid kuna pea- ja kaitseminister tuvastasid referentobjektina riigi kui terviku, siis nad rääkisid kaudselt ka valitsuse vastu suunatud eksistentsiaalsetest ohtudest, ning ainsana ütles välisminister otse välja, et küberründed on suunatud Eesti valitsusasutuste vastu. 2007. aasta küberründeid võib klassifitseerida ka kui eksistentsiaalseid ohte konkreetsete sektorite (majanduslik, poliitiline ja sotsiaalne sfäär) ning indiviidide kaudu ka keskkonnasektori vastu.

Nii Paet kui ka Ansip identifitseerisid „teisena" Venemaa, keda süüdistati küberrünnete läbiviimises, kuid samas on Hansen ja Nissenbaum tõdenud, et tegelikult ei olnud selget digitaalselt jälge, mis seoks Venemaa rünnetega, ning Eesti julgeolekustavad tegutsejad ei suutnud selles veenda ka rahvusvahelist auditooriumi (eelkõige ELi ja NATO-t).[268] Tegelikult on siiani ainult üks inimene (Konstantin Goloskokov, noorteorganisatsiooni

[268] Hansen *et al*. „Digital Disaster," 1170.

Naši liige) avalikult tunnistanud, et ta võttis osa küberrünnetest, seega hoolimata spekulatsioonidest poliitilisel tasandil,[269] ei ole rünnete tegelik päritolu kinnitatud.

Kuigi enamasti postitati just venekeelsetesse foorumitesse juhiseid Internetikasutajate poolt, ei saa ühegi valitsuse rolli rünnetes kinnitada.[270] Venemaad kui „teist" seostati Ansipi ja Paeti kõnedes vaenulikkuse, barbaarsuse, vägivalla, propagandasõja ja agressiivsusega. Paet nimetab Venemaad „Vene karuks" ja „siseasjadesse sekkujaks" ning Ansip ja Paet kaudselt „mitte Euroopa Liiduks" kuna tõdevad, et Venemaa ründas Euroopa Liitu. Kari Alenius on ka tõdenud, et Venemaa süüdistamine küberrünnetes oli vaenlase („teise") identifitseerimine, kes oli avalikus debatis vale, pahatahtlik ja kriminaalne.[271] Ainsana julgeolekustajatest ei seostanud küberründeid Venemaaga Aaviksoo, kes ütles, et küberrünnete korraldatajateks on vaenulikud jõud.

Eesti valitsuse diskursuses seostati häkkimine terrorismi[272] (näiteks „Välisministri avaldus") ja huligaansusega („Rünnak Eestile hoogustab kübersõja arutelu NATO-s" ja „Eesti-vastane kübersõda kerkis ühtlasi NATO väljakutseks"), kuid Ansip, Aaviksoo ja Paet nimetasid eksistentsiaalseteks ohtudeks lihtsalt ka küberründeid. Käesoleva magistritöö terminoloogilise aluspõhja alusel olid eksistentsiaalseteks ohtudeks referentobjektidele laiemalt küberründed ning kitsamalt kübervandalism ning küberkuritegevus ja veel kitsamalt DDoS ründed.

Peaminister Ansipil oli vaja veenda Riigikogu ehk seadusandlikku võimu, sest Vabariigi Valitsus peab astuma tagasi, kui Riigikogu avaldab valitsusele või peaministrile umbusaldust ja president ei ole kolme päeval jooksul valitsuse ettepanekul välja kuulutanud Riigikogu erakorralisi valimisi,[273] seega oli vaja peaministril veenda riigikogu liikmeid vahetust kontekstist lähtuvalt, et talle ei avaldataks umbusaldust seoses pronkssõduri teisaldamisega. Ansip pööras oma kõnes tähelepanu ka pronkssõdurile, kus ta kinnitas riigikogu liikmetele, et pronkssõduri teiseldamisega ei olnud võimalik venitada, sest 26. aprilli öösel Tallinnas puhkenud vandaalitsemiste

[269] Näiteks: Rand, Erik. 2007. „Laar: suutlikkus Venemaa küberrünnakud tõrjuda on tõstnud Eesti mainet." *Eesti Päevaleht* 11. juuli. http://epl.delfi.ee/news/eesti/laar-suutlikkus-venemaa-kuberrunnakud-torjuda-on-tostnud-eesti-mainet.d?id=51093834 (kasutatud 10.03.2014)

[270] Kaska *et al*. „Developments in the Legislative," 46.

[271] Alenius, Kari. 2013. „An Exceptional War that Ended in Victory for Estonia or and Ordinary E-Disturbance? Estonian Narratives of the Cyber-Attacks in 2007." In *Case Studies in Information Warfare and Security: For Researchers, Teachers and Students*, ed. Matthew Warren. Academic Conferences Limited, 61-62.

[272] Hansen *et al*. „Digital Disaster," 1171.

[273] Vabariigi Valitsuse seadus.

laine ja kurjategijate vägivald Eesti elanike turvalisuse ja vara vastu ei jätnud valitsusele teist võimalust.[274] Ansip sidus oma kõnes nii pronksõduri teisaldamise kui ka küberründed Eestis, mis näitab selgelt, et Ansip soovis küberrünnetega tähelepanu ära tõmmata pronkssõduri teisaldamisega seotud küsitavustelt.

Aaviksoo kõneaktid olid suunatud ajakirjanikele ja seeläbi Eesti avalikkusele. Paeti kõnede auditooriumiks olid Eesti avalikkus (UP1), Rootsi, Soome, Läti, Leedu, EL, NATO, USA ja Saksamaa (UP2) ning Euroopa Nõukogu liikmesriigid (UP3). Auditooriumiks võib pidada seega poliitikategijaid Eestis („Peaminister Andrus Ansipi kõne Riigikogu ees" ja „Välisministri avaldus") ja välismaal („Välisminister kõneles Euroopa Nõukogus"), sest Kingdoni „probleemide voole" on iseloomulik see, et poliitikategijad tajuvad teatud tingimusi poliitiliste probleemidena (eriti dramaatiliste sündmuste ajal) ning näevad vajadust nende vastu võidelda, seega tuleb teisi poliitikategijaid veenda, et konkreetne probleem on tõesti probleem. Viitamise kaudu kõnetasid Paet ja Aaviksoo ka rahvusvahelist auditooriumi.

Samuti võib auditooriumiks pidada ka konkreetse rahvuse indiviide, kodanikke ja valijaskonda kuna ministrite legitiimsus sõltub valijatest. Kuna Eestis toimunud küberründed mõjutasid nii üksikisikut, riigi esindajaid kui ka ettevõtjaid, siis ei olnud Ansipil, Paetil ja Aaviksool raske samastuda auditooriumi ehk Eesti avalikkuse ja poliitikategijate tunnetega, sest ka ministrid olid mõjutatud. Balzacqi järgi peab „volitav auditoorium" olema otseselt seotud probleemiga ja volitama julgeolekustajat probleemiga tegelema. Nii Eesti poliitikategijatel kui ka indiviididel oli otsene põhjuslik seotus küberrünnetega olemas ning nad volitasid julgeolekustajaid probleemiga tegelema läbi ministritele omistatud mõjuvõimu.

Eesti avalikkuse seotust küberrünnetega võib näha avaliku arvamuse küsitluste abil. Samas on Balzacq tõdenud, et arvamusküsitluste tulemusi peab käsitlema ettevaatlikkusega, sest neil on üldiselt piiratud tähtsus julgeolekustamise keerulise protsessi mõistmiseks. Küsitlused võivad mängida rolli julgeolekustavates liigutustes, kuid samal ajal võidakse neid ära kasutada julgeolekustamise juhtumite selgitamiseks.[275] Avaliku arvamuse küsitlused ei ole parimaks võimaluseks

[274] Peaminister Andrus Ansipi kõne Riigikogu ees. Valitsuse kommunikatsioonibüroo, 02.05.2007. http://www.valitsus.ee/et/valitsus/Valitsuse-liikmed/peaminister/Peaministri-koned/51/peaminister-andrus-ansipi-k%C3%B5ne-riigikogu-ees (06.04.2014)

[275] Balzacq. *Securitization Theory*, 42.

kontrollimaks auditooriumi nõusolekut, sest nad ei näita alati täielikku tõtt ühiskonna arvamuse kohta, kuid siiski on võimalik nende põhjal teha üldisi järeldusi.

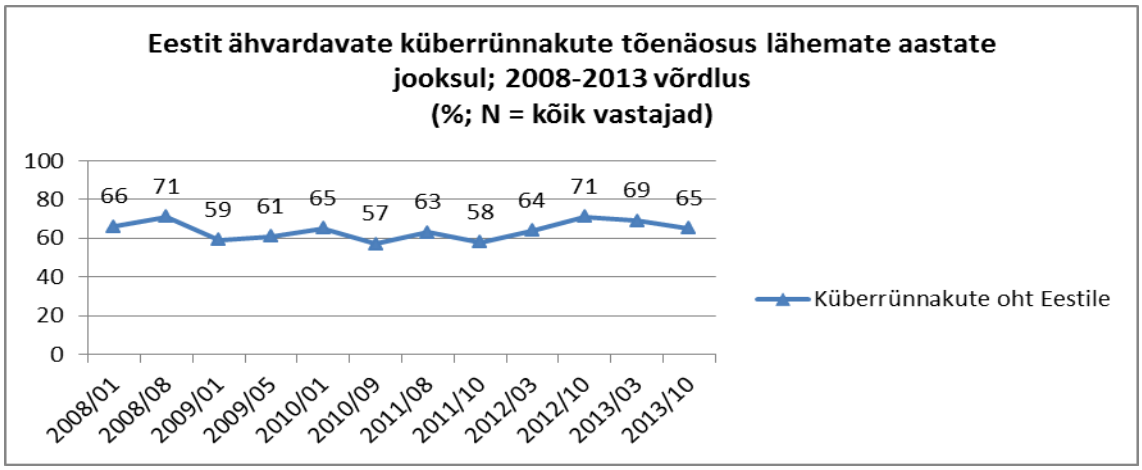
Eesti avalikkuse suhtumine küberrünnetesse kajastub uuringutes „Avalik arvamus ja riigikaitse", mille raames küsitletakse umbes 1000 eestimaalast (varieerub uuringust uuringusse) vanuses 15–74 eluaastat. Saamaks ülevaadet, millised on inimeste arvates Eesti riigile kõige tõenäolisemad ohud, palutakse vastajail hinnata mitmesuguste võimalike ohtude (näiteks küberrünnakud, ulatuslik merereostus, massilised tänavarahutused jne) tõenäosust lähemate aastate jooksul.[276]

Jooniselt 4, mis on tehtud erinevate aastate „Avalik arvamus ja riigikaitse" uuringute põhjal, on näha Eesti elanike suhtumine küberrünnakute tõenäosusesse. Küberrünnakute tõenäosust on peetud ajavahemikus 2008–2013 üsna suureks – 57-71%. Näitaja on graafikule kantud alates 2008. aasta jaanuarikuust, sest esimeses uuringus, mis avaldati pärast 2007. aasta küberrünnakuid juulikuus, ei olnud veel küberrünnete temaatikat sees.[277] Juba järgmises uuringus, mis ilmus 2008. jaanuaris, on küberründed leidnud kajastamist. Küberrünnakute põhjal on graafikule kantud kokkuliidetud protsent inimeste arvamusest, kes peavad küberrünnakuid väga või küllaltki tõenäoliseks.

Küberrünnakuid on uuringutes ajavahemikus 2008–2013 peetud peaaegu alati kõige tõenäolisemaks ohuks (välja arvatud 2008. aasta jaanuari, 2009. aasta jaanuari ja mai uuringutes, mil peeti esimeseks ohuks ulatuslikku merereostust, ning 2010. aasta jaanuari uuringus, kui küberrünnakud jagasid esimest kohta merereostusega). See näitab, et küberrünnakuid on teistest ohtudest vaieldamatult rohkem mainitud.

[276] Saar Poll. 2013. oktoober. *Avalik arvamus ja riigikaitse*. Tallinn: Kaitseministeerium, 4. http://www.kmin.ee/et/avalik-arvamus (kasutatud 30.11.2013)

[277] Turu-uuringute AS. 2007. juuli. *Avalik arvamus ja riigikaitse*. Tallinn: Kaitseministeerium, 4. http://www.kmin.ee/et/avalik-arvamus (kasutatud 05.04.2013)



Joonis 4. Küberrünnete tõenäosus Eestis avaliku arvamuse järgi, jaanuar 2008 – oktoober 2013 (%; N = kõik vastajad)
Allikas: Koostatud järgmiste uurimuste põhjal: Turu-uuringute AS. 2010. september. *Avalik arvamus ja riigikaitse*. Tallinn: Kaitseministeerium. http://www.kmin.ee/et/avalik-arvamus (kasutatud 05.04.2013); Turu-uuringute AS. 2011. august. *Avalik arvamus ja riigikaitse*. Tallinn: Kaitseministeerium. http://www.kmin.ee/et/avalik-arvamus (kasutatud 05.04.2013); Saar Poll. 2013. märts. *Avalik arvamus ja riigikaitse*. Tallinn: Kaitseministeerium. http://www.kmin.ee/et/avalik-arvamus (kasutatud 05.04.2013); Saar Poll. 2013. oktoober. *Avalik arvamus ja riigikaitse*.

Joonise 4 tulemuste põhjal saab järeldada, et Eesti riik teab, et avaliku arvamuse järgi on küberrünnakud ohtlikud referentobjektidele. Eesti elanikkond (avalikkust) võib pidada auditooriumiks ja referentobjektiks, kes tunnetab küberrünnete ohtu, mis annab ministrile õiguse neile omistatud legitiimsuse abil küberohtudega tegeleda.

Siiski oli Eesti võimudel raskusi, et veenda oma esmast rahvusvahelist auditooriumi ehk NATO liitlasi, et küberründed moodustasid rünnaku Eesti suveräänsuse vastu, millest tulenevalt oleks pidanud appi võtma Washingtoni leppe artikli 5,[278] millele viitas ka Aaviksoo oma kõneaktides. Artikkel 5 seisneb selles, et relvastatud rünnakut ühe või mitme NATO liikme vastu Euroopas või Põhja-Ameerikas käsitletakse rünnakuna nende kõigi vastu, mistõttu võib üksi või koos teiste lepingupooltega kasutada vajalikke abinõusid (ka relvajõudusid) julgeoleku taastamiseks ja säilitamiseks. Artikkel 6 täpsustab, et artikli 5 järgi on relvastatud kallaletung lepinguosalise relvajõudude, laevade või lennuväljade vastu.[279]

Kuna Washingtoni lepingu artikkel 5 ja 6 keskenduvad just relvastatud rünnakule laevade, relvajõudude ja lennuväljade vastu, siis ei mahu küberruumis toimuv küberrünne Põhja-Atlandi lepingu artikkel 5 alla. Kui vaadata Washingtoni leppe sisu,

[278] Hansen *et al*. „Digital Disaster," 1169.
[279] The North Atlantic Treaty Organization. 1949. *The North Atlantic Treaty*. Washington D.C. http://www.nato.int/cps/en/natolive/topics_89597.htm (kasutatud 15.02.2014)

siis on mõistetav, miks Aaviksoo on võrrelnud küberründeid rünnakuga riigi sadamate või õhuruumi vastu. Samas ei tähenda see seda, et Eesti ei saanud üldse liitlastelt toetust, vaid NATO, EL ja USA lähetasid küberjulgeoleku meeskondasid Eestisse,[280] näiteks NATO vaatleja toetas konsultatsiooni kaudu Eestit.[281]

Nii Ansip, Paet kui ka Aaviksoo andsid enda kõneakti(de)s 2007. aasta küberrünnete ajal lubaduse kaitsta referentobjekti. Pea-, kaitse- ja välisministrid astusid seega julgeolekustava liigutuse 2007. aasta küberrünnete ajal, millest lähtuvalt uuritakse järgmises peatükis julgeolekupraktikat, et analüüsida, kas ministrite julgeolekustavad liigutused on kooskõlas julgeolekupraktikaga.

