TARTU ÜLIKOOL

Sotsiaal- ja haridusteaduskond

Riigiteaduste instituut

Saskia Kiisel

Eesti välispoliitiline käitumine ja otsused 2007. aasta küberrünnakute tõrjumisel

Bakalaureusetöö

Juhendajad:

Eneken Tikk-Ringas, dr iur

Rein Toomla, MA

Tartu 2015

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.

……..

/töö autori nimi/

Sisukord

Sissejuhatus

Internet oli mõeldud telekommunikatsiooni vahendiks Ameerika Ühendriikide teaduslaboritele teadmiste vahendamisel. (Hafner ja Lyon 1998: 5) Ajapikku lisati sellele uusi funktsioone ja kasutamist muudeti pidevalt mugavamaks, internet levis ning kasvas kasutajaskond. Tänapäeval puutub peaaegu iga eluvaldkond suuremal või vähemal määral kokku informatsiooni- ja kommunikatsioonitehnoloogiaga (edaspidi IKT). Tehnoloogiline innovatsioon dikteerib valitsustele, millega peab tegelema, kui tahetakse tagada riigi areng ja püsima jäämine. Paradoksaalsel moel on inimeste poolt loodu rajanud uued ohud, teinud haavatavaks suured ja väikesed riigid ning ühiskonnad.

21. sajand on pannud riike mõistma, et küberjulgeoleku tagamiseks ning küberruumi ohtudega võitlemisel oluline püsida aja ja protsessidega kaasas. Ajaloost on teada mitmeid riigitasandil kogetud küberrünnakuid: Venemaa ja tšetšeenide konflikt 1994. aastal, mil viimased kasutasid propagandistlikel eesmärkidel interneti ära, et näidata õõvastavaid sõjategevuse pilte kogu maailmale; Kosovo 1999. aasta konflikt, kus rühmitus "Must Käsi" (ing kl *Black Hand*) ründas NATO interneti taristut, kui NATO lennukid hakkasid pommitama Serbiat; 2007. aasta laiaulatuslikud küberründed Eesti valitsuse ja ettevõtete vastu; Gruusia-Venemaa konflikt 2008. aastal, mil paralleelselt sõjategevusega rünnati ka Gruusia interneti taristut; 2010. aasta Stuxnet viiruse avastamine Iraani tuumaprogrammi arvutisüsteemides jpt. (Geers 2008; Tikk, Kaska ja Vihul 2010; Farwell ja Rohozinski 2012)

Riigid, rahvusvahelised ja regionaalsed organisatsioonid tegelevad küberprobleemidega, nendele lahenduste leidmisega, vanade kontseptsioonide kaasajastamisega, uute välja töötamistega. Ühtset kõigile ja igas olukorras töötavat kontseptsiooni ei pruugi esinedagi, sest riigid on oma välispoliitiliselt käitumiselt piisavalt erinevad, erinevate ambitsioonide ja toimimiste poolest. Olukorra teeb komplitseeritumaks ajatundlikkus – kui küberintsidentide lahendamismeetodite rakendamisega venitada, võivad kahjud olla suured. Ainuvõimaliku lahenduse puudumine ja võimatus ei tähenda, et tuleks või võiks loobuda sobivate meetmete leidmisest.

Käesolev töö esitleb küberjulgeoleku tagamisele suunatud meetmete ühe võimaliku valiku. Analüüsi alus on Eesti välispoliitilise käitumine 2007. aasta küberrünnakute kontekstis, esitab autor ülevaate välispoliitilistest meetmetest. Eesti kaasus on eriline selle poolest, et esimest korda said küberrünnakud riigi vastu suurt kõlapinda rahvusvahelisel areenil. Eesti kogemusest kirjutatakse senini peaaegu iga teises küberrünnakute valdkonda puudutavas teadusartiklis või –raamatus, millest enamik kirjutavad valdavalt kübersõja vaatevinklist. (nt Arquilla ja Ronfeldt 1993; Schmitt 2013; Clarke ja Knake 2014) Vaatamata hulgalistele käsitlustele ei ole Eesti kaasus poliitilist analüüsi leidnud ja vastupidiselt levinud arusaamale ei ületanud kübersõja künnist. Teiseks on tegu autori koduriigiga, mistõttu sai sündmuseid vahetult kogeda ning kolmandaks on võimalik nüüd tolleaegsele piiratud juurdepääsuga teabele ligipääseda. Lisaks on eesti keelt mittekõneleval keerulisem avaldet infot analüüsida.

Analüüsi struktuuri toetab Wingfieldi ja Tikk-i poolt välja pakutud ühte võimalikku küberjulgeoleku otsustusraamistik – Kuup, Püramiid ja Ekraan (edaspidi KPE kontseptsioon või Kontseptsioon). Autorid on loonud virtuaalse tööriista kontseptsiooni ehk nn Ekraani, mis võimaldab otsustajal näha küberruumis esinevaid kõiki olulisi – tehnilisi, poliitilisi ja juriidilisi – tahke (Kuup) ning selle pinnalt võetakse vastu otsuseid (Püramiidi rakendamine). (Wingfield ja Tikk 2010)

Kontseptsiooni rõhutab küberruumi ja selle vaimus tehtavate otsuste komplekssust. Enam ei piisa ründe või ohu korral ainult valdkonna sisendist ja meetoditest, sest see hõlmab rohkemaid valdkondi. Distsipliinid peavad töötama ühiselt julgeoleku tagamisel. Kontseptsioon koondab kolm relevantsemat haru: tehnoloogiline, poliitiline ja juriidiline. See võtab omakorda enda alla nendes harudes käsitletava terminoloogia, mis on tihti küberruumis esinevate probleemide raskuskiviks – üksteise mõistmine ekspertide vahel. Kõik, mis on olemas, peab kajastuma Ekraanil, vaid nii on võimalik võtta vastu kõige paremaid otsuseid, orienteeruda olukorras, hinnata ohte, areneda edasi.

Kuna seni on loodud Kontseptsioonile vaid raamistik, siis püüab käesoleva töö autor seda "täitma hakata". Arvestades, et Kontseptsioon on kolossaalne ja bakalaureusetöö maht

piiratud, saab antud töö aluseks võtta ainult kitsa osa – Püramiidi ehk võimalike lahendusmeetmete kogumikku.

Töö on jaotet nelja suuremasse peatükki. Esimene peatükk tutvustab KPE kontseptsiooni: mida see endast kujutab ning millised on selle erinevad osad. Teine peatükk kirjeldab Eesti 2007. aasta küberrünnakute perioodil toimunut tehnilises plaanis: kes tegelesid rünnetega, mis langesid ründajate sihtmärkideks, milliste ründetüüpide ja –vahendidega rünnati. Kolmas peatükk uurib poliitilise tasandi käitumist ehk mida tegid Riigikogu, Vabariigi Valitsuse liikmed ja President küberrünnakute perioodil. Viimane peatükk koondab tulemused kokku ühtseks Püramiidiks ja analüüsib vastuvõetud otsuseid.

Töös on kasutet tehnilisel tasandil Riigi Infosüsteemide Ameti veebilehel asuvaid uudiseid ja pressiteateid; küberrünnakute lahendamise juhtimisega tegelenud Hillar Aarelaiu ettekandeid, intervjuusid ja teisi kirjutisi; Kaitseväe Side- ja Infosüsteemide Väljaõppe ja Arenduskeskuse (KV SIVAK) küberkaitse jaoskonna ülema Rain Ottise memosid; Eesti poolt saadetud lühikokkuvõtteid NATO-le; ajalehtede artikleid ja uudiseid. Poliitilisel tasandil uuris autor Vabariigi Valitsuse, Riigikogu ja Vabariigi Presidendi veebilehti, eelpool nimetet memosid ja lühikokkuvõtteid ning ajalehtede artikleid ja uudiseid. Lisaks kasutati informatsiooni leidmisel otsingumootorit Google ja Booleani loogikaoperatooreid.

1 Eesti 2007. aasta küberründed: sündmuste kirjeldus (tehniline tasand)

2007. aasta 27. aprilli õhtul algasid küberrünnakud Eesti avaliku ja erasektori vastu. (Riigi Infosüsteemide Amet 28.04.2007) Riigi Infosüsteemide Ameti (edaspidi RIA) [1] infoturbeintsidendite käsitlemise osakonna juhataja Hillar Aarelaid tituleeris esimesed kolm päeva "kübermässuks" (ing kl *cyber riot*), kus frustreerunud indiviidid elasid end kübermaailmas välja Tundmatu Sõduri monumendi ja sõjahaudade teisaldamisotsuse pärast. (Aarelaid 2007a; Randel 2007) Ründed olid emotsionaalsed ja lihtsakoelised. Maist alates aga rünnakute profiil muutus – ründed intensiivistusid ja muutusid keerulisemaks oma olemuselt viidates organiseeritusele ja professionaalsusele. (Tikk, Kaska ja Vihul 2010: 18) Ründed kestsid kokku 22 päeva.

1.1 Rünnetele reageerijad

Asutustele ja ettevõtetele sooritet küberrünnakute tuvastamise ning töökeskkonna taastamise, sh analüüside koostamise, eest vastutab Eestis alates 2006. aastast CERT (ing kl *Computer Emergency Response Team*) Eesti,[2] mis kuulub RIA koosseisu, Majandus- ja Kommunikatsiooniministeeriumi haldusalasse. (Riigi Infosüsteemi Amet 2015) CERT Eesti tegi koostööd nii Eesti siseselt – telekomifirmadega (nt Elioniga); (Randel 2007; lühikokkuvõte NATO-le 10.05.2007) riigi- ja erasektori it-ekspertidega; (Tomberg Hanno intervjuu Hillar Aarelaiuga 02.05.2007) riigiasutuste (ministeeriumitega, riikliku kriisikomiteega, Kaitseväega, Kaitseliiduga, Riigikontroll, KV SIVAK-ga), (Ottise memod 04.05.2007 ja 07.05.2007; Aarelaid 2007a) jõustruktuuride ja eraettevõtetega; (Riigi Infosüsteemide Amet 02.05.2007; Schmidt 2013: 6–7) õiguskaitseorganitega (Riigi Infosüsteemide Amet 07.05.2007) – kui ka väliselt – NATO NCIRC (ing kl *NATO Computer Incident Response Capability*) ja USA välisvaatlejatega; (lühikokkuvõte NATO-

[1] Alates 1. juunist 2011 muudeti Riigi Infosüsteemide Arenduskeskus Riigi Infosüsteemide Ametiks (Riigi

[2] 2005. aastal kiideti Vabariigi Valitsuse otsusega nr 23 heaks "Infopoliitika tegevuskava 2006", mille üheks tegevussuunaks 16-st punktist oli eTurvalisus. Selle eesmärgiks oli luua infoturvet puudutava koordinatsioonimehhanism ning korraldada koostöö, suurendada infoturbe alast teadlikkust nii avalikus sektoris kui kogu ühiskonnas, mida pidi ühe osana täitma CERT Eesti loomine (Infopoliitika tegevuskava 2006: 12).

le 08.05.2007) välismaa teenusepakkujatega; riikide (nt USA ja Saksamaaga)[3] ja nende CERT meeskondadega (nt Soomega) (Randel 2007); rahvusvaheliste partneritega jt. (Riigi Infosüsteemide Amet 11.05.2007, 16.05.2007, 30.04.2007; Aarelaid 2007b)

1.2 Rünnete sihtmärgid

Tehnilisel tasandil rünnati Eesti interneti infrastruktuuri erinevaid osasid, mida Eesti infoühiskond on harjunud kasutama oma igapäevases elus. Järgnevalt ründe sihtmärkidest ja ülevaatlikult nende tähendusest.

1.2.1 Rünnakud serveritele

Serverid on oluline osa internetist. Need on arvutivõrgu funktsionaalüksused (riistvarast, tarkvarast või mõlemast koosnev moodustis, mis on võimeline täitma etteantud otstarvet), (IT terministandardi sõnastik. Funktsionaalüksus) mis annavad teenuseid tööjaamadele, personaalarvutitele või teistele funktsionaalüksustele ning kus teenused võivad olla spetsialiseeritud või ühisteenused. (IT terministandardi sõnastik. Server) Lühidalt öeldes on need nö informatsiooni hoiustajad, millele pääseb arvutivõrgu kaudu ligi. Näiteks veebiserver, mis annab veebi kasutajaile juurdepääsu failidele või muudele rakendustele. (IT terministandardi sõnastik. Veebiserver)

Eesti 2007. aasta aprillis–mais sattusid rünnaku alla: (Schmidt 2013; Aarelaid 2007a–b; Berendson 2007; Tikk, Kaska ja Vihul 2010: 22)[4]

1. riigisektori veebiserverid (Tikk, Kaska ja Vihul 2010: 22; Randel 2007; Riigi Infosüsteemide Amet 28.04.2007, 30.04.2007, 01.05.2007, 09.05.2007)
    a. Vabariigi Valitsus – www.valitsus.ee
    b. Peaminister – www.peaminister.ee (F-Secure 2007)
    c. Vabariigi President – www.president.ee
    d. Riigikogu – www.riigikogu.ee
    e. Riigikontroll – www.riigikontroll.ee
    f. ministeeriumid – Haridus- ja Teadusministeerium (www.hm.ee), Justiitsministeerium (www.just.ee), Kaitseministeerium (www.kmin.ee), Keskkonnaministeerium (www.envir.ee), Kultuuriministeerium

[3] Riigid pakkusid oma abi tuvastamisel ja rünnete peatamisel, mis tulid nende jurisdiktsioonist. Eesti võimaldas seejärel neile täpsemaid IP-aadresseid (lühikokkuvõte NATO-le 08.05.2007).
[4] Mõned veebilehed on tänaseks kas oma nime vahetanud või lõpetanud oma tegevuse. Näiteks Eesti Raadio ühines 1. juunil 2007 Eesti Televisiooniga ning hakkasid uut nimetust kandma – Eesti Rahvusringhääling. (Eesti Rahvusringhääling 2015)

(www.kul.ee), Majandus- ja Kommunikatsiooniministeerium (www.mkm.ee), Põllumajandusministeerium (www.agri.ee), Rahandusministeerium (www.fin.ee), Siseministeerium (www.siseministeerium.ee), Sotsiaalministeerium (www.sm.ee) ja Välisministeerium (www.vm.ee)
   g. Politsei – www.pol.ee ja www.tuvasta.pol.ee
   h. Vabariigi Presidendi Kantselei – www.kadriorg.ee
   i. Eesti Patendiamet – www.epa.ee
   j. Eesti Kaitsevägi – www.mil.ee
   k. Eesti Muusika- ja Teatriakadeemia – www.ema.edu.ee
   l. Eesti Raadio – www.er.ee
2. haridusasutuste veebiserverid
   a. Tartu Ülikool – www.ut.ee
   b. Tallinna Ülikool – www.tpu.ee
   c. Tallinna Ülikooli Eesti Humanitaarinstituut – www.ehi.ee
   d. Estonian Business School – www.ebs.ee
   e. Tallinna Tehnika Ülikool – www.est.ttu.ee
3. erasektori veebiserverid (Randel 2007; Riigi Infosüsteemide Amet 03.05.2007)
   a. Reformierakond – www.reform.ee
   b. pangad
      i. Hansapank – www.hanza.net (Riigi Infosüsteemide Amet 10.05.2007)
      ii. SEB Eesti Ühispank – www.unet.ee
      iii. Krediidipank – www.krediidipank.ee
   c. meediaväljaanded
      i. Postimees – www.postimees.ee (Berendson 2007)
      ii. Delfi – www.delfi.ee
      iii. Eesti Päevaleht – www.epl.ee
      iv. Baltic News Service – www.bns.ee
      v. Topix, Eesti uudised – http://www.topix.net/world/estonia
   d. ettevõtted
      i. Eesti Merelaevandus – www.eml.ee
      ii. Pärnu mööblifirma Woodman – www.woodman.ee
      iii. kinnisvarafirma Rime Kinnisvara – www.rime.ee
      iv. veebimajutuspakkuja Zone – www.zone.ee
      v. Infoatlas – www.infoatlas.ee
      vi. URL linke lühendav teenusepakkuja – www.zzz.ee
      vii. teenusepakkuja – www.ee.ee
4. DNS-serverid (Tikk, Kaska ja Vihul 2010: 22)

Domeeninimesüsteem on andmebaaside kogum, mis seab vastavusse IP-aadressi ja täieliku domeeninime. (IT terministandardi sõnastik. Domeeninimesüsteem) Nii ei pea me Tartu Ülikooli veebilehele minemiseks sisestama oma veebilehitsejasse “193.40.5.73”, vaid www.ut.ee. Kuigi mõlemad viivad meid soovitud lehele, on lihtsam ja mugavam tähti

sisestada. Vähemalt kolm Eesti suurimat internetiteenuse pakkujat rünnati DDoS-ga – Elion Ettevõtted, Elisa Andmesideteenused ja Starman. (Tikk, Kaska ja Vihul 2010: 22)

5. Meiliserverid

Johtuvalt Eesti avaliku info juurdepääsu põhimõtetele hoiti avaliku sektori veebilehedel e-posti aadressitega nimekirju. Seda kasutasid ründajad ära – kopeeriti nimekirjad ja lasti robotitel saata massiliselt rämpspostitusi, mis koormasid süsteemid üle.

