Tartu Ülikool
Tartu Ülikooli humanitaarteaduste ja kunstide valdkond
Ajaloo ja arheoloogia instituut
Uusima aja õppetool

Henry Narits

**NATO küberkaitsestrateegiad aastatel 2007-2015**

Bakalaureusetöö

Juhendaja: dotsent Vahur Made, PhD

Tartu 2017

**SISUKORD**

# TERMINOLOOGIAT

**CERT** – Ekspertgrupp spetsialiste, kes tuvastavad, jälgivad ja lahendavad arvutivõrkudes toimuvaid turvaintsidente ning teavitavad võimalikest ohtudest ja korraldavad ennetustegevusi.

**DDoS rünnak** – rünnak, kus arvutivõrke rünnatakse massiivselt informatsiooniga selleks, et need ülekoormata ja muuta kasutuskõlbmatuks ülejäänud kasutajatele.

**Küberekspluateerimine** – rünnak, kus üritatakse salaja saada informatsiooni teistest arvutitest või võrkudest.

**Küberkuritegu** – eraisiku poolt korraldatud või organiseeritud rünnak teise riigi avaliku- või erasektori vastu, mille eesmärk on varastada tundlikku informatsiooni kaubandusliku, poliitilise või sõjalise kasu saamiseks.

**Küberspionaaž**– riigi poolt korraldatud või organiseeritud rünnak teise riigi avaliku- või erasektori vastu, mille eesmärk on varastada tundlikku informatsiooni kaubandusliku, poliitilise või sõjalise kasu saamiseks.

**Küberterrorism** – rünnak, millel on samasugune mõju nagu traditsioonilisel terroriaktil.

# SISSEJUHATUS

Põhja-Atlandi Organisatsiooni (NATO) mõju Euroopa kaitsele alates tema loomisest 1949. aastal on andnud hindamatu mõju tänapäevase Euroopa poliitilisele korraldusele. Pärast Nõukogude Sotsialistlike Vabariikide Liidu lagunemist võis NATO kaotada oma pealmine oponendi, aga lisaks teistele riiklikele tegutsejatele hakkasid pead tõstma erinevad asümmeetrilised ohud, nagu näiteks terrorism, bioloogiliste ja keemiliste massihävitusrelvade levik ja sealhulgas ka küberrünnakud. Sarnaselt tuumarelvadele suudavad küberrelvad tänapäeval ohustada Euroopa heaolu seades seeläbi ohtu rahvusriikide julgeoleku[1]. Lisaks sellele tänapäeval aina suurem sõltuvus erinevatest kommunikatsioonivahenditest, internetivõrkudest ja digitaalsetest süsteemidest tähendab seda, et nüüdisajal on sisuliselt mõeldamatu, et relvastatud konflikti või laiemalt sõja seisundis olles ei kasutataks kõiki võimalusi, mida pakub meile internet, olgu selleks luureinfo varastamine või vastaspoole kaitsevõime häirimine[2]. Võttes arvesse käesoleva valdkonna kiiret arengut ning potentsiaalset ohtlikkust on mõistetav, et NATO peab käesolevale valdkonnale tähelepanu pöörama ning käima ajaga kaasas või olema isegi sammu ees selleks, et stabiilselt tagada oma liikmete turvalisus.

Erinevaid asümmeetrilisi ohte ei saa aga käsitleda üks-ühele nagu klassikalisi võimalikke vaenlasi ehk teisi riike. Näiteks küberrünnaku läbiviimine võrreldes traditsioonilise rünnakuga võib olla kiirem ja odavam ning ei sea ohtu rünnaku teostajat, kuna rünnak võib saada alguse ükskõik millisest maailma servast ning tihti on isegi võimatu rünnaku toimepanijat selgelt tuvastada. Selliste vahendite suurem kättesaadavus ning teadmiste omandamine ja rakendamine võib ohtu seada Euroopat ja Põhja-Ameerikat ning sobib oma olemuselt ideaalselt erinevatele mitte riiklikele tegutsejatele[3]. Võttes arvesse küberrünnakute anonüümsust ja globaalset omadust, siis on oht, et küberrünnakud võivad tulevikus saada kriminaalide ja terroristide seas eelistatud lahinguväljaks ning muutuda suuruselt teiseks ohuks rahvusriikidele[4]. NATO jaoks on just globaalne omadus oluline probleem, kuna kui rünnak pärineb selgelt väljastpoolt Põhja-Atlandi regiooni, siis tekib küsimus, kuidas peaks NATO sellele reageerima, et tagada oma liikmete nii passiivne kui

[1] Stephen Herzog. (2011). Revisiting the Estonian Cyber Attacks:
Digital Threats and Multinational Responses. Journal of Strategic Security. Vol 4, nr 2, lk 51.
[2] Schmitt, Michael N. (2015). The law of cyber targeting. Naval War College Review. Vol 68, nr 2, lk 12.
[3] Georgescu, Constantin. Tudor, Monica. (2015). Cyber terrorism threats to critical infrastructures
NATO's role in cyber defense. Knowledge Horizons / Orizonturi ale Cunoasterii. Vol 7, nr 2, lk 117.
[4] Seal samas.

ka aktiivne kaitse. See omakorda tõstatab küsimuse, kuidas vajadusel rakendada isegi oma kollektiivkaitse artiklit, mille ümber allianss on loodud. Asümmeetriliste ohtude suuremat probleemi on tunnistanud ka NATO ise, tuues 2010. aastal toimunud Lissaboni tippkohtumise deklaratsioonis välja, et tõenäosus, et mõni riik ohustab NATO liikmesriike läbi traditsioonilise rünnaku on madal ning seeläbi tuleb enim tähelepanu pöörata asümmeetrilistele ohtudele[5].

NATO küberkaitsestrateegiate juured ulatuvad eelmise sajandi vahetusse lõppu, kui sekkudes 1999. aastal Kosovo kriisi sattusid nii NATO kui ka operatsioonis osalevate alliansi liikmete valitsuste veebilehed küberrünnakute alla. Käesolev kogemus sundis NATO't juba järgneval tippkohtumisel, ehk 2002. aastal toimunud Praha tippkohtumisel, sõnastama oma esimesed seisukohad, mille alusel sai kübervõimekuse arendamine alguse. Sõltumata sellest varajasest reageerimisest uutele tekkivatele ohtudele, siis NATO kõige aktiivsem tegutsemiseperiood jääb siiski ajavahemikku 2007-2015. Sellele avaldasid suurt mõju 2007. aasta küberrünnakud Eesti valitsuse, meediaväljaannete ja erasektori vastu ning 2008. aasta augustis alanud Venemaa-Gruusia vaheline sõda, kus Gruusia vastu tehtud küberrünnakutest võis saada aimu, et milline näeb tulevikus välja hübriidsõda, kus samaaegselt tulistavad kineetilised- ja küberrelvad.

Käesolev uurimustöö keskendub NATO küberkaitsestrateegiate osas just tegevuste poolest niinimetatud kõige aktiivsemale perioodile, mis sai alguse pärast 2007. aasta sündmusi Eestis ja 2008. aasta omasid Gruusias. Samuti toob välja, et miks on võimalik just seda perioodi kutsuda aktiivsemaks kuigi tegelikult juba esimesi samme võis näha Praha tippkohtumise ajal 2002. aastal. Uurimise all on seeläbi nii poliitilised kui ka institutsionaalsed protsessid, mis on olnud suunatud NATO küberkaitse poliitikaloomele ja on seeläbi ka antud protsessi suuremad takistuskivid ning kuidas ja millal on need lahendatud. Antud uurimustöö eesmärk ei ole anda hinnang, kas aasta 2015 lõpuks on NATO turvaline ning suuteline tõrjuma küberrünnakuid teistelt riikidelt või asümmeetrilistelt ohtudelt, vaid olemasoleva informatsiooni põhjal tuua välja teatud murekohti, mis on käesoleva teema uurimisel korduva mustriga silma jäänud. Siinjuures rõhutatakse NATO suuremaid saavutusi, nagu näiteks efektiivse heidutuse loomist, koostöö edendamist NATO ja tema liikmesriikide vahel ning küberrünnakute juriidilist defineerimist. Ülesehituselt on

[5] North Atlantic Treaty Organization. (2010). Active engagement, modern defence: strategic concept for the defence and security of the members of the North Atlantic Treaty Organisation adopted by heads of state and government in Lisbon. North Atlantic Treaty Organization. 19.11.2010. Kasutatud. 28.03.2017. www.nato.int/cps/en/natolive/official_texts_68580.htm

antud töö jagatud kronoloogiliselt alustades 2002. aasta Praha tippkohtumisega ja lõpetades 2014. aastal Walesis toimunud sündmusega, tuues seeläbi kommenteeritult välja kõigi tippkohtumiste tähtsamad küberkaitsega seotud punktid. Lisaks sellele käsitletakse olulisemaid küberrünnakuid, mis on enim mõjutanud NATO poliitikat ja samuti on eraldi peatükk NATO Kooperatiivse Küberkaitse Kompetentsikeskusest Eestis ning "Tallinna käsiraamatust", et tuua esile nende tähtsust NATO'le ja antud teemale.

Historiograafiliselt tuleb arvestada, et kuna antud teemakäsitlus keskendub väga hiljutistele sündmustele, siis sellest tulenevalt on erinevate teadusartiklike arv tavapärasest väiksem ja on kasutatud ka mitmeid ajakirjanduslike väljaannete kirjutisi. Olulisteks allikateks on loomulikult olnud NATO enda avalikud dokumendid, siinhulgas nii tippkohtumiste deklaratsioonid kui ka muu dokumentatsioon, mis on antud teemaga seotud. NATO iga-aastased tippkohtumised on väga mitmetahulised sündmused, kus hinnatakse terve organisatsiooni tegevust ja analüüsitakse uusi probleeme ning mõtestatakse, kuidas NATO peaks nende kontekstis käituma ja lisaks sellele peaks iga üritus süvendama transatlantilise organisatsiooni ühiseid põhimõtteid ja koostööd[6]. Võrreldes NATO "Strateegiliste kontseptsioonidega", mis seab arengusuunad järgnevaks kümnendiks, annavad tippkohtumiste deklaratsioonid ülevaate kohapeal loodud uutest poliitilistest sammudest ning NATO aktuaalsematest probleemidest ja nendele lahendusi leidvast poliitikast[7].

NATO enda dokumentatsiooni suurim probleem tuleneb aga nende käsitletavast toonist, kus lubatakse olukorda parandada, viimistleda ja paremale tasemele viia. Tutvudes aga erinevate teadusartiklitega, siis nende analüüsist paistab küberkaitse seisukohalt välja tihti kriitilisem toon. Näiteks Häly Laasme toob mitmel korral hästi esile progresse, mis NATO on teinud, aga nende kõrval toob välja varjukülje, et tegevus võttis aega 20 aastat[8]. Samasugune tõdemus käib läbi ka Gergely Szentgáli ja Joe Burtoni vastavatest artiklitest. Samas neid teoseid, mis on selgelt keskendunud ainult küberstrateegiatele on piiratud ning needki on tihti seotud mõne konkreetsema küberruumi valdkonnaga, olgu selleks institutsionaalsed protsessid või näiteks juriidilised probleemid. Antud teemast annavad seepärast ülevaate mitmed analüüsid, mis keskenduvad puhtalt mõnele kindlale tippkohtumisele, nagu seda on

[6] North Atlantic Treaty Organization. (2012). Chicago Summit Declaration. North Atlantic Treaty Organization. Pressiteade (2012) 062. Kasutatud 28.03.2017.
www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en
[7] Georgescu, Constantin. Tudor, Monica. (2015). Cyber terrorism threats to critical infrastructures NATO's role in cyber defense. Knowledge Horizons / Orizonturi ale Cunoasterii. Vol 7, nr 2, lk 118.
[8] Laasme, Häly. (2012). The Role of Estonia in Developing Nato's Cyber Strategy. Cicero Foundation Great Debate Paper. Vol 12, nr 8, lk 12.

teinud autorid Daniel-Nicolae Banica (Walesi tippkohtumine), Timo Noetzel ning Benjamin Schreer (Lissaboni tippkohtumine), Andrew M. Dorman (Chicago tippkohtumine) ja Charles Cati (Praha tippkohtumine). Eelpoolnimetatud autorite kaudu on võimalik saada nendepoolne nägemus tippkohtumistel otsustatust ning alates Bukaresti tippkohtumisest on neistki igaüks rõhutanud või toonud välja seda, millega tegeleti küberkaitsepoliitika osas, kuigi ükski nendest ei keskendu antud teemale eksklusiivselt. Samamoodi leiab küberkaitse käsitlust ka nendes tekstides, mis käsitlevad NATO uut "Strateegilist kontseptsiooni", nagu seda on teinud David Y. Josti. Enamikele kasutatavatele allikatele pääseti ligi tänu EBSCO arhiivile. Käesolevat tööd kirjutades tuleb samuti mõista, et informatsioon ei ole avalik. Seepärast räägitakse käesolevas uurimustöös dokumentidest, nagu näiteks NATO Küberkaitse Kontseptsioon (*NATO Cyber Defence Concept)* ja NATO Küberkaitsepoliitika (*NATO Cyber Defence Policy*), aga kuna avalik ligipääs neile puudub, siis nende täpset sisu on keeruline uurida.