5.2. Julgeolekupraktika

On raske kohe öelda, kas küberjulgeolekustamine on toimunud, sest meetmeid küberrünnetega tegelemiseks ei ole alati võimalik koheselt ellu viia (näiteks arengukavade vastuvõtmine). Sellest tulenevalt ei keskenduta magistritöös ainult 2007. aasta küberrünnetele ja vahetutele meetmetele, vaid on oluline analüüsida meetmeid, mis on ette võetud pärast 2007. aasta ründeid pea-, kaitse- ja välisministri poolt.

Uurimistöös analüüsitakse julgeolekustajate meetmeid riiklikul poliitilisel tasandil koostatud arengukavade kaudu, milles on määratletud tegevussuunad ja meetmed nende saavutamiseks,[282] sest Eestis toimunud küberründed nõudsid riiklikke meetmeid. Kuna käesolevas töös käsitletakse julgeolekustajatena ministreid, siis nemad ei võta ette konkreetseid meetmeid juriidilisel ja tehnilisel tasandil, vaid võivad nendele valdkondadele viidata arengukavades määratletud tegevussuundade kaudu.

Ministrite kõneaktid väljendavad riigi seisukohta ja on sünkroniseeritud vastava ministeeriumi tegevussuundadega, seega on oluline analüüsida arenukavasid, milles pannakse paika vastava ministeeriumi tegevussuunad. Magistritöös analüüsitakse arengukavasid, mille koostamise aluseks on Vabariigi Valitsuse määrus „Strateegiliste arengukavade liigid ning nende koostamise, täiendamise, elluviimise, hindamise ja aruandluse kord". Strateegiliste arengukavade liikideks on valdkonna ja

[280] Hansen *et al*. „Digital Disaster," 1170
[281] Kaska *et al*. „Developments in the Legislative," 47.
[282] Strateegiliste arengukavade liigid.

organisatsioonipõhised arengukavad. Valdkonna arengukavad kajastavad ühe või mitme valdkonna eesmärke ja nende saavutamiseks vajalikke meetmeid, mille elluviimist korraldab kas üks ministeerium või mitu ministeeriumi koostöös. Organisatsioonipõhised arengukavad on ministeeriumi valitsemisala ja ministeeriumi valitsemisala riigiasutuste arengukavad, mis koostatakse järgmise eelarveaasta ning sellele järgneva kolme aasta kohta.[283] Uurimistöös käsitletakse valdkondlikke arengukavasid, milles määratletakse meetmed eesmärkide saavutamiseks, sest organisatsioonipõhised arengukavad keskenduvad eelarvele, kuid käesolevas töös on oluline tähelepanu pöörata meetmetele.

5.2.1. Arengukavad julgeolekustava liigutuse osana ja julgeolekupraktikana

Kuna ministrite kõneaktides on tavaliselt ainult pinnapealses sõnastuses antud lubadus kaitsta referentobjekti, siis võib siduda julgeolekustava liigutuse etapi julgeolekupraktikaga selles tähenduses, et analüüsida ministeeriumitega seotud valdkondlikke arengukavasid, millest võib tuvastada eesmärkide kaudu lubaduse kaitsta referentobjekti. Sellest tulenevalt pakutakse empiirika peatükis täiendus küberjulgeolekustamise teooriale, mis seisneb selles, et riigi esindajate lubadust võib kinnitada dokumentides määratletud sihtidega. Seda on võimalik uurida Eesti arengukavade abil, et tuvastada nendest kübervaldkonna käsitlemine ja meetmed küberrünnetega võitlemiseks. Arengukavade koostamise ja nendes identifitseeritud meetmete abil on võimalik analüüsida, kas pea-, kaitse- ja välisministri julgeolekustav liigutus on kooskõlas julgeolekupraktikaga.

Valdkonna arengukava viiakse ellu rakendusplaani alusel, mille vastutav minister esitab valitsusele hiljemalt kolme kuu jooksul dokumendi kinnitamisest arvates,[284] kuid riik ei avalikusta enamasti rakenduskavasid (näiteks „Küberjulgeoleku strateegia 2008–2013" rakendusplaane aastateks 2009–2011 ja 2012–2013).[285] Rakendusplaanid on strateegias nimetatud eesmärkide elluviimiseks vastuvõetud dokumendid, mille pinnalt saab

[283] Strateegiliste arengukavade liigid.
[284] Ibid.
[285] „Küberjulgeoleku strateegia 2008–2013" rakendusplaani aastateks 2009-2011 heakskiitmine. 2009. Riigi Teataja 2009, 43, 596. https://www.riigiteataja.ee/akt/13182154 (kasutatud 26.03.2014); Küberjulgeoleku strateegia 2008–2013" rakendusplaani 2012-2013 heakskiitmine. 2011. Riigi Teataja III, 2011, 5. https://www.riigiteataja.ee/akt/330122011005 (kasutatud 26.03.2014)

ülevaate, kas arengukavas antud lubadus kaitsta referentobjekti on kooskõlas rakendusplaaniga. Kuna kõik rakendusplaanid ei ole avalikult kättesaadavad, siis on uurimistöö sihiks uurida vastavalt arengukavades määratletud meetmele ministrite ettevõetud meetmeid, et hinnata iseseisvalt, kas ministri julgeolekustav liigutus on julgeolekupraktikaga kooskõlas.

Käesolevas magistritöös analüüsitakse kõiki Eestis kehtivaid arengukavasid, mida on Vabariigi Valitsuse andmeil 28. aprilli 2014. aasta seisuga kokku viiskümmend viis ja mille on heaks kiitnud valitsus ja Riigikogu.[286] Tekstide valiku alla kuuluvad seega kõik 55 arengukava, kuid analüüsiobjektideks võetakse ainult need arengukavad, milles käsitletakse kübervaldkonda ning mille eest on vastutavaks ministeeriumiks Kaitse- või Välisministeerium või millega on seotud valitsus. Peaministri kui valitsuse esindaja rolli analüüsitakse nende arengukavadega seoses selles tähenduses, kas valitsus on dokumendi heaks kiitnud või olnud seotud muudmoodi strateegia loomisega.

Kübervaldkonda on mainitud seitsmes arengukavas. Analüüsiobjektideks võetakse „Eesti julgeolekupoliitika alused" (2010), sest selle koostas valitsus Välisministeeriumi juhtimisel[287] ning Kaitseministeeriumi vastutusalasse kuuluvad „Riigikaitse strateegia" (2010)[288] ja „Küberjulgeoleku strateegia 2008-2013" (2008)[289]. Analüüsi aluseks ei võeta Riigikogu poolt heaks kiidetud arengukava „Eesti turvalisuspoliitika põhisuunad aastani 2015", sest selle põhimõtete elluviimise ja eesmärkide saavutamise üle valvab Siseministeerium ning seda ei kiitnud heaks ka valitsus,[290] seega ei saa sellest dokumendist tuvastada Ansipi, Aaviksoo või Paeti julgeolekupraktikat.

Magistritöös uuritakse põgusalt ülejäänud kolme strateegilist arengukava valitsuse ja Ansipi rolliga seoses. Valitsus kiitis heaks „Riigikaitse arengukava 2013-2022" (2013), mille eest vastutajaks on Kaitseministeerium.[291] Kuna nimetatud dokument võeti vastu 2013. aastal, mil Aaviksoo ei olnud enam kaitseministri ametis, siis kuulub see ainult

[286] Vabariigi Valitsuse koduleheküIg. http://valitsus.ee/et/valitsus/arengukavad (kasutatud 28.04.2014)
[287] Julgeolekupoliitika aluste töörühm. Eesti julgeolekupoliitika alused, 6.
[288] *Riigikaitse strateegia*. 2010. Tallinn, 17. http://www.kmin.ee/et/riigikaitse-alusdokumendid (kasutatud 15.04.2014)
[289] Küberjulgeoleku strateegia komisjon. *Küberjulgeoleku strateegia 2008-2013*.
[290] Eesti turvalisuspoliitika põhisuundade aastani 2015 heakskiitmine.
[291] Kaitseministeerium. *Riigikaitse arengukava 2013-2022*. 2013. Tallinn, 1. http://www.kmin.ee/et/riigikaitse-alusdokumendid (kasutatud 28.04.2014)

Ansipi julgeolekupraktika alla, sest Ansip kiitis selle heaks.[292] Põhjaliku uurimise alt jääb välja ka 2013. aastal Vabariigi Valitsuse poolt kinnitatud arengukava Eesti teadus- ja arendustegevuse ning innovatsiooni strateegia 2014-2020 „Teadmistepõhine Eesti", mille rakendamise eest vastutajateks on Haridus- ja Teadus- ning Majandus- ja Kommunikatsiooniministeerium ning teised ministeeriumid. Analüüsi aluseks olevate ministeeriumite hulgast on Kaitseministeerium selle arengukava järgi vastutav Eesti nähtavuse suurendamise eest rahvusvahelises teadus- ja arendustegevuse alases koostöös ning ühiskondliku ja majandusliku kasu suurendamises.[293] Samas ei kuulu see arengukava analüüsiobjektide hulka, sest selles on mainitud ainult joonealuses märkuses prefiksiga „küber-" seotud terminit. Nimetatud arengukava võib pidada seega ainult Ansipi praktikaks kuna valitsus (eesotsas Ansipiga) kiitis selle dokumendi heaks.

„Eesti infoühiskonna arengukava 2020" (2013) koostamist juhtis ja meetmete elluviimise eest üldvastutajaks on Majandus- ja Kommunikatsiooniministeerium,[294] mistõttu ei kuulu nimetatud dokument analüüsiobjektide alla. Samas võib selle strateegilise arengukava heaks kiitmist pidada Ansipi julgeolekupraktikaks.[295]

Kokku analüüsitakse süvitsi seega kolme arengukava. Esiteks uuritakse esmakordselt koostatud arengukava „Küberjulgeoleku strateegia 2008-2013", et tuvastada lubadust kaitsta referentobjekti ja kaitseministri julgeolekupraktikat. Kaitseminister Aaviksoo tegi ettepaneku koostada küberjulgeoleku strateegia aastaiks 2008-2013, mille kiitis valitsus heaks 15. novembril 2007. aastal,[296] seega võib seda pidada otseseks Aaviksoo julgeolekupraktikaks. Seejärel andis valitsus 2007. aastal Eesti küberruumi haavatavuste vähendamiseks Kaitseministeeriumile korralduse koostada „Küberjulgeoleku strateegia 2008-2013" koostöös Haridus- ja Teadus-, Justiits-, Majandus- ja Kommunikatsiooni-, Sise- ja Välisministeeriumi, CERT-EE ning Eesti ettevõtete ekspertidega. 2008. aastal kinnitas valitsus Kaitseministeeriumi juurde loodud komisjoni ettevalmistatud „Küberjulgeoleku strateegia 2008-2013".[297]

---

[292] „Riigikaitse arengukava 2013–2022" heakskiitmine. 2013. Riigi Teataja III, 2013, 8. https://www.riigiteataja.ee/akt/329012013008 (kasutatud 26.03.2014)
[293] Eesti teadus- ja arendustegevuse ning innovatsiooni strateegia 2014–2020, 1, 14, 16-17.
[294] Majandus- ja Kommunikatsiooniministeerium. *Infoühiskonna arengukava 2020*, 4, 19.
[295] „Eesti infoühiskonna arengukava 2020" ja selle rakendusplaani aastateks 2014–2015 heakskiitmine. 2013. Riigi Teataja III, 2013, 14. https://www.riigiteataja.ee/akt/319112013014 (kasutatud 26.03.2014)
[296] Eesti Suursaatkond Washingtonis koduleheküIg. http://www.estemb.org/press/us_media/aid-965 (kasutatud 09.04.2014)
[297] Küberjulgeoleku strateegia komisjon. *Küberjulgeoleku strateegia 2008-2013*, 8-9.

Küberjulgeoleku strateegia ettepaneku heaks kiitmist, valitsuse korraldust koostada küberjulgeoleku strateegia ning lõplikut strateegia kinnitamist võib pidada Ansipi julgeolekupraktikakas, sest Ansip kui valitsuse esindaja on nende tegevustega seotud. Kuigi Aaviksoo ei koostanud ise otseselt küberjulgeoleku strateegiat, siiski tegi ta ettepaneku valitsusele luua strateegia, mille koostamise komisjoni juhtis Kaitseministeerium, seega võib kaitseministrit pidada ka julgeolekupraktika elluviijaks.

Arengukavas „Küberjulgeoleku strateegia 2008-2013" tõdetakse, et küberjulgeolek tugineb Eestis riigi kui terviku küberruumi haavatavuste vähendamisele, seega määratletakse strateegias küberjulgeoleku tagamise eesmärgid ja meetmed.[298] Küberjulgeoleku strateegias antakse selge lubadus kaitsta referentobjekti ehk riiki kui tervikut konkreetsete tegevusvaldkondlike meetmete abil, mis seob julgeolekustava liigutuse etapi julgeolekupraktikaga ning võimendab Aaviksoo lubadust kaitsta referentobjekti. Aaviksoo meetmeid analüüsitakse uurimistöö viimases alapeatükis vastavalt küberjulgeoleku strateegiale.

Küberjulgeoleku strateegias eristatakse küberjulgeoleku tagamiseks ja tugevdamiseks viite tegevusvaldkonda ja meetmeid nende saavutamiseks. Tegevusvaldkondadeks on esiteks turvameetmete süsteemi arendamine ja rakendamine (tegevused organisatoorse koostöö, tehniliste meetmete ja füüsilise turbe valdkonnas) ning teiseks küberjulgeoleku alase kompetentsuse tõstmine (küberkaitse alane väljaõpe ning teadus- ja arendustegevus põhiõppes ja täiendusõppes). Kolmandaks valdkonnaks on küberjulgeoleku tagamiseks vajaliku õigusruumi täiendamine (õigusaktide väljatöötamine, olemasoleva seadusandluse täiendamine ja rahvusvahelise õiguse arendamine). Neljandaks on rahvusvahelise koostöö edendamine (Eesti teadmiste jagamine, rahvusvahelise teadlikkuse tõstmine ja koostöö ennetus- ja kaitsemeetmete valdkonnas). Viiendaks valdkonnaks on küberjulgeoleku alane teavitustegevus nii riigisisesel kui ka rahvusvahelisel tasandil.[299]

Nimetatud valdkondadest ei käsitleta turvameetmete süsteemi, õigusruumi kujundamist ja kompetentsuse tõstmist, sest nii õiguslikud, tehnoloogilised kui ka teadus- ja arendustegevuse meetmed kuuluvad vastavate valdkonda spetsialistide (näiteks juristid, infotehnoloogia spetsialistid jne) pädevusse, mitte ministri tööülesannete hulka.

[298] Küberjulgeoleku strateegia komisjon. *Küberjulgeoleku strateegia 2008-2013*, 4-6.
[299] Ibid., 4-6, 27-35.

Uurimistöös ei analüüsita ka otseselt ministri poolset rahvusvahelise koostöö arendamist, vaid sellele keskendutakse küberjulgeoleku alase teavitustegevuse analüüsi juures, et juhtida tähelepanu asjaolule, et teavitustöö võib aidata kaasa koostöö edendamisele. Koostöö aspekti ei uurita süvitsi, sest ministrid ei tegele otseselt koostööga kaitse- ja ennetusmeetmete valdkonnas Eesti teadmiste jagamise kaudu. Käesolevas töös uuritakse meetmena teavitustööd koostöö loomiseks nii siseriiklikul kui ka rahvusvahelisel tasandil, mida analüüsitakse järgnevas alapeatükis.