Serveri tööd saab takistada mitmel erineval viisil. Kõneall oleva kaasuse puhul kasutati ping-käsu ja teenusetõkestusründeid, millest lähemalt peatükis 2.3.

1.2.2 Rünnakud ruuteritele

Teadaolevalt rünnati ka Elioni ruutereid. (lühikokkuvõte NATO-le 10.05.2007) Ruuter on funktsionaalüksus, mis loob tee läbi ühe või mitme arvutivõrgu. (IT terministandardi sõnastik. Marsruuter) Lihtsamalt, ruuter on nö "vahemees" või "pikendaja", mis ühendab arvutit (ja muid seadmeid) internetivõrgus.

1.3 Ründetüübid ja -vahendid

Ründed olid esialgu primitiivsed – hõlmates endas lihtsat "ping" rünnet ja rämpspostidega[5] elektrooniliste edastussüsteemide harjumuspärase töö häirimist. Sellele lisandusid vigased veebipäringud.[6] (Randel 2007) Protestijad said detailseid juhiseid erinevatelt veebilehtedelt, foorumitelt ja ka e-kirja vahendusel. Hiljem, kui rünnakud olid organiseeritumad, esines näotustamisründeid ning hajusteenusetõkestusründeid (DDoS, ing kl *Distributed Denial of Service*). (Aarelaid 2007a) Jose Nazario jälgis veebiteenuse ATLAS (http://atlas.arbor.net) kokku kogutud DoS-rünnakute infot ning tuvastas kahe nädala jooksul 128 erinevat tüüpi DDoS-rünnakuid Eesti vastu. Keskmiselt kestis üks rünnak *ca* tund aega, ent kõige pikemad rünnakud kestsid koguni 10 tundi. (Nazario 2007) Järgnevalt lühike selgitus

[5] Rämpspost – soovimatu elektronkiri, mis võib edastada pahatahtlikku sisu ja/või petusõnumeid (ISO/IEC 27033).

[6] Autor ei leidnud mujalt täpsemaid selgitusi, milles seisnes vigaste veebipäringute tegemine Eesti puhul, kuid tõenäoliselt oli selle sisuks selliste päringute (nõue võtta infot andmebaasist teatud tingimustel) tegemine, millele server vastata ei osanud (nt pole soovitud sisu olemas). See koormab omakorda süsteemi, kogu energia kulutatakse mujale, selmet need, kes seda tegelikult vajavad, peavad kas ootama või ei saagi veebile, infole ligi.

rünnakutüüpidest ja kahest vahendist – robotvõrgust ja arvutikasutajate ära kasutamisest – mis mängisid olulist rolli rünnakute läbiviimisel.

1.3.1 *Ping*-käsk

Ping-käsuga (ing kl *ping command*) kontrollitakse tavapäraselt seadmete vahelise ühenduse olemasolu. Sisestades käsuviibale (ing kl *Command Prompt*) *ping*-käsu ja sihtkoha seadme IP-aadressi (nt ping 8.8.8.8) saadetakse päring sihtkoha aadressile, mis ühenduse olemasolul saadab vastuseks "suhtlemiseks" kulunud informatsiooni. Kui selliseid päringuid saadetakse massiliselt, kurnab see süsteemi, mis võib viimaks end süsteemi kaitseks välja lülitada. See tähendab, et kodulehe ühenduse kontrollimisel oma arvutiga ei pruugi enam kodulehele juurde pääsedagi. Selle lahenduseks on blokeerida kasutaja või kasutajad, kes seda sorti kontrolle põhjendamatult läbi teostavad.

Nii nagu arenevad rünnakute lahendajad, arenevad ka ründajad. Mõne aja pärast hakati kasutama BAT-faile, mis võimaldas sooritada ping-käsu-rünnet automaatselt käsitsi sisestamise asemel. (Randel 2007) Alates sellest olid viidad olemas, et kasutatakse spetsiaalseid vahendeid ja tegu ei ole enam pelga "kübermässuga". (Randel 2007)

1.3.2 Rämpspost ehk spämm

Rämpspost on elektronkiri, mida saaja ei ole soovinud ning kannab endas enamasti ärilist sõnumit (reklaam). (AKIT. Spämm) Rämpspost on ka üks viise, millega saadetakse pahatahtlikku sisu ja/või petusõnumeid. Näiteks võib see sisaldada ka viiruseid, mille nakatumisel saab kasutada nakatunud meiliaadressit või isegi ka arvutit pahavara levitamisel.

Nagu eelnevalt mainitud, olid tollal avaliku sektoris töötavate inimeste kontaktid, sh e-maili aadressid, avalikult kättesaadavad asutuste veebilehtedel. Sealt oli ründajatel lihtne kopeerida need kokku ja levitada nimekirju, mida rünnata. Võtmeisikute postkastide ummistamisel, ei saa nad oma tavapärast suhtlust pidada ja suurem rünnak võib rivist välja viia ka terve meiliserveri. (Ottise memo 02.05.07)

1.3.3 Näotustamisrünne (ing kl *defacement*)

Üks osa rünnakutest hõlmas endas veebilehe sisu pahatahtlikku muutmist vandalismina. (AKIT. Sodimine) Info ja/või propogandasõnumi edastamine toob endaga kaasa kahju.

Kasutades ära veebilehel olevat turvaauku muudetakse veebilehe sisu. “Nii muudeti Reformierakonna veebilehte, lisades sinna venekeelne tekst Ansipi „vabandusega.” Selliseid ründeid viivad tavaliselt läbi amatöörhäkkerid, kes tahavad koguda prestiiži oma kolleegide seas. Suhteliselt tüüpiline on ka poliitilise sõnumi edastamine (nt Iisraeli vastased sõnumid islamiründajate poolt muudetud veebilehtedel). Antud juhul võib tegu olla spontaanse ründega, sisseostetud teenusega või sihiliku ründega. Viimase vastu räägib asjaolu, et hetkel ei ole teada teiste sarnaste rünnakute läbi viimisest.” (Ottise memo 02.05.2007)

1.3.4 Teenusetõkestusrünne ja hajus teenusetõkestusrünne (DoS ja DDoS)

Teenusetõkestusründe (või ka ummistusrünne) sisuks on saata serverile suures koguses mõttetuid infopakette ja päringuid. Selle tulemusena ummistatakse sideliinid ja/või koormatakse server üle, mis tõttu kasutaja ei saa enam teenustele ligi. (Ottise memo 02.05.2007) Sõna “hajus” tähistab seda, et rünnakul kasutatakse “sihtsüsteemi või -võrgu liikluse mahu tunduvaks suurendamiseks suurt arvu ründavaid süsteeme,” (AKIT. Hajus ummistusrünne ja ummistusrünne) nt robotvõrke.

1.3.5 Robotvõrk

Robotvõrk koosneb nakatunud arvutitest, mida kontrollitakse häkkeri(te) poolt üle interneti. Arvutiomanik ei pruugi ise teadlik ollagi, et tema arvutit kasutatakse ära küberrünnakuteks. (Sophos 2013: 12; Riigi Infosüsteemide Amet 08.05.2007) Robotvõrku kasutati Eesti küberrünnakute ajal peamiselt pankade ja meediaväljaannete ründamisel. (Randel 2007)

2 Eesti 2007. aasta küberründed: sündmuste kirjeldus (poliitiline tasand)

28. aprilli öösel kell 1, 2007. aastal, teavitas Kaitseministeeriumi avalike suhete osakonna töötaja, et valitsuse veebilehele ei saa pressiteateid üles laadida – "Me oleme sattunud küberrünnaku alla". (Kash 2008) Koheselt pärast mõistmist, et toimuvad küberrünnakud Eesti vastu, pandi kokku ekspertide tiim, mida hakkas juhtima CERT Eesti. (Kash 2008) 55 minutit hiljem pandi Vabariigi Valitsuse uudiste rubriiki teade pealkirjaga "Elektroonilistes kanalites võib leida väärinfot". Uudises kirjutati, et Eesti valitsuse veebilehed on sattunud rünnakute alla ning seetõttu võib valitsuse briifinguruum (www.valitsus.ee/brf) olla ajutiselt piiratud ligipääsuga väljaspool Eestit ning et Valitsuse kommunikatsioonibüroo palub olla tähelepanelik ja vajadusel kontrollida infot. (Vabariigi Valitsuse uudised 28.04.2007)

Riigikaitselise ohu korral võib Riigikogu Vabariigi Presidendi või Vabariigi Valitsuse ettepanekul välja kuulutada erakorralise seisukorra vastavalt PS §-le 129. Erakorralise seisukorra seaduse § 3 annab loetelu Eesti põhiseaduslikku korda ähvardavatest ohtudest, mis võivad tuleneda:

1) Eesti põhiseadusliku korra vägivaldse kukutamise katsest;
2) terroristlikust tegevusest;
3) vägivallaga seotud kollektiivsest surveaktsioonist;
4) ulatuslikust vägivallaga seotud isikugruppide vahelisest konfliktist;
5) Eesti Vabariigi mõne paikkonna vägivaldsest isoleerimisest.[7]

Tolleaegne Riigikogu esimees Ene Ergma on kirjutanud, et pronksiöö rahutuste ajal toetas Riigikogu viis erakonda täielikult ja üks mööndustega valitsuse tegevust kriisi ajal, "sellise raske olukorra reguleerimine ongi valitsuse pärusmaa. Riigikogu liikmete tegevus oli põhiliselt suunatud situatsiooni selgitamisele kolleegidele väljaspool Eestit – nii intervjuude kui ka otsekontaktide kaudu". (Ergma 2007) Seega tekib siin kaks rünnetele reageerijat – Vabariigi Valitsus ja Riigikogu liikmed.

[7] Täiendavalt lisati 2009. aastal ka kuues punkt: vägivallaga seotud pikaajalistest massilistest korratustest (Erakorralise seisukorra seadus).

Riigikogu ja Vabariigi Valitsuse liikmete tegevuse – situatsiooni selgitamisele kolleegidele – kaardistamiseks küberrünnete kontekstis kasutas autor populaarseimat otsingumootorit Google (Kumar 2015; Mobile Info Guru 2015; Krawczyk 2014) ning Booleani loogikaoperaatoreid: AND, OR ja NOT; [8] päringu fraasina "[Riigikogu liikme eesnimi] AND [Riigikogu liikme perekonnanimi] AND (küber OR cyber)." Otsingu teostamisel filtreeritakse välja nimetet Riigkogu liikmega seonduvad eesti- ja ingliskeelsed tulemused koos sõnaga "küber" või "*cyber*". Otsingumootor võimaldab kohandada kuupäevavahemikku, milleks autor määras küberrünnakute toimumisperioodi – 27. aprill 2007 kuni 18. mai 2007.

Poliitikute selgitusi otsiti nii Eesti sise- kui ka välisuudiste, intervjuude ja pressiteadete seast. Samuti vaatas autor veel lisaks Riigikogu, Vabariigi Valitsuse, Kaitseministeeriumi, Välisministeeriumi, Majandus- ja Kommunikatsiooniministeeriumi veebilehti, täpsemalt uudiseid ja pressiteateid küberrünnete toimumise vahemikus.

Mõned veebilehed ei sisaldanud enam nii kaugele ulatuvaid andmeid, nt Riigikogu veebilehte (www.riigikogu.ee) uuendati hiljuti (Riigikogu pressiteated 23.04.2015) ja ainsana on võimalik pääseda ligi vahemikus aprill–mai 2007. aasta stenogrammidele, Majandus- ja kommunikatsiooniministeeriumi veebilehel (www.mkm.ee) on võimalik teavet (pressiteateid, uudiseid) saada alates 2009. aastast, Kaitseministeeriumi veebilehe (www.kmin.ee) otsingusüsteem on katki (veebileht ei suutnud laadida infot).

Võttes täiendavalt arvesse, et välissuhtlusega tegelevad "Riigikogu esimees, komisjonid ja fraktsioonid, samuti Riigikogu üksikliikmed näiteks parlamendirühmade kaudu" (Riigikogu. Välissuhtlus 2015) ning asjaolu, et tegu oli valdavalt siiski ka julgeolekualase küsimusega, kitsendas autor uuritavaid üksusi Valitsuse, Riigikogu juhatuse ja valdkonnaga seotud komisjonide tasemele, täpsemalt Riigikaitsekomisjoni, Õiguskomisjoni, Väliskomisjoni, Euroopa Liidu asjade komisjonile. (Riigikogu Kantselei 2007)

Arvestades, et alati ei pruukinud Riigikogu liige oma nime all selgitustööd teha, teostas töö autor otsingu läbi ka märksõnadega "Riigikaitsekomisjon", "Väliskomisjon", "Euroopa

[8] Vaata rohkem Booleani loogikaoperaatoridest: https://sisu.ut.ee/otsing/p%C3%A4ringu-koostamine.

Liidu asjade komisjon", "Õiguskomisjon" ja "Riigikogu", kasutades seejuures otsingu sooritamisel eelnevalt kirjeldet põhimõtet, mis Riigikogu liikmete tegevuse leidmiselgi.

2.1.1 Riigikogu liikmete tegevus küberrünnakute lahendamisel

10. ja 11. mail 2007. aastal arutati Euroopa Liidu asjade komisjoni ja Väliskomisjoni istungitel küberrünnakute üle. Näiteks arutati Väliskomisjonis, kas Eesti võiks algatada küberründe vastu suunatud konventsiooni väljatöötamise. Mõlema nimetet komisjoni liige Marko Mihkelson pidas vajalikuks küberrünnakuid põhjalikumalt uurida ja kaaluda, näiteks "millised samme on võimalik astuda rahvusvahelise küberründe vastase konventsiooni loomise suunas". (Masing 2007) Samuti leidis ta, et teema vajab tõstatamast nii vastavates siseriiklike kui ka rahvusvahelistes instantsides. (Masing 2007)

Otsingud andsid veel ainult ühe relevantse tulemuse. Küberrünnete eelviimasel päeval, so 17. mail 2007. aastal, väitis tolleaegne Riigikogu liige ja Väliskomisjoni kuuluv Silver Meikar, et põhinedes vastavalt erinevatele vestlustele julgeolekuvaldkonna töötajatega on tugevaid indikatsioone Venemaa osaluse kohta küberrünnakutes. (Koman 2007)

Ülejäänud tulemustesse sattus artikleid, kus liige oli avaldanud arvamust proksiöö rahutuste ning monumendi ja sõjahaudade teisaldamise kohta, aga kordagi isegi mitte ei viidatud küberrünnakutele.