# 1. KOSOVO KRIIS

Maailma üks tuntumaid ja enim esile toodud küberrünnakuid oli 2007. aastal toimunud rünnak, mis oli suunatud Eesti valitsuse, meediaväljaannete ja erasektori vastu. Kuigi seda on tihti esile toodud sündmusena, mis avas maailma silmad potentsiaalsetele kübervaldkonnaga seotud ohtudele, siis NATO enda tegevus saab alguse 2002. aastal toimunud Praha tippkohtumisega ning sellele eelnenud sõjalisele sekkumisele 1999. aastal Kosovos. Just Kosovos joonistusid välja tol hetkel NATO jaoks kõige olulisemad prioriteedid oma kübervõimekuse arendamiseks vastavalt seal saadud kogemustele.

1999. aasta märtsikuus sekkusid NATO väed ÜRO mandaati omata Kosovo kriisi ning alustasid õhuoperatsioone Slobodan Miloševići vägede vastu[9]. Mandaadita sekkumine tekitas rahvusvahelises kogukonnas käesolevale operatsioonile vastuseisu, aga sellest sõltumata jätkusid need kuni 1999. aasta juunikuuni. Käesolevatele õhurünnakutele vastukaaluks alustasid Serbia päritolu organisatsioon Must käsi *(Black hand)* vahetult pärast NATO tegevuse algust omapoolseid rünnakuid NATO struktuuride vastu, mis olid just küberrünnakud[10]. Nende tegevuse tulemusena olid häiritud näiteks NATO enda veebileht, kaasaarvatud just see osa, mis õigustas Kosovosse sõjaliselt sekkumist ning põhjendas selle vajalikkust[11]. Samaaegselt olid segatud erinevad NATO teenused, nagu näiteks olid mitmeks päevaks häiritud e-posti kasutamise võimalused[12]. Pealegi on välja toodud, et Must käsi üritas ligi pääseda ka NATO andmebaasidele ja seeläbi varastada tundlikku informatsiooni, aga nende suurim saavutus oli ligipääs NATO õhuvägede arvutivõrkudele, kuid informatsiooni nad NATO väidete kohaselt kätte ei saanud[13].

NATO pommitamisoperatsioonide ägenedes tulistati kogemata Hiina Demokraatliku Rahvavabariiki saatkonda Belgradis, mille tulemusel said surma kolm seal viibinud ajakirjanikku. Selle tagajärjel hakkasid küberrünnakud NATO vastu ägenema ning üheskoos Vene päritolu häkkeriorganisatsiooniga Venemaalt armastusega (*From Russia with love*), suudeti häirida lisaks NATO enda veebilehele veel 14 erineva valitsuse veebivõrke kuni

[9] Szentgáli, Gergely. (2013). The NATO Policy on Cyber Defence: The Road so Far. Academic & Applied Research in Military & Public Manageme. Vol 12, nr 1, lk 1.
[10] Seal samas.
[11] Burton, Joe. (2015). NATO's cyber defence: strategic challenges and institutional adaptation, Defence Studies. Vol 15, nr 4, lk 305.
[12] Georgescu, Constantin. Tudor, Monica. (2015). Cyber terrorism threats to critical infrastructures NATO's role in cyber defense. Knowledge Horizons / Orizonturi ale Cunoasterii. Vol 8, nr 2, lk 116.
[13] Szentgáli, Gergely. (2013). The NATO Policy on Cyber Defence: The Road so Far. Academic & Applied Research in Military & Public Manageme. Vol 12, nr 1, lk 1.

Kosovo operatsiooni lõpuni[14]. Sealhulgas võeti maha Ameerika Ühendriikide Valge maja veebileht kolmeks päevaks[15].

Kuigi käesoleva rünnaku mõju lahingutegevusele Balkanil oli hinnanguliselt madal, siis näitas see esimest korda potentsiaalset haavatavust ning võimalikke tulevasi uusi ohte. Eelkõige tõi see esile, et küberruumis toimuv ei ole vaid privilegeeritud suurematele, jõukamatele ja tehnoloogiliselt enim arenenud riikidele vaid antud keskkonnas võivad olla tugevateks tegutsejateks ka väiksemad rühmitused. See tõstatas NATO's küsimuse ning püsistas probleemi, kuidas oma võrke tulevikus turvalisemaks muuta ning selgeid samme on võimalik näha juba vahetult Kosovo kriisile järgnenud esimesel korralisel tippkohtumisel Prahas[16]. Põhjus, miks Kosovo kriisist ei saanud omaaegselt suurt äratust ning NATO küberkaitsestrateegiad ei hakanud valmima, oligi just sellepärast, et neid küberrünnakuid nähti väikese probleemina, mis vajasid vähest ressursside ümberpaigutamist ja ei mõjutanud esmapilgul ei sõjalist operatsiooni kohapeal ega NATO teadvustamistöid konflikti olulisusest ning sekkumise põhjustest[17].

## 2. PRAHA TIPPKOHTUMINE

Praha tippkohtumisele läks NATO vastu sisemises lõhes, kus mitmes erinevas valdkonnas tegeleti omavahel tugevalt eristuvate tegevustega. Ühelt poolt kutsus USA oma liitlasi võitlusesse terrorismiga ning kui Euroopa riigid oleksid kõrvale jäänud, oleks see võib-olla tekitanud lõhe NATO suurima rahastaja ja ülejäänud liikmesriikide vahel[18]. Tänapäeval tagasi vaadates toimusid Praha tippkohtumise eel kaks omavahel vastukäivat protsessi. Ühelt poolt oli laual võimalus võtta mitmed Ida- ja Kesk-Euroopa riigid oma liikmeskonda ning teisena arendati aina soojemaid suhteid Venemaaga, kellega toimusid tippkohtumise ajal ka läbirääkimised tulevase koostöö osas[19]. Seeläbi oli õhus küsimus, milline võib NATO tulevikus üleüldse välja näha pärast Ameerika Ühendriikide vastu tehtud terrorirünnakut ning võimalike uute ohtude kasvu Lähis-Ida piirkonnas. Seeläbi ka küsimus, kas on võimalik

[14] Szentgáli, Gergely. (2013). The NATO Policy on Cyber Defence: The Road so Far. Academic & Applied Research in Military & Public Manageme. Vol 12, nr 1, lk 1.
[15] Messmer, Ellen. (1999). Kosovo cyber war intensifies: Chinese hackers targeting U.S. sites, government says. CNN. 12.05.1999. Kasutatud 21.04.2017.
http://edition.cnn.com/TECH/computing/9905/12/cyberwar.idg/
[16] Journal of International Affairs. (2016). Is cyber defense possible? Journal of International Affairs. Vol. 70, nr 1, lk 185.
[17] Georgescu, Constantin. Tudor, Monica. (2015). Cyber terrorism threats to critical infrastructures NATO's role in cyber defense. Knowledge Horizons / Orizonturi ale Cunoasterii. Vol 8, nr 2, lk 116.
[18] Gati, Charles. (2002). All That NATO Can Be: To Prague and Beyond. The National Interest. Vol 68, lk 86.
[19] Seal samas.

edendada Venemaaga sõbralikke suhteid, kui NATO piir ulatuks tulevikus Venemaa riigipiirini.

Praha tippkohtumise suuremate teemade varjus on lihtne kahe silma vahele jätta asjaolu, et seal võeti vastu mitmeid punkte seoses enda küberkaitse arendamisega ning läbi seal vastu võetud otsuste tegeles allianss esimest korda küberruumiga seotud küsimusega konkreetsemalt ja see kõik toodi välja ka kohtumise lõppdeklaratsioonis. Seeläbi lubati tulevikus pühendada oma küberkaitse võimekuse arendamisele, kuid selle lausega tekstiosa piirduski ning tegelikult ei olnud see deklaratsioonis isegi eraldi paragrahvina ega peatükina[20]. Prahas vastu võetud NATO Küberkaitseprogramm (*NATO Cyber Defence Program*) oli järgmine oluline samm ning selle üks esimesi programmilisi tegevusi oli algatada uue institutsioonina NATO Võrkude Küberkaitse Üksus (*NATO Computer Incident Response Capability, NCIRC)*[21]. NCIRC'i eesmärgiks sai ennetada DDoS rünnakuid NATO võrkude suunas ning luua seeläbi efektiivsem kaitse. Selle saavutamiseks tuli koordineerida paremini omavahelist koostööd, jälgida reaal-ajas võimalikke ohte ja korraldada paremini infovahetust nendest ohtudest[22]. Samuti kutsuti deklaratsioonis NATO't üles kasutama kõige moodsamat tehnoloogiat selleks, et kaitsta ennast küberrünnakute eest ning looma ühiseid CERT'i meeskondi[23].

Praha tippkohtumine on teistele rahvusvahelistele organisatsioonidele kindlasti eeskujuks. See näitab, kuidas üks organisatsioon peaks reageerima uutele väljakutsetele ning nendega toime tulema. Seeläbi poliitilised ja institutsionaalsed protsessid, mis Prahas algatati, olid tugevaks näitajaks, et NATO on valmis tagama oma transatlantilise ühenduse turvalisust ning on kiire otsustusvõimega[24]. Teiselt poolt ei olnud vastu võetud otsused eksklusiivselt suunatud just küberkaitse loomiseks, vaid olid seotud suurema otsustepaketiga, mis tegelikult oli üldse seotud eelkõige terrorismiga võitlemiseks, mis pärast 11. septembri sündmusi aastal 2001 olid NATO'le üheks suurimaks väljakutseks[25]. Samuti mitmed ettepanekud olid suunatud pigem NATO enda internetivõrkude turvalisemaks muutmiseks

[20] NATO Public Diplomacy Division. (2002). The Praegue Summit and NATO's Transformation. NATO Public Diplomacy Division. Kasutatud 03.04.2017. www.nato.int/docu/rdr-gde-prg/rdr-gde-prg-eng.pdf
[21] Burton, Joe. (2015). NATO's cyber defence: strategic challenges and institutional adaptation, Defence Studies. Vol 15, nr 4, lk 305.
[22] Hughes, Rex B. (2009). NATO and Cyber Defence. Mission Accomplished. Atlantische Commissie. Kasutatud 03.04.2017. www.atlcom.nl/ap_archive/pdf/AP%202009%20nr.%201/Hughes.pdf
[23] Ashmore, William C. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review. Vol 11, nr 1, lk 13.
[24] Seal samas.
[25] NATO Public Diplomacy Division. (2003). The Praegue Summit and NATO's Transformation. NATO Public Diplomacy Division. Kasutatud 03.04.2017. www.nato.int/docu/rdr-gde-prg/rdr-gde-prg-eng.pdf

ja seeläbi jäeti NATO liikmed ise omapäi hakkama saama ning seeläbi neile abikätt ei ulatatud[26].