Lisaks küberjulgeoleku strateegia koostamisele on Eesti Vabariik viinud küberjulgeoleku teema ka mitmesugustesse riigikaitse alusdokumentidesse. Esiteks käsitletakse „Eesti julgeolekupoliitika aluseid", mille muutmise algatas Vabariigi Valituses välisminister Paet. 20. mail 2009. aastal moodustas Paet „Julgeolekupoliitika aluste" (2010) eelnõu koostamiseks töörühma, mis koosnes Välis-, Kaitse-, Sise-, Majandus- ja Kommunikatsiooni-, Sotsiaal-, Keskkonna-, Rahandus- ja Justiitsministeeriumi esindajatest. Töörühma töö tulemusena valmis 2010. aasta märtsis „Julgeolekupoliitika aluste" eelnõu.[300] „Eesti julgeolekupoliitika alused" (2010) koostas valitsus (Välisministeeriumi juhtimisel), kes määratles Eesti julgeolekupoliitika eesmärgid, põhisuunad ja andis julgeolekuolukorra üldhinnangu.[301] Paeti julgeolekupraktikaks võib pidada seda, et ta algatas „Julgeolekupoliitika aluste" muutmise ning moodustas arengukava koostamiseks töörühma, mida juhtis Välisministeerium.

Rahuaja riigikaitse seaduse § 26 käsitleb julgeolekupoliitika aluseid, kus sätestatakse, et enne julgeolekupoliitika aluste või nende muudatuste heakskiitmist valitsuses kuulavad välis- ja kaitseminister ära Riigikogu välis- ja riigikaitsekomisjoni seisukohad,[302] mis toimus 8. märtsil 2010. aastal.[303] Välisminister Paet arutas strateegiat selle eri valmimisetappides Riigikogu välis- ja riigikaitsekomisjonidega, kelle esitatud märkusi võeti arvesse.[304] Nii kaitseminister Aaviksoo kui ka välisminister Paet kohtusid Riigikogu riigikaitse- ja väliskomisjonidega nende seisukohtade kuulmiseks ja

[300] *Eesti julgeolekupoliitika alused 2010. Seletuskiri*, 1.
[301] Julgeolekupoliitika aluste töörühm. Eesti julgeolekupoliitika alused, 6.
[302] Rahuaja riigikaitse seadus. 2002. Riigi Teataja I, 2002, 57, 354. https://www.riigiteataja.ee/akt/12751452 (kasutatud 08.04.2014)
[303] *Eesti julgeolekupoliitika alused 2010. Seletuskiri*, 2.
[304] Ibid., 1-2.

muudatusettepanekute sisseviimiseks, seega võib ka seda pidada Paeti ja Aaviksoo julgeolekupraktikaks.

2010. aastal Vabariigi Valitsuse esitatud „Eesti julgeolekupoliitika alustes", mille kiitis heaks Riigikogu, on esmakordselt räägitud kübervaldkonnast, mida eelmises ehk 2004. aasta kontseptsioonis veel ei mainitud.[305] „Julgeolekupoliitika alustes" (2010) on öeldud, et küberrünnakutega võidakse ühiskonnale tekitada märkimisväärset kahju terroristlike rühmituste ja organiseeritud kuritegevuse poolt. Eesti julgeolekupoliitika eesmärk on kindlustada Eesti riigi iseseisvus ja sõltumatus, põhiseaduslik kord, territoriaalne terviklikkus ja rahva turvalisus.[306] Dokumendis on antud lubadus kaitsta referentobjekti (suveräänset riiki kui tervikut ning kitsamalt rahvast ja ühiskonda) kuna on tõdetud, et küberkuritegude ennetamiseks ja tõkestamiseks tugevdatakse ametkondade koostööd riigi ja rahvusvahelisel tasandil. Lisaks arendatatakse seadusandlust, soodustatakse inimeste teadlikkuse tõstmist ning tagatakse küberkuritegevusevastase võitluse jätkusuutlikkus ja vajaliku tehnilise oskusteabe kättesaadavus.[307]

Sarnaselt Eesti küberjulgeoleku strateegiale on ka julgeolekupoliitika alustes määratletud meetmed referentobjekti olukorra paremaks muutmiseks, kuid „Eesti julgeolekupoliitika alustes" väljatoodud meetmed ei kuulu otseselt ministri pädevusse. Uurimise alt jäävad välja „Eesti julgeolekupoliitika alustes" määratletud meetmed, sest seadusandluse ja tehnilise taseme arendamise, inimeste teadlikkuse tõstmise, oskusteabe levitamise ja küberkuritegevusevastase võitlusega tegelevad vastava valdkonna spetsialistid, mitte ministrid, kes puutuvad nendega kaudselt kokku. Magistritöös analüüsitakse seega vastavalt „Küberjulgeoleku strateegiale 2008-2013" julgeolekupraktikana teadvustamist koostöö saavutamiseks riigi- ja rahvusvahelisel tasandil.

Lisaks julgeolekupoliitika alustele on oluliseks arengukavaks ka „Riigikaitse strateegia" (2010), mis tugineb Riigikogus 2010. aastal heaks kiidetud „Eesti julgeolekupoliitika alustele", ning asendab „Sõjalise kaitse strateegilise kava" (2005),[308] millest viimases ei

[305] Eesti Vabariigi julgeolekupoliitika alused. 2004. Riigi Teataja I, 2004, 49, 344. https://www.riigiteataja.ee/akt/773389 (kasutatud 26.03.2014)
[306] Julgeolekupoliitika aluste töörühm. Eesti julgeolekupoliitika alused, 4, 6.
[307] Ibid., 16.
[308] Sõjalise kaitse strateegilise kava kehtestamine. 2005. Riigi Teataja I, 2005, 5, 17. https://www.riigiteataja.ee/akt/840391 (14.04.2014)

olnud veel kübervaldkonnast juttu. Valitsus kehtestas „Riigikaitse strateegia" kaitseministri ettepanekul,[309] mis on seeläbi Aaviksoo ja Ansipi julgeolekupraktikaks. „Riigikaitse strateegia" järgi koordineerib Kaitseministeerium küberkaitset oma valitsemisalas, Kaitseliit arendab küberkaitsevõimet ning Politse- ja Piirivalveamet ennetab ja tõrjub küberruumi ähvardavaid ohte,[310] kuid kuna „Riigikaitse strateegias" ei ole määratletud konkreetseid meetmeid küberjulgeoleku tagamiseks, siis ei analüüsita julgeolekustajate poolset meetmete elluviimist „Riigikaitse strateegia" põhjal.

Käesoleva alapeatüki pinnalt lisandus täiendus küberjulgeolekustamise teooriale, kui julgeolekustajatena analüüsitakse riigi esindajaid, sest riigi esindajate kõnedest ei ole võimalik tavaliselt nii täpselt eristada lubadust referentobjekti kaitsta. Kuna ministeeriumid koostavad ja viivad ellu arengukavasid, milles määratletakse tavaliselt tegevussuunad ja meetmed, siis võib pidada ka arengukavades määratletud eesmärke lubaduseks kaitsta referentobjekti.

Valdkondlike arengukavasid võib pidada seega vaheastmeks küberjulgeolekustamise protsessis, milles osalevad riigi esindajad, sest nende põhjal saab süvitsi uurida julgeolekustavat liigutust ja julgeolekupraktikat. Arengukavade analüüsi tulemusel võib tõdeda, et ministrite julgeolekustav liigutus on kooskõlas julgeolekupraktikaga arengukavade koostamise ja vastuvõtmise kaudu, seega Eestis on aset leidnud küberjulgeolekustamine. Samas on järgmise alapeatüki abil võimalik uurida ministrite julgeolekupraktikat meetme elluviimise kaudu, mille pinnalt saab teha järeldusi, kuidas on aset leidnud küberjulgeolekustamine Eestis ministrite näitel. Meetmest analüüsitakse teavitustööd küberjulgeoleku tagamiseks arengukava „Küberjulgeoleku strateegia 2008-2013" põhjal.

5.2.2. Meetmete elluviimine ehk julgeolekupraktika

Eelneva empiirilise analüüsi tulemusel jõuti järeldusele, et nii pea-, kaitse- kui ka välisminister astusid julgeolekustava liigutuse oma kõneaktidega, mille sõnumit tugevdavad arengukavad. Läbi arengukavade koostamise ja vastuvõtmise on pea-, kaitse- ja välisministri julgeolekustavad liigutused kooskõlas julgeolekupraktikaga.

[309] *Riigikaitse strateegia*, 3.
[310] Ibid., 7, 9, 13.

Käesolevas alapeatükis uuritakse arengukavas „Küberjulgeoleku strateegia 2008-2013" määratletud teavitustöö meedet Ansipi, Paeti ja Aaviksoo julgeolekupraktikana.

Ministrite meetmeid referentobjekti olukorra paremaks muutmiseks analüüsitakse läbi küberjulgeoleku teadvustamise koostöö loomiseks nii siseriiklikul kui ka rahvusvahelisel tasandil, sest see on kõige otsesem meede, mida ministrid saavad oma volitustest tulenevalt ellu viia. Ministri meetmetena ei uurita turvameetmete süsteemi arendamist, õigusruumi kujundamist ja kompetentsuse tõstmist ning koostöö arendamist kaitse- ja ennetusmeetmete valdkonnas Eesti teadmiste jagamise kaudu, sest nii õiguslikud, tehnoloogilised kui ka teadus- ja arendustegevuse meetmed kuuluvad vastavate valdkonda spetsialistide (näiteks juristid, infotehnoloogia või haridusega seotud inimesed) pädevusse, mitte ministri tööülesannete hulka.

Ka Eesti küberjulgeoleku strateegias on tõdetud, et on vaja osutada poliitilist tähelepanu küberjulgeolekule, mille abil on võimalik algatada vajalike rahvusvaheliste normide ja õigusaktide väljatöötamist ning teha koostööd. Selleks on vaja juhtida teiste riikide kõrge poliitilise tasandi tähelepanu küberjulgeolekule.[311] Meetmete osa eesmärgiks on uurida, kas arengukavade alapeatükis analüüsitud arengukavades määratletud meede (teadvustamine) on aset leidnud pea-, kaitse- ja välisministrite kõnedes, et vastata uurimisküsimusele, kuidas on aset leidnud küberjulgeolekustamine Eestis.

Julgeolekustava liigutuse kooskõla julgeolekupraktikaga uuritakse läbi ministrite poolse küberjulgeoleku teema teadvustamise nii siseriiklikult kui ka rahvusvahelisel tasandil. Küberjulgeoleku strateegia järgi tuleks rahvusvahelise koostöö raames tutvustada küberjulgeoleku probleeme, osaleda erialakonverentsidel, -seminaridel ja -foorumeil ning käsitleda seal pidevalt küberjulgeoleku probleeme ja parimaid tavasid. Siseriiklikul tasandil tuleks korralda küberjulgeoleku tagamisel kogu ühiskonda (tavakasutajad, ettevõtted, riigiasutused, õpilased ja üliõpilased) hõlmavat teavitustööd, mille eest vastutajateks on Majandus- ja Kommunikatsiooni-, Välis- ja Kaitseministeerium,[312] kuid käesoleva magistritöö kontekstis keskendutakse Kaitse- ja Välisministeeriumile ning Vabariigi Valitsusele, sest nimetatud valitsusasutuste ministrid astusid 2007. aasta küberrünnete ajal julgeolekustava liigutuse sammu.

[311] Küberjulgeoleku strateegia komisjon. *Küberjulgeoleku strateegia 2008-2013*, 22.
[312] Ibid., 32, 35.

Selleks, et analüüsida, kas Ansipi, Aaviksoo ja Paeti julgeolekustav liigutus on julgeolekupraktikaga kooskõlas lisaks eelnevas peatükis analüüsitud ministrite julgeolekupraktikatele arengukavadega seoses, uuritakse pea-, välis- ja kaitseministrite ministeeriumite koduleheküljelt kõnesid, intervjuusid ja arvamusartikleid, et tuvastada nende elluviidud meetmeid. Analüüsiobjektide hulka kuuluvad nüüd ainult ministeeriumi koduleheküljel olevad kõneaktid, mitte enam Postimehes, Eesti Päevalehes ja Õhtulehes avaldatud kõned. Valiku aluseks on tõdemus, et valdavalt viitavad Eesti ajalehed ministeeriumilt saadud infole, mistõttu võib tulla kattuvusi kõneaktide loendamises ja analüüsimiseks ning enam ei ole oluline intertekstuaalsuse tuvastamine. Ajaliseks piiranguks on Ansipi (ametis 27.04.2007-26.03.2014), Aaviksoo (ametis 27.04.2007-06.04.2011) ja Paeti (ametis 27.04.2007-…) ametisoleku aeg, seega ei analüüsita pea-, välis- ja kaitseministri ametijärglasi, sest oluline on julgeolekustava liigutuse astunud isiku elluviidud meetmeid.

Selleks uuritakse eesliidete „küber-" või „cyber-" esinemist vastavate ministrite suulistes ja kirjalikes kõnedes, intervjuudes ja arvamusartiklites, sest ministeeriumid avaldavad oma Internetilehekülgedel nii inglise kui ka eesti keeles kõneakte. Parima pildi annab ühest allikast (vastava ministri ministeeriumi ja valitsuse koduleheküljelt) kõnede arvu kokku lugemine ning selle kõrvutamine teiste julgeolekustajatega ning võrdlemine ministri kogu kõneaktide arvuga küberrünnetest kuni ministri ametiaja lõpuni. Kübervaldkonna seotud kõneaktide arvu moodustavad analüüsiobjektide arv, mitte prefiksi „küber-" esinemissagedus. Töö piiritlemise huvides analüüsitakse ainult julgeolekustajate isiklikke kõnesid, ettekandeid ja intervjuusid, mitte ei uurita kõiki tekste, milles räägitakse ministrite kohtumistest ja töövisiitidest, kus nad käsitlesid/arutavad küberjulgeoleku teemadel.

Tabel 5. Prefiksit „küber-"/„cyber-" sisaldavad tekstid ministri kogu kõneaktide arvu suhtes

Ministri nimi	*Ansip*	*Aaviksoo*	*Paet*
„Küber-iga" seotud /kõikide kõneaktide arv	6/87	25/76	16/46

Allikas: Koostatud järgmiste allikate põhjal: Vabariigi Valitsuse koduleheküg. http://valitsus.ee/et/valitsus/Valitsuse-liikmed/peaminister/Peaministri-koned; Välisministeeriumi koduleheküg. http://www.vm.ee/?q=taxonomy/term/28; Kaitseministeeriumi koduleheküg. http://www.kmin.ee/et/uudised (kasutatud 20.-27.04.2014)

Nii välisminister Paet kui ka kaitseminister Aaviksoo on maininud 1/3 oma kõnedes, arvamusartiklites ja intervjuudes eesliitega „küber-"/„cyber-" seotud termineid.

Peaminister Ansip on ainult vähestes kõnedes (6-s kõneaktis 87-st) maininud kübervaldkonda ning kõige sagedamini ja üsna võrdsel tasemel on küberjulgeolekut teadvustanud Paet ja Aaviksoo.

Paet on küberjulgeolekust enamasti välismaal rääkinud, näiteks Saksa Välispoliitikaühingus, OSCE Ministrite Nõukogul Helsingis, Riias USA-Aadria Partnerluse Harta plenaaristungil, Madridis Euroopa Nõukogu Ministrite Komitee 119. istungil, Hanois Aasia ja Euroopa välisministrite kohtumisel, Vilniuses XV Balti Nõukogu istungil, Ateenas OSCE Ministrite Nõukogul ning Varssavis mõttekojas „demosEuropa". Lisaks on Paet kübervaldkonda käsitlenud Madridis XVIII Euroopa Liidu ja ASEANi välisministrite kohtumisel, Alma-Atas OSCE mitteametlikul välisministrite kohtumisel, Riias XVI Balti Nõukogu istungil, Lissabonis NATO noortefoorumil, Haagis internetivabaduse konverentsil, Istanbulis Euroopa Nõukogu Ministrite Komitee 121. istungil ning Budapestis 10. Aasia ja Euroopa välisministrite kohtumisel.[313] Paet on oma kõnedes, intervjuudes ja artiklites kõnetanud eelkõige rahvusvahelist auditooriumi (organisatsioone ja teisi riike), et tõhustada küberjulgeoleku alast koostööd ja võitlust küberrünnete vastu.