Pärast rünnakuid leidus siiski sõnavõtte rohkem. (Näiteks Nutt 2013; Šmutov 2007; Meikar 2007) Enam kõlapinda (Ergma 2007; Davis 2007) sai tolleaegne Riigikogu esimees, Ene Ergma, kui võrdles juhtunut tuumapommiplahvatusega:

"Me peame teadvustama küberrünnakuid reaalse, aktuaalse ja ülisuure ohuna demokraatlikele riikidele ja rahvastele. Paljud meist ei ole seda uut ohtu endale veel täie teravusega teadvustanud. Tõepoolest, küberrünnet ei iseloomusta tavarelvade plahvatusmüra, küberründe ajal ei pimesta meid valgussähvatus, ei raputa maapinna (seismiline) ega õhu võnkumine, ei uputa hiidlaine, me ei tunne lõhna ega maitset – kõigest hoolimata on hävitav küberplahvatus toimunud. Kuid tänapäeva elektroonika suudab küberrünnet, küberplahvatust fikseerida ja mõõta, see on väga sarnane tuumapommi plahvatusega." (Ergma 2007)

Küberrünnete toimumisperioodil toimus 11 Riigikogu istungit, millest ainult ühes puudutati küberründeid, so 2. mail 2007. (Riigikogu stenogrammid) Infotunnis viitas Majandus- ja Julgeolekuasutuste järelevalve erikomisjoni kuuluv Marek Strandberg (Riigikogu kantselei 2011: 75) Välisministri eelmisel päeval esitet avaldusele (Valitsuse uudised 01.05.2007) ning uudisele Eestisse loodavast küberkaitsekeskusest, mida tutvustati avalikult "kui selliste rünnete analüüsi ja kaitse keskust" ning küsis Kaitseministrilt "kas kõnealuste rünnete tuvastamisel, analüüsimisel ja nende vastu toimimisel on osalenud ka selle sama küberkaitsekeskuse meeskond?" (Riigikogu stenogrammid 02.05.2007)

Samal päeval toimunud täiendaval istungil esines peaminister Riigikogule poliitilise avaldusega, kus andis ülevaate Pronksiööga seotud olukorrast, sh viidates küberrünnetele ainult ründajakontekstist lähtuvalt – "See koos jätkuvate küberrünnakutega Venemaa riigiaparaadi serveritest, koos Eesti lipu rebimisega meie suursaatkonnalt, koos duuma saadikute üleskutsega vahetada Eestis valitsust näitab, et meie suveräänne riik on tugeva rünnaku all." (Riigikogu stenogrammid 02.05.2007) Kõnesoove Peaministrile ei esitet. (Riigikogu stenogrammid 02.05.2007)

2.1.2 Valitsusliikmete tegevus küberrünnakute lahendamisel

Kõige esimesena andis poliitilisel tasandil küberrünnete kohta informatsiooni Vabariigi Valitsus. Ministritest esimesena tegi avalduse välisminister Urmas Paet, (Valitsuse uudised 01.05.2007) seejärel esines peaminister Riigikogu ees poliitilise avaldusega, puudutades vaid korra küberründeid. (Riigikogu stenogrammid 02.05.2007) Peaminister, President ja Riigikogu esimees tegid ühisavalduse 8. mail 2007, (Valitsuse uudised 8. mai 2007) kuid küberrünnakuid ei puudutatud kordagi. Järgnevalt kirjeldabki autor Peaministri, Välisministri, Kaitseministri, Justiitsministri ja Presidendi sõnavõtte küberrünnakute kontekstis.

Peaminister

Peaministri sõnavõtud olid valdavas osas üldiselt Pronksiöö konflikti kohta. Küberrünnakute kontekstis jagati Välisministri seisukohta. Näiteks osas, kust küberrünnakud pärinesid ning kes oli süüdlane (vt lähemalt järgmist alapeatükki 3.1.2.2). Ta rõhutas: "kuid ründed saatkonna ja suursaadiku vastu, küberründed ja meediamanipulatsioon ei jää kindlasti tähelepanuta, need ei ole jäänud tähelepanuta. Ja

selles võib kindel olla, et nii Euroopa Liit kui ka NATO hakkavad küberturvalisusele tulevikus märksa suuremat tähelepanu pöörama kui veel paar nädalat tagasi." (Poom ja Jõgis-Laats 2007)

Välisminister

Välisministeeriumi suhtumine Venemaa tegevusse andis tooni juba enne küberrünnakuid seoses rahutustega tänavatel, Moskvas asuva Eesti saatkonnaga jt Venemaa poliitiliste sammudega Eesti suunal (nt majanduslik blokaad). (Masing 2007; Poom 2007; Välisministeeriumi uudised) Seega tõenäoliselt seetõttu nägi Välisministeerium koheselt seost Venemaaga, kui esimesed küberrünnakud tabasid Välisministeeriumi kodulehte: "Välisministeerium vabandab, et meie koduleht polnud vahepeal väljaspool Eestit kättesaadav. Selle põhjustasid ida suunalt tulnud pahatahtlikud ründed meie kodulehe vastu organiseeritud ja kunstlikult kõrge päringute arvu näol." (Välisministeeriumi uudised 29.04.2007) Venemaas süüdlase nägemise tendents kestis läbivalt kogu küberrünnakute vältel ja edasigi.

Välisministri esimene avaldus seoses küberrünnakutega oli 1. mail 2007. Avalduses süüdistati Venemaad küberrünnakute korraldamisel:

"Euroopa Liit on rünnaku all, sest Venemaa ründab Eestit. ... aga Venemaa koordineeritud tegevus Eesti vastu on kogu Euroopa Liidu asi. ... On tuvastatud IP aadresside kaudu, et küberterroristide rünnakud Eesti valitsusasutuste ja Presidendi kantselei internetisaitidele on tulnud konkreetsetest arvutitest ja isikutelt Vene valitsusorganites, kaasa arvatud Vene Föderatsiooni Presidendi administratsioonis." (Valitsuse uudised 01.05.2007)

Sündmuste taustal jättis välisminister ning sh ka teised Valitsuse liikmed, ära kohtumise Venemaa duuma saadikutega, kelle visiit Eestisse toimus suures osas Saksamaa kantsleri Angela Merkeli ja Vene presidendi Vladimir Putini telefonikõne tulemusena. (Välisministeeriumi uudised 01.05.2007) Paet leidis, et delegatsiooni vastuvõtuga näitas Eesti omapoolset tahet pidada Venemaaga avatud ja läbipaistvat dialoogi, ent saadikute käitumine Eestis ei olnud aktsepteeritav ja seega ei näe ta põhjust nendega kohtumiseks. "Duuma delegatsiooni liikmete käitumine on olnud sügavalt vastuvõetamata nagu ka nende senised väljaütlesmised ... . Ma ei kohtu delegatsiooniga, mille liikmed levitavad Eestis

olles jõhkraid valesid siin toimuva kohta ja kelle eesmärgiks pole mitte olukorra adekvaatne kujutamine, vaid valimispropaganda tegemine." (Välisministeeriumi uudised 01.05.2007)

Välisministril on oluline roll riigi välispoliitikas kanda. Ta kujundab Eesti riigi seisukohti välispoliitilisel maastikul. Teise riigi aluseta süüdistamine on selgelt poliitiline meede. See järeldus avaldub ka samas välisministri avalduses, kus Urmas Paet loodab, et meetmed, mida Euroopa Liit Eesti ettepanekul läbi viib, peavad "mõjuma Venemaale nii, et Venemaa lõpetab rünnakud ja siseasjadesse sekkumise ning asub täitma Viini diplomaatiliste suhete konventsiooni." (Valitsuse uudised 01.05.2007) Näiteks ühena meetmetest pakub Paet välja "erinevate kõneluste peatamist või nende mittealustamist Euroopa Liidu ja Venemaa vahel. Tõsiselt tuleb kaaluda Euroopa Liidu–Venemaa tippkohtumise edasilükkamist." (Valitsuse uudised 01.05.2007) Viimase puhul pidas välisminister silmas Samaras 18. mail 2007 toimuvat tippkohtumist Euroopa Liidu ja Venemaa vahel. Siiski loobus Eesti tegemast ettepaneku lükata tippkohtumine edasi ning välisminister lootis hoopis veenda Euroopa kolleege võtma kohtumise päevakorda Venemaalt Eesti vastu suunatud rünnakud. (Poom 2007; BBC News 17.05.2007) Viimasega nõustusid ka Riigikogu komisjonid – Euroopa Liidu asjade komisjon ja Väliskomisjon – Eesti peab võimalusena tippkohtumist ära kasutama. (Masing 2007)

Rahvusvaheliste kohtumiste ning relevantsete projektide ära jätmine on poliitilisel areenil üks meetmeteist survestada teist osapoolt tundlikku teema osas. 2009. aastal loodi USA Presidendi Barack Obama ja Venemaa tolleaegse Presidendi Dmitry Medvedevi poolt USA ja Venemaa presidentide kahepoolsete suhete komisjon (ing kl *US–Russian Bilateral Presidential Commission*), mille põhiliseks eesmärgiks oli koostöö tegemine kahe suurriigi vahel. (2009 U.S.–Russian Bilateral Presidential Commission) Üks selliseid ühisprojekte oli info- ja kommunikatsiooni tehnoloogia julgeoleku valdkonnas, (Valge Maja pressiteated 17.06.2013) mis peatus kaheks aastaks Ukraina sündmuste taustal, Venemaa Krimmi anakteerimises; projektide ja kohtumistele mõeldud rahastus suunati hoopis Ukraina abistamisele. (U.S.–Russia Bilateral Presidential; RFL/RL 2014; Schreck 2015)

Ühtlasi kutsus välisminister Venemaad ühinema ka "Euroopa Nõukogu küberkuritegevuse konventsiooniga ja tegema koostööd küberkuritegevuse vastu võitlemisel." Rõhudes, et

“21. sajandil on kontsentreeritud küberrünnakud ühiseks ohuks kõikidele riikidele”. (Anvelt 2007)

Kuigi välispartnerid avaldasid mitmetes kõnedes toetust Eestile, (Välisministeeriumi uudised 27.04.2007, 30.04.2007–02.05.2007) eelkõige Eesti suursaatkonna olukorra üle Moskvas, siis küberrünnakute kohapealt jäädi kidakeelseks. Näiteks tolleaegne Euroopa Liidu eesistuja Saksamaa välisministri Frank-Walter Steinmeier lubas “kiiret assisteermist Euroopa Liidult olukorra normaliseerumiseks Eesti saatkonna osas Moskvas,” (DW.DE 2007) aga küberrünnakutele ei viidatud sõnagi. Kui Päevaleht uuris Saksamaa toetuse kohta Samaras päevakorda lisada Eesti-Vene suhted, ei andnud viimane kindlaid lubadusi: “EL-i ja Venemaa tippkohtumise organiseerijatena on meil veel see eelis, et saame arutada kõiki asju, mis pooltele parasjagu huvi pakuvad.” (Poom 2007) Saksamaa Välisministeeriumi pressiesindaja kommenteeris Euroopa Liidu üld- ja välisasjade nõukogu arutelu järgnevalt: “Nõukogule esitatakse informatsioon ja sellele järgneb diskussioon. Kõik, mis puutub otsustesse, tuleb langetada ühehäälselt.” (Poom 2007) Rootsi välisminister jäi veelgi napisõnalisemaks, Päevalehe uurimise peale saadeti lühike sõnum: “Me ei kommenteeri.”(Poom 2007) Ameerika Ühendriikide riigisekretär Condoleezza Rice piirdus tõdemusega President Toomas Hendrik Ilvese küberrünnakutele viitamise peale, et “sedalaadi surve sõltumatule riigile ei ole aktsepteeritav”. (Vabariigi Presidendi Kantselei 03.05.2007)

Küberrünnakute algusperioodil korrutab välisminister veendunult, et kõigi väidete tõestamiseks on piisavalt tõestusmaterjale, (Paet 2007) mis tundub aga väärarvamus olevat, sest hiljem neid tõendusmaterjale ei tundu olevat. Kui alguses räägiti üldistatult Venemaa poolsest ründest, siis hiljem räägiti ühest IP-aadressist, mis asus Venemaa valitsuse hoones. Viiteid, et rünnakud tulevad mujalt oli marginaalselt. Neutraalse hoiaku selles osas võttis Hillar Aarelaid, nt Eesti Raadio ajakirjaniku küsimuse peale “kust need rünnakud pärinevad?” vastas Aarelaid “ikka tervest maailmast, arvutitel piire ju ei ole ja viirustega nakatunud arvuteid on hästi palju, neid kasutada meie vastu on imelihtne”. (Hanno Tombergi intervjuu Hillar Aarelaiuga 02.05.2007) Kui ajakirjanik Välisministri seisukoha kohta kommentaare küsis, siis tundus Aarelaid ebalev olevat vastates, et ta isiklikult ei ole neid väiteid kontrollinud. (Hanno Tombergi intervjuu Hillar Aarelaiuga 02.05.2007) Hiljem

leidsid analüütikud viiteid selle kohta, et küberrünnakuid juhiti Venemaa territooriumilt, on olemas, kuid samuti pärinesid pahatahtlikud ründed ka USA-st, Kanadast, Brasiiliast, Vietnamist ja mujalt. (Kirk 2007)

Faktidega sattuti eksiteele veelgi. Näiteks väitis Paet, et rünnati ühtlasi ka hädaabikõnede süsteeme. (Bright 2007) Kuigi Rain Ottis kirjutas 7. mai 2007. aasta memos, et on teateid rünnetest hädaabitelefoni vastu, (Ottise memo 07.05.2007) siis need kahtlused lükati ümber 10. mail 2007. (Ottise memo 10.05.2007) Paeti avalduseks oli hädaabitelefonide rünne ümber lükatud, kuid miskipärast info välisministri ei olnud jõudnud. See võib viidata kas kehvale (aeglasele) asutuste vahelisele kommunikatsioonile, ettejuhtuvale apsule või tahtlikkule teole.