Kuigi siinkohal oleks võinud eeldada, et järgnevatel tippkohtumistel hakkab NATO aina rohkem tähelepanu pöörama oma küberkaitse arendamisele seoses käesoleva ohu iga aastase kasvuga, siis tegelikult läks vastupidi. Kaks aastat hiljem toimunud Istanbuli tippkohtumise deklaratsioonis, või dokumentatsioonis laiemalt, ei leidu punkte, mis täiendaksid Prahas otsustatut või algataksid uusi projekte. 2006. aastal toimunud Riia tippkohtumine on sellevõrra konkreetsem, kuna sündmuse lõppdeklaratsioonis vähemalt mainitakse küberrünnakutega seotud teemasid kuigi nad on jälle osakene suuremast teemavaldkonnast, mille eesmärk on võidelda uute kasvavate ohtudega. Seeläbi tuuakse Riias välja, et selleks, et kaitsta ennast küberrünnakute eest, on vaja teha kiiret koostööd ning regulaarselt nii uuendada kui ka edasi arendada oma olemasolevaid kaitsemeetmeid[27]. Riia tippkohtumise järel jätkus siiski laiemalt NATO poliitika, kus esiprioriteetideks olid NATO'l enda infrastruktuuri kaitse tagamine ning liikmesriikidele pöörati vähem tähelepanu[28]. Seeläbi jäid jätkuvalt tahaplaanile liikmesriikide vajadused ning ühise kaitsevõrgu kujundamine, mis tõusis päevakorda Riiast mitte nii kaugel juba aasta aega hiljem, kui selle vajaduse tõi selgelt esile Eesti vastu tehtud küberrünnak 2007. aastal.

## 3. 2007. AASTA KÜBERRÜNNAKUD EESTI VASTU

NATO küberkaitsestrateegiate ühe suurima teerajajana on tihti esile toodud 2007. aastal aset leidnud küberrünnakuid Eesti vastu, mis toimus paralleelselt Tallinnas aset leidnud meeleavaldusega Pronkssõduri eemaldamiseks eelkõige venekeelse elanikkonna poolt. Pronkssõdurist tulenevad probleemid olid juba aastakümneid Eestis aktuaalsed olnud. Ühtedele sümboliseeris see Eesti vabastajaid, teistele okupeerijaid ning olukorda ei teinud lihtsamaks igal aastal toimunud suursündmused 9. mail ja 22. septembril, mis igal aastal tõstatasid uuesti päevakorda antud monumendi asukoha Tallinna kesklinnas ning ühtlasi lõppesid rohkem kui ühel korral vägivaldselt[29]. Kui nüüd 27. aprillil otsustas Eesti valitsus käesoleva monument eemaldada, siis puhkesid tänavatel meeleavaldused ning paralleelselt

[26] Szentgáli, Gergely. (2013). The NATO Policy on Cyber Defence: The Road so Far. Academic & Applied Research in Military & Public Manageme. Vol 12, nr 1, lk 1.
[27] North Atlantic Treaty Organization. (2006). Riga summit declaration. North Atlantic Treaty Organization. Pressiteade (2006) 150. Kasutatud 03.04.2017. www.nato.int/docu/pr/2006/p06-150e.htm
[28] Burton, Joe. (2015). NATO's cyber defence: strategic challenges and institutional adaptation, Defence Studies. Vol 15, nr 4, lk 306.
[29] Rantapelkonen, Jari. Salminen, Mirva. (2013). Victory in Exceptional War: The Estonian Main Narrative of the Cyber Attacks in 2007. Alenius, Kari. The Fog of Cyber Defence, lk 79. Tampere. Juvenes Print Oy.

toimusid ka küberrünnakud valitsuse asutuste ning mitmete meediaväljaannete ja erakondade vastu[30].

9. mail alanud küberrünnakud Eesti suunal ei kasutanud moodsat või varasemalt mittetuntud tehnoloogiat vaid DDoS rünnakutega üritati sulgeda Eesti IT sektor ning esimeses etapis olid rünnakud selles vallas edukad[31]. Selle tulemusena hakati mitmeid veebilehti, mida tavapäraselt külastati kuni 1000 korda päevas järsult külastama 2000 korda sekundis ja sellega muudeti nende kasutamine võimatuks[32]. Niinimetatud Eesti vastaste patriootlike venelaste poolt läbiviidud rünnakute tulemusena olid erinevad teenused häiritud kuni kolmeks nädalaks ning selle aja jooksul suudeti erinevaid rünnakuid toime panna 178 riigist ning umbkaudu ühest miljonist erinevast arvutist[33]. Kuigi rünnakute tulemusel ei tehtud permanentset kahju infrastruktuurile, siis suudeti ikkagi päevadeks maha võtta valitsuse jaoks olulised veebilehed ja infokanalid selleks, et takistada suhtlust väljapoole ja jagada infot kohapeal toimuvast[34]. Samas tuleb arvesse võtta, et mõnes teises riigis, mis ei ole nii hästi ettevalmistunud kui Eesti, võib küberrünnak lõppeda sellega, et riik kaotab kontrolli oma elektrijaamade, veepumpade või ka relvasüsteemide üle[35].

Kuigi Eesti suunal toimunud küberrünnakud polnud esimesed seesugused maailmas, olid need võrreldes näiteks Kosovo küberrünnakutega, mille eesmärk oli valeinformatsiooni levitamine ning tundlikku informatsiooni varastamine, esimestena selgelt suunitletud selleks, et nõrgestada ja seada ohtu ühe riigi julgeolek[36]. Juba pikalt enne 2007. aastat arendas Eesti jõudsalt välja paberivaba valitsuse ja e-riigi lahendusi ning tegi nende rakendamises suuri edusamme, mis tähendas, et võrreldes mõne teise riigiga oli Eesti sõltuvus erinevatest internetiteenustest suurema kaaluga, mis muutis Eesti ahvatlevaks sihtmärgiks võimalikele küberrünnakute seoses võimalusega teha rohkem kahju[37]. Ühtlasi

[30] Ashmore, William C. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review. Vol 11, nr 1, lk 6-7.
[31] Seal samas, lk 7.
[32] Stephen Herzog. (2011). Revisiting the Estonian Cyber Attacks:
Digital Threats and Multinational Responses. Journal of Strategic Security. Vol 4, nr 2, lk 53.
[33] Joshua Davis. (2007). Hackers Take Down the Most Wired Country in Europe. Wired Magazine. 21.09.2007. Kasutatud 14.05.2017. www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=1
[34] Ashmore, William C. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review. Vol 11, nr 1, lk 8.
[35] Stephen Herzog. (2011). Revisiting the Estonian Cyber Attacks:
Digital Threats and Multinational Responses. Journal of Strategic Security. Vol 4, nr 2, lk 52.
[36] Ashmore, William C. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review. Vol 11, nr 1, lk 4.
[37] Stephen Herzog. (2011). Revisiting the Estonian Cyber Attacks:
Digital Threats and Multinational Responses. Journal of Strategic Security. Vol 4, nr 2, lk 51.

oli tegu ühe enim meediakajastust saanud küberrünnakuga 2007. aastal, mis hilisemalt aitas kaasa käesoleva teema aktualiseerimisele.

Käesolevate küberrünnakute võimalike süüdlaste tuvastamine algas juba vahetult pärast rünnakute algust ning sellega algas Eesti ja Venemaa omavaheline süüdistuste loopimine, kus nii Eesti valitsus kui ka meedia tituleerisid Venemaa nende rünnakute süüdlaseks enne, kui suudeti seda korralikult tõestada[38, 39]. Ühelt poolt oli see rutakas reaktsioon, kuna tänapäevani ei ole ei Euroopa Liit ega NATO leidnud vettpidavaid tõendeid, mis tõestaksid Venemaa valitsuse osalust, kuid teiselt saab teoretiseerida, et kelle huve selline küberrünnak võiks kõige paremini teenida ning sellisel juhul kõige tugevam kandidaat oleks just Venemaa[40]. Kui võtta arvesse käesolevate rünnakute mastaapsust, siis on raske uskuda, et hobihäkkerid oleksid olnud suutelised sellist rünnakut läbi viima ning nende rünnakute ajastus viitab samuti kaudsele suuremale koordineeritusele, nagu oli ka meelerahutus Tallinna vanalinnas ise[41]. Kuigi lõpuks võtsid süü enda peale kremlimeelne noorteorganisatsioon Našhi, siis see sisuliselt ei muutnud olukorda paremaks. Käesolevat noorteorganisatsiooni rahastavad ettevõtjad, kes toetavad Venemaa valitsust ja niimoodi suudab Kreml näiliselt eristada ennast käesolevast noorteorganisatsioonist ja kaudselt jätta mulje, et nad pole omavahel seotud[42]. Samuti ei järgnenud Venemaal nende suhtes mingisuguseid sisulisi karistusi.

Sarnast käekirja, kus mitmeid riike on tabanud just samalaadsed küberrünnakud kaudselt sarnastes olukordades, võib märgata mujalgi. Leedu vastu toimusid küberrünnakud 2008. aastal pärast seda, kui võeti vastu seadus, mis keelas ära Nõukogude Sotsialistlike Vabariikide Liidu ja kommunistliku sümboolika laiemalt ning olukorra tegi ainult keerulisemaks Venemaa ja Leedu vaheline külmenenud suhtlus seoses sellega, et Leedu takistas Euroopa Liidu ja Venemaa vahelisi läbirääkimisi, kuna Venemaa keeldus tasumast Leedu küüditatutele reparatsioone[43]. 2008. aastal sattusid ka Gruusia valitsuse veebilehed

[38] Ashmore, William C. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review. Vol 11, nr 1, lk 8.
[39] Stephen Herzog. (2011). Revisiting the Estonian Cyber Attacks:
Digital Threats and Multinational Responses. Journal of Strategic Security. Vol 4, nr 2, lk 53.
[40] Seal samas.
[41] Rantapelkonen, Jari. Salminen, Mirva. (2013). Victory in Exceptional War: The Estonian Main Narrative of the Cyber Attacks in 2007. Alenius, Kari. The Fog of Cyber Defence, lk 80. Tampere. Juvenes Print Oy.
[42] Ashmore, William C. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review. Vol 11, nr 1, lk 25.
[43] McLaughlin, Daniel. (2008). Lithuania accuses Russian hackers of cyber assault after collapse of over 300 websites. Irish Times. 02.07.2008. Kasutatud 24.04.2017. www.irishtimes.com/news/lithuania-accuses-russian-hackers-of-cyber-assault-after-collapse-of-over-300-websites-1.942155

küberrünnakute alla, kuid viimane oli pigem eellöök kuu aega hiljem algavale Venemaa-Gruusia vahelisele sõjale[44]. Kõrgõzstaniga juhtus sarnane situatsioon 2009. aastal, kui viimane ei andnud järgi Venemaa nõudmistele ja lubas jätkuvalt Ameerika Ühendriikide vägedel kasutada üht Kõrgõzstani lennuväebaasi, mida ameeriklased kasutasid oma operatsioonide elluviimiseks Afganistanis[45]. Ühtlasi on seesugune käekiri silma paistnud hiljem, näiteks 2014. aasta alguses enne Venemaa ja Ukraina vahelist sõjalist konflikti, kui juba siis toimusid Ukraina vastu DDoS rünnakud, valeinformatsiooni levitamise kampaaniad ning tundlike andmete vargused[46]. Samal aastal toimusid NATO peakeskuse suunas mitmed küberrünnakud, mis toimusid pärast seda, kui NATO liikmesriigid mõistsid hukka Ukrainas toimuva sõjalise konflikti ning ühtlasi toimusid sarnased rünnakud Walesis aset leidnud tippkohtumise ajal aasta teisel poolel[47]. Kõiki neid rünnakuid iseloomustab teatud määral see, et pole kindel, kes on süüdi, aga tihti on viidatud Venemaale, kui võimalike süüdlasele või kaasosalejale või kaudselt kõige suuremale kasusaajale nendest.

2007. aastal toimunud küberrünnak on NATO küberkaitsestrateegiate arendamise kontekstis sama oluline, kui Kosovo mitmed aastat tagasi. Kui Kosovos tunnistas NATO esmakordselt oma võrkude haavatavust ja hakkas sellest tulenevalt keskenduma oma süsteemide tsentraliseeritud kaitsele, siis Eestis toimunud rünnakud tõestasid, et sama tähtis kui oma võrkude arendamine, on ka oma liikmesriikide süsteemide ennatlik kaitse ja paljudel juhtudel järgi aitamine. Eesti näitel nägid 2007. aastal NATO juhid, milline võib tulevikus kübersõda välja näha. Seeläbi ilmnes, et NATO varasem enda süsteemide keskne lahendus ei ole piisav ning samatähtis on oma liikmesriikide keskendumine[48]. Kuigi varasemalt keskendus NATO eelkõige võitlusele terrorismiga, siis Eestis toimunud sündmused tõestasid, et lisaks erinevatele asümmeetrilistele ohtudele võivad julgeolekut negatiivselt mõjutada nii erinevad riiklikult rahastatud organisatsioonid kui ka teised suurriigid ise[49].