Riigisiseselt on Paet kirjutanud arvamusloo Eestipäevalehe lisasse „Riigi kaitse", Postimehesse Eesti-USA diplomaatiliste suhete kaheksakümne viiendal aastapäeval ning julgeolekut kajastavasse erilehesse riigikaitse.ee-s ning on rääkinud kübervaldkonnast Riigikogu ees, Viljandis ja Balti Nõukogul.[314] Samas osades nendes kõneaktides pöördub Paet ka rahvusvahelise auditooriumi poole (näiteks Eesti-USA diplomaatilistest suhetest rääkides või Balti Nõukogul esinedes), seega on Paet kõnetanud pigem rahvusvahelist auditooriumi ja Eesti-siseselt eelkõige Riigikogu.

Ka Aaviksoo on maininud küberjulgeolekust eelkõige välismaal rääkides, et tõhustada koostööd rahvusvahelise auditooriumiga kübervaldkonnas. Aaviksoo on tõstatanud küberjulgeoleku teema näiteks Pariisis Rahvusvahelise Globaalse Julgeoleku konverentsil, Washingtonis asuvas Strateegiliste ja Rahvusvaheliste Uuringute Keskuses, Helsingis Paasikivi Seltsis, OSCE julgeolekukoostöö nõukogus, George Washingtoni ülikoolis peetud sümpoosioni avakõnes ning Londonis mainekal julgeolekukonverentsil „Riskid 21. sajandil: kliimamuutus, küberkuritegevus ja

[313] Välisministeeriumi kodulehekülg. http://www.vm.ee/?q=taxonomy/term/28 (kasutatud 20.-27.04.2014)
[314] Ibid.

piraatlus", OSCE küberkaitse-seminari avaettekandes. Lisaks on Paet kübervaldkonnale tähelepanu pööranud Londonis Westminster'i konverentsikeskuses kõrgetasemelise küberteemalise ümarlaua Cityforum avakõnes, Singapuris toimuval rahvusvahelisel küberjulgeoleku konverentsil, Stanfordi Ülikoolis toimunud küberturvalisuse ettevõtete foorumi avakõnes, Ameerika Ühendriikides Silicon Valley's toimuval kõrgetasemelisel küberjulgeolekukonverentsil ja Londonis asuvas Suurbritannia Kuninglikus Kaitseuuringute Kolledžis küberkaitseteemalises loengus.[315]

Aaviksoo on rääkinud küberjulgeolekust ka Eestis Tallinnas, näiteks rahvusvahelise küberjulgeoleku foorumi avakõnes, NATO CCD COE ja rahvusvahelise kaitseuuringute keskuse korraldatud rahvusvahelisel kübersõja konverentsil, NATO küberkaitseseminaril ning rahvusvahelisel küberkaitsekonverentsil „Rahvuslik julgeolek piirideta maailmas".[316] Samas on nimetatud üritustel osalenud inimesi üle maailma, mistõttu on Aaviksoo kõned olnud valdavalt suunatud rahvusvahelisele auditooriumile.

Ansip on kõnelenud kübervaldkonnast eelkõige Eestis, sest kuuest kõnest viis on Ansip pidanud Eesti auditooriumi ees, kelleks olnud Riigikogu (näiteks „Peaministri ettekanne Riigikogus valitsuse Euroopa Liidu poliitikast" 2007. aastal) ning Politsei- ja Piirivalveamet („Peaminister Andrus Ansipi kõne Politsei- ja Piirivalveameti aastapäeva kontsertaktusel, 18. novembril 2011 Tartus Vanemuise kontserdimajas"). Samuti on auditooriumiks olnud ka Eesti kodanikud („Peaminister Andrus Ansipi kõne Vanemuise kontserdimajas, 23. veebruar 2011" ja „Peaminister Andrus Ansipi kõne Tartus, 23. veebruaril 2014"). Ainsaks Ansipi rahvusvahelise auditooriumi ees peetud kõneks on olnud „Peaminister Andrus Ansipi kõne Stanfordi Ülikooli Hooveri Instituudis" 2007. aastal.[317]

Kokkuvõttes võib järeldada, et nii peaminister Ansipi, kaitseminister Aaviksoo kui ka välisminister Paeti julgeolekustav liigutus on julgeolekupraktikaga kooskõlas, mistõttu võib tõdeda, et Eesti riigi diskursuses on aset leidnud küberjulgeolekustamine 2007. aasta küberrünnete ajal ja nende järgselt. Kui julgeolekustav liigutus toimus eelkõige 2007. aasta küberrünnete ajal ning selle järgselt arengukavades, siis julgeolekupraktika on aset leidnud küberrünnest alates kuni vastavate ministrite ametiaja lõpuni. Kuna

[315] Kaitseministeeriumi koduleheküg. http://www.kmin.ee/et/uudised (kasutatud 20.-27.04.2014)
[316] Ibid.
[317] Vabariigi Valitsuse koduleheküg. http://valitsus.ee/et/valitsus/Valitsuse-liikmed/peaminister/Peaministri-koned (kasutatud 20.-27.04.2014)

ministrid kui täidesaatva võimu esindajad saavad kõige otsesemalt julgeolekupraktikat ellu viia läbi küberjulgeoleku teadvustamise, siis võib tõdeda, et pea-, kaitse- ja välisminister on aktiivselt nii Eesti-siselt kui ka välismaal küberjulgeolekut propageerinud oma kõnedes. Ka arengukavade koostamise ja vastuvõtmisega seoses võib tuvastada pea-, välis- ja kaitseministri julgeolekupraktikaid, mis on vastavuses julgeolekustava liigutuse etapiga. Käesoleva magistritöö empiirika peatükiga on seega vastatud uurimisküsimusele, kas ja kuidas on aset leidnud küberjulgeolekustamine Eestis. Julgeolekustamine on kuju võtnud julgeolekustava liigutuse etapis ministrite kõneaktides ja lisaks ka arengukavades ning julgeolekupraktika astmes arengukavades ja ministrite kõnedes läbi teavitustöö.

Magistritöö põhjal võib väita, et uurimistöö käigus loodud küberjulgeolekustamise teooria põhjal on võimalik analüüsida erinevaid julgeolekustajaid, auditooriume ja referentobjekte ning väljaarendatud küberjulgeolekustamise teooriat on võimalik rakendada ka teistele riikidele. Julgeolekupraktika etapis elluviidavate meetmete liigid olenevad suuresti julgeolekustaja ametist, pädevustest ja volitustest ning ka erinevate riikide praktikast, mis määratlevad ära, milliseid meetmeid saab julgeolekustaja astuda astuda referentobjekti kasuks. Samas see ei olegi küberjulgeolekustamise teoreetilises raamistikus ära fikseeritud, milliseid meetmeid peab julgeolekustaja ette võtma.

6. KOKKUVÕTE, JÄRELDUSED NING ETTEPANEKUD

Uurimistöö eesmärgiks oli analüüsida küberjulgeolekustamise teoreetilist käsitlust Kopenhaageni koolkonna julgeolekustamise teooria põhjal. Lisaks oli magistritöö sihiks uurida küberjulgeolekustamise protsessi julgeolekustava liigutuse etappi Eesti näitel 2007. aasta küberrünnete ajal ja nende järgselt Lene Hanseni poststrukturalistliku diskursusanalüüsi abil teose „Security as Practice: Discourse Analysis and the Bosnian War" (2007) põhjal.

Teema olulisus tuleneb sellest, et küberjulgeoleku integreerimine rahvusvahelistesse suhetesse võimaldab luua efektiivseid poliitikaid ning edendada koostööd riikide ja mitte-riiklike toimijate vahel. Küberjulgeolekut on tähtis uurida, sest küberjulgeoleku praktiseerijatel ei ole tihti aega teoreetiliselt tõlgedada küberjulgeoleku teemasid, mistõttu on teadlaste ülesandeks rakendada erinevaid teooriaid kübervaldkonna sündmuste ja poliitikate hindamisele ning kirjeldamisele. Selles töös analüüsiti küberjulgeolekut Eesti Vabariigi näitel, sest 2007. aastal Eestis toimunud küberrünnakud juhtisid tähelepanu vajadusele tõsta rahvusvahelist teadlikkust küberrünnetest ja edendada koostööd.

Magistritöö teoreetiliseks eesmärgiks oli uurida Kopenhaageni koolkonna esialgset ja edasiarendatud raamistikku küberjulgeoleku analüüsimiseks, et vastata seeläbi uurimisküsimusele, kuidas toimub küberjulgeolekustamine Kopenhaageni koolkonna järgi. Töö sihiks oli ka analüüsida, kas ja kuidas on küberjulgeolekustamine aset leidnud reaalsuses Eesti kaasuse näitel, et leida vastus uurimisküsimusele, kas Eestis on toimunud 2007. aastal ja selle järgselt küberjulgeolekustamine.

Sissejuhatuses anti ülevaade teema taustast, aktuaalsusest ja olulisusest, kaardistati töö ülesehitus, uurimisküsimused, peamised allikad ning varasemad teemaga seotud kirjandus. Kuigi kübervaldkonnas ei eksisteeri universaalseid definitsioone, oli töö eesmärgiks määratleda uurimistöö esimeses sisupeatükis magistritöös kasutavad terminid kübervaldkonnaga seoses. Selleks analüüsiti kübervaldkonna peamisi termineid ja nende defineeringuid, omavahelisi seoseid ja takistusi kübervaldkonna oskussõnade määratlemisel.

Kõikehõlmavate definitsioonide loomist takistab lisaks keelelistele eripäradele asjaolu, et kübervaldkond on seotud väga erinevate tehnoloogiate, strateegiate ja sektoritega,

ning küberjulgeolekuga seotud inimesed määratlevad erinevalt termineid oma töö olemusest lähtuvalt. Mõistetest kasutati magistritöös eelkõige termineid „küberruum", „küberjulgeolek" ja „küberrünne" ning küberrünnete liike (kübersõda, -terrorism, -vandalism, -kuritegevus ja -spionaaž). Küberkaitse on küberjulgeoleku osa, millest tulenevalt kasutati uurimistöös läbivalt küberjulgeoleku terminit ja ainult spetsiifilisematel juhtudel mõistet „küberkaitse".

Magistritöö teises sisupeatükis analüüsiti Kopenhaageni koolkonna esialgset teoreetilist raamistikku, mida põimiti teise põlvkonna edasiarendustega, et uurida küberjulgeolekustamist. Kopenhaageni koolkonna sektoriaalset ja julgeolekustamise käsitlust rakendati küberjulgeolekule ning analüüsiti küberjulgeolekut kui eraldi julgeolekusektorit, millel on oma julgeolekustajad, eksistentsiaalsed ohud, referentobjektid ja -subjektid ning auditooriumid.

Kübervaldkonna referentobjektideks on laiemalt Kopenhaageni koolkonna sektorid (majanduslik, sotsiaalne, poliitiline ja sõjaline sfäär) ning osaliselt ka keskkonnasektor indiviide kaudu. Kitsamas plaanis on referentobjektideks nende tegevusalade sees olevad referentobjektid (riik ja institutsioonid, ettevõtted, rahvus, indiviidid jne). Lisaks esialgsele Kopenhaageni koolkonna eristusele võib referentobjektina tuvastada ka meedia, finantsinstitutsioonid, transpordi ja võrgud. Eksistentsiaalseteks ohtudeks on küberründed ning kitsamalt küberrünnete liigid (kübersõda, -terrorism, -vandalism, -kuritegevus ja -spionaaž). Referentsubjektideks on nende küberrünnete läbiviijad ehk kriminaalid, terroristid, rahvusriigid, luureteenistused ja „skriptijuntsud".

Kübervaldkonnas võivad olla julgeolekustajateks suuremad üksused nagu riik, rahvusvahelised organisatsioonid ja korporatsioonid. Kitsamalt on julgeolekustajateks ka kodanikuühiskonna organisatsioonid (ametiühingud ja rahvaliikumised), eraettevõtted (näiteks pangad), indiviidid (näiteks küberjulgeoleku spetsialistid ja arvutiprogrammeerijad). Küberjulgeoleku sektoris eksisteerivad kolm suuremat auditooriumi: institutsionaalsed organid (poliitikud riigiinstitutsioonide sees), avalikkus (avalik arvamus ning kitsamalt valijaskond, rahvuse indiviidid ja kodanikud) ning veel kitsamalt tehnokraadid ja spetsialistid. Auditoorium(id) saavad volitada julgeolekustajat ette võtma hädaolukorrameetmeid küberrünnetega võitlemiseks.

Kopenhaageni koolkonna julgeolekustamise käsitlus toetub kõneakti teooriale (John Langshaw Austin, „How to do Things with Words", 1975), millele pöörati magistritöös

tähelepanu, sest selle pinnalt uuriti julgeolekustava liigutuse ja julgeolekupraktika eristust, mida rakendati omakorda küberjulgeolekustamise protsessile. Teooria peatükis defineeriti küberjulgeolekustamist kui eesliitest „küber-" ja terminist „julgeolekustamine" koosnevat kontseptsiooni, mis on kaheastmeline protsess. Esimeseks etapiks on julgeolekustav liigutus ja teiseks sammuks on julgeolekupraktika. Küberjulgeolekustav liigutus ehk illokutiivne akt on etapp, kus julgeolekustav toimija ütleb kõneaktis välja, et eksisteerib eksistentsiaalne oht referentobjektile, hoiatades referentsubjekti või lubades referentobjekti kaitsta.

Julgeolekupraktika on küberjulgeolekustamise protsessi teine samm, mis seisneb selles, et julgeolekustavast liigutusest saab ainult siis praktikas eksisteeriv olukord, kui toimub muutus julgeolekustava toimija asjakohases käitumises auditooriumi nõusolekul (perlokutiivne akt). See tähendab seda, et julgeolekustaja öeldud illokutiivne kõneakt peab olema vastavuses ettevõetud meetmetega ohule reageerimiseks. Kuigi Kopenhaageni koolkond omistab auditooriumi nõusoleku julgeolekustamise teisele etapile meetmete ettevõtmiseks, võib siiski auditooriumi rolli siduda ka julgeolekustava liigutusega, sest julgeolekustaja püüab auditooriumi juba oma kõneaktis veenda.

Sisu kolmandas osas keskenduti magistritöö metodoloogilisele baasile, mille abil uuriti käesoleva töö uurimisküsimusest lähtuvalt empiiriliselt küberjulgeolekustamist Eesti näitel. Uurimistöö meetodiks võeti Hanseni poststrukturalistlik diskursusanalüüs, mille põhjal on võimalik analüüsida ametlikku diskursust välispoliitika-identiteedi suhte pinnalt ning tuvastada auditooriumini jõudmist. Metodoloogia peatüki eesmärgiks oli luua metodoloogiline raamistik põimituna küberjulgeolekustanise teooriaga, et selle abil uurida julgeolekustavaid liigutusi ministrite kõneaktides.

Hanseni poststrukturalistliku diskursusanalüüsi järgi on välispoliitika diskursuses „mina" Kopenhaageni koolkonna tähenduses eksistentsiaalselt ohustatud referentobjekt ning „teine" on ohu põhjustaja ehk referentsubjekt. Kuigi Hanseni poststrukturalistlik diskursusanalüüs toetub „mina-teise" eristusele, on siiski oluline eristada ka „meid", kes on magistritöö tähenduses lisaks referentobjekti(de)le ka julgeolekustaja. „Meie" identifitseerimine aitab veenvamana mõjuda relevantse auditooriumi jaoks. Lisaks on tähtis analüüsida ka „sind" ehk auditoorium, kes peab heaks kiitma diskursuse.