Välisminister võttis juba varases staadiumis Venemaad süüdistava seisukoha ja jätkas sellega oma edaspidistes ülesastumistes.[9] Taolist käitumist esineb maailmaareenil veelgi: üks tüüpilisemaid näiteid võib tuua Korea poolsaarelt, kus ühe rünnaku alla sattumisel süüdistatakse pikalt ründeid analüüsimata teist poolt, vastavalt siis kas Lõuna-Korea Põhja-Koread või *vice versa*. (Näiteks, Park 2013; Ashford 2013; SecurityWeek 2015; Esentire 2015)

Süüdistav hoiak on üldse kõigi uuritavate poliitikute (lisaks välisministrile ka kaitseminister ja ka peaminister) seisukohavõttudes. Näiteks justiitsiminister Rein Lang ütles intervjuus Aktuaalsele kaamerale, et "küberrünnakud Eesti riigiasutuste internetisaitide vastu tulevad "riiklikelt IP-aadressidelt Moskvas"." (Eesti Ekspress 2007) Sellegipoolest ei ole ta oma sõnavõttudes nii radikaalne olnud kui Paet, nt Eesti Raadio intervjuus viitas ta võimalusele, et Venemaa administratsiooni infosüsteemid on nii kehva turvalisuse tasemega, et neid süsteeme on kerge ära kasutada ja ka kasutatudki. Samas täiendab, et mõlemad variandid on kehvad, nii see, kui Venemaa süsteemid on haavatavad ning ära kasutatud teise riigi küberrünnakutes kui ka see, kui see oli Venemaa teadlik ja sihilik küberrünne. (Hanno Tombergi interjuu Rein Langiga 09.05.2007)

[9] Näiteks kirjutab Paet terve artikli ulatuses, kuidas Venemaa ei respekteeri Eestit, kuidas ta töötab Eesti vastu ning siis lõpus viimases lauses alles pakub lootva õlekõrrena välja dialoogi. Paeti sõnavõtud on olnud üsnagi üheülablised, Venemaad süüdistatav, aga mitte lahendusi pakkuv. Nendest sõnavõttudest saab lugeda välja ainult vaenu ja mitte viisi, mille tulemusena küberrünnakud võiksid lõppeda, vaid pigem jätkuda. (Paet 2007)

Kaitseminister Aaviksoo seisukoht küberrünnakute taga seisjast olid küllaltki vastakad. Näiteks vastas ta esiti Raadio Vaba Euroopa intervjueerija küsimuse peale konfliktiosapooltest, et sellele on keeruline vastata, ent kui ajakirjanik küsis järgmisena, kas Venemaa võib otseselt või kaudselt üks osapooltest olla, siis selles oli jällegi Aaviksoo veendunud – "*Yes, I have no doubt of that*" ("Jah, mul ei ole kahtlusi selles"). (RFL/RL 2007) Samas tunnistas Aaviksoo, et vettpidavad tõendid Venemaa valitsuse rollist küberrünnakutes puudusid, indikatsioon sellele võimalikkusele oli aga olemas. (Blomfield 2007) Ning intervjuus Eesti Ekspressile ütles ta, et paraku ei teata, kes see on. Samuti ei olnud küberrünnakute lõpuks antud ametlikult Vene poolele logisid, et selgust küsida. "Võimalik, et seda tehakse tulevikus, kui infot toimunu kohta on kogutud praegusest rohkem." (Eesti Ekspress 2007) Siinkohal tuleb märkida, et logid sai Venemaa siiski Eesti õigusabitaotluse raames. (Õigusabitaotlus; Prokuratuuri pressiteated 02.05.2007)

Võrreldes Välisministriga, ei viidanud kaitseminister ka nii järjepidevalt rünnakute allikaks ühte riiki, vaid selgitas, et rünnakutes osales umbkaudu miljon arvutit ülemaailmselt ning pigem esialgsed ründed tulid Venemaa administratsiooniasutustest. (Blomfield 2007)

Peaminister on Välisministriga ühel nõul – rünnakud tulenesid Venemaa riigiaparaadi serveritest ning arvestades veel Eesti lipu rebimisega Eesti suursaatkonnalt ja Venemaa duuma saadikute üleskutsega vahetada Eestis valitsust näitab, et Eesti suveräänne riik on tugeva rünnaku all. "Kõik need sündmused kinnitavad, et meil ei ole tegu riigi sisemiste probleemidega. Meil on tegu Venemaa koordineeritud ja räige sekkumisega Eesti riigi asjadesse. Me oleme pöördunud Euroopa Liidu poole ja me palume neil reageerida kohaselt, sest ühe liikmesriigi ründamine on kogu Euroopa Liidu ründamine." (Riigikogu stenogramm 2007b)

Ka President hoidis Ansipi ja Paetiga sama hoiakut. 2. mai avalduses Eestile lõpetas Ilves pöördumisega Venemaa poole: "Lõpetuseks pöördun Eesti naabri Venemaa poole ning ütlen selgelt – püüdke jääda tsiviliseerituks! Euroopas pole kombeks nõuda suveräänse riigi demokraatlikult valitud valitsuse tagasiastumist. Euroopas pole kombeks korraldada riigiasutuste arvutitest küberrünnakuid teise maa riigiasutuste vastu. Euroopas nagu mujal tsiviliseeritud maailmas ei arvata, et Viini konventsiooni võib rikkuda kui tegemist on

piisavalt väikese riigi saatkonnaga." (Vabariigi Presidendi Kantselei pressiteated 02.05.2007)

Ministritest joonduvad nii teised poliitikud kui ka kodanikud, nende sõnades ei peaks ega tohikski iseenesest kahelda. Nii näiteks ei küsitagi, mille alusel või kuidas on kindlaks ründajate info tehtud, vaid seda lihtsalt nenditakse, kui kaheldamatut informatsiooni. Näiteks alustab toonane Riigikogu liige Marek Strandberg oma arupärimisega: "Meeldivat päeva! Küsimus on kaitseminister Jaak Aaviksoole. Nagu me teame Urmas Paeti eilsest avaldusest, on rünnakud Eesti Vabariigi Interneti-serverite ja võrgukülgede vastu lähtunud valdavalt Venemaa riigistruktuuride arvutivõrkudest." (Riigikogu stenogramm 2007a)

Kaitseminister

Küberrünnakute perioodil avaldet sõnavõtte võib iseloomustada ka terminite järjekindlusetu kasutamisega. Kord sattus Eesti küberrünnakute alla, siis toimus juba kübersõda, ühtäkki sai sõjast jälle terrorism. (Näiteks, Sydney Morning Herald 2007; Blomfield 2007) Kõige äärmuslikumana võiks nimetada kaitseminister Aaviksoo võrdlust Ameerika Ühendriikidele tehtud rünnakutega saatuslikul 11. septembril 2001. (The Economist 2007) Rünnakute lõpus tunnistas kaitseminister: "Meil puudub nii kontseptuaalne, õiguslik kui ka tehnoloogiline käsitlus." (Eesti Ekspress 2007)

Ühes siiski oldi kindel – tegu on laiaulatuslike, valitud sihtmärkidega ja läbimõeldud rünnakutega, mida ei saa vaadata kui spontaanset vastukaja avalikkuse rahulolematusega Valitsuse tööle. Ning rünnakute lõpuks leidis kaitseminister väljapääsu terminoloogia kasutuses: rääkida tuleb organiseeritud rünnetest kaasaegse taristu vastu. (Koman 2007)

Toibudes esimestest ootamatutest küberrünnakutest hakati konkreetsemalt rääkima toimunu tähendusest õiguslikus plaanis. Mõisteti, et Eesti siseriiklikus ja ka rahvusvahelises õigussüsteemis on puudusi. Näiteks arutleti, kas "küberrünnakuid võib käsitleda kui reaalset rünnakut Eesti riigi vastu, mille puhul võiks rääkida Põhja-Atlandi lepingu artikkel 5st,[10] mis käsitleb rünnakut ühe NATO liikmesriigi vastu kui rünnakut kõigi vastu"

[10] Põhja-Atlandi lepingu ehk Washingtoni lepingu artikkel 5: Lepinguosalised lepivad kokku, et relvastatud rünnakut neist ühe või mitme vastu Euroopas või Põhja-Ameerikas käsitatakse rünnakuna nende kõigi vastu ning kui sedalaadi relvastatud rünnak aset leiab, abistab igaüks neist, rakendades Ühinenud Rahvaste

(Anvelt, Ojakivi 2007; Valitsuse pressikonverentsi stenogramm 10.05.2007)[11] või kuidas üldse defineerida küberrünnakut, millised on NATO ja Euroopa Liidu liikmesriikide õigused ja kohustused, kui sellised sündmused aset leiavad. (The Sydney Morning Herald 2007; Riigikogu stenogramm 02.05.2007)

Kaitseminister Aaviksoo maalis olukorra tõsidusest kõigile arusaadava pildi: "kui liikmesriigi kommunikatsioonikeskus hävitatakse raketiga, siis on selge, et tegu on sõjalise rünnakuga. Kuid kuidas sa nimetad sama teguviisi, mis on sooritatud küberründega?"[12]

Kuigi mõisteti, et olemasolev regulatsioon on puudulik, siis millegi pärast avalikkusega suheldes (meedia intervjuudes, kõnedes) ei olnud rõhuasetus olemasoleva reeglistiku seast võimalike normide leidmisel. Ligipääsetava materjali hulgast leidis autor ainult ühe viite Valitsuse pressikonverentsilt, kus Andrus Ansip täiendas Kaitseministri vastust, ent siiski laskumata detailidesse: "Eestis on teatud tegevused, mida, klassifitseerimisena küberrünnakute alla, on juba seaduse järgi karistatavad. Me ju teame ka seda, et üks inimene on viibinud uurimise all ja kindlasti ei või rahulikult hingata ka need, kes on sooritanud taolisi kuritegusid väljaspool Eestit. On võimalik välja anda üle-euroopaliiduline vahistamise määrus ja kui mõni inimene, kes elab väljaspool Euroopa Liidu liikmesriike ja soovib kunagi külastada mõnd 27st Euroopa Liidu liikmesriigist, siis võib paraku juhtuda nii, et külastades mõnd teist riiki, ta kaotab oma vabaduse ja selle sama meie palve alusel toimetatakse ta Eestisse." (Valitsuse pressikonverentsi stenogramm 10.05.2007)

Riiklikul tasandil võeti vahetult pärast sündmusi mitmeid parendusi vastu, (vt Tikk, Kaska ja Vihul 2010) sh vaadati üle Eesti küberjulgeoleku strateegia. (Kaitseministeerium 2008)

Organisatsiooni põhikirja artiklis 51 sätestatud õigust individuaalsele või kollektiivsele enesekaitsele, viivitamatult sel viisil rünnatud lepingupoolt või lepingupooli, kasutades üksi ja koos teiste lepingupooltega vajalikke abinõusid, mida ta peab vajalikuks, sealhulgas relvajõudusid, eesmärgiga taastada ning säilitada Põhja-Atlandi piirkonna julgeolek.
Igast sellisest relvastatud rünnakust ning selle vastu kasutatud abinõust teatatakse viivitamatult Julgeolekunõukogule. Nimetatud abinõude kasutamine lõpetatakse, kui Julgeolekunõukogu on rakendanud vajalikud abinõud, et taastada ja säilitada rahvusvaheline rahu ja julgeolek. (Põhja-Atlandi leping. RT II 2004, 5, 14.)

[11] Näiteks, Aaviksoo vastus arupärimisele Vabariigi Valitsuse pressikonverentsil: "Ma arvan, et täna ei ole ühtegi kaitseministrit, kes sellele ühemõtteliselt vastata võiks, ka mina jätan selle vastamata. Aga ma arvan, et see küsimus peab lähiajal vastuse saama ja tõenäoliselt tõstatub see küsimus ka esmaspäeval Euroopa Liidu kaitseministrite kokkusaamisel Brüsselis." (Valitsuse pressikonverentsi stenogramm 10.05.2007)

[12] Sama küsis ka Eesti suursaadik NATO juures Harri Tiido. (Kalamees ja Kuimet 2007)

Eesti sündmused ajendasid oma küberjulgeoleku strateegiat välja töötama teistegi riikide poolt. (Wingfield ja Tikk 2010: 16)

Võib öelda, et (rahvusvahelise) poliitika tasandil hakati innustatumalt arutama küberründe ja kübersõja tähenduse üle. (Kirk 2007) Paljud tol hetkel tähelepanu külvavad probleemid on senini vastuseta, nt riigivastutuse küsimused – milliste tingimuste täites saab riiki vastutusele võtta? Eriti problemaatiline on tõendamine.

Justiitsminister

Eesti õigusteadlane Raul Narits kirjutab: "Inimühiskonna normaalse eksisteerimise jaoks on tähtis, et selles ühiskonnas arvestatakse ja austatakse kehtivaid sotsiaalseid norme. Kes eksib moraali või tava vastu, peab paratamatult arvestama ühiskonna negatiivse reaktsiooniga, mis eksija suhtes võib olla vähem või rohkem kahjulik." (Narits 2004: 23) Tehnoloogia kiire areng on toonud muudatusi ka inimühiskonda, mida viimane peab nö "õigeks käitumiseks" ja mida mitte. Eesti küberründed näitasid, et kuigi riik on tehnoloogiliselt arenenud, ei ole õiguse rakendajad alati suutnud sammu pidada. Nii seisiski Justiitsminister probleemi ees – kuidas leida juhtunule kohta õiguses? Ka rahvusvaheline õiguspraktika ei anna otsest vastust, kuidas juhtunut kuriteona käsitleda: "Kui me võtame seaduse analoogia järgi, siis teise riigi sadamate või õhuruumi blokeerimine on ju selge aggressioon, aga teise riigi küberruumi blokeerimine või selle kahjustamine ei ole ühegi rahvusvahelise kokkuleppega täna aggressiooniks tunnistatud ja see muudab selle teema väga sensitiivseks ja see on põhjustanud ka laiaulatusliku arutelu nii NATO sees kui ka NATO liikmesriikides sees. See, et NATO liikmesriikide esindajad on meile selles küsimuses appi tulnud, saatnud siia oma spetsialiste on muidugi väga tervitatav." (Hanno Tombergi intervjuu Rein Langiga 09.05.2007; The Economist 10.05.2007)

Selgusele, mis on küberrünnakud, kübersõda ja küberterrorism ning kuidas neid kohaldada vastavalt seaduse järgi, ei ole jõutud ka tänapäeval. Diskussioonid erinevate valdkondade ekspertide seas kestavad senini. Ühe näitena võib tuua ÜRO valitsusekspertide gruppi (ing kl *Group of Governmental Experts of United Nations*), mille üks liikmeid ka Eesti on, mille mandaadiks on arutleda olemasolevate ja võimalikke ohtude üle küberruumis ning võimalikke koostöövorme nende probleemide lahendamiseks. (United Nations Office for Disarmament)

2.1.3 Presidendi tegevus küberrünnakute lahendamisel

Pronksiööga seoses tegi Ilves kolm avaldust, (Presidendi avaldused 27.04.2007, 02.05.2007, 08.05.2007) millest ainult üks oli seotud küberrünnakutega ja sedagi ainult korra mainituna, Venemaa tegude loetlemisel Eesti vastu. Ülejäänud kaks kutsusid inimesi mõistlikkusele ja rahu säilitamisele.

Suheldes NATO peasekretäri Jaap de Hoop Schefferiga andis viimane märku oma murest Eestit tabanud küberrünnakute osas. Seepeale informeeris President, et "osa neist rünnakuist lähtuvad Venemaa valitsusasutuste arvutitest." (Vabariigi Presidendi Kantselei 02.05.2007)

Nii nagu Peaministrile oli iseloomulik kommenteerida sündmusi kui tervikut, st mitte küberrünnakuid eraldiseisvana nii toimis ka President. Erimeelsuste lahendajana nägi Ilves diplomaatide ja poliitikute poolt tehtut mitte tänavarahutuste ja arvutirünnakute vahendusel. (Yasmann 2007)

3 Eesti küberrünnakute lahendamine 2007. aastal

3.1 Küberjulgeoleku otsustusmudel

21. sajandi üheks kübertrendiks võib pidada riikide küberjulgeolekupoliitika ülevaadet ja korrastamist. Eesti on selle elavaks näiteks ja mõneti trendi hoogustamise põhjustajaks: küberrünnakud mais ja aprillis 2007. aastal raputasid riike piisavalt, et mõista – riik ja ühiskond sõltuvad internetist palju ning lihtsate ja soodsate vahenditega on võimalik ohustada tugevalt interneti püsimist ja ka meie harjumuspärast elu. Riigi püsima jäämise seisukohtalt on tarvis julgeolekut tagavaid ja rajavaid akte kooskõlastada uue reaalsusega.