[44] Ashmore, William C. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review. Vol 11, nr 1, lk 20.
[45] Seal samas, lk 11-12.
[46] Ducaru, Sorin D. (2016). The cyber dimension of modern hybrid warfare and its relevance for NATO. Europolity. Vol 10, nr 1, lk 18.
[47] Seal samas.
[48] Szentgáli, Gergely. (2013). The NATO Policy on Cyber Defence: The Road so Far. Academic & Applied Research in Military & Public Manageme. Vol 12, nr 1, lk 1.
[49] Burton, Joe. (2015). NATO's cyber defence: strategic challenges and institutional adaptation, Defence Studies. Vol 15, nr 4, lk 306.

# 4. NATO KOOPERATIIVNE KÜBERKAITSE KOMPETENTSIKESKUS EESTIS

Vahetult pärast NATO'ga liitumist tegi Eesti omapoolse ettepaneku, et tuleks luua rahvusvaheline küberkaitsekeskus. Tegu on olnud pika protsessiga, mis sai alguse juba aastal 2003, kui Eesti oli veel läbirääkimisi alles pidamas, et astuda NATO liikmeks[50]. Samuti nägi Eesti oma küberjulgeoleku strateegias vajadust kindlustada sellise keskuse loomine Eestisse ja seeläbi saavutada Eesti otsene ühendus ülejäänud NATO küberkaitsestruktuuridega[51]. Sellise keskuse nii üleüldse loomine kui ka Eestisse toomine muutus aga jällegi aktuaalseks pärast 2007. aasta rünnakuid, kuna eelnevalt ei olnud selget otsust, kuhu see keskus rajada ning sellele konkureerisid lisaks Eestile mitu teist riiki.

2008. aastal panidki Eesti, Itaalia, Hispaania, Slovakkia, Saksamaa, Läti ja Leedu seljad kokku ning lõid üheskoos Tallinna NATO Kooperatiivse Küberkaitse Kompetentsikeskuse (*NATO Cooperative Cyber Defence Centre of Excellence*)[52]. Tegu oli järjekorras kümnenda sarnase asutusega NATO's ja selle eesmärgiks said nii alliansi liikmete küberkaitse võimekuse suurendamine, teadlikkuse tõstmine, koolituste läbiviimine kui ka teadus- ja uurimustöö korraldamine ja läbiviimine[53]. Selline teadus- ja arenduskeskus aitab igapäevapoliitika kujundamisel ning jällegi toob võõrustajariiki ehk Eestisse erinevatele konverentsidele ning seminaridele kokku oma ala küberkaitse eksperte, aidates sellega säilitada Eesti kui antud valdkonna spetsialisti kuvandit[54]. Küberkaitsekeskuse üks positiivseid näiteid on samuti nii "Tallinna käsiraamat" kui ka selle järeltulija "Tallinna käsiraamat 2.0". Samas peab tõdema, et kuigi käesoleva asutuse nimetuses on sees NATO, ei tähenda see, et kõik NATO liikmesriigid on selles osalejad. Kuigi asutuse eesmärk on parandada ja täiendada NATO liikmesriikide kaitsevõimekust küberruumis, siis tegelikkuses isegi NATO ei rahasta käesolevat asutust täielikult ja see on keskuse kodumaa ja programmis

[50] Ashmore, William C. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review. Vol 11, nr 1, lk 9.
[51] Küberjulgeoleku strateegia komisjon. (2008). Küberjulgeoleku strateegia 2008–2013. Kaitseministeerium Kasutatud 03.04.2017.
https://valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf, lk 34.
[52] Laasme, Häly. (2011). Estonia: Cyber window into the future of NATO. JFQ: Joint Force Quarterly. Vol 63, nr 4, lk 61.
[53] Seal samas.
[54] Tiirmaa-Klaar, Heli. (2010). Rahvusvaheline koostöö küberjulgeoleku tagamisel. Diplomaatia. September nr. 85. Kasutatud 28.12.2016. www.diplomaatia.ee/artikkel/rahvusvaheline-koostoo-kuberjulgeoleku-tagamisel/

osalejate ning toetajate teha jäetud[55]. Seeläbi ei ole Küberkaitsekeskus NATO juhtimise struktuuris vaid hoopis sõjaväestruktuurides[56]. Sellest tulenevalt saab esile tuua, et käesoleva keskuse eesmärk ei ole olla NATO sõjalise võimekuse väljundiks, vaid pigem teadus- ja uurimistöökeskus[57].

NATO Kooperatiivne Küberkaitse Kompetentsikeskus on korraldanud mitmeid küberjulgeolekuga seotud konverentse ja seminare, millest tähelepanuväärseimad on 2009. aastal toimunud Esimene Küberkaitsekonverents, aga ka sellele järgnenud sarnased tegemised, millest suur hulk on toimunud Eestis[58]. Samuti on traditsiooniks saanud iga-aastased suurõppused koos liitlastega. Esile on võimalik tuua 2010. aastal toimunud õppust "Balti kilp" koos Rootsi Riikliku Kaitsekolledži, Rootsi Kaitseuuringute Ameti ja Eesti Küberkaitseliidu"[59]. Tegu oli suuremahulise üritusega, kus kehastati nii sõbralikke kui ka vaenulikke jõude ning mitme päeva jooksul pidid sinised pooled kaitsma enda arvutivõrke erinevate rünnakute eest kasutades endale kõiki olemasolevaid vahendeid[60]. Niimoodi üritati võimalikult tõetruult simuleerida potentsiaalseid rünnakuid, mis võivad ühe riigi suunal toimuda, ja just selliseid, mis Eestis 2007. aastal reaalselt juhtusidki[61]. Nüüdseks on saanud iga-aastaseks traditsiooniks korraldada õppus *Locked Shield's* ja 2013. aastast hakati lisaks korraldama õppust nimega Küberkoalitsioon (*Cyber Coalition*)[62] .

## 5. TALLINNA KÄSIRAAMAT

2007. aastal toimunud küberrünnakud Eesti suunal tõstatasid ka küsimuse, kuidas seesuguseid rünnakuid rahvusvahelise õiguse kontekstis käsitleda. Maikuu sündmustele järgnenud päevadel ja kuudel ilmnes kiiresti tõsiasi, et võimalike süüdlasi on võimatu tuvastada ning lisaks sellele ei osutunud Venemaa ka kõige tugevamaks koostööpartneriks õigluse jalule seadmisel. Ühtlasi tõusis päevakorda küsimus, millisel tingimusel on

[55] Ashmore, William C. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review. Vol 11, nr 1, lk 13.
[56] Szentgáli, Gergely. 2013. The NATO Policy on Cyber Defence: The Road so Far. Academic & Applied Research in Military & Public Manageme. Vol 12, nr 1, lk 2.
[57] Seal samas
[58] Laasme, Häly. (2011). Estonia: Cyber window into the future of NATO. JFQ: Joint Force Quarterly. 63:4, lk 61-62.
[59] Geers, Kenneth. (2010). Valmistume kübersõjaks. Diplomaatia. September nr. 85. Kasutatud 28.12.2016. www.diplomaatia.ee/artikkel/valmistumine-kubersojaks/
[60] Seal samas.
[61] Seal samas.
[62] Majandus- ja Kommunikatsiooniministeerium. (2014). Küberjulgeoleku strateegia 2014 – 2017. Majandus- ja Kommunikatsiooniministeerium. Kasutatud 03.04.2017.
www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf, lk 3.

küberrünnak piisav, et oleks õigust pöörduda Põhja-Atlandi Nõukogu poole sooviga jõustada Washingtoni leppe 5. artikkel ning kutsuda NATO endale appi. Sellest tulenevalt kui 2008. aastal avati Eestis NATO Kooperatiivne Küberkaitse Kompetentsikeskus, siis ühena esimestest asjadest algatati kolmeaastane projekt, mille eesmärk oli välja töötada põhimõtted, kuidas küberrünnakuid käsitleda rahvusvahelise õiguse kontekstis ning valminud dokumendi nimeks sai "Tallinna käsiraamat"[63].

Antud olukorra illustreerimiseks on võimalik luua mitmeid hüpoteetilisi stsenaariumeid ja seeläbi küsida "kas" küsimus. Nagu näiteks, et kui Tallinna börsid lastakse tiibraketiga tükkideks või sisuliselt sama tulemus saavutatakse küberrünnakutega kustutades ära kõik andmed serveritest, ehk siis olukorras, kus lõpptulemus on sama ja me saame rääkida füüsilisest kahjust, siis kuidas saab riik ennast kaitsta ning kuidas peaks ta üleüldse reageerima[64]. Samas probleem pole niivõrd selles, kui suur või kui sarnane on kahju võrreldes kineetilise rünnakuga, vaid selles, kas küberrünnak üksi on piisav argument, et algatada kahepoolne sõjaline konflikt ning milline see peaks siis välja nägema[65]. Teiseks on siiamaani iga suurema avaliku küberrünnaku puhul rünnaku läbiviijaks olnud mitteriiklikud organisatsioonid (kuigi on üritatud tõestada võimalikke sidemeid riiklike institutsioonidega) ja seeläbi tekib küsimus, kuidas võtta neid vastutusele. Antud põhjusel oli Eestil 2007. aastal väga keeruline Venemaad süüdistada, kuna viimasel puudusid formaalselt seotused rünnaku läbiviimisega ning süü langes Venemaa territooriumil tegutsenud patriootlikult meelestatud mitteriiklikele rühmitustele[66].

Suurim probleem küberrünnakutega tegelemisel on arutelu punkt, kas see ületab jõu kasutamise piiri või mitte. Oletame, et toimub küberrünnak ülikooli võrgu vastu, mille tulemusena kasutajad ei pääse ligi andmebaasidele. Kokkuvõttes võib ülikool kaotada osa oma andmebaasist ja kasutajatele on see, kui pole võimalik tegeleda teadus- ja õppetööga, ebameeldivuseks. Aga kui antud küberrünnak laieneb ja kohaliku lennujaama lennujuhtimiskeskus lülitatakse välja ning seeläbi toimub lennuõnnetus, siis ei ole tegemist enam ebameeldivusega, vaid füüsilise vägivallaga, millel on potentsiaal lõppeda surmaga.

[63] Schmitt, Michael N. (2015). The law of cyber targeting. Naval War College Review. Vol 68, nr 2, lk 12.
[64] Seal samas, lk 14.
[65] Seal samas.
[66] Majandus- ja Kommunikatsiooniministeerium. (2014). Küberjulgeoleku strateegia 2014 – 2017. Majandus- ja Kommunikatsiooniministeerium. Kasutatud 03.04.2017, lk 3.
[66] Schmitt, Michael N. (2015). The law of cyber targeting. Naval War College Review. Vol 68, nr 2, lk 15.

Seeläbi teoreetiliselt võiks rahvusvaheline kogukond reageerida küberrünnakule alles siis, kui see toob kaasa füüsilist kahju, aga siinkohal võivad tekkida jälle varem esile toodud probleemid, kus süüdlase kindlaks tegemine ja tema suhtes mingisuguste meetmete rakendamine eeldab, et riik, kus rünnak alguse sai, on koostöövalmis süüdlast välja andma ning eksisteerib seda protsessi toetav seadusandlus või rahvusvahelised kokkulepped[67].

Üks probleemi osa ongi selles, et varasemalt eksisteeris väga vähe rahvusvahelisi kokkuleppeid, mis sätestasid, kuidas riigid peaksid küberrünnakute puhul koostööd tegema selleks, et võimalik süüalune üles leida ja kohtu alla anda[68]. Varasemalt on näiteks Euroopa Nõukogu üritanud seesugust seadusandlust 2004. aastal luua, aga siis ilmnes teistsugune probleem, kus mõned riigid ei olnud nõus selliseid rahvusvahelisi kokkuleppeid ratifitseerima, nagu näiteks oli üheks selliseks riigiks Venemaa[69, 70]. Seaduste puudumine teeb lihtsaks mitmetel hobihäkkeritel toime panna küberrünnakuid kartmata, et näiteks Venemaa neid välja annaks või neid ise karistaks, soodustades seeläbi küberkuritegude kasvu[71]. Lisaks sellele eksisteerib veel USA poolt algatatud Küberkuritegude Konventsioon, aga jällegi käesolevat dokumenti on ratifitseerinud ainult 23 riiki, mis piirab tugevalt selle võimalusi ja lisaks sellele ei käsitleta seal küberrünnakuid, mille eesmärk on teha sõjalist kahju, vaid on piiritletud ainult küberkuritegevusega[72].