Töö metodoloogilises sisupeatükis anti ülevaade empiirilisele analüüsile aluseks olevast analüütilisest raamistikust Hanseni uurimiskava alusel ning pöörati tähelepanu tekstide

valimisele ja kontekstile Margaret Wetherelli („Discourse Theory and Practice: A Reader", 2011) vahetu ja distaalse konteksti eristuse põhjal. Vahetuks kontekstis 2007. aasta küberrünnetele olid pronkssõduri julgeolekustamine ning Eesti Moskvas asuva saatkonna piiramine.

Analüüsi kaasati Hanseni uurimiskava, sest valikute tegemine Hanseni poststrukturalistlikus uurimiskavas võimaldab piiritleda ajalist raami ja sündmuste arvu, mille pinnalt saab teha tekstilisi valikuid. Uurimiskava intertekstuaalsuse mudelite hulgast valiti esimene mudel (ametlik diskursus), sest julgeolekustajateks valiti riiklikul tasandil Eesti täidesaatva võimu esindajad. Ministritel on oma pädevustest tulenevalt võimalik viia julgeolekustav liigutus julgeolekupraktikaga kooskõlla ning neil on võimu ja legitiimsust julgeolekust rääkida. „Minade" all võeti aluseks üksik „mina" ehk Eesti riik. Ajalise perspektiivi alt valiti üks hetk (27.04-19.05.2007), ning sündmuste arvu all võeti analüüsiobjektiks üks sündmus (2007. aasta küberründed Eestis), mida kasutatakse tavaliselt pingelise sündmuse analüüsimiseks.

Analüüsi aluseks võeti valitsus ja ministeeriumid (Justiits-, Kaitse-, Majandus- ja Kommunikatsiooni-, Haridus- ja Teadus-, Sise- ning Välisministeerium), mis on küberjulgeolekuga seotud. Analüüsiobjektideks valiti ainult nende ministeeriumite ministrite kõneaktid, kes olid 2007. aasta küberrünnete ajal ametis. Eestis toimunud küberrünnete ajal oli peaministriks Andrus Ansip (ametis 13.04.2005-26.03.2014), justiitsministriks Rein Lang (ametis 13.04.2005-06.04.2011), kaitseministriks Jaak Aaviksoo (ametis 05.04.2007-06.04.2011), majandus- ja kommunikatsiooniministriks Juhan Parts (ametis 05.04.2007-26.03.2014), haridus- ja teadusministriks Tõnis Lukas (ametis 05.04.2007-06.04.2011), siseministriks Jüri Pihl (ametis 05.04.2007-21.05.2009) ning välisministriks Urmas Paet (ametis 13.04.2005-...).

Diskursusanalüüsi analüüsiobjektiks valimiseks pidi vastavate ministeeriumite ja valitsuse koduleheküIgedel või Eesti suurimates üleriiklikes ja üldloetavates päevalehtedes (Postimees, Eesti Päevaleht, Õhtuleht) ajavahemikus 27.04.2007-19.05.2007 avaldatud ministri kõneaktides sisalduma viide Eestis toimunud küberrünnetele. Analüüs keskendus ministrite kõikidele kõnedele, intervjuudele ja arvamusartiklitele ning ministrit tsiteerivatele artiklitele, et selgitada välja kõned, milles räägiti 2007. aasta küberrünnetest. Valikusse valiti Ansipi viis, Aaviksoo kaks ja Paeti viis kõneakti, seega kokku kaksteist kõneakti.

Magistritöö neljandas sisulises osas keskenduti empiirilisele analüüsile teoreetilise ja metodoloogilise raamistiku põhjal. Peatüki eesmärgiks oli rakendada küberjulgeolekustamise teoreetilist käsitlust ja Hanseni poststrukturalistliku diskursusanalüüsi meetodit praktilisele kaasusele, et jõuda järeldusele, kas ja kuidas on aset leidnud küberjulgeolekustamine Eestis 2007. aasta küberrünnete tulemusel ministrite näitel. Empiirilises osas analüüsiti peaminister Ansipi, kaitseminister Aaviksoo ja välisminister Paeti kõneaakte, et tuvastada julgeolekustavaid liigutusi kõnedes. Kui nimetatud ministri kõneaktist võis identifitseerida julgeolekustava liigutuse (lubaduse kaitsta referentobjekti või hoiatuse referentsubjektile), siis võeti nimetatud kõneakt valimisse. Valitud kõneakte uuriti perlokutiivse akti, identiteedi ja välispoliitika vahelise suhte, konteksti ja intertekstuaalsuse alusel poststrukturalistlikust diskursusanalüüsist ja küberjulgeolekustamise teooriast lähtuvalt. Valimisse võeti üks Ansipi, kaks Aaviksoo ja kolm Paeti kõneakti, millest tuvastati lubadus referentobjekti kaitsta, seega kokku kuus kõneakti.

Valitud kõnede põhjal olid 2007. aasta küberrünnete ajal julgeolekustajateks nii pea-, kaitse- kui ka välisminister. Eksistentsiaalseteks ohtudeks olid 2007. aastal Eestis toimunud küberründed Ansipi, Aaviksoo ja Paeti kõneaktide alusel ning nende alaliikideks küberkuritegevus (kitsamalt DDoS ründed) ja kübervandalism. Eestis toimunud küberründeid ei kvalifitseeru küberterrorismiks ja kübersõjaks, kuigi Eesti ministrite diskursuses seostati häkkimine terrorismiga. Nii Paet kui ka Ansip tuvastasid „teisena" ehk referentsubjektina Venemaa, keda seostatati barbaarsuse, vaenulikkuse, vägivalla, propagandasõja ja agressiivsusega. Ainsana julgeolekustajatest ei seostanud küberründeid Venemaaga Aaviksoo, kes ütles, et küberrünnete korraldatajateks olid vaenulikud jõud.

Referentobjektiks oli laiemalt Eesti riik. Kitsamalt olid referentobjektideks ühiskond, riiklik suveräänsus, majandus, rahvus (Eesti indiviidid/elanikkond/valijaskond), võrgud, riigiinstitutsioonid (valitsus, president, ministeeriumid, parlament) ning poliitikategijad, finantsinstitutsioonid (pangad), meedia (ajalehed, uus meedia jne) ja ettevõtted (ettevõtjad), sest küberründeid riigi vastu ei ole kerge tõestada. Nii Paeti, Aaviksoo kui ka Ansipi kõnest võib tuvastada referentobjekti ehk „minana" Eesti riigi, keda identifitseeritakse Euroopa Liidu, väärika, rahumeelse, kristliku, armsa, koostööalti, NATO, heade suhete otsijana, diplomaatilisest tavadest kinni pidaja, Baltimaade osa,

endise liiduvabariigi ja Venemaa naaberriigina. Ansip ja Paet tuvastasid referentobjektina ka Euroopa Liitu. Selleks, et mõjuda veenvamana relevantse auditooriumi jaoks, määratles Ansip „meiena" eestlased, Aaviksoo Eesti koos partneritega EL-is ja NATO-s ning Paet Euroopa Nõukogu liikmesriigid.

Auditooriumiks olid Eesti avalikkus, Eesti riigiinstitutsioonid (Riigikogu jne), teised riigid ja rahvusvahelised organisatsioonid (näiteks NATO ja EL). Peaminister Ansipil oli vaja veenda seadusandlikku võimukandjat Riigikogu, et talle või valitsusele ei avaldataks umbusaldust seoses pronkssõduri teisaldamisega, sest valitsus peab astuma tagasi, kui Riigikogu avaldab valitsusele või peaministrile umbusaldust.

Aaviksoo kõneaktid olid suunatud ajakirjanikele ja seeläbi Eesti avalikkusele. Paeti kõnede auditooriumiks oli ka Eesti avalikkus ning lisaks Rootsi, Soome, Läti, Leedu, Saksamaa, Euroopa Liit, NATO, USA ning Euroopa Nõukogu liikmesriigid. Läbi viitamiste kõnetasid nii Paet kui ka Aaviksoo rahvusvahelist auditooriumi. Samuti võib auditooriumiks pidada konkreetse rahvuse indiviide, kodanikke ja valijaskonda (avalikkust), sest ministrite legitiimsus sõltub valijatest. Kuna Eestis toimunud küberründed mõjutasid üksikisikut, riigi esindajaid ja ettevõtjaid, siis ei olnud Ansipil, Paetil ja Aaviksool raske samastuda auditooriumiga veenmise eesmärgil, sest ka ministrid olid mõjutatud.

Neljanda sisupeatüki edasiseks eesmärgiks oli analüüsida, kas nimetatud ministrite julgeolekustav liigutus (lubadus kaitsta referentobjekti) on kooskõlas julgeolekupraktika ehk meetmetega referentobjekti olukorra paremaks muutmiseks. Meetmete analüüs piiritleti 2007. aasta küberrünnete järgselt kübervaldkonnaga seotud valdkondlikele arengukavadele, mis on valitsuse poolt heaks kiidetud, ministeeriumite koostatud või milles on pandud vastutus ministeeriumi(te)le meetmete elluviimise eest. Selleks uuriti läbi kõik Eestis kehtivad viiskümmend viis arengukava, et tuvastada küberjulgeolekuga seotud arengukavad. Analüüsi kaasati seitse küberjulgeolekuga seotud arengukava, kuid julgeolekupraktikat uuriti nende arengukavade põhjal, mis on seotud Välis- ja Kaitseministeeriumi ning valitsusega.

Vabariigi Valitsuse rolli nende arengukavadega seoses analüüsiti selles tähenduses, kas valitsus on analüüsiobjektideks olevad arengukavad heaks kiitnud või osalenud muudmoodi nende valmimise protsessis. Seeläbi võib Ansipi julgeolekupraktikaks pidada arengukavade „Riigikaitse arengukava 2013-2022", Eesti teadus- ja

arendustegevuse ning innovatsiooni strateegia 2014-2020 „Teadmistepõhine Eesti" ning „Eesti infoühiskonna arengukava 2020" heaks kiitmist. Nimetatud arengukavasid ei uuritud põhjalikult, sest nad ei olnud seotud Paeti ja Aaviksooga.

Süvitsi analüüsiti Välis- ja Kaitseministeeriumi ning valitsusega seotud kolme arengukava, milleks on „Küberjulgeoleku strateegia 2008-2013", „Julgeolekupoliitika alused" (2010) ja „Riigikaitse strateegia" (2010). Kuigi Aaviksoo ei koostanud ise otseselt arengukava „Küberjulgeoleku strateegia 2008-2013", siiski tegi ta ettepaneku valitsusele koostatada strateegia ning Kaitseministeerium juhtis arengukava koostamise komisjoni, mille läbi on kaitseminister kui Kaitseministeeriumi esindaja julgeolekupraktika elluviija. Kaudselt võib küberjulgeoleku strateegia ettepaneku heaks kiitmist, valitsuse korraldust strateegia koostamiseks ning lõplikut strateegia kinnitamist pidada Ansipi kui valitsuse esindaja julgeolekupraktikakas.

Paeti julgeolekupraktikaks on „Julgeolekupoliitika aluste" muutmise algatamine ning arengukava koostamiseks töörühma moodustamine, mida juhtis Välisministeerium. Vabariigi Valitsus kehtestas „Riigikaitse strateegia" kaitseministri ettepanekul, mis näitab seda, et Aaviksoo ja Ansipi julgeolekustav liigutus on julgeolekupraktikaga kooskõlas.

Arengukavade pinnalt loodi täiendus küberjulgeolekustamise teooriale, mis on seotud asjaoluga, et kuna riigi esindajate kõnedes on tavaliselt lubadus kaitsta referentobjekti pinnapealselt antud, siis võib kõneaktidest identifitseeritud lubadust võimendada arengukavade abil. Nii „Küberjulgeoleku strateegias 2008-2013", „Julgeolekupoliitika alustes" kui ka „Riigikaitse strateegias" anti lubadus. Samas on arengukavade kaudu võimalik tuvastada ka tegevusvaldkondi ja meetmeid sihtide saavutamiseks, mistõttu on arengukavad küberjulgeolekustamise vaheastmeks. Arengukavade analüüs on omane nii julgeolekustava liigutuse kui julgeolekupraktika etapile, sest nendest võib tuvastada lubadusi ja samas võib neid pidada julgeolekupraktikateks kuna ministrid on seotud nende koostamise või heakskiitmisega.

Arengukavadest tuvastatud meetmete põhjal on võimalik uurida ministrite julgeolekupraktikat ka selles tähenduses, et järeldada, kas arengukavades määratletud meede on elluviidud ministrite poolt. Analüüsi aluseks võeti „Küberjulgeoleku strateegia 2008-2013", sest selles dokumentides on ära määratletud teavitustöö meede küberjulgeoleku tagamiseks. Valiku aluseks on tõdemus, et teavitustöö on kõige

otsesem julgeolekupraktika lisaks arengukavade koostamise protsessile, mida on võimalik ministritel oma pädevustest tulenevalt ette võtta. Käesolevas uurimistöös võeti arengukavadest ministrite meetmete analüüsi aluseks kübervaldkonna teadvustamine nii siseriiklikul kui ka rahvusvahelisel tasandil koostöö loomiseks.

Selleks, et uurida, kas Ansipi, Aaviksoo ja Paeti julgeolekustav liigutus on julgeolekupraktikaga kooskõlas lisaks ministrite julgeolekupraktikatele arengukavadega seoses, uuriti vastavaid ministeeriumite koduleheküIgi. Analüüs keskendus pea-, kaitse- ja välisministri kõnedele, intervjuudele ja arvamusartiklitele, et uurida nendes eesliidetega „küber-" või „cyber-" seotud terminite esinemist. Ajaliseks piiranguks oli Ansipi, Aaviksoo ja Paeti ametisolekuaeg, seega ei analüüsitud pea-, kaitse- ja välisministri ametijärglasi.

Selleks, et analüüsida, kui aktiivselt on minister kübervaldkonda maininud, loeti kokku kõik ministriga ja küberjulgeolekuga seotud kõneaktid, mida võrreldi omavahel ning kõrvutati omakorda teiste julgeolekustajate kõnede arvuga. Nii välisminister Paet kui ka kaitseminister Aaviksoo on maininud 1/3 oma kõnedes ja ettekannetes eesliitega „küber-" või „cyber-" seotud oskussõnu. Peaminister Ansip on ainult vähestes kõnedes (6-s kõneaktis 87-st) ja eelkõige Eesti-siseselt maininud kübervaldkonda. Kõige tihedamalt on küberjulgeolekut teadvustanud Paet ja Aaviksoo, kes on küberjulgeolekust enamasti välismaal rääkinud.

Kuna ministrid kui täidesaatva võimu esindajad saavad kõige otsesemalt julgeolekupraktikat ellu viia läbi küberjulgeoleku teadvustamise, siis võib tõdeda, et pea-, kaitse- ja välisminister on aktiivselt nii Eesti-siselt kui ka välismaal küberjulgeolekut propageerinud oma kõnedes. Sellest tulenevalt on Ansipi, Paeti ja Aaviksoo julgeolekustav liigutus julgeolekupraktikaga vastavuses.

Käesoleva magistritöö analüüsi tulemusel võib öelda, et küberjulgeolekut on võimalik analüüsida kui eraldi julgeolekusektorit Kopenhaageni koolkonna teooria tähenduses ning selle pinnalt arendati töö käigus välja põhjalik küberjulgeolekustamise teooria, mille alusel uuriti Eesti Vabariigis toimunud küberründeid 2007. aastal ja nende järgselt. Eesti näitel järeldus, et küberjulgeolekustamine on aset leidnud Eestis ministrite kõneaktide ning vastavate ministeeriumite ja valitsuse poolt koostatud, vastuvõetud ja/või elluviidud arengukavade põhjal.