Wingfield ja Tikk-Ringas on pakkunud välja kontseptsiooni, mis arvestaks olulisi tahke küberjulgeoleku kindlustamisel, mis adresseeriks kõiki relevantseid komplekssusi, kuid samas pakuks piisavat selgust neile, kes vastutavad riikide ja võrgu kaitsmise eest, võttes vastu legitiimseid, koordineeritud ja proaktiivseid otsuseid. Kontseptsiooni aluseks on võetud kolm kujundit: kuup, püramiid ja ekraan. Kuup hõlmab endas kolme lahutamatut telge kaasaaja küberjulgeolekust, püramiid tähistab erikihtidel baseeruvat õiguslikku vastust/vastukaja küberjulgeoleku probleemidele ja ekraan on digitaalne keskkond, mille abil näevad otsustajad (ing kl *decision-makers*) võimalikult täielikku ülevaadet küberruumist, kus küberintsidendid, sh küberründed aset leiavad. Järgnevalt igast kujundist eraldi lähemalt.

1. Kuup

Kuup kajastab kolme dimensiooni, kus x-telg tähistab tehnoloogiat – see, mis on võimalik – y-telg õigust – seda, mis on lubatav – ja z-telg poliitikat – see, mida eelistatakse.

Poliitiline telg jaguneb omakorda kuude kategooriasse, mida tuntakse ka DIMPLE[13] nime all: diplomaatia, luure, sõjandus, poliitika, juriidiline ja majanduslik. DIMPLE on loodud selleks, et küberintsidendi raporteerimisel, kus kasutatakse tehnilisi detaile, oleksid sündmused kajastet selliselt, et nad oleksid arusaadavad ka teistele kaasatavate valdkondade ekspertidele.

[13] DIMPLE on edasiarendus DIME-st, vt rohkem Wingfield ja Tikk 2010.

Juriidiline telg riiklikul tasandil hõlmab endas kõikvõimalikke asjasse puutuvaid õigusakte, sh õiguslikud arvamused, kohtulahendid, tunnustet standardid ja kontseptsioonid-põhimõtted.

Tehniline telg võib baseeruda kas küberohu hinnangule ja intsidendi kogemusele või küberintsidentide tüüpidele, mis erinevaid riike ja rahvusvahelisi organisatsioone ohustavad, väljapakutud proaktiivsed ja kaitsvad meetmed ning reageerivatele tasemetele.

Kuup annab oskusteabe, millised õiguslikud ja poliitilised instrumendid on olemas, mida poliitik peab arvesse võtma lahendades küberintsidenti. Kujund näitab samuti ära lüngad ja vasturääkivused, millega on vaja riigil tegeleda.

2. Püramiid

Püramiid koosneb kolmes kihist: eeldusest, algoritmist ja õigusest, mis peegeldavad kolme otsustusprotseduuritaset lähtudes reageerimisajast.

Kõige alumine kiht – eeldus – tähistab must-valget regulatsiooni, nn kui-siis otsustusprotseduuri, mis rakenduvad automaatselt, kellegi kolmanda isiku sekkumiseta. Näiteks, serveri automaatne lahti ühendamine viiruse allalaadimisel. Sarnane põhimõte väljendub näiteks tulekahju süttimisel, mille järel alarm aktiveerub ja vihmutid hakkavad tööle. Selle eeliseks on suutlikkus koheselt reageerida, pärast ohu või ründe ilmingut.

Järgmises kihis – algoritm – toimib samuti automaatse süsteemi poolt, kuid edasise kaitsetegevuse puhul on tarvis heakskiitu. Näiteks, arvutisüsteemid annavad interneti liikluse jälgimise põhjal märku kahtlasest, ebatavapärasest tegevusest, siis ei ole mõistlik pelgalt kahtluse puhul ühendust piirata, vaid jälgida lähemalt radari ette jäänud tegevust ja alles siis johtuvalt otsustada edasine plaan.

Kõrgeim püramiidi kiht on õigus ehk inimotsustaja tasand, mis on nüansirikkaim ja aega nõudvaim. Siin võetakse kõrgetasemelisi otsuseid vastu põhinedes ebaselgele või isegi vastukäivale informatsioonile. Ohule või rünnakule reaktsioon võtab rohkem aega võrreldes kahe esimese kihiga, võides ulatuda tundideni. Võib tähendada tõenäoliselt nõupidamist ekspertidega, ei piisa ainult ühe süsteemi või isiku kiirest otsustamisest.

Põhjalik ja konkreetne õigusanalüüs on siinkohal kriitilise tähtsusega. Meetmed, mida vältida või kasutada küberintsidendi lahendamisel peavad lõpuks tuginema vastavatele õigusaktidele, ent selles ei pruugi alati ühene mõistmine ja selgus olla.

Väljakutse seisneb kõigis kolmes kihis omada maksimaalselt võimalikke võimalusi, muuta automaatseks nii palju kui juriidiliselt, poliitiliselt ja tehnoloogiliselt lubatav. Aeg mängib väga olulist rolli, mida kiiremini suudetakse tuvastada ja reageerida edukalt, seda parem.

3. Ekraan

Kogu Kontseptsiooni hõlmatud informatsioon peab olema formaadis, millele on võimalik kiirelt ja lihtsalt ligi pääseda neil, kes on seotud küberintsidendi haldamisega. Ekraan on tehnoloogiline lahendus, mis võimaldab korraga saada ülevaate ajaloost, hetkeseisust, trendidest, ohtudest, võimalustest, tõenäosustest ja info lünkadest.

Ekraanis leidub kõiksugu õppematerjale, õpitud kogemusi, juhendeid, õiguslikke ja poliitilise instrumente ning samas ka inimesi ja asutusi, kes saavad panustada küberintsidendi haldamisse.

Käesolev töö proovib luua Eesti küberrünnakute lahendamisel kasutatud meetmete baasil Püramiidi. Selleks on uuritud kolme valdkonda – tehnilist, poliitilist ja juriidilist ehk Kuubi tahke. Mida Eesti tegi küberrünnakute lõpetamiseks, milliseid meetmeid kasutusse võttis. Töö lõpuks loodab autor täita Püramiidi kõik kolm kihti – eeldus, algoritm ja õigus ehk inimotsustaja tasand.

3.2 Eesti küberrünnakute lahendamise meetmed

Aluskiht: eeldus

Aluskihi kõiki telgi iseloomustab informatsiooni jagamine. See on loomulik osa, sest tõenäoliselt ei soovita rohkem paanikat kodanike seas külvata, kui seda ründajate tegevusega juba tehtud on. Sellegi poolest tuleb märkida, et poliitikute tegevus – küberrünnakute sildistamine esimese kübersõjaga, hiljem tuumaõnnetuse võrdlemisega – võis pigem vastupidist effekti tekitada.

Tehniline telg

- **Turvameetmete rakendamine: turvaaukude paikamine, kasutati (tõhustati kasutust) tulemüüre ja ründeavastussüsteeme, lihtsustati veebilehti (mida vähem ülemäärast infot seda parem), dubleeriti servereid ja ühendusi, kasutati nö musta nimekirja, kasutati rämpsposti filtreid ning muudeti efektiivsemaks teisi filtreid, õpiti ründeid tundma** – loetletud meetmed olid ühed esimesed reaktsioonid, mida CERT Eesti tegi. Mõned neist, nt veebilehe lihtsustamine, serverite ja ühenduste dubleerimine, musta nimekirja loomine ning rünnete tundmine võib olla ka algoritmi kihis, kuna nt veebilehe lihtsustamise puhul oli tõenäoliselt vaja luba asutuselt saada või pidi täiendavalt (nt väliste IT-ekspertide kogemuse baasilt) oma meetmeid efektiivsemaks tegema. See võib kehtida iga uudse küberintsidendi puhul: on olemas automaatsed protsessid ja siis on võimalik neid olemasolevaid protsesse pärast teistega kogemuste vahetamist või arutlemist otsustada parendada. Seeläbi liigub muudatus taas alumisse kihti.
- **Ründaja blokeerimine** – memode baasilt võib järeldada, et IT-spetsialistid pidid esiti analüüsima logisid selleks, et tuvastada ründajad ning seeläbi nad eraldi blokeerima (eriti esines seda ründajate osas, kes ründasid väljast poolt Eestit, nt USA-s). Hiljem rünnakute käigus suudeti koostööd parendada ning nt blokeeriti Elioni ja ASO koostöös suur osa rünnakutest enne sihtmärkideni jõudmist. Siinkohal on oluline mõelda läbi tehnilise lahenduse võimalusi, kas ja kuidas on võimalik ning mõistlik teatud käitumise põhjal või vähemasti, kui rünnete perioodil õpitakse tundma ründaja "käekirja", automaatset blokeerimist. Esiti blokeeritakse automaatselt ja hiljem peaks järgneva algoritmi kiht, kus otsustaja vaatab üle, kas blokeering on olnud õige või mitte ja vastavalt edasi toimida. Automaatne protsess võiks olla järgnev: kui kasutaja toimib viisil a, b, c, ..., siis blokeeri kasutaja ligipääs veebilehtedele ja mujale. Või koostada analüüside põhjal ründaja profiil ning enneantud tingimuste esinedes, blokeeri kasutaja.
- **Ründaja tuvastamine ja rünnete lõpetamine** – Interneti liikluse monitoorimisel kujuneb ründaja profiil või käekiri, mille alusel võiks muuta ründaja tuvastamise automaatseks. Esialgu tuleks meetme puhul IT-eksperdil sekkuda niivõrd, kuivõrd tuleb pärast ebatavapärase liikluse selgumisel (automaatne protsess), suunata tähelepanu lähemalt kasutajale. Info välise ründaja kohta tuleb edastada läbi

tehniliste ja/või poliitiliste asutuste välisriikidele, kes saaksid omakorda aidata ründajaid tuvastada ja nende tegevust lõpetada – see on esiti automaatne, ent edasine tegutsemine eeldab algoritmi kihti, kuna tegu on juba teise riigi õigussüsteemiga ja erineva regulatsiooniga, erinevate asutustega, kes juhtumile reageerib (nt siseasjadega tegelejad vs välisriikide asjadega tegelejad).

- **Serverite omanikud võtsid maha üleskutseid ja juhendeid, mis olid seotud Eesti küberrünnakutega** – meede on alumises kihis, sest selline vaenuõhutav teguviis peaks olema eelduslikult automaatse protsessi osa.

Poliitiline telg

- **Pidev üleskutse mitte alluda provokatsioonidele ning säilitada rahumeelne käitumine** – see on esimene asi, mida võiks pidada poliitilisel tasandil automaatseks käitumiseks – rahu säilitamine.

Keskmine kiht: algoritm

Siin kihis vastuvõetud meetmeid vajavad täiendavat tegutsemist. Lisaks nö automaatsele tegutsemisviisile või meetmele on vajalik heakskiit (näiteks, kui meetmeid, mida rakendada on mitmeid, mis võivad tuua kaasa erinevaid (tehnilisi, õiguslikke, poliitilisi) tagajärgi). Tuleb arvestada riskiga.

Tehniline telg:

- **Võrguühenduse piiramine Eestist väljapoole jäävate kasutajate poolt nii, et välismaalt ei olnud võimalik ligipääseda Eesti serverites asuvatele informatsioonile** – iseenesest võiks kaaluda meetme lisamist "automaatseks" ja seega ka aluskihti lisamisega (automaatne protsess: kui välisterritooriumilt ületab internetiliiklus teatud piirmäära (arvestades Eesti tavapärast liiklust), siis lülita välisühendus välja. Kuna selline automaatsus puudus, siis on ta käesolevalt algoritmi kihis.
- **Võrguühenduse läbilaskevõime suurendamine** – ka seda meedet võiks kaaluda liigutada alumisse kihti (automaatne protsess: kui on teadaolevalt huvikasv mingi

sündmuse tõttu, nt tuludeklaratsiooni esitamine kevadel, siis tõsta Eesti Maksu- ja Tolliameti ning pankade võrguühenduse läbilaske võimet).

- **Arvutikasutajate manitsemine kahtlase informatsiooni kontrollimisele** – arvestades, et Eesti kaasuse puhul ilmnes meede alles küberrüünakute keskel, siis see kõneleb meetmest, mis ei olnud kohe automaatselt käiku läinud, kuigi oleks pidanud olema. CERT Eesti loomisel oli tema üks põhiülesannetest kasutajate teadlikkuse tõstmine. Arvutikaitse 2009 soovitusi jagati alles 8. mail, kuigi oleks pidanud jagama juba varem, kui ohuhinnangud andsid mõista, et foorumites ja jututubades plaanitakse Eesti vastu küberründeid korraldada. Seega, meede peaks olema alumises kihis (automaatne protsess: kui ilmneb, et peagi võib poliitilisi sündmusi arvesse võttes toimuda küberintsident, siis lisama veebilehtele ja mujale aegsasti teavitusi ja meeldetuletusi kasutajatele oma turvasüsteeme kontrollida).
- **Koostöö teiste asutustega** – iseenesest oli CERT Eestil vahetult enne rünnakuid lepitud interneti teenusepakkujatega koostööleping kokku ja see peakski eeltööna tehtud olema, ent see olemasolu ei tähenda koheselt automaatset meedet, mis aitaks lahendada küberrünnakuid. Koostöö sõltub igast kaasusetüübist erinevalt ja seega liigitas autor selle meetme ka algoritmi kihti.

  Siia alla käib ka meede, kus edastati teistele asutustele ründajate informatsiooni (nt Elion edastas ründajate kohta info CERT Eestile ja see omakorda NATO CERT-le ehk NCIRC-le). Kehtib eelpool kirjeldatuga sama põhimõte.
- **Andmetöötlusvõimekus, mis võimaldab koguda ja analüüsida suuremahulisemaid logisid** – Meetme rakendamine eeldab eelneva vastava regulatsiooni olemasolu ning teatud bürokraatia läbimist, mida võib omakorda lugeda algoritmi kihti. Ressursside suunamine ja täiendavate juhiste andmine ei saa iseenesest olla automaatne protsess, vaid eeldab mingisuguse otsustusprotseduuri läbimist, eriti, mis puudutab finatsilist osa. Seega võib meede paikneda teatud määral paikneda kõigil kolmel kihil.

Poliitilisel teljel:

- **Riigikogu liikmete selgitused** – otseset arutelu, mil Riigikogu otsustas eriolukorda mittevälja kuulutada ja usaldada täielikult Vabariigi Valitsust konflikti

lahendamisel, ei suutnud autor tuvastada. Järelikult, muidu relevantne diskussioon võiks olla kõrgemal – õiguse ehk inimotsustuse kihis – ent nii olulise arutelu laiakõlapinna puudumisel võib järeldada, et meedet ei peetud niivõrd kõrgetähtsusega olevaks.