Seega olukorras, kus enamik rahvusvahelisi seadusi olid kirjutatud enne internetiaega või ei käsitlenud konkreetselt küberrünnakutest tulenevaid juhtumeid, kutsus Eestisse loodud NATO Kooperatiivse Küberkaitse Kompetentsikeskus kokku oma ala ekspertide kolleegiumi, kelle töö viljana valmis aastaks 2013. "Tallinna käsiraamat", mis üritas rahvusvahelise õiguse kontekstis vastata küsimusele, kuidas peaksid riigid käituma küberrünnakute puhul. "Tallinna käsiraamatu" omaaegne uuenduslikus (omaaegne sellepärast, et nüüdseks on väljas "Tallinna käsiraamatu" teine versioon ehk "Tallinna käsiraamat 2.0") seisneb selles, et see ei teinud ettepanekuid, kuidas tuleks rahvusvahelist

[67] Ottis, Rain. (2013). Kübersõja küsimärgid ja eripärad. Diplomaatia. September, nr. 121. Kasutatud 28.12.2016. www.diplomaatia.ee/artikkel/kubersoja-kusimargid-ja-eriparad/
[68] Ashmore, William C. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review. Vol 11, nr 1, lk 14.
[69] Council of Europe. (2001). Convention on Cybercrime. Council of Europe. 23.11.2001. Kasutatud 03.04.2017. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
[70] Council of Europe. (2004). Chart of signatures and ratifications. Council of Europe. 01.07.2004. Kasutatud 03.04.2017. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG
[71] Ashmore, William C. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review. Vol 11, nr 1, lk 17.
[72] Seal samas, lk 18.

õigust täiendada, vaid seletas olemasolevate ja kehtivate õiguste kontekstis lahti, et küberrünnakud mahuvad juba sinna sisse ning ei vaja seepärast eraldiseisvat käsitlust[73].

"Tallinna käsiraamat" tõi antud ideede selgemaks esitamiseks välja 95 kommenteeritud rahvusvahelise õiguse reeglit, mida saab ühtlustada küberrünnakutele[74]. Seega võiks küberrünnak antud tingimustel tuua kaasa ÜRO Julgeolekunõukogu loa kasutada rahvusvaheliselt jõudu ja lisaks sellele NATO kollektiivkaitse jõustumise[75]. Ühtlasi anda laiemalt loa iseennast kaitsta teise riigi rünnakute eest ja lubada rahvusvahelisel kogukonnal kasutada jõudu rahu taastamiseks. Samuti "Tallinna käsiraamat" viitab kaudselt sellele, et 2007. aastal toimunud rünnaku toime panijad olid vastuolus rahvusvahelise õigusega ja sooritasid antud olukorras kuriteo. See oli üpriski Eestit soosiv lähenemine, aga ei teinud Eestile olukorda paremaks 2007. aasta rünnaku toimepanijate leidmisel ja kohtu ette toomisel[76].

"Tallinna käsiraamat" on siiski oma ala ekspertide arvamus sellest, kuidas saab rahvusvahelist õigust tõlgendada, lähtudes üldtunnustatud arusaamadest rahvusvahelisest õigusest ja on vähem ettekirjutis sellest, kuidas seda tuleks kindlasti teha[77,]. Rahvusvahelise õiguse kohaselt tuleks kasutada enda kaitseks proportsionaalset jõudu. Aga mis on proportsionaalne jõud küberrünnaku puhul? Seega kahjuks enne kui ei ilmne uus reaalne stsenaarium mõne NATO või Euroopa Liidu liikme suunal, jääb see küsimus tõenäoliselt vastuseta. Seeläbi ilmneb, et kindlasti ei esinda "Tallinna käsiraamat" NATO ametlikku doktriini ja on NATO jaoks pigem nõuandev dokument kui omaette ettekirjutis[78].

## 6. BUKARESTI TIPPKOHTUMINE

Vahetult enne Venemaa ja Gruusia vahelise sõjalise konflikti puhkemist aprillis toimunud Bukaresti tippkohtumine on pärast kuus aastat varem toimunud Praha tippkohtumist üks olulisemaid uute algatuste poolest küberkaitsestrateegiate osas. Kuigi augustis ilmnes terve maailma silme all, milline võib hübriidsõda kahe riigi vahel välja näha, siis sellest sõltumata

[73] Mälksoo, Lauri. (2013). "Tallinna käsiraamat" kui rahvusvahelise elu sündmus. Diplomaatia. August nr. 120. Kasutatud 28.12.2016. www.diplomaatia.ee/artikkel/tallinna-kasiraamat-kui-rahvusvahelise-elu-sundmus/
[74] Seal samas.
[75] Seal samas.
[76] Seal samas.
[77] Meikar, Silver. (2013). Sõda internet pärast. Diplomaatia. September, nr. 121. Kasutatud 28.12.2016. www.diplomaatia.ee/artikkel/soda-interneti-parast/
[78] Szentgáli, Gergely. 2013. The NATO Policy on Cyber Defence: The Road so Far. Academic & Applied Research in Military & Public Manageme. Vol 12, nr 1, lk 4.

astuti siin esimesi samme jätkusuutlikuma tugevama turvalisuse suunas. Seega kui võrrelda Bukaresti ja varasemate NATO tippkohtumiste omavahelisi deklaratsioone ja põhilisi seisukohti, siis paistab neis välja väga suur erinevus, mille algeid saab leida NATO varasemast kogemusest. Kui Kosovo kriisi ajal sattusid NATO enda struktuurid küberrünnakute alla, siis võeti kiirelt vastu seisukohad uuendada NATO enda küberkaitse võimekust ja nende teostamiseks loodi mitmeid uusi institutsioone. Kuigi tegelikult Kosovo kriisi ajal sattusid küberrünnakute alla ka alliansi liikmete valitsuste veebilehed, siis sellele ei pööratud tähelepanu. Kuigi ühelt poolt on seeläbi võimalik tuua esile NATO't kui eeskujulikku organisatsiooni, kes nägi oma võimekuses probleemi ning reageeris sellele kohe esimesel võimalusel, siis teisalt Istanbuli tippkohtumisel 2004. aastal polnud ülddeklaratsioonis sõnakestki küberkaitsest. 2006. aastal toimunud tippkohtumine Riias parandas selle vea ja tõi oma deklaratsioonis esile ühiste võrkude kaitse olulisuse, kuid siiski puudusid Riia tippkohtumise ajal uued algatused ning Prahas 2002. aastal algatatud NCIRC ei olnud 2006. aastaks tööle rakendatud.

Pärast 2007. aastat toimus aga selles osas drastiline ning etapiline muutus, mis sai alguse Bukarestis. Sealses liikmesriikide esindajate deklaratsioonis tunnistati küberrünnakutest tekkivad võimalikku ohtu ja kutsuti kõiki üles kaitsma enda kriitilist ja eluks vajalikku infrastruktuuri ning tegema selle saavutamiseks omavahel varasemast tihedamat koostööd nii võrkude tugevandamiseks kui ka ennatliku töö tegemiseks[79]. Samuti rõhutas deklaratsioon selgelt NATO ja tema liikmesriikide vahelise ühise koostöö olulisust[80].

See oli selge poliitikamuutus, mille tegemiseks hakati järgnevatel aastatel ellu kutsuma uusi algatusi ja projekte ning mida aasta edasi, seda selgemaks selles osas NATO seisukohad muutusid. Bukaresti tippkohtumisel kiideti heaks aasta varem algatatud NATO Küberkaitsepoliitika (*NATO Policy on Cyber Defence*) ja loodi Brüsselis baseeruv Küberkaitse Juhtimiskeskus (*Cyber Defence Management Authority)*, mille eesmärk oli hakata tsentraliseerima terve NATO küberkaitset ühise kaitse alla ja teisalt olla kiirelt abiks võimalike küberrünnakute puhul[81]. Ühtlasi ei saa välja jätta Tallinna NATO Küberkaitse Kompetentsikeskuse loomise otsustamist, millest kujunes välja teadus- ja uurimiskeskus

[79] Ashmore, William C. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review. Vol 11, nr 1, lk 13.
[80] North Atlantic Treaty Organization. (2008). Bucharest summit declaration. North Atlantic Treaty Organization. Pressiteade (2008) 049. Kasutatud 03.04.2017. www.nato.int/cps/in/natohq/official_texts_8443.htm
[81] Hughes, Rex B. (2009). NATO and Cyber Defence. Mission Accomplished. Atlantische Commissie. Kasutatud 03.04.2017. www.atlcom.nl/ap_archive/pdf/AP%202009%20nr.%201/Hughes.pdf

kübervaldkonnaga seotud ohtude uurimiseks ja nendega tegelemiseks[82]. Viimasena sai iga liikmesriik kohustuse luua endale kohapealseid CERT meeskondi selleks, et aktiivselt võidelda ja end erinevateks küberrünnakuteks lokaalselt ette valmistada, mis on jällegi 180 kraadine muutus suhtumisest, mis valitses aastaid varem[83]. Juba järgmisel aastal toimunud NATO 60. aastapäevale pühendatud Strasbourg/Kehli tippkohtumine ainult kinnitas Bukarestis vastu võetud otsuseid ja rõhutas vajadust kaitsta enda võrke ning uue tõi tegevusena välja, kuidas Eestis avatud küberkaitsekeskus aitab kaasa NATO, tema liikmesriikide ning partnerite omavahelise koostöö arendamisele[84].

# 7. VENEMAA-GRUUSIA SÕDA

Kui 2007. aastal toimunud küberrünnakud Eesti vastu tõestasid, et üht riiki on võimalik isoleerida ning seega seada tema julgeolek ohtu, siis 2008. aastal aset leidnud Venemaa-Gruusia sõda on olulisema tähtsusega, kuna seda võib pidada üheks esimeseks sõjaks, kus lisaks traditsioonilistele väeliikidele käis toimusid koordineeritud küberrünnakud ja toimus tänapäeva mõistes hübriidsõda[85]. Seeläbi on Gruusias toimunu põhjal hea uurida, milline võib hübriidsõda, kus samaaegselt tulistavad nii kineetilised- kui ka küberrelvad, reaalsuses välja näha.

Esimesed küberrünnakud Gruusia vastu algasid juba enne augusti, kui juulikuus toimusid rünnakud Gruusia presidendi veebilehe suunal. See oli alles eelmäng sellele, mis sai alguse 8. augustil, kui paralleelselt lahingutega Gruusia-Venemaa piiril ägenesid ka küberrünnakud Gruusia valitsuse veebilehtede vastu[86]. Selliste rünnakute eesmärk oli selgelt kujundada rahva meelsust Gruusia valitsuse vastu ning rünnakud viidi läbi kasutades DDoS meetodit ja omakorda tegeleti alternatiivseid veebilehti luues aktiivselt uue tõe loomise ja levitamisega[87]. Kuna Gruusia internetiteenused ei olnud 2008. aastal niivõrd kaitstud (võrreldes näiteks Eesti omadega), siis need rünnakud olid ka mõjuvamad ning

[82] Wallander, Celeste. A. (2000). Institutional assets and adaptability: NATO after the Cold War. International Organization. Vol 54, nr 4, lk 705–735.
[83] Szentgáli, Gergely. (2013). The NATO Policy on Cyber Defence: The Road so Far. Academic & Applied Research in Military & Public Manageme. Vol 12, nr 1, lk 2.
[84] North Atlantic Treaty Organization. (2010). Strasbourg/Kehl summit declaration.
North Atlantic Treaty Organization. Pressiteade (2009) 004. Kasutatud 14.05.2017. www.nato.int/cps/en/natohq/official_texts_68828.htm
[85] Shakarian, Paulo. (2011). The 2008 Russian Cyber Campaign Against Georgia. Military Review. Vol 91, nr 1, lk 63.
[86] Ashmore, William C. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review. Vol 11, nr 1, lk 10.
[87] Seal samas.

pikemaajalised[88]. Sarnaselt aasta varem toimunud rünnakutele Eestis oli käekiri ligilähedane, kus rünnakute eesmärk oli isoleerida Gruusia välismaailmast ning kasutades psühholoogilise sõja meetodeid demoraliseerida grusiine teadmatusega, mis toimub välismaailmas[89].