Käesoleva magistritöö tulemusi on võimalik kasutada teiste julgeolekustajate uurimiseks Eesti näitel ning teoreetilises peatükis väljaarendatud küberjulgeolekustamise teoreetilist käsitlust on võimalik rakendada ka teiste riikide analüüsimiseks. Uurimistöös keskenduti töö piiritlemise huvides ministrite kui täidesaatva võimu esindajate kõneaktidele, kuid seda teemat saab edasi arendada doktoritöö raames. Hanseni poststrukturalistliku diskursusanalüüsi alusel tuleb käsitleda ka seadusandliku võimu kandjate ehk Riigikogu liikmete kõneakte, et süvitsi analüüsida küberjulgeolekustamist Eesti näitel juriidiliste meetmete põhjal.

On oluline ka uurida küberjulgeolekuga seotud ministrite ehk pea-, kaitse-, sise-, majandus- ja kommunikatsiooni-, haridus- ja teadus-, justiits- ja välisministri ametijärglasi, kes ei olnud 2007. aasta küberrünnete ajal ametis. Nende julgeolekustavaid liigutusi (lubadust kaitsta referentobjekti) saaks tuvastada arengukavade põhjal, ning selle pinnalt analüüsida, kas julgeolekustav liigutus on julgeolekupraktikaga kooskõlas arengukavade koostamise ning strateegiates tuvastatud meetmete elluviimise kaudu.

Lisaks ministritele ja Riigikogu liikmetele tuleb käsitleda ka IT-spetsialiste ning nende meetmeid tehnilises sfääris. Samuti on tähtis edasi uurida, kas Eestis toimunud küberjulgeolekustamine on edukas olnud, sest poststrukturalistiku diskursusanalüüsi abil on võimalik analüüsida ainult seda, kas julgeolekustamine on aset leidnud ja kuidas ta on kuju võtnud.

Küberjulgeolekustamine uurimine Eesti näitel ministrite tasandil aitas välja arendada küberjulgeolekustamise teoreetilise käsitluse, mis on siiani üsna üldiselt varasemas kirjanduses kaetud. Kuna küberjulgeolekustamine võib aset leida nii mitmetel tasanditel ja sfääridel, siis on töös käigus loodud küberjulgeolekustamise teooria abil võimalik analüüsida erisuguseid küberjulgeolekustamise näiteid erinevate meetodite abil.

KASUTATUD KIRJANDUSE LOETELU

Raamatud ja artiklid

Albert, Mathias, and Barry Buzan. 2011. „Securitization, Sectors and Functional Differentiation." *Security Dialogue* 42 (4-5): 413-425. http://sdi.sagepub.com/content/42/4-5/413 (kasutatud 02.01.2014)

Ansip, Andrus. 2007. „Andrus Ansipi poliitiline avaldus riigikogu ees," *Postimees* 02. mai. http://arvamus.postimees.ee/1656331/andrus-ansipi-poliitiline-avaldus-riigikogu-ees (kasutatud 06.04.2014)

Ansip, Andrus. 2007. „Peaminister Andrus Ansipi kõne Riigikogu ees." *Valitsuse kommunikatsioonibüroo* 02. mai. http://www.valitsus.ee/et/valitsus/Valitsuse-liikmed/peaminister/Peaministri-koned/51/peaminister-andrus-ansipi-k%C3%B5ne-riigikogu-ees (kasutatud 06.04.2014)

Anvelt, Kärt, ja Mirko Ojakivi. 2007. „Rünnak Eestile hoogustab kübersõja arutelu NATO-s." *Eesti Päevaleht* 11. mai. http://epl.delfi.ee/news/eesti/runnak-eestile-hoogustab-kubersoja-arutelu-nato-s.d?id=51086579 (kasutatud 21.03.2014)

Arquilla, John, and David Ronfeldt, eds. 2001. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Rand Corporation.

Austin, John L. 1975. *How to Do Things with Words*. 2nd ed. Oxford: Oxford University Press.

Balzacq, Thierry. 2005. „The Three Faces of Securitization: Political Agency, Audience and Context." *European Journal of International Relations*, 11 (2): 171-201. doi: 10.1177/1354066105052960 (kasutatud 14.04.2013)

Balzacq, Thierry, ed. 2011. *Securitization Theory: How Security Problems Emerge and Dissolve*. New York: Routledge.

Barnard-Wills, David, and Debi Ashenden. 2012. „Securing Virtual Space: Cyber War, Cyber Terror, and Risk." *Space and Culture* XX(X): 1-14. http://sac.sagepub.com/content/15/2/110 (kasutatud 02.02.2014)

Bayuk, Jennifer L. *et al*. 2012. *Cyber Security Policy Guidebook*. Hoboken: Wiley.

BBC News. 2007. „Russia Accused of 'Attack on EU'." *BBC kodulehekülg* 02. mai. http://news.bbc.co.uk/2/hi/europe/6614273.stm (kasutatud 23.12.2013)

Bendiek, Annegret, and Andrew L. Porter. 2013. „European Cyber Security Policy within a Global Multistakeholder Structure." *European Foreign Affairs Review* 18 (2): 155-180. http://www.kluwerlawonline.com/abstract.php?area=Journals&id=EERR2013011 (kasutatud 29.12.2013)

Buzan, Barry. 1983. *People, States, and Fear: The National Security Problem in International Relations*. Brighton: Wheatsheaf Books.

Buzan, Barry. 1991. *People, States, and Fear: An Agenda for International Security Studies in the Post-Cold War Era*. 2nd ed. Harlow: Longman.

Buzan, Barry. 1997. „Rethinking Security after the Cold War." *Cooperation and Conflict* 32 (1): 5-28. http://cac.sagepub.com/content/32/1/5 (kasutatud 03.04.2013)

Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. London: Lynne Rienner Publishers.

Buzan, Barry, and Richard Little. 2000. *International Systems in World History: Remaking the Study of International Relations.* New York: Oxford University Press.

Buzan, Barry, and Lene Hansen, eds. 2007. *International Security. Volume IV: Debating Security and Strategy and the Impact of 9-11*. London: SAGE

Carleton, Jarad. 2012. *Cybersecurity: A Global Economic Security Crisis*. Frost & Sullivan, 4. http://www.frost.com/reg/file-get.do?id=2958781&file=1 (kasutatud 03.03.2014)

Cavelty, Myriam Dunn. 2008. *Cyber-Security and Threat Politics: US efforts to Secure the Information Age*. London; New York: Routledge.

Cavelty, Myriam Dunn. 2008. „Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate." *Journal of Information Technology & Politics* 4 (1): 21. http://dx.doi.org/10.1300/J516v04n01_03 (kasutatud 24.12.2013)

Collins, Alan, ed. 2007. *Contemporary Security Studies*. Oxford: Oxford University Press.

Czosseck, Christian, and Karlis Podins, eds. 2010. *Conference on Cyber Conflict. Proceedings 2010*.Tallinn: CCD COE Publications.

Czosseck, Christian, Rain Ottis and Katharina Ziolkowski, eds. 2012. *4th International Conference on Cyber Conflict. Proceedings 2012*. Tallinn: NATO CCD COE Publications.

Davì, Marco. 2010. *ESDF Workshop 4: Cyber Security: European Strategies and Prospects for Global Cooperation*. London: Cratham House. http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/1110esdf_davi.pdf (kasutatud 12.11.2013)

Deibert, Ronald. 2012. „Cybersecurity: The New Frontier." *Foreign Policy Association Great Decisions*. http://www.fpa.org/ckfinder/userfiles/files/Cybersecurity%20Intro.pdf (kasutatud 15.04.2013)

Donnelly, Faye. 2013. *Securitisation and the Iraq War: The Rules of Engagement in World Politics*. London: Routledge.

Ellam, Haldi. 2007. „Ansip: Eestis katsetati kübersõda." *Eesti Päevaleht* 30. mai. http://www.epl.ee/news/eesti/ansip-eestis-katsetati-kubersoda.d?id=51088956 (kasutatud 29.12.2013)

Eriksson, Johan. 1999. „Observers or Advocates? On the Political Role of Security Analysts." *Cooperation and Conflict* 34 (3): 311-330. http://cac.sagepub.com/content/34/3/311 (kasutatud 06.04.2013)

Evron, Gadi. 2008. „Battling Botnets and Online Mobs. Estonia's Defence Efforts during the Internet War." *Georgetown Journal of International Affairs* Winter/Spring: 121-126. http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/geojaf9&section=19 (kasutatud 07.03.2014)

Fairclough, Norman. 1999. *Discourse and Social Change.* Cambridge: Polity Press.

Floyd, Rita. 2010. *Security and the Environment: Securitisation Theory and US Environmental Security Policy*. Cambridge: Cambridge University Press.

Floyd, Rita. 2011. „Can Securitization Theory be used in Normative Analysis? Towards a Just Securitization Theory." *Security Dialogue* 42 (4-5): 427-439. http://sdi.sagepub.com/content/42/4-5/427 (kasutatud 05.02.2014)

Geers, Kenneth. 2010. „A Brief Introduction to Cyber Warfare." *Common Defense Quarterly*, 16-18. http://commondefensequarterly.com/archives/CDQ5/index.html (kasutatud 13.11.2013)

Goderdzishvili, Nata. 2010. *Legal Assessment of Cyber Attacks on Georgia*. Tbilisi, Georgia: Data Exchange Agency, Ministry of Justice of Georgia. http://www.e-government.ge/uploads/library/2.%20Nov.9_FINAL_Nata's%20Presentation.pdf (kasutatud 03.01.2014)

Hansen, Lene, and Ole Waever, eds. 2003. *European Integration and National Identity: The Challenge of the Nordic States*. Taylor & Francis e-Library.

Hansen, Lene. 2007. *Security as Practice: Discourse Analysis and the Bosnian War*. London, New York: Routledge.

Hansen, Lene, and Helen Nissenbaum. 2009. „Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly* 53 (4): 1155-1175. doi: 10.1111/j.1468-2478.2009.00572.x (kasutatud 04.04.2013)

Hardy, Cynthia, Bill Harley, and Nelson Phillips. 2004. „Discourse Analysis and Content Analysis: Two Solitudes?" *Qualitative Methods*, 2 (1): 1-40. https://www.maxwell.syr.edu/uploadedFiles/moynihan/cqrm/Newsletter2.1.pdf (kasutatud 07.03.2014)

Kalamees, Kai. 2007. „Eesti-vastane kübersõda kerkis ühtlasi NATO väljakutseks." *Postimees* 11. mai. http://www.postimees.ee/1659637/eesti-vastane-kubersoda-kerkis-uhtlasi-nato-valjakutseks (kasutatud 21.03.2014)

Kello, Lucas. 2013. „The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 2 (38): 7-40. http://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00138#.U2eg0xBpeAE (kasutatud 05.02.2014)

Kingdon, John W. 1984. *Agendas, Alternatives, and Public Policies*. Boston: Little, Brown & Co.

Klimburg, Alexander, ed. 2012. *National Cyber Security Framework Manual*. Tallinn: NATO CCD COE Publications.

Kross, Eerik-Niiles. 2011. „Eerik-Niiles Kross: küünteta kübertiiger," *Postimees* 13. aprill. http://arvamus.postimees.ee/418624/eerik-niiles-kross-kuunteta-kubertiiger (kasutatud 10.02.2014)

Landler, Mark, and John Markoff. 2007. „Digital Fears Emerge After Data Siege in Estonia." *The New York Times* 29. mai.

http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (kasutatud 13.11.2013)

Latham, Robert, ed. 2003. *Bombs and Bandwidth: The Emerging Relationship between Information Technology and Security*. New York: The New Press.

Lawson, Sean. 2013. „Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats." *Journal of Information Technology & Politics*, 10 (1): 86-103. http://dx.doi.org/10.1080/19331681.2012.759059 (kasutatud 03.03.2014)

Lehti, Marko, Matti Jutila, and Markku Jokisipilä. 2008. „Never-Ending Second World War: Public Performances of National Dignity and the Drama of the Bronze Soldier." *Journal of Baltic Studies* 39 (4): 393-418. http://estudijas.lu.lv/pluginfile.php/158478/mod_resource/content/0/Bronzas_karav.pdf (kasutatud 07.04.2013)

Lipschutz, Robert D., ed. 1995. *On Security*. New York: Columbia University Press.

Longworth, Guy. 2012. „John Langshaw Austin." *The Stanford Encyclopedia of Philosophy*. http://plato.stanford.edu/entries/austin-jl/ (kasutatud 29.12.2013)

Loonet, Teelemari. 2014. „Kaitseministeeriumis alustas tööd küberpoliitika osakond." *Postimees* 04. veebruar. http://www.postimees.ee/2684832/kaitseministeeriumis-alustas-tood-kuberpoliitika-osakond (kasutatud 29.03.2014)

Lord, Kristin M., and Travis Sharp, eds. 2011. *America's Cyber Future: Security and Prosperity in the Information Age*. Washington, D.C.: Center for a New American Security.

McNally, Mark, and John Schwarzmantel, eds. 2009. *Gramsci and Global Politics: Hegemony and Resistance*. London; New York: Routledge.

Mutov, Martin. 2007. „Rein Langi sõnul ründavad Vene riigiasutused Eesti veebiservereid." *Postimees* 30. aprill. http://www.postimees.ee/1655903/rein-langi-sonul-rundavad-vene-riigiasutused-eesti-veebiservereid (kasutatud 22.03.2014)

Mälksoo, Maria. 2009. „Akadeemilised julgeoleku-uuringud sõja ja rahu vahel." *Akadeemia* 21 (9): 16-29.

Nissenbaum, Helen. 2005. „Where Computer Security Meets National Security." *Ethics and Information Technology* 7 (2): 61-73. DOI 10.1007/s10676-005-4582-3 (kasutatud 06.06.2013)

Ottis, Rain, ed. 2011. *Proceedings of the 10th European Conference on Information Warfare and Security*. Tallinn: Tallinn University of Technology.

Podins, Karlis, Jan Stinissen, and Markus Maybaum. 2013. *5th International Conference on Cyber Conflict. Proceedings 2013*. Tallinn: NATO CCD COE Publications.

Postimees.ee. 2007. „Ansip: meie suveräänne riik on tugeva rünnaku all." *Postimees* 02. mai. http://www.postimees.ee/1656303/ansip-meie-suveraanne-riik-on-tugeva-runnaku-all (kasutatud 06.04.2014)

Postimees.ee. 2007. „Paet: Vene karu jätkab vana joont." *Postimees* 04. mai. http://www.postimees.ee/1657319/paet-vene-karu-jatkab-vana-joont (kasutatud 21.03.2014)

Rand, Erik, ja Aivar Pau. 2007. „Paet: Venemaa ründab Eesti kaudu Euroopa Liitu." *Eesti Päevaleht* 01. mai. http://epl.delfi.ee/news/eesti/paet-venemaa-rundab-eesti-kaudu-euroopa-liitu.d?id=51085322 (kasutatud 26.03.2014)

Rand, Erikf. 2007. „Laar: suutlikkus Venemaa küberrünnakud tõrjuda on tõstnud Eesti mainet." *Eesti Päevaleht* 11. juuli. http://epl.delfi.ee/news/eesti/laar-suutlikkus-venemaa-kuberrunnakud-torjuda-on-tostnud-eesti-mainet.d?id=51093834 (kasutatud 10.03.2014)

Riigi Infosüsteemide Amet. 2007. „CERT Eesti: Varahommikul kordistati rünnakuid Eesti küberruumi vastu." *Riigi Infosüsteemide Amet* 01. mai. https://www.ria.ee/cert-eesti-varahommikul-kordistati-runnakuid-eesti-kuberruumi-vastu/ (kasutatud 01.03.2014)

Rid, Thomas. 2012. „Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (1): 20. http://dx.doi.org/10.1080/01402390.2011.608939 (kasutatud 15.04.2013)

Roe, Paul. 2008. „Actor, Audience(s) and Emergency Measures: Securitization and the UK's Decision To Invade Iraq." *Security Dialogue* 39 (6): 615-635. http://sdi.sagepub.com/content/39/6/615 (kasutatud 03.04.2013)

Rosenau, James N., and J. P. Singh, eds. 2002. *Information Technologies and Global Politics: The Changing Scope of Power and Governance*. Albany: State University of New York Press.