- **Vaatlejate kutsumine olukorra hindamiseks** – teadaolevalt ei ole mingeid automaatseid protsesse rakendumas, kui küberintsident aset leiab, siis kutsuda vaatlejaid. See peaks olema iseenesest johtuvalt kaasusele.
- **Poliitikute sõnavõtud (kõneaktid)** – meede iseenesest rakendub küll automaatselt: kui on poliitiliselt tähtis sündmus, siis tuleb seda selgitada, kajastada. Ent selle sisu on erinev johtuvalt sündmusele. Seetõttu on paigutanud autor meetme keskmisesse kihti. Pole teada, kas poliitikud eelnevalt leppisid kokku oma strateegias, kuidas ja mida avalikkusele öelda, kuid tõsiasi on see, et tänu poliitikute tegevusele, nende sõnavõttudele, teadlikustati Eesti olemasolu ja juhtunut maailmapoliitika areenil. Poliitikud läbivalt kasutasid ka süüdistavat alatooni, nt välisminister igas oma küberrünnakutega seotud sõnavõtus mainis, et ründajaks on Venemaa.
- **Meedia kasutamine** – meede on mõneti sarnane eelpoolsega. Pole teada, kuidas ja kas kooskõlastatult (tasub eeldada), plaaniti ära kasutada meediat sündmuste kajastamisel. Eesti tegevusest järeldub siiski see, et meediat kasutati ära (Ottis 10.05.2007). Näiteks anti teada, et esimene kurjategija on arreteeritud ning et välisriikidega tehakse koostööd; levitati Eesti ajakirjanduses informatsiooni, et kõigi ründajate vastutusele võtmiseks on algatet kriminaalmenetlus. Nimetet uudistega näeb nö hirmutamispoliitikat, millel pidi olema "distsiplineerivmõju" ja mida arvati ka mõjuvat vähemasti teatud määral. Samuti kutsusti üles tagama kindlustunde tagamist kõigi poolt, neile, kes selle kaotanud on.

Juriidiline telg

- **Rünnakute ja logide analüüs koostamine ja sellest järelduste tegemine** – Eesti puhul oli esiti vaja üldse anda logide analüüsi koostamiseks volitus KV SIVAK-le, seejuures tuli eraldi rõhutada, et sellega ei vähendata mitte CERT Eesti mandaati, vaid pigem aidatakse tema tööle kaasa. Meede eeldab ka vastava regulatsiooni olemasolu, mis pärast logide analüüsi suudab rakendada õigussüsteemi, st ründaja

tegude üle õiguse mõistmine. Kahju pahatahtlikkul tekitamisel peaksid rakenduma sanktsioonid. Eesti 2007. aasta õigussüsteem ei olnud kindlasti ühiskonda rahuldavalt küps. Seda näitab ka regulatsioonide muudatused, mis järgnesid küberrünnakutele (nt karistusseadustiku uuendamine).

- **Kriminaalasja algatamine küberrünnakute uurimiseks** – meede vajas ekspertide eelnevat tegutsemist. Olukorra analüüsi ja olemasoleva põhjal kiiret otsuste tegemist.

Ülemine kiht: õigus ehk inimotsustaja tasand

Tehniline telg

- **Kaaluda valitsusasutusi ühendava intraneti välja töötamist olukorral, kus telekomifirmad (Elion jt) ei suuda vajalikku sidet tagada** – Ottise memost nähtub, et ühe ettepanekuna kaaluti olukorra halvenemisel ning samuti ka tuleviku mõtteis, luua eraldi võrguühendus valitsuse asutustele, kelle omavaheline kommunikatsioon kriisis on oluline. Kuna töö uuris konkreetset ajavahemikku, siis selle meetme rakendamise või mitterakendamise kohta info hetkel puudub.

Poliitiline telg

- **Regionaalsel tasandil juhtunu tõstatamine: kaitseminister kutsus üles Euroopa Liidu kaitseministrite kohtumisel Brüsselis küberrünnakute probleemiga tegelema ja infovahetusele, sh arutada teemat ka järgmistel kohtumistel** – meede ei ole niivõrd koheselt ja otseselt asetleidvate küberrünnakute lahendusmeetmeks, ent siiski annab teatud määral küberründaja(te)le märku – probleemile pööratakse tähelepanu mitte ainult siseriiklikul tasandil, vaid rahvusvaheliselt. Kui probleemi arutletakse ja seisukohti võetakse, siis sellega võib näidata oma toetust ja abivalmidust olukorra eskaleerumisel võtta vastu täiendavaid samme.
- **Rahvusvahelise organisatsiooni kaasamine protsessi**: Eesti edastas NATO-le soovitusi, mida võiks viimane Eestit toetades teha – NATO-l soovitati hukka mõista küberründed Eesti vastu; pakkuda abi ründajate tuvastamisel; saata NCIRC-i vaatlejad Eestisse ja julgustama riike liituma loodava Küberkaitsekeskusega (CCD

COE). Kolm meedet on otseselt abistavad asetleidvatele küberrünnakute lahendamisel, viimane on pigem tulevikule suunatud meede (mis kõik ka täitusid). Rahvusvahelise organisatsiooni kaasamine ja abi on kindlasti meede, mis ei saa olla automaatne protsess otseselt. Selleks on vaja läbida teatud protseduur ning arutleda iga kaasuse puhul eraldi, mida on mõistlik edasi teha.

- **Regionaalse organisatsiooni kaasamine**: Välisministri ettepanekud Euroopa Liidule, milliseid meetmeid peaks viimane vastu võtma seoses Venemaaga:
    - meetmed peavad mõjuma nii, et Venemaa lõpetaks rünnakud ja Eesti siseasjadesse sekkumise ning asuks täitma Viini diplomaatiliste suhete konventsiooni;
    - meetmed peaksid puudutama Euroopa Liidu ja Venemaa suhteid täies ulatuses;
    - peetakse oluliseks, et Euroopa Liit reageeriks Venemaa käitumisele maksimaalse tugevusega (see võib tähendada erinevate kõneluste peatamise või nende mittealustamist Euroopa Liidu ja Venemaa vahel. Tõsiselt tuleks kaaluda ka Euroopa Liidu–Venemaa tippkohtumise edasilükkamist).

Meede on samuti ülemisse kihti jääv, sest iga kaasus võib olla erinev ja igal korral võib olla vajalik erinev lähenemisviis.

Juriidiline telg

- **Vastutajate määramine, esialguse hinnangu andmine juhtunule ning edasiste tegevuskavade kinnitamine** – Meede eeldab nii tehniliste, poliitiliste kui ka juriidiliste ekspertide kaasamist ja ühist erutelu. Meede on kindlasti laiaulatuslikke küberrünnakute korral ülemises kihis. Eesti kaasuse puhul võib pidada seda kindlasti üks kriitilisemaks meetmeks, sest olukord oli täiesti uudne kõigile asjaosalistele.
- **Õigusabipalve esitamine** – meetme kasutamisel arutati otsustajate tasandil ja koostöös ekspertidega, kuidas oleks olukorral kõige õigem läheneda ning millise õigusakti kasutamisel olukorda lahendada (millise õigusakti alusel õigusabitaotlust esitada).

3.3 Eesti küberrünnakute lahendamine: poliitiline käitumine

2007. aasta küberründed puudutasid enim Eesti suhteid Venemaa, Ameerika Ühendriikide, Saksamaa, Euroopa Liidu, Euroopa Nõukogu ja NATO-ga. Venemaa vastutavaks pidamine oli kooskõlas nii Eestile kättesaadavate tehniliste andmete, Venemaa enda käitumisega (abist keeldumine ja rünnete moraalne toetamine) ning Eesti ühe olulisima välispoliitilise hoiakuga (Kaitsepolitsei aastaraamat 2007; Tikk, Kaska ja Vihul 2010: 28; Henno 2008).

Käesoleva töö seisukohalt on olulised eeskätt diplomaatilised, poliitilised ja juriidilised meetmed, mida Eesti kaitseks ja edendamiseks rakendas oma välispoliitilistes huvides (vt DIMPLE esimeses peatükis).

Eesti diplomaatilised meetmed keskendusid küberjulgeoleku kui Eesti jaoks teise olulise välispoliitilise prioriteedi propageerimisega ning selle rahvusvahelisel tasandil tähelepanu juhtimisel. Ministrid Paet ja Aaviksoo tõstatasid küberjulgeolekuteemad nii Euroopa Liidus kui ka NATO-s. Eesti plaan oli samuti kutsuda üles riike liituma Euroopa Nõukogu arvutikuritegevuse konventsiooniga. Küberrünnakute algul olid Eesti poliitikud seisukohal, et mingisugust küberründeid reguleerivaid rahvusvahelise akte ei ole. (nt Hanno Tombergi intervjuu Rein Langiga 09.05.2007)

Luureandmete ja infooperatsioonide ning kaitseorganisatsioonide roll rünnete tõrjumisel ning Eesti välispoliitiliste huvide tagamisel oli marginaalne, muuhulgas seetõttu, et ründed ei ületanud jõu kasutamise lävendit. See kummutab ühe enimlevinud müüdi, mida ka Eesti poliitikute sõnavõttudes esialgselt märgata oli – diskuteerimine, et tegu võiks olla NATO kollektiivkaitse alla kuuluva juhtumiga. Hoolimata Aaviksoo esialgsest juhtunu kvalifitseerimisest kui kübersõjast, muutis ta hiljem oma seisukohta ning ei soovinud üheselt öelda, kas tegu võiks olla NATO Põhja-Atlandi lepingu artikkel 5 kaasusega: “Ma arvan, et praegu ei ole ühtegi kaitseminisrit, kes sellele ühemõtteliselt vastata võiks. Ka mina jätan sellele vastamata.” (Kalamees 2007)

Poliitikute kõneaktid jagunesid peaasjalikult poliitilisteks ja juriidilisteks, kuigi esines ka sündmuste sildistamist sõjalises ja tehnilises kontekstis. Välispoliitiliste meetmete kasutamist saab suures plaanis iseloomustada Eesti varasema ja ka senise poliitilise agenda jätkamist: kuulutada Läänele, et Venemaad ei saa ega tohi usaldada. Esialgu nõuti isegi, et

Moskvat ei tohiks ka mitte diskussiooni kaasata, leiti, et Euroopa Liidu ja Venemaa tippkohtumine tuleks ära jätta. Hiljem siiski muudeti oma taktikat ja otsustati probleem kohtumise päevakorda arutlemisele võtta, kuid Venemaa kaasamist ei soositud. Jääb mulje, et partnerriigid proovisid Eestit veenda siiski vähemalt dialoogi pidamises, mida Paet lõpuks oma pika süüdistava kõne lõpus ka lõpuks viimasena välja pakub (vt joonealust märkust nr 10).

Eesti välispoliitilist käitumist saab võtta kokku märksõnadega: üldine Venemaa tegutsemise hukkamõistmine, küberruumi regulatsiooni arutelule võtt ning rahvusvahelise koostöö välja töötamine. Eesti 2007. aasta küberrünnakutega lisandus Eesti välispoliitilisse agendasse uus punkt – küberjulgeoleku valdkond. Eesti mõistis oma kogemuste baasilt, et rahvusvahelises õiguses on suuri puudujääke, mis puudutab küberjulgeoleku tagamist ja küberrünnetega tegelemist. Ainuüksi siseriikliku regulatsiooni muutmisest ei piisa, tegu on piirideülese probleemiga, mille lahendamisel peaksid kõik osapooled ühiselt koos töötama. Valdav osa Eesti küberrünnetest oli ju välisterritooriumilt pärit ja kuigi Eesti puhul tuli kasuks tema väiksus, siis kindlasti sama meede ei pruugi olla lahenduseks teistele suurematele riikidele, kui nad peaksid sarnaste küberrünnakute alla sattuma.

Seevastu Eesti sisepoliitilised meetmed olid peaasjalikult suunatud kodanike rahustamisele, olukorra taastamisele ja turvatunde tõstmisele. Läbivalt saab iseloomustada, eriti peaministri ja Presidendi sõnavõttude alusel, et inimesi kutsuti üles kainele mõistusele ja rahulikule suhtumisele. Ent samas, ei informeeritud avalikkust, kas ja kuidas täpselt küberrünnetega tegeleti. Küberintsidentide puhul oli Eesti taristu, kuidas käituda, mida teha, praktiliselt olematu.

Töö näitab, et Eestil küll oli olemas huvi küberjulgeoleku vastu (nt soov luua Eestisse NATO Küberkaitsekeskuse algatati juba 2005. aastal), kuid puudus konkreetne sedalaadi küberrünnakute tegelemiseks mõeldud tegevusplaan (seda tõendab nii ajaline reageerimine, kui ka hilisem Eesti tegevus (vt Kaska, Talihärm, Tikk 2010)). Ühelt poolt saab seda pidada arusaadavaks, sest Eestis ei olnud varem sellise kaliibriga küberründeid olnud, kuid teisalt, ühiskond, mis reklaamib end infoühiskonnana ja IT valdkonnas arenenuna, peaks olema rajanud endale ka vastava turvasüsteemid ja regulatsiooni sedalaadi rünnakute puhuks.

3.3.1 Eesti pärast 2007. aasta küberrünnakuid

Tuginedes Kaska, Talihärma ja Tikk-i analüüsile, saab välja tuua järgnevad tegevused, millega Eesti on tegelenud pärast 2007. aasta küberrünnakuid:

- Küberjulgeoleku strateegia 2008–2013,
- Karistusseadustikku ja jälitustegevuse seaduse uuendamine 2008. aastal,
- uue hädaolukorra seaduse vastuvõtmine 2009. aastal,
- Eesti Riigi Infosüsteemide Ameti struktuuri muutused 2010. aastal – loodi juurde kriitilise informatsiooni infrastruktuuri kaitse osakond,
- Eesti infoühiskonna arengukava uuendamine,
- Küberkaitseliidu osakonna loomine,
- ÜRO valitsusekspertide grupiga ühinemine (United Nations Office for Disarmament).

Kokkuvõte

Käesolev töö annab ülevaate riikide kasutuses olevatest poliitilistest meetmetest küberjulgeolekuohtude tõrjumisel ja küberintsidentide lahendamisel. Tegemist on kasvava, erialakirjanduses põhjalikumalt käsitlemata ja praktilise probleemiga. Eesti 2007. aasta kogemuse põhjal analüüsib autor riigi välispoliitiliste huvide tagamise võimalusi ja praktikat ning riigi käitumise kujunemist tehniliste, poliitiliste ja juriidiliste tingimuste ning asjaolude koosmõjul.

Töös selgitatakse esmalt millised asjaolud – tehnilised, poliitilised ja juriidilised – küberrünnakute lahendamisel rolli mängivad ning esitatakse otsustusprotseduuri faasid, milles meetmete kasutamise üle otsustatakse. Otsustuste ja kaalutluste mõistmise hõlbustamiseks on esitatud sündmuste ülevaade – milliste rünnete alla Eesti 2007.a. aprillis ja mais sattus, kes olid rünnetele reageerijad, mis oli rünnakute sihtmärkideks, milliseid ründetüüpe ja -vahendeid ründajad kasutasid. Teine peatükk uurib poliitilisel tasandil toimunut ehk kuidas reageerisid küberrünnetele poliitikud (otsustajad). Kolmas peatükk asetab meetmete valiku ja kasutamise küberjulgeoleku otsustusmudelisse. Viimases peatükis esitab autor analüsi võetud meetmete seostest Eesti välispoliitika suundade ja huvidega.

Töös järeldatakse, et Eesti kohaldas 2007.a. küberrünnete tõrjumiseks nii tehnilisi, poliitilisi kui juriidilisi meetmeid. Võetud meetmetest tuleb edukaimaks pidada välispoliitilisi samme, sest küberrünnete tõrjumisest on saanud välispoliitiline edulugu, mis päädis Eesti tunnustamisega kui küberruumis arvestatava toimijaga, kelle kogemust hinnatakse. Eesti edu ‘mõõdikuteks’ võib pidada näiteks ÜRO I Komitee valitsusekspertide töörühma kuulumist alates 2009.a., OSCE küberjulgeoleku vastumeetmete (ing kl cyber security countermeasures) kujunemisse panustajat ning figureerimist rahvusvahelistes edetabelites, mis mõõdavad riikide edukust küberruumis.