Gruusia vastu suunatud küberrünnakud saab oma olemuselt jagada kahte etappi, millest esimene faas koosnes eelkõige DDoS rünnakutest, millega üritati Gruusia võrgusüsteemid ülekoormata ning nende kättesaadavus võimatuks muuta[90]. Sellised rünnakud said võimalikuks läbi botnettide, mille näol on tegemist viirusega nakatatud arvutiga, mis aktiviseerimiskäsu peale hakkavad kindlaid ülesandeid täitma[91]. Pärast sõda tehti selgeks, et antud olukorras olid käesolevad botnetid venelaste kuritegeliku organisatsiooni *Russian Business Network'i* käsutada ja esimeses etapis olid rünnakud suunatud eelkõige valitsuse ja meediaväljaannete veebilehtede suunas[92]. Rünnaku teises faasis toimus sihtmärkide laiendamine, kus lisaks juba rünnaku alla sattunud veebilehtedele võeti nüüd rünnaku alla rahanduse, ettevõtluse ja haridusega tegelevad asutused[93].

Ühtlasi hakati teises faasis kasutama lisaks DDoS'ile ka meetodit, mida kutsutakse SQL-süstiks *(SQL injection)*, mille kaudu on võimalik kindlasse andmebaasi sisse tungida ja saada kätte nii sisselogimise andmed, pangaväljavõtted kui ka kogu veebilehe sisu[94]. Kõige uudsema tegevusena hakati teises faasis läbi interneti värbama vabatahtlikke häkkereid. Üheks kõige paremaks näiteks sellest on sõja ajal üles seatud veebileht StopGeorgia.ru, mis postitas õpetusi sellest, kuidas läbi viia lihtsamaid DDoS rünnakuid Gruusia suunal ilma, et peaksid omama erilisi arvutioskusi[95]. Käesolevad küberrünnakud olid selgelt efektiivsed. Näiteks löödi Gruusia pangandussektor kümneks päevast rivist välja ja lisaks sellele suudeti

[88] Ashmore, William C. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review. Vol 11, nr 1, lk 10.
[89] Shakarian, Paulo. (2011). The 2008 Russian Cyber Campaign Against Georgia. Military Review. Vol 91, nr 1, lk 65.
[90] Mirkovic, Jelena. Reiher, Peter. (2004). A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. ACM SIGCOMM Computer Communication. Vol 34, nr 2, lk 39-53.
[91] Shakarian, Paulo. (2011). The 2008 Russian Cyber Campaign Against Georgia. Military Review. Vol 91, nr 1, lk 64.
[92] Seal samas.
[93] Seal samas.
[94] Seal samas.
[95] Danchev, Dancho. (2008). Coordinated Russia vs. Georgia Cyber Attack in Progress. ZDNet. 11.08.2008. Kasutatud 03.04.2017. www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/

mobiilvõrgud ajutiselt välja lülitada[96, 97]. Samuti on spekuleeritud, et häkkeritel oli ligipääs kriitilisele Gruusia infrastruktuurile, nagu näiteks vee- ja energiatootmissüsteemidele, aga neid ei rünnatud selleks, et mitte teha permanentset kahju ja puutumata jäi ühtlasi füüsiline internet[98].

Käesolevate küberrünnakute süüdlasi otsides tekkis kiirelt täpselt sarnane olukord nagu aasta varem Eestis, kus Kreml isegi tunnistas, et küberrünnakud võidi toime panna Venemaa pinnalt, aga väidetavalt polnud tegu Vene valitsusega seotud inimeste ega organisatsioonidega. Kremli sõnumite järgi oli tegu patriootlike venelastega ning organiseeritud kuritegevuse liikmetega, kes võisid seda teha Venemaa pinnalt, aga neil puudus seos Venemaa sõjaväe ning valitsusega[99]. See tõi jälle välja, et küberrünnakute üks suurimaid probleeme võibki olla nende teostajate selge tuvastamine, mis võib muutuda äärmiselt keeruliseks. Sõltumata sellest, kui otseselt või kaudselt või kas üldse Vene valitsus oli antud küberrünnakute korraldamisega seotud, siis on selge, et igal juhul kõige suuremaks kasulõikajaks oli jällegi Kreml[100]. Samas usuvad osad julgeolekueksperdid, et tegu oli korralikult etteplaneeritud küberrünnakuga, mille märke oli võimalik juba ennatlikult näha, kuna nii suurtes kogustes botnette ei ole võimalik nii väikese ajaga endale koguda ning need, kelle suunal tehti SQL rünnakuid toime pandi, pidid olema varasemalt põhjalikult ettevalmistatud[101]. Kuigi ametlikult jääb lõpuni välja selgitamata, kui suur oli tegelikult Vene väeüksuste ning niinimetatud Venemaa allilma vaheline koostöö käesoleva sõja vältle[102].

Venemaa-Gruusia sõda on aga kindlasti oluline näide sellest, kuidas tulevikus võib hübriidsõda välja näha. Tihtipeale on manööverüksuste suutlikkust lihtsam hinnata ja sellele vastavalt enda kaitset kohandada, aga objektiivselt hinnata vastase kübervõimekust on keerulisem, kuna seda esineb harvem ja sellepärast on Venemaa-Gruusia sõda oluline koht

[96] Bumgarner, John. Borg, Scott. (2009). Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008. U.S. Cyber Consequence Unit Special Report. August 2009, lk 2.
[97] Corbin, Kenneth. (2009). Lessons from the Russia-Georgia Cyberwar. Real time IT News. 12. 03. 2009. Kasutatud 20.03.2017. www.internetnews.com/government/article.php/3810011/Lessons-From-the-Russia-Georgia-Cyberwar.htm
[98] Zmijewski, Earl. (2008). Georgia Clings to the Net. Reneysys: The Internet Intelligence Authority. 10.08.2008. Kasutatud 20.03.2017. http://dyn.com/blog/georgia-clings-to-the-net/
[99] Shakarian, Paulo. (2011). The 2008 Russian Cyber Campaign Against Georgia. Military Review. Vol 91, nr 1, lk 67.
[100] Ashmore, William C. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review. Vol 11, nr 1, lk 10.
[101] Shakarian, Paulo. (2011). The 2008 Russian Cyber Campaign Against Georgia. Military Review. Vol 91, nr 1, lk 66.
[102] Seal samas.

kust õppida[103]. Näiteks Venemaa-Gruusia sõja puhul saaksime me luua võimaliku näidisdoktriini, kuidas Vene konventsionaalsed väeüksused võivad Venemaal tegutsevate kriminaalsete organisatsioonidega ühise eesmärgi saavutamise nimel koostööd teha[104]. Rünnaku käigus võidakse maha võtta valitsuste veebilehed kui ka meediaväljaanded ning seeläbi proovida riiki sulgeda välisele informatsioonile rünnaku algusfaasis, kus kommunikatsioon nii välismaailma kui ka enda rahvaga on võtmetähtsusega[105]. Samuti tõi Venemaa-Gruusia sõda välja, et tänapäeval ei kübersõda pea ainult riigid vaid ka tsiviilisikud, kelle arvutid nende enese teadmata muudetakse botnettideks ja seeläbi pööratakse nende enda riigi vastu. Sellepärast on oluline rõhutada vajadust hoida oma arvuteid turvalisena ning uuendada näiteks viirusetõrjeid[106].

# 8. LISSABONI TIPPKOHTUMINE

2010. aastal toimunud Lissaboni tippkohtumisele läks NATO vastu suurte avalike ootustega, et Lissabonist väljub tugevam ja ühisem NATO, kes on enda uuendamiseks võimeline tegema vajalikke reforme, et vastata 21. sajandi ohtudele. Pärast Külma sõja lõppu on nii terrorism kui ka küberrünnakud muutunud NATO'le aina suurematekss ohtudeks. Just terrorismiga võitlemise nimel oli NATO oma haardelt muutumas aina globaalsemaks organisatsiooniks, kus tema tähelepanu hakkas enam liikuma näiteks Euroopalt Aasiale. Seda protsessi toetas ühe kindla suure vaenlase puudumine ning selle asemel tegeleti mitmete asümmeetriliste ohtudega üle maailma[107]. NATO ja Venemaa vahelised suhted olid muutunud märgatavalt halvemaks, sest Venemaad sooviti näha olulise partnerina, aga viimase aina agressiivsemad sammud oma naaberriikide vastu tõid esile selle keerulisuse ning teisalt illustreerisid, et NATO kollektiivkaitse pruugib tulevikus olla olulisem kui kunagi varem, kui Venemaa sellist välispoliitikat jätkab[108].

[103] Shakarian, Paulo. (2011). The 2008 Russian Cyber Campaign Against Georgia. Military Review. Vol 91, nr 1, lk 66.
[104] Seal samas
[105] Georgescu, Constantin. Tudor, Monica. (2015). Cyber terrorism threats to critical infrastructures NATO's role in cyber defense. Knowledge Horizons / Orizonturi ale Cunoasterii. Vol 7, nr 2, lk 116 – 117.
[106] Rantapelkonen, Jari. Salminen, Mirva. (2013). Offensive Cyber Capabilities are
Needed Because of Deterrence. Limnéll, Jarno. The Fog of Cyber Defence, lk 206. Tampere. Juvenes Print Oy.
[107] Noetzel, T. Schreer, B. (2012). More flexible, less coherent: NATO after Lisbon. Australian Journal of International Affairs Vol 66, nr 1, lk 22-23.
[108] Yost, David S. (2010). NATO's evolving purposes and the next Strategic Concept. International Affairs. Vol 86, nr 2, lk 499.

Käesoleva sündmuse keskmes oli NATO uue "Strateegilise kontseptsiooni" (*Strategic Concept*) vastu võtmine. Mitmete uuenduste kõrval käsitles see esmakordselt kübermaailmas olevaid ohtusid ja oli seeläbi selgeks märgiks, et NATO on pühendunud oma küberkaitse arendamisele. Sellega ei olnud tegu ainult sõnakõlksudega iga-aastastes deklaratsioonides, vaid küberkaitse arendamist nähti olulise valdkonnana, millele tuleb järgnevatel kümnenditel tähelepanu pöörata[109].

NATO eelmine "Strateegiline kontseptsioon" võeti vastu aastal 1999 ning Lissaboni tippkohtumise ajaks oli see tugevalt aegunud ning ei vastanud uutele ohtudele, mis olid viimastel aastatel esile kerkinud ning ajaga ainult intensiivistunud. Sündmused, nagu näiteks Kosovo konflikt, 9. septembri sündmused Ameerika Ühendriikides ning sellele järgnenud terrorivastased operatsioonid Lähis-Idas ja Aasias, tõid selgelt välja, et tulevikus on vaja paindlikumat riikide ühendust, et tagada NATO liikmesriikide julgeolek. Seda eriti sellepärast, kuna on selge, et ebastabiilsus väljaspool Euroopat mõjutab tugevalt Euroopa ja Põhja-Ameerika heaolu ning seega tuleb näiteks küberruumis toimuvale tähelepanu pöörata[110]. Selle tõdemuseni jõudis ka NATO, kes tõi Lissaboni deklaratsioonis välja, et oht, kus keegi tavarelvastust kasutades ründab mõnda NATO liikmesriiki on madal, ja seeläbi valmistavad kõige suuremat ohtu just erinevad asümmeetrilised ohud, millega tuleb varasemast aktiivsemalt võidelda[111].