Salter, Mark. B, and Can E. Mutlu. 2013. „Securitisation and Diego Garcia." *Review of International Studies* 39(4): 815-834. http://dx.doi.org/10.1017/S0260210512000587 (kasutatud 03.02.2014)

Smith, Steve, Amelia Hadfield, and Tim Dunne, eds. 2012. *Foreign Policy: Theories, Actors, Cases*. 2nd ed. Oxford: Oxford University Press.

Stritzel, Holger. 2011. „Security, the Translation." *Security Dialogue* 42 (4-5): 343-355. http://sdi.sagepub.com/content/42/4-5/343 (kasutatud 27.12.2013)

Sulbi, Raul. 2011. „Ilves: Venemaa pole küberkaitse lepingutega ühinenud." *Postimees* 06. veebruar. http://www.postimees.ee/383820/ilves-venemaa-pole-kuberkaitse-lepingutega-uhinenud (kasutatud 10.02.2014)

The Atlantic Treaty Association. 2012. „The Growing Cyber-Threat: What Role for the Transatlantic Alliance?" Atlantic Voices 2 (5): 1-12. http://issuu.com/atlantic_treaty_association/docs/vol._2__no._5__may_2012_ (kasutatud 04.02.2014)

Tiks, Oliver. 2007. „Ansip: juhtunu oli šokk terve maailma jaoks." *Postimees* 10. mai. http://www.postimees.ee/1659579/ansip-juhtunu-oli-okk-terve-maailma-jaoks (kasutatud 22.03.2014)

Tiks, Oliver. 2007. „Paet: küberrünnakute teema tuleb tõstatada tippkohtumisel." *Postimees* 14. mai. http://www.postimees.ee/1660761/paet-kuberrunnakute-teema-tuleb-tostatada-tippkohtumisel (kasutatud 22.04.2014)

Thomas, Nicholas. 2009. „Cyber Security in East Asia: Governing Anarchy." *Asian Security* 5 (1): 3-23. http://dx.doi.org/10.1080/14799850802611446 (kasutatud 02.02.2014)

Tikk, Eneken, and Anna-Maria Talihärm, eds. 2010. *International Cyber Security. Legal & Policy Proceedings*. Tallinn: CCD COE Publications.

Uma, M., and G. Padmavathi. 2013. „Survey on Various Cyber Attacks and their Classification". *International Journal of Network Security*, 15 (6): 391-397. http://ijns.femto.com.tw/contents/ijns-v15-n5/ijns-2013-v15-n5-p390-396.pdf (kasutatud 03.02.2014)

Vaks, Toomas. 2012. „Riigi Infosüsteemi Ameti roll Eesti küberturvalisuse tagamisel." *Eesti infoühiskonna aastaraamat 2011/2012*. http://www.riso.ee/et/content/riigi-

infos%C3%BCsteemi-ameti-roll-eesti-k%C3%BCberturvalisuse-tagamisel#.UzBU7X8XjyU (kasutatud 24.03.2014)

Van Dijk, Teun A. 1993. „Principles of Critical Discourse Analysis." *Discourse & Society*, 4 (2), 249-250. doi: 10.1177/0957926593004002006 (kasutatud 03.03.2014)

Välisministeerium. 2007 „Välisministri avaldus." *Välisministeeriumi koduleheküIg* 01. mai. http://www.vm.ee/?q=node/2874 (kasutatud 21.03.2014)

Välisministeerium. 2007. „Välisminister kõneles Euroopa Nõukogus." *Välisministeeriumi koduleheküIg* 11. mai. http://www.vm.ee/?q=node/2892 (kasutatud 22.03.2014)

Värk, René. 2008. „The Siege of the Estonian Embassy in Moscow: Protection of a Diplomatic Mission and Its Staff in the Receiving State." *Juridica International* 13: 144-153. http://www.juridicainternational.eu/public/pdf/ji_2008_2_144.pdf (kasutatud 04.04.2014)

Walt, Stephen. 1991. „The Renaissance of Security Studies." *International Studies Quarterly* 35 (2): 211-239. http://www.jstor.org/stable/2600471 (kasutatud 06.04.2013)

Warren, Matthew, ed. 2013. *Case Studies in Information Warfare and Security: For Researchers, Teachers and Students*. Academic Conferences Limited.

Weldes, Jutta. 1999. *Cultures of Insecurity: States, Communities, and the Production of Danger*. Minneapolis, MN: University of Minnesota Press.

Wetherell, Margaret, Stephanie Taylor, and Simeon J. Yates, eds. 2001. *Discourse Theory and Practice: A Reader*. Thousand Oaks, CA: Sage.

Williams, Michael C. 2003. „Words, Images, Enemies: Securitization and International Politics." *International Studies Quarterly* 47 (4): 511-531. http://www.samorzad.pwsz.krosno.pl/gfx/pwszkrosno/pl/defaultaktualnosci/675/5/1/s08b_rm_williams.pdf (kasutatud 03.03.2013)

Williams, Paul D.,ed. 2012. *Security Studies: An Introduction*, 2nd ed. London; N.Y.: Routledge.

Dokumendid ja õigusaktid

„Eesti infoühiskonna arengukava 2020**”** ja selle rakendusplaani aastateks 2014–2015 heakskiitmine. 2013. Riigi Teataja III, 2013, 14. https://www.riigiteataja.ee/akt/319112013014 (kasutatud 26.03.2014)

Eesti julgeolekupoliitika alused 2010. Seletuskiri. 2010. Välisministeeriumi kodulehekülg. http://www.vm.ee/?q=node/9180 (kasutatud 08.04.2014)

Eesti teadus- ja arendustegevuse ning innovatsiooni strateegia 2014–2020 „Teadmistepõhine Eesti” heakskiitmine. 2014. Riigi Teataja III, 2014, 2. https://www.riigiteataja.ee/akt/329012014002 (kasutatud 26.04.2014)

Eesti turvalisuspoliitika põhisuundade aastani 2015 heakskiitmine. 2008. Riigi Teataja I, 2008, 25, 165. https://www.riigiteataja.ee/akt/12979629 (kasutatud 26.04.2014)

Eesti Vabariigi julgeolekupoliitika alused. 2004. Riigi Teataja I, 2004, 49, 344. https://www.riigiteataja.ee/akt/773389 (kasutatud 26.03.2014)

Eesti Vabariigi põhiseadus. 1992. Riigi Teataja 1992, 26, 349. https://www.riigiteataja.ee/akt/633949 (kasutatud 26.03.2014)

Hallingstad, Geir, and Luc Dandurand. 2010. *Cyber Defence Capability Framework – Revision 2. Reference Document RD-3060*. The Hague: NATO C3 Agency.

Hädaolukorra seadus. 2009. Riigi Teataja I, 2014, 25. https://www.riigiteataja.ee/akt/HOS (kasutatud 23.04.2014)

ISO/IEC JTC 1/SC 7. 2004. „ISO/IEC 18019:2004. Software and System Engineering – Guidelines for the Design and Preparation of User Documentation for Application Software.” https://www.iso.org/obp/ui/#iso:std:iso-iec:18019:ed-1:v1:en (kasutatud 23.03.2014)

ISO/IEC JTC 1/SC 27. 2012. „ISO/IEC 27032:2012. Information Technology – Security Techniques – Guidelines for Cybersecurity.” https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en (kasutatud 05.01.2014)

ITU. 2008. *Series X: Data Networks, Open System Communications and Security: Overview of Cybersecurity. Recommendation X.1205*. ITU-T Publications, ii. http://www.itu.int/rec/T-REC-X.1205-200804-I (kasutatud 21.04.2014)

Julgeolekupoliitika aluste töörühm. 2010. *Eesti julgeolekupoliitika alused*. Tallinn. http://www.vm.ee/?q=node/9180 (kasutatud 01.03.2014)

Kaitseministeerium. *Riigikaitse arengukava 2013-2022*. 2013. Tallinn. http://www.kmin.ee/et/riigikaitse-alusdokumendid (kasutatud 28.04.2014)

Kriminaalpoliitika arengusuunad aastani 2018 heakskiitmine. 2010. Riigi Teataja III, 2010, 26, 51. https://www.riigiteataja.ee/akt/13329831 (kasutatud 07.04.2014)

„Küberjulgeoleku strateegia 2008–2013" rakendusplaani aastateks 2009-2011 heakskiitmine. 2009. Riigi Teataja 2009, 43, 596. https://www.riigiteataja.ee/akt/13182154 (kasutatud 26.03.2014)

Küberjulgeoleku strateegia 2008–2013" rakendusplaani 2012-2013 heakskiitmine. 2011. Riigi Teataja III, 2011, 5. https://www.riigiteataja.ee/akt/330122011005 (kasutatud 26.03.2014)

„Küberjulgeoleku strateegia 2014–2017" koostamise ettepaneku heakskiitmine. 2013. Riigi Teataja III, 2013, 9. https://www.riigiteataja.ee/akt/326032013009 (kasutatud 20.02.2014-05.05.2014)

Küberjulgeoleku strateegia komisjon. 2008. *Küberjulgeoleku strateegia 2008-2013*. Tallinn: Kaitseministeerium. http://valitsus.ee/et/valitsus/arengukavad (kasutatud 04.04.2013-12.05.2014)

Majandus- ja Kommunikatsiooniministeerium. 2013. *Infoühiskonna arengukava 2020*. http://valitsus.ee/et/valitsus/arengukavad (kasutatud 28.04.2014)

NATO Heads of State and Government. 2010. *Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*. Lisbon. http://www.nato.int/cps/en/natolive/official_texts_68580.htm (kasutatud 03.01.2014)

Poliitikaosakonna põhimäärus. 2012. Välisministeeriumi koduleheküg. http://www.vm.ee/?q=node/9220 (kasutatud 08.04.2014)

Rahuaja riigikaitse seadus. 2002. Riigi Teataja I, 2002, 57, 354. https://www.riigiteataja.ee/akt/12751452 (kasutatud 08.04.2014)

Randel, Tarmo. 2007. *CERT Eesti tegevuse aastakokkuvõte 2007*. https://www.ria.ee/public/CERT/CERT_2007_aastakokkuv6te.pdf (kasutatud 23.03.2014)

Riigi Infosüsteemi Ameti põhimäärus. 2011. Riigi Teataja I, 2011, 1. https://www.riigiteataja.ee/akt/128042011001 (kasutatud 09.03.2014)

„Riigikaitse arengukava 2013–2022" heakskiitmine. 2013. Riigi Teataja III, 2013, 8. https://www.riigiteataja.ee/akt/329012013008 (kasutatud 26.03.2014)

Riigikaitse strateegia. 2010. Tallinn. http://www.kmin.ee/et/riigikaitse-alusdokumendid (kasutatud 15.04.2014)

Siseministeeriumi infotehnoloogia- ja arenduskeskuse põhimäärus. 2013. SMIT-i kodulehekülg. http://www.smit.ee/pohimaarus.html (kasutatud 06.04.2014)

Siseministeeriumi põhimäärus. 2012. Riigi Teataja I, 2012, 4. https://www.riigiteataja.ee/akt/128012014003 (kasutatud 06.04.2014)

Strateegiliste arengukavade liigid ning nende koostamise, täiendamise, elluviimise, hindamise ja aruandluse kord. 2005. Riigi Teataja I, 2005, 67, 522. https://www.riigiteataja.ee/akt/12790098 (kasutatud 28.04.2014)

Sõjalise kaitse strateegilise kava kehtestamine. 2005. Riigi Teataja I, 2005, 5, 17. https://www.riigiteataja.ee/akt/840391 (kasutatud 14.04.2014)

The North Atlantic Treaty Organization. 1949. *The North Atlantic Treaty*. Washington D.C. http://www.nato.int/cps/en/natolive/topics_89597.htm (kasutatud 15.02.2014)

UK Cabinet Office. 2009. *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space*. Norwich: The Stationery Office.

Vabariigi Valitsuse seadus. 1995. Riigi Teataja I, 1995, 94, 1628. https://www.riigiteataja.ee/akt/1011049?leiaKehtiv (kasutatud 26.03.2014)

Wamala, Frederick. 2011. *ITU National Cybersecurity Strategy Guide*. Geneva: ITU, 5. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf (kasutatud 05.02.2014)

Elektroonilised infokanalid

Aaviksoo, Jaak. 2007. „Eesti küberjulgeolek: küberkaitse ja NATO küberkaitse." *Konverentsil Visioonist lahendusteni*. https://www.youtube.com/watch?v=113XjfYDPYs (kasutatud 21.03.2014)

CCDCOE kodulehekülg. https://www.ccdcoe.org/ (kasutatud 24.04.2014)

EastWest Institute'i kodulehekülg. http://www.ewi.info/ (kasutatud 03.03.2014)

Eesti Ajalehtede Liidu koduleheküg. http://www.eall.ee/index.html (kasutatud 26.04.2014)
Eesti Suursaatkond Washingtonis koduleheküg. http://www.estemb.org/est (kasutatud 09.04.2014)
ENISA koduleheküg. http://www.enisa.europa.eu/ (kasutatud 03.03.2014)
Europoli koduleheküg. https://www.europol.europa.eu/ec3 (kasutatud 03.03.2014)
Haridus- ja Teadusministeeriumi koduleheküg. http://www.hm.ee/index.php?0 (kasutatud 06.04.2014)
Intress.ee koduleheküg. http://seb.intress.ee/ (kasutatud 07.04.2014)
ITU koduleheküg. http://www.itu.int/en/Pages/default.aspx (kasutatud 21.04.2014)
Justiitsministeeriumi koduleheküg. http://www.just.ee/ (kasutatud 06.04.2014)
Kaitseministeeriumi koduleheküg. http://www.kmin.ee/ (kasutatud 29.03.2014-01.05.2014)
Majandus- ja Kommunikatsiooministeeriumi koduleheküg. http://www.mkm.ee/ (kasutatud 29.03.2014-01.05.2014)
Riigi Infosüsteemi Ameti koduleheküg. https://www.ria.ee/ (kasutatud 15.04.2014)
Siseministeeriumi koduleheküg. https://www.siseministeerium.ee/?404 (kasutatud 06.04.2014)
Swedbanki koduleheküg. https://www.swedbank.ee/private (kasutatud 07.04.2014)
Techopedia.com. http://www.techopedia.com (kasutatud 14.03.2014)
TechTerms.com. http://www.techterms.com (kasutatud 02.02-30.03.2014)
The Free Dictionary'i koduleheküg. http://www.thefreedictionary.com/ (kasutatud 09.04.2014)
Vabariigi Valitsuse koduleheküg. http://valitsus.ee/et/valitsus (kasutatud 25.04.2014-01.05.2014)
Välisministeeriumi koduleheküg. http://www.vm.ee/?q=et (kasutatud 06.04.2014)
Postimehe koduleheküg. http://www.postimees.ee/ (kasutatud 06.04.2014)
Eesti päevalehe koduleheküg. http://epl.delfi.ee/ (kasutatud 06.04.2014)
Õhtulehe koduleheküg. http://www.ohtuleht.ee/ (kasutatud 06.04.2014)

Uuringud

Saar Poll. 2013. oktoober. *Avalik arvamus ja riigikaitse*. Tallinn: Kaitseministeerium. http://www.kmin.ee/et/avalik-arvamus (kasutatud 30.11.2013)

Turu-uuringute AS. 2007. juuli. *Avalik arvamus ja riigikaitse*. Tallinn: Kaitseministeerium. http://www.kmin.ee/et/avalik-arvamus (kasutatud 05.04.2013)

Turu-uuringute AS. 2010. september. *Avalik arvamus ja riigikaitse*. Tallinn: Kaitseministeerium. http://www.kmin.ee/et/avalik-arvamus (kasutatud 05.04.2013)

Turu-uuringute AS. 2011. august. *Avalik arvamus ja riigikaitse*. Tallinn: Kaitseministeerium. http://www.kmin.ee/et/avalik-arvamus (kasutatud 05.04.2013)

Saar Poll. 2013. märts. *Avalik arvamus ja riigikaitse*. Tallinn: Kaitseministeerium. http://www.kmin.ee/et/avalik-arvamus (kasutatud 05.04.2013)

Bakalaureuse- ja magistritööd

Dinesen, Sofia Lisa, and Heidi Bruvik Sæther. 2013. „Cyber Security – Securitizing Cyber Threats in Denmark." Master's thesis. Copenhagen Business School. http://studenttheses.cbs.dk/handle/10417/3949 (kasutatud 11.11.2013)

Halvordsson, Dennis. 2012. „Securitizing the Virtuality of the Real: A Gramscian Analysis of the Securitization of U.S. Cyberspace Governance." Bachelor's thesis. Gothenburg University. https://gupea.ub.gu.se/handle/2077/32833 (31.10.2013)

Hart, Catherine Elizabeth, 2012. „Securing Freedom: A Media Framing Analysis of Cybersecuritization." Master's thesis. Simon Fraser University. http://summit.sfu.ca/item/12560 (01.11.2013)

Hjalmarsson, Ola. 2013. „The Securitization of Cyberspace: How the Web Was Won." Bachelor's thesis. Lund University. http://www.lunduniversity.lu.se/o.o.i.s?id=24965&postid=3357990 (28.10.2013)

Klingova, Katarina. 2013. „Securitization of Cyber Space in the United States of America, the Russian Federation and Estonia." Master's thesis. Central European University. http://www.etd.ceu.hu/2013/klingova_katarina.pdf (27.10.2013)

SUMMARY

Cyber Securitization According to the Theory of the Copenhagen School Based on the Example of the Estonian Discourse

One of the main goals of this thesis was to assess the process of cyber securitization on the basis of the theory of the Copenhagen School. This research was undertaken to evaluate the process of cyber securitization in practice, thus the case of cyber attacks in the Republic of Estonia in 2007 and the time thereafter were chosen as the central focus. It is important to investigate cyber security because of the growing tendency of states to integrate cyber security into international relations and domestic politics.