Igal meetmete komplektil või kooslusel on omad eelised, kuid ka piirid ja puudused. Tehnilised on kiired ja automatiseeritud/automatiseeritavad, kuid lühiajalised ja mittejätkusuutlikud; poliitilised pole siduvad ning juriidilised võtavad aega

väljakujunemiseks ja juurdumiseks. Seega on oluline rakendada mistahes küberjulgeolekuohu tõrjumisse kõiki meetmed.

Eesti valitud ja rakendatud meetmed ei ole ammendavad ega ainuvõimalikud. Töö peamine järeldus on, et valitavad meetmed sõltuvad tehnilistest, poliitilistest ja juriidilistest asjaoludest ning soovitavast tagajärjest ja mõjust, mida riigiti ja sündmuste kaupa soovitakse saavutada. Sony küberrünnakute järel kehtestas Ameerika kümnele indiviidile ja kolmele asutusele, kes olid seotud Põhja-Korea valitsusega, sanktsioonid – nende varale, mis asus Ameerikas, piirati juurdepääsu. (Chabrow 2015)

Autor on seisukohal, et laiem teoreetiline käsitlus küberjulgeoleku tagamisele suunatud välispoliitilistest meetmetest oleks kasulik eelkõige otsustajatele, kes pingelises olukorras peavad suutma orienteeruda infod ja andmetes ning leidma efektiivseid lahendusi. Seda eelkõige seetõttu, et kui ründed juba aset leiavad, siis ei ole praktiline raisata aega juba tuvastatud võimalike lahenduste leiutamise peale, vaid samal ajal, kui testitakse eelnevalt välja töötatud meetmeid on võimalik väärtuslikku aega kokku hoida ja panustada energiat uute võimalike lahenduste välja mõtlemisse. Antud temaatika vääriks edasist uurimist, et leida paremaid viise, kuidas maandada küberrünnetega kaasnevaid kahjusid ja vältida rünnete eskaleerumist, sest ohud ei kao ja ründajad kavandavad pidevalt uusi meetodeid.

Kasutatud kirjandus

1. "2009 U.S.–Russian Bilateral Presidential Commission: Mission Statement." U.S. Department of State http://www.state.gov/p/eur/ci/rs/usrussiabilat/c38418.htm (Viimati külastet: 17.05.15).
2. "Developments in the Field of Information and Telecommunications in the Context of International Security." *United Nations Office for Disarmament*. http://www.un.org/disarmament/topics/informationsecurity/ (Viimati külastet: 17.05.15).
3. "Infopoliitika tegevuskava aastaks 2006" http://www.riso.ee/sites/default/files/TG06_05.pdf (Viimati külastet: 17.05.15).
4. "Northe Korea Accuses U.S. & South Korea of Cyber Attacks." *Esentire*. https://www.esentire.com/north-korea-accuses-u-s-south-korea-of-cyber-attacks/ (Viimati külastet: 17.05.15).
5. "Päringu koostamine." Tartu Ülikool. https://sisu.ut.ee/otsing/p%C3%A4ringu-koostamine (Viimati külastet: 17.05.2015).
6. "U.S.–Russia Bilateral Presidential." U.S. Department of State http://www.state.gov/p/eur/ci/rs/usrussiabilat/index.htm (Viimati külastet: 17.05.15).
7. "Välissuhtlus." Riigikogu. http://www.riigikogu.ee/tutvustus-ja-ajalugu/riigikogu-ulesanded-ja-tookorraldus/mida-riigikogu-teeb/valissuhtlus/ (Viimati külastet: 17.05.15).
8. 2007. "Estonia and Russia: A cyber-riot." *The Economist* May, 10. http://www.economist.com/node/9163598 (Viimati külastet 17.05.15).
9. 2007. "Estonia hit by 'Moscow cyber war.'" *BBC News* May, 17. http://news.bbc.co.uk/2/hi/europe/6665145.stm (Viimati külastet: 17.05.15).
10. 2007. "Estonia urges firm EU, NATO response to new form of warfare: cyber-attacks." *The Sydney Morning Herald* May, 16. http://www.smh.com.au/news/Technology/Estonia-urges-firm-EU-NA TO-response-to-new-form-of-warfarecyberattacks/2007/05/16/1178995207414.html (Viimati külastet: 17.05.15).

11. 2007. “Estonia: Defense Minister Says Bronze Soldier Had To Go.” *Radio Free Europe. Radio Liberty* May, 9. http://www.rferl.org/content/article/1076363.html (Viimati külastet: 17.05.15).
12. 2007. “EU Pledges Help in Estonia-Russia Row.” DW.DE 1.mai. http://www.dw.de/eu-pledges-help-in-estonia-russia-row/a-2463643-1 (Viimati külastet 17.05.15).
13. 2007. “Kaitsepolitsei aastaraamat 2007.” https://www.kapo.ee/cms-data/_text/38/44/files/aastaraamat-2007-est.pdf (Viimati külastet 18.05.15).
14. 2007. “KÕIK PRONKSSÕDURI UUDISED 01.05.07: Eesti saatkonnalt Moskvas rebiti maha lipp.” *Eesti Ekspress* 1. mai. http://ekspress.delfi.ee/news/paevauudised/koik-pronkssoduri-uudised-010507-eesti-saatkonnalt-moskvas-rebiti-maha-lipp?id=69110443 (Viimati külastet 17.05.15).
15. 2007. “Old Wars and New: Estonians Accuse Kremlin of Cyberwarfare.” Spiegel Online International May, 17. http://www.spiegel.de/international/world/old-wars-and-new-estonians-accuse-kremlin-of-cyberwarfare-a-483394.html (Viimati külastet: 17.05.2015).
16. 2007. “Ummistusrünnakute tule all.” *Eesti Ekspress* 17. mai. http://ekspress.delfi.ee/news/paevauudised/ummistusrunnakute-tule-all?id=69113781 (Viimati külastet 17.05.15).
17. 2007. “Unrest in Estonia.” *F-Secure* April, 28. https://www.f-secure.com/weblog/archives/00001181.html (Viimati külastet: 17.05.15).
18. 2013. “FACT SHEET: U.S.–Russian Cooperation on Information and Communications Technology Security.” *The White House. Office of the Press Secretary* June, 17. https://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol (Viimati külastet: 17.05.15).
19. 2013. “Threatsaurus. The A-Z of computer and data security threats.” *SOPHOS.*
20. 2014. “U.S. Suspends Russian Projects Over Ukraine.” *Radio Free Europe. Radio Liberty* April, 2. http://www.rferl.org/content/us-russia-bilaterl-ukraine/25319151.html (Viimati külastet: 17.05.15).

21. 2015. “List of Top Search Engines In the World – Search Engines.” *Mobile Info Guru* February, 15. http://www.mobileinfoguru.com/list-of-top-search-engines-in-the-world/ (Viimati külastet: 17.05.15).
22. 2015. “Riigikogu uuenenud veebileht pakub rohkem pildimaterjali ja infograafikat.” Riigikogu pressiteated 23. aprill. http://www.riigikogu.ee/pressiteated/muu-pressiteade-et/riigikogu-uuenenud-veebileht-pakub-rohkem-pildimaterjali-ja-infograafikat/ (Viimati külastet: 17.05.15).
23. 2015. “South Korea Accuses North of Cyber-attacks on Nuclear Plants.” *SecurityWeek* March, 17. http://www.securityweek.com/south-korea-accuses-north-cyber-attacks-nuclear-plants (Viimati külastet: 17.05.15).
24. AKIT sõnastik. http://akit.cyber.ee/ (Viimati külastet 17.05.15).
25. Anvelt, Kärt ja Ojakivi, Mirko. 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?id=51086579 (Viimati külastet 17.05.15).
26. Anvelt, Kärt. 2007. “Aaviksoo viis kübersõja EL-i.” *Eesti Päevaleht* 15. mai. http://epl.delfi.ee/news/eesti/aaviksoo-viis-kubersoja-teema-el-i?id=51086979 (Viimati külastet 17.05.15).
27. Arquilla, John ja Ronfeldt, David. 1993. “Cyberwar is coming!” *Comparative Strategy* 12.2, 141–165.
28. Ashford, Warick. 2013. “South Korea accuses North Korea of launcing cyber attacks.” *ComputerWeekly* April, 11. http://www.computerweekly.com/news/2240181276/South-Korea-accuses-North-Korea-of-launching-cyber-attacks (Viimati külastet: 17.05.15).
29. Berendson, Risto. 2007. “Küberrünnakute taga seisavad profid.” *Postimees* 3. mai. http://www.postimees.ee/1656489/kuberrunnakute-taga-seisavad-profid (Viimati külastet 17.05.15).
30. Blomfield, Adrian. 2007. “Aaviksoo Russia accused over Estonian ‘cyber-terrorism.’” *Telegraph* May, 17. http://www.telegraph.co.uk/news/worldnews/1551850/Russia-accused-over-Estonian-cyber-terrorism.html (Viimati külastet: 17.05.15).

31. Bright, Arthur. 2007. "Estonia accuses Russia of 'cyberattack.'" *CSMonitor* May, 17. http://www.csmonitor.com/2007/0517/p99s01-duts.html (Viimati külastet: 17.05.15).
32. Chabrow, Eric. 2015. "Obama Imposes Sanctions on North Korea for Hack." GovInfoSecurity January, 2. http://www.govinfosecurity.com/obama-imposes-sanctions-on-north-korea-for-hack-a-7746 (18.05.15).
33. Clarke, Richard A., ja Robert K. Knake. 2014. *Cyber war*. Tantor Media, Incorporated.
34. Davis, Joshua. 2007. "Hackers Take Down the Most Wired Country in Europe." *Wired Magazine* 15.09. http://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all (Viimati külastet: 17.05.15).
35. Eesti Rahvusringhääling. http://info.err.ee/ (Viimati külastet: 17.05.15).
36. Erakorralise seisukorra seadus. RT I 1996, 8, 164; 1999, 57, 598 ja RT I, 16.12.2014, 12.
37. Ergma, Ene. 2007. "Küberjulgeolekule teed rajades." *Riigikogu Toimetised* 15.
38. Farwell, James P., and Rafal Rohozinski. 2011. "Stuxnet and the future of cyber war." *Survival* 53.1.
39. Geers, Kenneth. 2008. "Cyberspace and the Changing Nature of Warfare." *BlackHat*. https://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Geers/BlackHat-Japan-08-Geers-Cyber-Warfare-Whitepaper.pdf (Viimati külastet: 17.05.15).
40. Hafner, Katie, and Lyon, Matthew. 1998. *Origins of the Internet. Where the Wizards Stay Up Late*. 1th ed. New York, NY: Touchstone.
41. Hanno Tombergi intervjuu Hillar Aarelaiuga. Eesti Raadio. http://arhiiv.err.ee/vaata/4649 (Viimati külastet: 17.05.2015).
42. Hanno Tombergi intervjuu Hillar Aarelaiuga. Eesti Raadio. https://arhiiv.err.ee/vaata/uudised-uudised-2007-kuberrunnakud-eesti-vastu (Viimati külastet: 17.05.15).
43. Hanno Tombergi intervjuu Rein Langiga. Eesti Raadio. https://arhiiv.err.ee/vaata/uudised-uudised-09-05-2007 (Viimati külastet: 17.05.15).

44. Henno, Erki. 2008. "Venemaa keeldub endiselt koostööst küberrünnakute uurimisel." Postimees 13. detsember. http://www.postimees.ee/58258/venemaa-keeldub-endiselt-koostoost-kuberrunnakute-uurimisel (Viimati külastet: 18.05.15).
45. Herodes, Kristiina. 2007. "Alustati kriminaalasi küberrünnakute uurimiseks." Prokuratuur 2. mai. http://www.prokuratuur.ee/et/pressiteated/alustati-kriminaalasi-kuberrunnakute-uurimiseks (Viimati külastet: 17.05.15).
46. Hillar Aarelaid. 2007a. Overview.
47. Hillar Aarelaid. 2007b. ENISA Overview of Recent Incidents. http://www.enisa.europa.eu/activities/cert/events/files/ENISA_overview_of_recent_incidents_Aareleid.pdf/view (Viimati külastet 17.05.15).
48. ISO standard. ISO/IEC 27033.
49. IT terministardardi sõnastik. http://www.eki.ee/dict/its/ (Viimati külastet: 17.05.15).
50. 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 (Viimati külastet 17.05.15).
51. Kash, Wyatt. 2008. "Lessons from the cyberattacks on Estonia." GCN !une, 13. http://gcn.com/Articles/2008/06/13/Lauri-Almann--Lessons-from-the-cyberattacks-on-Estonia.aspx?Page=1 (Viimati külastet: 17.05.15).
52. Kaska, Kadri, Talihärm, Anna-Maria ja Tikk, Eneken. 2010. "Developments in the Legislative, Policy and Organisational Landscapes in Estonia Since 2007." In *International Cyber Security. Legal & Policy Proceedings*, eds. Eneken Tikk ja Anna-Maria Talihärm. Tallinn: CCD COE, 40–66.
53. Kirk, Jeremy. 2007. "Estonia recovers from massive DDoS attack." *Computerworld* May, 17. http://www.computerworld.com/article/2545237/security0/estonia-recovers-from-massive-ddos-attack.html (Viimati külastet: 17.05.15).
54. Koman, Richard. 2007. "Estonia reeling from massive cyberattack from Russia." *ZDNet* May, 18. http://www.zdnet.com/article/estonia-reeling-from-massive-cyberattack-from-russia/ (Viimati külastet: 17.05.15).
55. Konrad, Krawczyk. 2014. "Google is easily the most popular search engine, but have you heard who's in second?" *Digital Trends* July, 3.

http://www.digitaltrends.com/web/google-baidu-are-the-worlds-most-popular-search-engines/ (Viimati külastet: 17.05.15).

56. Kumar, Rakesh. 2015. "10 Most Popular Search Engines in the World." Top World Fact April, 20. http://www.topworldfact.com/technology-latest-10/top-10-search-engines-in-the-world/ (Viimati külastet: 17.05.15).
57. Lühikokkuvõte NATO-le 8. ja 10. mai 2007.
58. Masin, Kadri. 2007. "Riigikogu komisjonid tõstavad küberründe teema." *Eesti Päevaleht* 11. mai. http://epl.delfi.ee/news/eesti/riigikogu-komisjonid-tostavad-kuberrunde-teema?id=51086660 (Viimati külastet 17.05.15).
59. Meikar, Silver. 2007. "Silver Meikar: Venemaa toetab terrorismi." *Meikar blog* 10. juuli. http://www.meikar.ee/blog/?m=20070710 (Viimati külastet: 17.05.15).
60. Narits, Raul. 2004. *Õiguse entsüklopeedia*. 2. täiendet ja parandet trükk. Tallinn: Kirjastus Juura.
61. Nazario, Jose. 2007. "Estonian DDoS Attacks – A Summary to Date." Arbor Networks June, 17. http://www.arbornetworks.com/asert/2007/05/estonian-ddos-attacks-a-summary-to-date/ (Viimati külastet: 17.05.15).
62. Nutt, Mart. 2013. "Mart Nutt: kärgjas julgeolek." *Postimees* 5. märts. http://www.eihr.ee/mart-nutt-kargjas-julgeolek/ (Viimati külastet: 17.05.15).
63. Ottis, Rain. 2007. "Memo: Eesti Vabariigi vastased küberründed pronkssõduri konflikti ajal." 2., 4., 7. ja 10. mai.
64. Paet, Urmas. 2007. "Vene karu jätkab vana joont." *Postimees* 4. mai. http://www.postimees.ee/1657319/paet-vene-karu-jatkab-vana-joont (Viimati külastet 17.05.15).
65. Park, Ju-min. 2013. "South Korea accuses North of cyber attacks." *Reuters* July, 16. http://www.reuters.com/article/2013/07/16/net-us-korea-cyber-idUSBRE96F0A920130716 (Viimati külastet: 17.05.15).
66. Poom, Raimo ja Jõgis-Laats, Jan. 2007. "Andrus Ansip: otsustage, mis riigiga te oma tulevikku seote." *Eesti Päevaleht* 16. mai. http://epl.delfi.ee/news/eesti/andrus-ansip-otsustage-mis-riigiga-te-oma-tulevikku-seote?id=51087148 (Viimati külastet 17.05.15).