Suurim erinevus 1999. aastal ning 2010. aastal vastu võetud dokumendis küberkaitse seisukohast seisneb selles, et kui varasemas dokumendis toodi välja, et tulevikus suureneb sõltuvus erinevatest arvutivõrkudest ning seeläbi on käesoleva valdkonna arendamine oluline, siis 2010. aasta dokument ütleb selgelt, et tegevus küberruumis ei tohi olla lihtsalt toetusrollis, vaid seda tuleb käsitleda samaväärse väeliigina, nagu selleks varasemalt on olnud mere-, õhu-, ja maavägi ning samuti rõhutati, et ilma küberväeosade kaasamiseta on tänapäeval ja tulevikus võimatu sõjalisi operatsioone läbi viia[112]. Sellised sammud muudavad küberkaitse NATO jaoks varasemast olulisemaks ning tegu on poliitilise

[109] Noetzel, T. Schreer, B. (2012). More flexible, less coherent: NATO after Lisbon. Australian Journal of International Affairs Vol 66, nr 1, lk 21.
[110] North Atlantic Treaty Organization. (2010). Active engagement, modern defence: strategic concept for the defence and security of the members of the North Atlantic Treaty Organisation adopted by heads of state and government in Lisbon. North Atlantic Treaty Organization. 19.11.2010. Kasutatud 28. 03. 2017. www.nato.int/cps/en/natolive/official_texts_68580.htm
[111] Seal samas.
[112] US Department of Defense. (2010). Quadrennial Defense Review Report. Washington DC: US Department of Defense. Veebruar 2010, lk 37.

läbimurdega, mida on vaja selleks, et käesolev valdkond saaks tulevikus paljuoodatud tähelepanu.

Täiesti eraldiseisva teemana tõusis Lissabonis arutelu selle üle, millal on küberrünnak piisav selleks, et oleks põhjust ellu kutsuda Washingtoni leppe 5. artikkel ning selles osas jõuti hoopis kokkuleppele, et küberrünnakud iseseisva rünnakuna ei ole piisavad ning neid tuleks käsitleda hoopis Washingtoni leppe 4. artikli kaudu[113]. Selle põhjendus seisneb selles, et küberrünnak on oma olemuselt liiga ebamäärane ning iseseisva rünnakuna liiga raskesti eristatav selleks, et kollektiivkaitse iseseisva küberrünnaku pärast peaks käivituma[114]. Samas tuleb mõista, et rünnak NATO liikme vastu ei tähenda automaatselt kollektiivkaitse punkti jõustumist ning kõik toimub juhtumipõhiselt ja otsusega täpselt nii, nagu ülejäänud väeliikide puhul, millega viimane võrdsustati ja seeläbi teeb lõpliku otsuse Põhja-Atlandi Nõukogu, mis vastavalt olukorrale võib otsustada ka teistmoodi[115]. Seeläbi jäeti Lissaboni tippkohtumise järgselt kogu vastutus Põhja-Atlandi Nõukogule.

See on üpriski kahetsusväärne, kuna tegelikkuses oli selleks hetkeks toimunud mitmeid märkimisväärse mõjuga küberrünnakuid ning neid ka NATO liikmesriikide, nagu näiteks Eesti suunal. Eesti näide tõestas, et küberrünnak võib omada täpselt samasugust mõju, nagu keskajal sadamakoha tõkestamine, mille tulemusena suletakse riigi ühendus välismaailmaga ja seatakse ohtu rahvuslik julgeolek, mille peale NATO peaks reageerima[116]. Kuigi "Strateegiline kontseptsioon" rõhutas, et küberrünnakutel on potentsiaal tekitada samaväärset või isegi suuremat kahju kui kineetilised rünnakud, siis võrdsustamine oleks ennetavalt mõjunud paremini efektiivse küberheidutuse loomisel[117]. Ühtlasi otsustati Lissabonis, et kui toimub küberrünnak NATO liikmesriigi vastu, siis juhul kui NATO reageerib, siis ta võib kasutada kõiki oma arsenalis olevaid relvi ning vastulöök ei pruugi piirduda ainult omapoolse küberrünnakuga[118].

[113] Noetzel, T. Schreer, B. (2012). More flexible, less coherent: NATO after Lisbon. Australian Journal of International Affairs Vol 66, nr 1, lk 26.
[114] Yost, David S. (2010). NATO's evolving purposes and the next Strategic Concept. International Affairs. Vol 86, nr 2, lk 499.
[115] Journal of International Affairs. (2016). Is cyber defense possible? Journal of International Affairs. Vol. 70, nr 1, lk 183.
[116] Yost, David S. (2010). NATO's evolving purposes and the next Strategic Concept. International Affairs. Vol 86, nr 2, lk 510.
[117] Georgescu, Constantin. Tudor, Monica. (2015). Cyber terrorism threats to critical infrastructures NATO's role in cyber defense. Knowledge Horizons / Orizonturi ale Cunoasterii. Vol 7, nr 2, lk 116.
[118] Spillius, Alex. (2011). US could respond to cyber-attack with conventional weapons. Daily Telegraph. 01.06.2011. Kasutatud 27.03.2017. www.telegraph.co.uk/news/worldnews/northamerica/usa/8550642/US-could-respond-to-cyber-attack-with-conventional-weapons.html

Küberheidutust tuleks käsitleda erinevalt kui näiteks tuumaheidutust, mis kujunes välja 1950ndatel. Lihtsalt öeldes tähendab tuumaheidutusteooria seda, et potentsiaalse rünnaku eest heidutab sind see, et tagajärjed oleksid hullemad kui rünnakuga teenitav potentsiaalne kasu. Selle põhimõtte tulemusena on tuumaheidutus maailmas töötanud tänase päevani, aga kahjuks ei ole antud valdkonna erinevuste tõttu võimalik samu põhimõtteid küberheidutusele üle kanda[119]. Lisaks küberrünnakute anonüümsele ja globaalsele omadusele, on nende mõju väga raske hinnata enne rünnaku enda toimumist võrreldes näiteks kineetilise rünnakuga, kus see on mõnevõrra lihtsam ja võimaldab kergemini ennast ennetavalt ette valmistada teades vastase tankide arvu[120].

Kuna küberrünnak võib saada alguse ükskõik millisest maailma servast, siis loob see NATO'le erinevaid probleeme, kuna rünnak võidakse toime panna väljastpoolt NATO poolt kokku lepitud kaitseala[121]. See tõstatabki küsimuse, kuidas peaks NATO käituma, kui küberrünnak tuleb näiteks Hiina Rahvavabariigist ning viimane ei ole nõus koostööd tegema. Just sellised probleemid nõrgestavad NATO võimalikku heidutust ja seeläbi turvalisust, kuna ei ole vahet, kas NATO reageerib kineetilise või küberrünnakuga, kui ta ei ole suuteline adekvaatselt reageerima. Seeläbi, kui eksisteerivad nii riigid kui ka mitte riiklikud organisatsioonid, kes tunnetavad, et nad on internetis puutumatud, on tõsine oht, et küberrünnakute arv võib hüppeliselt tulevikus kasvada. Kui Lissabonis oleks öeldud, et küberrünnak on piisav NATO 5. artikli jõustumiseks, siis oleks see võinud mõjuda tugevama heidutusmeetmena, kuna küberrünnak vajab erinevat lähenemist heidutuse loomisel kui näiteks kineetilised relvad[122].

Sellest tulenevalt võib esile tuua, et selleks, et luua küberheidutus tuleks suuremat rõhku panna küberrelvadele ning tegelikkuses on aina suurem hulk riike avalikult ka tunnistanud, et nad liiguvad selle suunas[123]. Näiteks on Ameerika Ühendriikide valitsus kaudselt tunnistanud, et Stuxnet oli nende loodud. Stuxnet, mida kasutati 2010. aastal Iraani tuumaprogrammi vastu, tõi selgelt välja, kuidas hästi läbi viidud küberrünnak võib riigi kriitilisi infrastruktuure ohustada ja neid saboteerida ilma, et ükski sõdur peaks sinna sisse

[119] Rantapelkonen, Jari. Salminen, Mirva. (2013). Offensive Cyber Capabilities are Needed Because of Deterrence. Limnéll, Jarno. The Fog of Cyber Defence, lk 201. Tampere. Juvenes Print Oy.
[120] Seal samas, lk 201-202.
[121] Burton, Joe. (2015). NATO's cyber defence: strategic challenges and institutional adaptation. Defence Studies. Vol 15, nr 4, lk 302.
[122] Seal samas, lk 307 – 308.
[123] Rantapelkonen, Jari. Salminen, Mirva. (2013). Offensive Cyber Capabilities are Needed Because of Deterrence. Limnéll, Jarno. The Fog of Cyber Defence, lk 202. Tampere. Juvenes Print Oy.

astuma või pommi kukutama[124]. Samasugune olukord valitses ka 2007. aastal, kui vahetult enne kui Iisraeli lennukid läksid pommitama Süüria väidetavat tuumaelektrijaama, oli Süüria õhutõrje võimekus blokeeritud küberrünnaku tulemusena[125]. Seda võib pidada avalikuks kübervõimekuse demonstratsiooniks ja seeläbi heidutuse loomiseks, aga kahjuks on seda jällegi väga raske efektiivselt rakendada, kuna NATO eesmärk ei ole teha küberrünnakuid selleks, et tõestada oma võimekust[126].

NATO küberkaitsestrateegiate seisukohalt võib välja tuua Lissaboni tippkohtumist ja sellele järgnenud tegemisi kui murrangulisi võrreldes eelnevate aastatega, kuna need seadsid NATO'le ette uued eesmärgid tulevikuks ja küberrünnakuid hakati käsitlema varasemast suuremate ohtudena olles seeläbi võrdsel tasemel traditsiooniliste väeliikidega. Samuti rõhutati tugevalt, et küberrünnakutel on võimalus ohustada: "*heaolu, turvalisust ja riiklikku stabiilsust Euroopas ja üle Atlandi*[127]". Lissaboni tippkohtumise tähtsamad teemad on seotud eelkõige uue "Strateegilise kontseptsiooniga" ning sinna lisatud punktid, mis olid seotud küberruumiga, kus laiemas pildis nähti, et kiirendatud korras on vaja välja arendada efektiivsem küberkaitse võimekus, mis aasta pärast Lissaboni, ehk 8. juunil 2011, võeti vastu ka tegevusplaanina[128]. Samuti võeti uuesti käsile mõned varasemad murekohad, nagu näiteks lubati, et NATO NCIRC saab 2012. aastaks tööjõuliseks ehk see sama institutsioon, mis tegelikult algatati juba 2002. aastal Praha tippkohtumise tulemusena[129]. Oluline on see, et kohtumisel leiti, et küberkaitse loomiseks on vaja tugevat transatlantilist koostööd ning enam ei tohiks olla olukorda, kus NATO ja tema liikmesriigid ning partnerid tegelevad eraldiseisvalt küberkaitse tagamisega, kuna see nõrgestab NATO ühist kaitsekilpi[130].

[124] Nakashima, Ellen. (2012). With Plan X, Pentagon seeks to spread U.S. military might to cyberspace. Washington Post. 30.05.2012. Kasutatud 14.05.2017. www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-tospread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html

[125] Fulghum David A. Wall, Robert. Butler, Amy. (2007). Cyber-combat's first shot. Aviation Week & Space Technology. Vol 167, nr 21, lk 28.

[126] Rantapelkonen, Jari. Salminen, Mirva. (2013). Offensive Cyber Capabilities are Needed Because of Deterrence. Limnéll, Jarno. The Fog of Cyber Defence, lk 203. Tampere. Juvenes Print Oy.

[127] Georgescu, Constantin. Tudor, Monica. (2015). Cyber terrorism threats to critical infrastructures NATO's role in cyber defense. Knowledge Horizons / Orizonturi ale Cunoasterii. Vol 7, nr 2, lk 116.

[128] Seal samas.

[129] Abrial, Stéphane. (2011). NATO Builds Its Cyberdefenses. The New York Times. 27.02.2011. Kasutatud 03.04.2017. www.nytimes.com/2011/02/28/opinion/28iht-edabrial28.html

[130] North Atlantic Treaty Organization. (2010). Lisbon summit declaration. North Atlantic Treaty Organization. Pressiteade (2010) 155. Kasutatud 03.04.2017. www.nato.int/cps/en/natohq/official_texts_68828.htm

# 9. CHICAGO TIPPKOHTUMINE

Kaks aastat tagasi astuski Lissaboni tippkohtumiselt välja tugevam NATO, kes suutis uue "Strateegilise kontseptsiooni" vastuvõtmisega pöörata paremini tähelepanu uutele 21. sajandi ohtudele ning leidis endale läbi vajalike reformide uut hingamist. Samas toimus Chicago kohtumine olukorras, kus lõppemas oli Afganistani missioon ning aina suurem hulk liikmesriike oli vähendamas oma kaitsekulutusi, mis tõstatas õhku küsimuse, kuidas on ohu korral riikide ühendus reaalselt võimeline oma piire kaitsma, kui kaitsekulutusi vähendatakse. Aina külmenevad suhted Venemaaga ning Afganistani järgse tegevuse planeerimine ei teinud olukorda kergemaks[131].