On a larger scale, it is important to pay attention to cyber security because politicians and other practitioners do not have enough time to theorize over different aspects of cyber security. Therefore, it is the task of scholars to apply different theories to the analysis of cyber security. The case study of this research is based on the example of Estonia because the cyber attacks in Estonia in 2007 had a great impact on raising awareness of cyber attacks and the necessity to improve cooperation on cyber security topics on the international level.

In the introduction of this master's thesis, the background, importance and actuality of the topic were analyzed. Also, the research questions and goals, the former literature on the topic and the main sources of this thesis were examined. In the first content chapter, an overview of the basic terms in the field of cyber security was given. There are no universally defined terms in this area, hence there was a necessity to evaluate different definitions and eventually develop one definition for every term to be used in the rest of the research.

In this terminology chapter, the research also discussed the reasons why there are no universally defined terms and how the different terms of the cyber domain are related to each other. There are no universally defined terms in the cyber security field because the cyber domain consists of several technologies, strategies and sectors, and different people who are associated with cyber security have different definitions depending on the nature of their job. Also, the lack of cooperation between countries and differences in languages are among the reasons why there are no universally defined terms in the cyber security field. In this chapter, the focus was on the following terms: cyber

security, cyber space, cyber attack and classification of cyber attacks (cyber war, cyber espionage, cyber terrorism, cyber vandalism and cyber crime). As the term cyber defense is narrower than cyber security, the master thesis mainly used the term cyber security and only in specific cases the term cyber defense.

In the second content chapter, the aim was to analyze the initial and the second generation theory of the Copenhagen School, and pay attention to the sectors as well as the securitization theory. Simultaneously, the theory of the Copenhagen School (securitizing actors, existential threats, referent object, referent subject and audience) was applied to the cyber domain. The four sectors (economic, social, political and military) are the referent objects in the cyber security field, partially also including the environmental sector. Narrowly, the referent objects are state, institutions, business, nation, individual, sovereignty and so on. Also, in the cyber security sector, the referent objects are the media, financial institutions, transport and networks.

Existential threats are cyber attacks and its types (cyber war, cyber espionage, cyber terrorism, cyber vandalism and cyber crime). Referent subjects are criminals, terrorists, states, espionage services and script kiddies. Securitizing actors are the state, international organizations, corporations, and more narrowly civil society organizations, private businesses and individuals. There are three main audiences in the cyber domain: institutional bodies (politicians), publicity (electors and citizens), technocrats and specialists in cyber security.

According to the definition of securitization, it is associated with the speech act theory (John Langshaw Austin, "How to do Things with Words", 1975) which was analyzed to evaluate the differences between a securitizing move and security practice. This differentiation was applied to the theory of cyber securitization. In the theoretical chapter, cyber securitization ("cyber" + "securitization") was defined as the two-stage process where the first is the securitizing move (or illocutive act) where the securitizing actor securitizes the existential threats to the referent objects (illocutive act) based on the acceptance of the audience (perlocutive act) and warns the aggressor or gives the promise to protect the referent object. The second stage is the security practice where the securitizing actor has to take measures to improve the situation of the referent object which means that the illocutive act has to be consistent with the security practice.

Although the initial theory of the Copenhagen School provides that the second stage of the securitization process is the acceptance of the audience (perlocutive act), it is more reasonable to attribute the acceptance of the audience to both stages of the securitization process. The perlocutive act should usually be a part of both steps of securitization because in the first stage, the securitizing actor tries to persuade the audience and in the second stage, the audience has to give permission for measures to improve the situation of the referent objects.

In the third content chapter, the research focused on the methodology for investigating the process of securitization. The master's thesis centered on post-structural discourse analysis on the basis of the approach of Lene Hansen ("Security as Practice: Discourse Analysis and the Bosnian War", 2007). The chapter discussed the analytical framework for the discourse analysis and concentrated on the sample of texts and context. The aim of this chapter was to give thorough methodological guidelines for the post-structural discourse analysis for the empirical chapter to analyze the case of Estonia. This chapter bound the methodology and the theory of cyber securitization because it gave a deeper base to analyze the securitizing moves in speeches.

According to the post-structural discourse analysis, it is important to identify the "self" and "other" in foreign policy discourse. The "self" is the referent object in cyber securitization theory and the "other" is the referent subject. Also, it is important to identify the "us" which is the referent object and securitizing actor together. Identifying the "us" helps to analyze the tools which the securitizing actor uses to persuade the audience who is "you" in the cyber securitization process more deeply.

In the methodology chapter, the research focused on the Hansen research agenda which was the base for specifying the texts for the empirical chapter. Also, the chapter focused on the context according to Margaret Wetherell ("Discourse Theory and Practice: A Reader", 2011) who has distinguished the proximate and distal contexts. The proximate context for the cyber attacks in Estonia in 2007 was the securitization of the Bronze Soldier monument and the siege of the Estonian embassy in Moscow.

According to Hansen's research agenda, the research used model one (official discourse) because the master thesis focused on the executive power (ministers, ministries and the government) as the representatives of executive powers have enough power and legitimacy to take the measures for improving the situation of referent

objects. The aim was to evaluate the speech acts of the securitizing actors who have authority to undertake the measures. Thus, the texts of the methodological analysis were limited to the speech acts of the ministers as the representatives of executive power whose ministries are responsible for designing and coordinating the policy of cyber security. According to research agenda, the "self" was Estonia, the time was 27.04-19.05.2007 and the event was cyber attacks in Estonia in 2007.

The Ministry of Defense, the Ministry of Economic Affairs and Communications, the Ministry of Education and Research, the Ministry of Foreign Affairs, the Ministry of Internal Affairs, the Ministry of Justice and the Government of the Republic of Estonia were associated with the cyber security. Hence, the analysis focused on the ministers who were in office when the cyber attacks in Estonia occurred in 2007. These ministers were the Minister of Foreign Affairs (Urmas Paet, since April 2005), the Minister of Defense (Jaak Aaviksoo, between 2007-2011), the Prime Minister (Andrus Ansip, between 2005-2014), the Minister of Justice (Rein Lang, between 2005-2011), the Minister of Education and Research (Tõnis Lukas, between 2007-2011), the Minister of Economic Affairs and Communications (Juhan Parts, between 2007-2014) and the Minister of Internal Affairs (Jüri Pihl, between 2007-2009).

In order to analyze the speech acts of the ministers, the research investigated the homepages of the ministries and the government as well as sources of the media ("The Postimees", "The Õhtuleht" and "The Eesti Päevaleht"). The discourse analysis was limited to the written and spoken texts (interviews, speeches and opinion articles) of these Estonian ministers. The analysis was further limited to three ministers (and two ministries and the government) due to their speech acts being associated with the cyber attacks in Estonia in 2007.

The following were studied: the Minister of Foreign Affairs (Urmas Paet), the Minister of Defense (Jaak Aaviksoo) and the Prime Minister (Andrus Ansip) because they were the three ministers who were in office in 2007 and they made statements about the cyber attacks in Estonia in 2007. Altogether, the methodology chapter brought twelve speech acts which were analyzed in depth in the empirical chapter.

In the last content chapter, the research focused on the empirical analysis on the basis of the theoretical and methodological frameworks. The aim of the empirical analysis was to apply the theory of cyber securitization to a case in practice. The Minister of Foreign

Affairs (Paet) made a promise to protect the referent object in three speech acts, the Minister of Defense (Aaviksoo) in two speech acts and the Prime Minister (Ansip) in one speech act, thus they made the securitizing move.

The securitizing moves and perlocutive acts (acceptance of the audience) and the creation of a relationship between the identity and foreign policy were analyzed in these six speech acts according to the securitization theory and post-structural discourse analysis. According to Paet, Aaviksoo and Ansip, the referent objects ("self") were Estonia and the European Union. Estonia was described as peaceful, Christian, co-operative, lovely, part of the Baltics, a former part of the Soviet Union, and the neighbor of Russia. The "us" were Estonians, partners in the European Union and NATO, and the member states of the Council of Europe.

The referent objects were the state but also the institutions (politicians), business, nation, individuals, the media, banks, networks, society, sovereignty and economy. Existential threats were cyber attacks and more narrowly its types cyber vandalism and cyber crime although the Minister of Defense identified cyber attacks and cyber terrorism in his speech acts. According to the speech acts of Paet and Ansip, the referent subject ("other") was Russia who was described as aggressive and hostile. Aaviksoo did not associated the cyber attacks with Russia, instead he said that the source of attacks were hostile forces.

The audience was legislative power (parliament), publicity and international organizations (the EU and NATO) and other states. An intertextual approach indicated that Aaviksoo and Paet managed to address the international audience. The audience included politicians in Estonia and abroad, and also electors because the legitimacy of ministers is depending on the voters.

An additional aim of the last content chapter was to evaluate if the securitizing move (the securitizing actor makes a warning to the aggressor or promise to protect the referent object) is consistent with the security practice because the process of securitization is fully completed if the securitizing actor is taking the measures to protect and improve the situation of the referent objects. In order to evaluate the real measures taken to accomplish that the investigation focused on the direct measures taken by these three ministers after these cyber attacks.

The analysis focused on Estonia's fifty-five development plans to distinguish the development plans associated with the cyber domain. According to the analysis, seven development plans were associated with the cyber security. The study focused on the development plans because ministers are involved in the creation of these documents and their ministries are responsible for implementing the measures identified in these documents.

The thesis focused on three development plans which were created or implemented by these two ministries and the government and associated with the cyber domain. These three development plans were the Cyber Security Strategy (2008), the National Security Concept of Estonia (2010) and the National Defense Strategy (2010).

Based on the development plans, the master's thesis proposed to complement the cyber securitization theory because these documents unite the processes of the securitizing move and security practice. It is not always easy to identify the explicit promise to protect the referent object from the speeches, thus the development plans are associated with the process of the securitizing move.

In the empirical analysis chapter, the investigation proposed improvements to the theory of cyber securitization. In the first cyber securitization stage, it should be enough if the securitizing actor says that there is an existential threat to the referent object and gives a curt promise or warning. It is important to analyze the promise inside the taken measures (e.g. in the development plans) to reinforce the securitizing move (the promise or warning). Also, the development plans are important for the stage of security practice because there are goals and measures identified in these documents which help to analyze if the securitizing actor has completed the securitization process by implementing the identified measures.

Aaviksoo proposed to create the Cyber Security Strategy and the Ministry of Defense coordinated its creation, so the securitizing move of the minister of defense is consistent with security practice. Also, this strategy is the security practice of the Prime Minister because the government approved Aaviksoo's proposal and approved the final draft of this strategy. The securitizing move of the Minister of Foreign Affairs is also consistent with the security practice because Paet initiated the founding of the National Security Concept of Estonia, created the working team to set this up. Aaviksoo made the

proposal to the government to approve the National Defense Strategy, so this shows that the securitizing move of Ansip and Aaviksoo is consistent with the security practice.

In all three development plans, it is possible to identify the promise to protect the referent object. As only in the National Security Concept of Estonia and Cyber Security Strategy the measures to improve the cyber security are identified, the analysis that followed focused on these two documents. In the development plan of the National Defense Strategy there were no measures identified so the analysis did not focus on this document. According to the two aforementioned documents, the main measures to be analyzed were the announcements by Ansip, Aaviksoo and Paet because are the direct measures which belong to the ministers' competence. Making announcements about the cyber domain is helpful for co-operation between the states and organizations and for the legislative sphere.

To analyze the apprising done by ministers, the analysis focused on the webpages of the Ministry of Defense, the Ministry of Foreign Affairs and the government to count the speeches, interviews and opinion articles were the ministers are making announcements about the cyber domain. The counting and comparison indicated that Paet and Aaviksoo had been on the same level in their notifications of cyber security because in 1/3 of their speech acts, they mentioned the cyber domain. Paet and Aaviksoo had mainly referred to the cyber domain on the international level (several conferences, meetings etc.). Ansip had mention the cyber security in a few speeches and mainly in Estonia but regardless of this, we can conclude that making announcements about the cyber domain by these three ministers indicates that the securitizing moves of Paet, Ansip and Aaviksoo are consistent with the security practice.

This study has shown that the cyber security can be analyzed on the basis of the theory of the Copenhagen School and this was the base for developing the theory of cybersecuritization. The case study relying on the example of cyber attacks in Estonia in 2007 showed that cyber securitization has fully occurred in Estonia. In the speech acts of these three ministers (Ansip, Aaviksoo and Paet) and in the development plans, the research identified the securitizing move (promise to protect the referent objects) and the security practice (creation and approval of development plans and making announcements about the cyber domain in speech acts) showed that the securitizing move is consistent with the security practice.

The current investigation was limited to the speech acts of the Estonian ministers whose ministries or government are associated with cyber security. This research has raised some questions in need for further investigation. It is recommended that further research be undertaken in the following areas in doctoral theses: speech acts of the IT-specialists and other politicians (e.g. members of the parliament). This would help to investigate more thoroughly how the cyber securitization process has emerged in Estonia.

In addition to the speech acts of Urmas Paet, Andrus Ansip and Jaak Aaviksoo, it would be necessary to analyze the successors in their positions. Furthermore, although the Minister of Economic Affairs and Communications (Juhan Parts), the Minister of Internal Affairs (Jüri Pihl) and the Minister of Justice (Rein Lang) did not make the securitizing move with reference to cyber attacks against Estonia in 2007, it would be possible to analyze these ministers as securitizing actors based on development plans.

Also, the measures of securitizing actors (e.g. members of the parliament and IT-specialists) in the juridical and technical sphere should be analyzed. Further research might explore if the process of cyber securitization in Estonia has been successful. This master's thesis explored if and how cyber securitization has been taken place in Estonia, but the post-structural discourse analysis is not sufficient to analyze the success of the process. The present study makes several noteworthy contributions to the theory of cyber securitization which has formerly been evaluated only to a limited extent.