67. Poom, Raimo. 2007. “Samara proovikivi: kas Eesti on suutnud end euroliidus kehtestada?” *Eesti Päevaleht* 12. mai. http://epl.delfi.ee/news/eesti/samara-proovikivi-kas-eesti-on-suutnud-end-euroliidus-kehtestada?id=51086697 (Viimati külastet 17.05.15).
68. Poulsen, Kevin. 2007. “‘Cyberwar’ and Estonia’s Panic Attack.” *WIRED* August, 22. http://www.wired.com/2007/08/cyber-war-and-e/ (Viimati külastet: 17.05.15).
69. Põhja-Atlandi leping. RT II 2004, 5, 14.
70. Randel, Tarmo. 2007. “CERT Eesti tegevuse aastakokkuvõte 2007.”
71. Riigi Infosüsteemi Amet. 2007. Küberrünnete tulv on kontrolli all. 11. mai. https://www.ria.ee/kuberrunnete-tulv-on-kontrolli-all/ (Viimati külastet: 17.05.2015).
72. Riigi Infosüsteemi Amet. 2007. Arvutikaitse 2009 soovitused tavakasutajale arvuti turvalisuse tõstmiseks. 8. mai. https://www.ria.ee/arvutikaitse-2009-soovitused-tavakasutajale-arvuti-turvalisuse-tostmiseks/ (Viimati külastet: 17.05.2015).
73. Riigi Infosüsteemi Amet. 2007. CERT Eesti teatab: küberründed Eesti vastu ei ole vaibunud. 30. aprill. https://www.ria.ee/cert-eesti-teatab-kuberrunded-eesti-vastu-ei-ole-vaibunud/ (Viimati külastet: 17.05.2015).
74. Riigi Infosüsteemi Amet. 2007. CERT Eesti: Rünnete tõrjumise muudab edukaks koostöö. 7. mai. https://www.ria.ee/cert-eesti-runnete-torjumise-muudab-edukaks-koostoo/ (Viimati külastet: 17.05.2015).
75. Riigi Infosüsteemi Amet. 2007. CERT Eesti: Varahommikul kordistati rünnakuid Eesti küberruumi vastu. 1. mai. https://www.ria.ee/cert-eesti-varahommikul-kordistati-runnakuid-eesti-kuberruumi-vastu/ (Viimati külastet: 17.05.2015).
76. Riigi Infosüsteemi Amet. 2007. Internetiliikluse maht on endiselt tavapärasest kõrgem. 3. mai. https://www.ria.ee/internetiliikluse-maht-on-endiselt-tavaparasest-korgem/ (Viimati külastet: 17.05.2015).
77. Riigi Infosüsteemi Amet. 2007. Küberründed ei ole peale 9. maid vaibunud. 10. mai. https://www.ria.ee/kuberrunded-ei-ole-peale-9-maid-vaibunud/ (Viimati külastet: 17.05.2015).

78. Riigi Infosüsteemi Amet. 2007. Küberrünnakute eesmärgiks võib olla Eesti infoblokaad. 9. mai. https://www.ria.ee/kuberrunnakute-eesmargiks-voib-olla-eesti-infoblokaad/ (Viimati külastet: 17.05.2015).
79. Riigi Infosüsteemi Amet. 2007. Südaööks küberrünnete tase normaliseerus. 16. mai. https://www.ria.ee/sudaooks-kuberrunnete-tase-normaliseerus/ (Viimati külastet: 17.05.2015).
80. Riigi Infosüsteemide Amet. 2007. CERT Eesti kommentaar küberrünnakutele. 28. aprill. https://www.ria.ee/cert-eesti-kommentaar-kuberrunnakutele/ (Viimati külastet: 17.05.2015).
81. Riigi Infosüsteemide Amet. 2007. CERT uudised – hommik Eesti internetiruumis kulgeb harjumuspäraselt. 2. mai. https://www.ria.ee/cert-eesti-luhiinfo-hommik-eesti-internetiruumis-kulgeb-harjumusparaselt/ (Viimati külastet: 17.05.2015).
82. Riigi Infosüsteemide Amet. 2015. RIA kujunemislugu. https://www.ria.ee/ria (Viimati külastet 17.05.15).
83. Riigikogu Kantselei. 2011. "Riigikogu XI koosseis. Statistikat ja ülevaateid." http://www.riigikogu.ee/wpcms/wp-content/uploads/2014/11/XIstatistikakogumik.pdf (Viimati külastet: 17.05.15).
84. Riigikogu stenogrammid. http://stenogrammid.riigikogu.ee/et/20070430-20070517/?search=k%C3%BCber&type=all (Viimati külastet: 17.05.15).
85. Riigikogu. 2007. XI Riigikogu stenogramm. I istungjärk. 2. mai. http://stenogrammid.riigikogu.ee/et/200705021300 (Viimati külastet 17.05.15).
86. Riigikogu. 2007. XI Riigikogu stenogramm. I istungjärk. 2. mai. http://stenogrammid.riigikogu.ee/et/200705021400 (Viimati külastet 17.05.15).
87. Schmidt, Andreas. 1986. "The Estonian cyberattacks." In *The fierce domain – conflicts in cyberspace, 1986-2012*, ed. Jason Healey, Washington DC: Atlantic Council, 2013.
88. Schmitt, Michael N. 2013. *Tallinn manual on the international law applicable to cyber warfare*. ed. New York: Cambridge University Press.
89. Schreck, Carl. 2014. "Freeze Settles On U.S.-Russia Commission Amid Ukraine Standoff." *Radio Free Europe. Radio Liberty* March, 28.

http://www.rferl.org/content/us-russia-commission/25312837.html (Viimati külastet: 17.05.15).

90. Šmutov, Martin. 2007. "Ergma arvates võivad küberrünnakud korduda." *Virumaa* 25. mai. http://www.virumaa.ee/2007/05/ve-kuberrunnakud/ (Viimati külastet: 17.05.15).
91. Tikk-Ringas, Eneken. 2015. "Comprehensive Normative Approach to Cyber Security." *ICT4Peace Foundation*. http://ict4peace.org/wp-content/uploads/2015/04/ICT4Peace-concept-paper-a-comprehensive-normative-approach-to-cyber-security.pdf (Viimati külastet: 17.05.15).
92. Tikk, Eneken, Kaska, Kadri ja Vihul, Liis. 2010. *International Cyber Incidents: Legal Considerations*. Tallinn: CCD COE.
93. Vabariigi President. 2007. NATO peasekretär vabariigi presidendile: allianss toetab Eestit. 2. mai. http://president.ee/et/meediakajastus/pressiteated/205-nato-peasekretvabariigi-presidendile-allianss-toetab-eestit/index.html#sthash.W47fNtFP.dpuf (Viimati külastet 17.05.2015).
94. Vabariigi President. 2007. President Toomas Hendrik Ilvese avaldus seoses rahutustega Tallinnas ööl vastu 27. aprilli. 27. aprill. http://president.ee/et/meediakajastus/avaldused/2782-president-toomas-hendrik-ilvese-avaldus-seoses-rahutustega-tallinnas-oeoel-vastu-27-aprilli/index.html (Viimati külastet 17.05.2015).
95. Vabariigi President. 2007. USA riigisekretär Eesti presidendile: Ühendriigid toetavad Eestit. 3. mai. http://president.ee/et/meediakajastus/pressiteated/207-usa-riigisekreteesti-presidendile-endriigid-toetavad-eestit/index.html#sthash.9Z45mXJD.dpuf (Viimati külastet 17.05.2015).
96. Vabariigi President. 2007. Vabariigi presidendi, riigikogu esimehe ja peaministri ühisavaldus. 8. mai. http://president.ee/et/meediakajastus/avaldused/2784-vabariigi-presidendi-riigikogu-esimehe-ja-peaministri-uehisavaldus-8-mail-2007/index.html (Viimati külastet 17.05.2015).
97. Vabariigi President. 2007. Vabariigi President: me suudame kokkuleppida ühises tulevikus. 2. mai http://president.ee/et/meediakajastus/pressiteated/204-vabariigi-

president-me-suudame-kokku-leppida-es-tulevikus/index.html (Viimati külastet 17.05.2015).

98. Vabariigi Valitsus. 2007. Elektroonilistes kanalites võib levida väärinfo. 28. aprill. https://valitsus.ee/et/uudised/nb-tapsustatud-teade-elektroonilistes-kanalites-voib-levida-vaarinfo (Viimati külastet: 17.05.2015).
99. Vabariigi Valitsus. 2007. Vabariigi presidendi riigikogu esimehe ja peaministri ühisavaldus. 8. mai. https://valitsus.ee/et/uudised/vabariigi-presidendi-riigikogu-esimehe-ja-peaministri-uhisavaldus-8-mail-2007 (Viimati külastet: 17.05.2015).
100. Vabariigi Valitsus. 2007. Vabariigi valitsus ja kriisikomisjon pidasid erakorralise istungi. 27. aprill. https://valitsus.ee/et/uudised/vabariigi-valitsus-ja-kriisikomisjon-pidasid-erakorralise-istung (Viimati külastet: 17.05.2015).
101. Vabariigi Valitsus. 2007. Valitsuse pressikonverentsi stenogramm 03.05.2007. 3. mai. https://valitsus.ee/et/uudised/valitsuse-pressikonverentsi-stenogramm-03052007 (Viimati külastet: 17.05.2015).
102. Vabariigi Valitsus. 2007. Valitsuse pressikonverentsi stenogramm. 26. aprill. https://valitsus.ee/et/uudised/valitsuse-pressikonverentsi-stenogramm-26042007 (Viimati külastet: 17.05.2015).
103. Vabariigi Valitsus. 2007. Valitsuse pressikonverentsi stenogramm. 10. mai. https://valitsus.ee/et/uudised/valitsuse-pressikonverentsi-stenogramm-10052007 (Viimati külastet: 17.05.2015).
104. Vabariigi Valitsus. 2007. Välisministri avaldus. 1. mai. https://valitsus.ee/et/uudised/valisministri-avaldus (Viimati külastet: 17.05.2015).
105. Vabariigi Valitsus. 2013. Küberjulgeoleku strateegia. 20. august. https://valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf (Viimati külastet: 17.05.2015).
106. Wingfield, Thomas ja Tikk, Eneken. 2010. "Framework for International Cyber Security: The Cube, the Pyramid, and the Screen." In *International Cyber Security. Legal & Policy Proceedings*, eds. Eneken Tikk ja Anna-Maria Talihärm. Tallinn: CCD COE, 16–22.

107. Välisministeerium. 2007. EL lubas abi olukorra normaliseerimiseks Eesti-Moskva saatkonna ümber. 1. mai. http://vm.ee/et/uudised/el-lubas-abi-olukorra-normaliseerimiseks-eesti-moskva-saatkonna-umber (Viimati külastet 17.05.2015).

108. Välisministeerium. 2007. Leedu välisminister avaldas Eestile toetust. 2. mai. http://vm.ee/et/uudised/leedu-valisminister-avaldas-eestile-toetust (Viimati külastet 17.05.2015).

109. Välisministeerium. 2007. Makedoonia avaldas Eestile toetust. 1 mai. http://vm.ee/et/uudised/makedoonia-avaldas-eestile-toetust (Viimati külastet 17.05.2015).

110. Välisministeerium. 2007. Välisministeeriumi kodulehekülg on taas kättesaadav. 29. aprill. http://vm.ee/et/uudised/valisministeeriumi-kodulehekulg-taas-kattesaadav-koigile (Viimati külastet 17.05.2015).

111. Välisministeerium. 2007. Välisminister ei kohtu riigiduuma saadikutega. 1.mai. http://vm.ee/et/uudised/valisminister-ei-kohtu-riigiduuma-saadikutega (Viimati külastet 17.05.2015).

112. Välisministeerium. 2007. Välisminister tänas Rootsi välisministrit toetuse eest. 30. aprill. http://vm.ee/et/uudised/valisminister-tanas-rootsi-valisministrit-toetuse-eest (Viimati külastet 17.05.2015).

113. Välisministeerium. 2007. Välsiminister tänas Lätit ja Leedut toetuse eest. 27. märts. http://vm.ee/et/uudised/valisminister-tanas-latit-ja-leedut-toetuse-eest (Viimati külastet 17.05.2015).

114. Välisnimisteeriumi uudised. http://vm.ee/et/uudised (Viimati külastet: 17.05.15).

115. Õigusabitaotluse kriminaalsasjas nr 00700000033. 10.05.2007, nr RP-2-12/07/842.

116. Yasmann, Victor. 2007. "Monument Dispute With Estonia Gets Dirty." *Radio Free Europe. Radio Liberty* May, 8. http://www.rferl.org/content/article/1347550.html (Viimati külastet: 17.05.15).

Summary

"Estonian foreign policy behaviour and decision-making in the context of 2007 cyber attacks"

As technology has been developing, new threats have been developing simultaneously. Old concepts are not sufficient anymore when providing security. Interested parties are trying to figure out new concepts that could work. Nevertheless one-size-fits-all kind of concepts are not useful when it comes to state behaviour. The reason for it being that states have too different ambitions and goals, therefore acting often unexpectedly, causing various consequences that are hard to foresee.

This thesis is an attempt to show how one state has acted in case of cyber attacks. What were the political, technical and legal measures it took? What was the procedure of decision-makers? In order to try to answer these questions, the author has taken a comprehensive approach named the Cube, the Pyramid, and the Screen that is explained in the first paragraph. With the help of the concept, the background conditions are being laid out – first, the technical events, then political reactions – that are divided between the second and third paragraphs and are preconditions for the main paragraph in which the measures are being classified and conclusions made.

Main findings are that as Estonia used technical, political and as well legislative measures to stop the attacks the particularly successful ones were foreign political measures. How else to explain that a small state is one of the members in the Group of Governmental Expertise of the First Committee in the United Nations or working together on cyber security countermeasures in OSCE or that Estonia is ranked as one of the top states when it comes to cyber security.

The main thesis outcome is as follows: although every measure can be effective in its own way, it also has its own defaults and limitations. For example, technical measures are just a quick way for a solution, meaning they are effective in the short run but in the long run it is not enough to fight ongoing attacks. Whereas political measures are not binding and legislative measures are too time consuming to take an effect when needed. So it is highly

necessary to use them all together in order to achieve the maximum impact when resolving the cyber attacks.

Measures that Estonia used are not one and only choice for managing a conflict. There are more available options that are suitable for a specific state. Hence, the main conclusion is that it all comes down what the state wants to achieve and what is its political agenda.

In the end, the author finds that further research in the field is necessary. Cyber threats are not going away any time soon if ever and attackers are continuously trying to find better and easier ways to achieve their political goals or earn profit.