Kui võrrelda omavahel Lissaboni ja Chicago tippkohtumisi, siis on Chicagot võimalik esile tuua pigem olemasolevate teemade edasiarendajana kui konkreetselt uute ettevõtmiste algatajana. Chicago tippkohtumise otsustena loodi mitmeid uusi osakondi ning allüksusi, kes pidid keskenduma alliansi küberkaitsele. Üheks selliseks on Kiirreageerimise meeskonnad *(Rapid Reaction Team)*, mis koosnesid kuueliikmelistest rühmadest, kelle ülesanne on reaalajaks küberrünnakutele reageerimine ja sedasi nii NATO institutsioonide aitamine kui ka vajadusel NATO liikmesriikide abistamine[132]. Ennetava tegevusena hakati planeerima ja ette valmistama NATO ühisvõrkude kaitset ehk viima need ühise tsentraliseeritud kaitse alla ja seda tegevust pidi korraldama hakkama loodav NATO Kommunikatsiooni- ja Informatsiooniagentuur *(NATO Communications and Information Agency)*[133]. Samuti pidi Chicago tippkohtumise järgselt rakenduma NCIRC, mis algatati 10 aastat varem Praha tippkohtumisel[134].Sellega hakati aina rohkem rõhutama lähenemist, mis ei keskendu lihtsalt sellele, et rünnaku puhul ähvardatakse NATO kollektiivkaitse aktiviseerimisega vaid tegeletakse ennetavalt ja tugevdatakse enda võrke, et vältida olukordi, kus potentsiaalne rünnak tekitab kahju[135].

Täiesti eraldiseisva ja olulise teemana on võimalik välja tuua, et tõstatus (siinkohal ka küberkaitse kontekstis) arutelu selle üle, kuidas peaks NATO reageerima ohtudele, mis ei

[131] Dorman, Andrew M. (2012). NATO's 2012 Chicago summit: a chance to ignore the issues once again? International Affairs. Vol 88, nr 2, lk 301-302.
[132] Burton, Joe. (2015). NATO's cyber defence: strategic challenges and institutional adaptation, Defence Studies. Vol 15, nr 4, lk 308.
[133] Georgescu, Constantin. Tudor, Monica. (2015). Cyber terrorism threats to critical infrastructures NATO's role in cyber defense. Knowledge Horizons / Orizonturi ale Cunoasterii. Vol 7, nr 2, lk 116.
[134] Seal samas.
[135] Burton, Joe. (2015). NATO's cyber defence: strategic challenges and institutional adaptation, Defence Studies. Vol 15, nr 4, lk 308.

tulene kokkulepitud Põhja-Atlandi piirkonnast[136]. Mitmete asümmeetriliste ohtude korral ei ole NATO kollektiivkaitse lihtsalt piisav ning võib-olla peaks NATO tegelema just suuremal hulgal erinevate ohtudega ning muuhulgas ka nendega, mis ei pärine ainult Põhja-Atlandi regioonist[137]. Selline mõte teeks NATO varasemast globaalsemaks organisatsiooniks ning aitaks kaasa tugevama julgeoleku tagamisele, kuna annab signaali, et NATO reageerib kõikidele potentsiaalsetele vaenlastele üle maailma, kes ohustavad Põhja-Ameerikat ja Euroopat.

Ühtlasi toimus Chicagos arutelu selle üle, kas NATO 5. artikkel peab ilmtingimata aktiveeruma vahetult pärast seda, kui on toimunud surmaga lõppenud sündmus või on rünnak ise juba piisav põhjus, millele NATO peaks reageerima, nagu juhtus 2007. aastal Eestis[138]. Konkreetse näitena saab välja tuua olukorra, kus pangandussektori hävitamine võib olla oma olemuselt agressioon, millele NATO võiks reageerida, aga sõltumata teemapüstitusest ei jõutud siin otsusele[139]. Kuigi Chicago tippkohtumise ajaks oli sisuliselt valmis "Tallinna käsiraamat", mis toob selgemalt välja, kuidas küberrünnakuid käsitleda, siis on näha, et Chicagos leidis käesolev teema käsitlust, aga ei jõutud veel ühisele meelele.

Chicagos tõdeti, et liikmesriigid võiksid ja isegi peaksid tõstma enda kaitsekulutusi ning nende kärpimine võib viia olukorrani, kus riigid arendavad ainult enda traditsioonilisi väeliike ja ei arenda välja uusi võimekusi, mille algatamine võib olla kallim ja vajab rohkem spetsialiste, nagu näiteks küberkaitse arendamine selleks on [140]. Kuigi 2012. aastal valitses trend, kus NATO liikmed vähehaaval langetasid oma panuseid riigikaitsesse ja säilitavad olemasolevaid väeliike, ning sellest tulenevalt ei leitud motivatsiooni ka küberkaitsevõimekuse arendamisele uue tulijana. Siinkohal peaks samuti arvestama, et NATO kaitsevõime on täpselt sama tugev, kui tema kõige nõrgem lüli ning, nagu eespool välja toodi, siis kuigi viimastel aastatel on NATO täheldanud, et küberkaitsevõimekus peab olema samaväärne traditsiooniliste väeliikidega, siis see ei vasta alati tõele ning siinkohal ei piisa ainult mõttest, et tuleb arendada, vaid NATO peab rohkem tähelepanu pöörama sellele, et tema liikmesriigid oma küberkaitset kaasajastavad.

[136] Dorman, Andrew M. (2012). NATO's 2012 Chicago summit: a chance to ignore the issues once again? International Affairs. Vol 88, nr 2, lk 309-310.
[137] Seal samas, lk 301.
[138] Seal samas, lk 309-310.
[139] Seal samas, lk 310.
[140] Seal samas.

# 10. WALESI TIPPKOHTUMINE

Walesi tippkohtumine toimus Chicago tippkohtumisega võrreldes märkimisväärselt teistsuguses rahvusvahelises olukorras, kus Venemaa agressioon oma naabrite vastu jätkus ning selgeks viiteks sellele oli Krimmi poolsaare annekteerimine sama aasta alguses ning lisaks nii Ukraina separatistide toetamine kui ka oma vägedega Ida-Ukrainas tegutsemine. Käesolev pingelisem olukord peegeldub selgelt Walesi tippkohtumises endas, kus deklaratsioonis võeti vastu NATO mõistes mitmeid uuendusi, nagu näiteks nii iga liikmesriigi lubadus suurendada oma kaitsekulutusi kui ka küberkaitsele suunatud punktid, mis toovad selgemalt esile, kuidas tuleks seda rahvusvahelise õiguse kontekstis käsitleda.

Walesi tippkohtumise üks suurim uuendus väljendub selgelt juba selle deklaratsiooni küberkaitset puudutavas osas. 2007. aastast alates on olnud õhus küsimus, kuidas käsitleda küberrünnakuid ning aastast aastasse muutus käesolev teema paberil aina selgemaks. Näiteks on võimalik Lissaboni tippkohtumiselt välja tuua, et küberruum kui omaette väeliik muutus võrdseks, aga siiski ei olnud kokkulepitud, kas see omaette on piisav, et kutsuda tinglikult ellu 5. artikkel. Walesi tippkohtumise deklaratsioon toobki seeläbi välja, et rahvusvaheline õigus kehtib ühtemoodi ka küberrünnakutele ning NATO jaoks on küberkaitse osakene kollektiivkaitsest ja sellest tulenevalt võidakse 5. artikkel ellu kutsuda[141, 142]. Siinkohal tuleb arvestada, et lõpliku otsuse teeb siiski Põhja-Atlandi Nõukogu, kuid siiski võrreldes näiteks Lissaboni tippkohtumisega, on see suur hüpe edasi, kuna jõuti järeldusele, et eraldiseisev küberrünnak on piisav, et kollektiivkaitse rakenduks agressori vastu[143]. See on märk sellest, et 2014. aastaks ei ole küberkaitse kui selline ainult tehniline küsimus, vaid võrdväärne väeliik ülejäänutega ning samaväärne nii, nagu see 2010 aastal kokkulepiti. Samas NATO laituseks tuleb tõdeda, et sellise tulemuseni jõuti alles Walesi tippkohtumise ajaks ja see võttis aega seitse aastat ning selle aja jooksul õnneks keegi ei kasutanud seda olukorda kurjasti ära NATO ja tema partnerite vastu.

Ühtlasi on võimalik Walesi tippkohtumisest välja tuua teisi uusi algatusi ning täiendusi. Näiteks sai tähelepanu NATO Kaitseplaneerimise Protsess *(NATO Defence Planning*

[141] Rasmussen, Anders. F. (2014). Press conference following the meeting of the North Atlantic Council at the level of Heads of State and Government during the NATO Wales Summit. North Atlantic Treaty Organization. Kasutatud 28.03.2017. www.nato.int/cps/en/natohq/opinions_112871.htm
[142] North Atlantic Treaty Organization. (2014). Wales summit declaration. North Atlantic Treaty Organization. Pressiteade (2014) 120. Kasutatud 03.04.2017. www.nato.int/cps/cn/natohq/official_texts_112964.htm
[143] Burton, Joe. (2015). NATO's cyber defence: strategic challenges and institutional adaptation, Defence Studies. Vol 15, nr 4, lk 308.

*Process)* ja just selle peastaabi osa ning selle loodi omaette ühine küberkaitse võimekus[144]. Lisaks on NATO ajanud pärast Chicago tippkohtumist poliitikat, millest esimene on Intelligentne Kaitse (*Smart Defence)*. Selle eesmärk on teha kõiksugu tegevusi - nagu näiteks info kogumine, töötlemine ja väljastamine - üheskoos, mitte igaühte eraldi ja seeläbi parandada terve organisatsiooni võimekust[145]. Teiseks uuendati juba 2008. aastal alustatud NATO Küberkaitsepoliitikat (*NATO Cyber Defence Policy*), mida kutsuti nüüd NATO Täiendatud Küberkaitsepoliitikaks (*NATO Enhanced Cyber Defence Policy*)[146]. Käesoleva dokumendiga pöörati varasemast suuremat tähelepanu nendele NATO liikmesriikidele, kes ei ole erinevatel põhjustel pööranud piisavat tähelepanu oma küberkaitse arendamisele, ja sellega kohustati NATO liikmesriike tegema omavahel koostööd selleks, et teineteise küberkaitse taset võrdsustada[147]. Üheks väljundiks said näiteks aina tihedamad ja suuremad ühised küberkaitseõppused Eestis.

Üks laiemaid punkte, mis puudutab tugevalt ka küberkaitse arendamist on Walesis tehtud kaitseministrite ühine kokkulepe, kus kõik alliansi liikmesriigid lubasid iga-aastaselt tõsta enda kaitsekulutusi ja sellest tulenevalt pöörata varasemalt suuremat tähelepanu küberkaitse võimekuse arendamisele - seda traditsiooniliste väeliikide kõrval - andes seeläbi lootust, et kõigi 28 liikmesriigi tase võiks tulevikus selgemalt ühtlustada[148]. See on jällegi tugev kontrast sellele, mis juhtus kaks aastat varem Chicagos, kus oli probleemiks, et NATO liikmesriigid vähendavad oma kaitsekulutusi ja see muudab NATO ühist heidutust nõrgemaks.

Samuti tõdeti küberkaitse all esmakordselt, et on vaja tugevamat koostööd nii erasektori kui ka teiste rahvusvaheliste organisatsioonidega, nagu näiteks Euroopa Liiduga. See on oluline järgmine etapp küberkaitse arendamisel ning mõneti sama oluline, kui see, et pärast 2008. aastat hakati tähelepanu pöörama liikmesriikide küberkaitse võimekusele. Tuleb mõista, et isegi siis kui iga riigi avalik sektor on turvatud, tuleb tähelepanu pöörata ka erasektorile, kellele võib kuuluda suur hulk kriitilist või eluks vajalikku infrastruktuuri. Seepärast on

[144] North Atlantic Treaty Organization. (2013). The Secretary General's Annual Report 2013. 27.01.2014. North Atlantic Treaty Organization. Kasutatud 11.04.2017. www.nato.int/cps/en/natolive/opinions_106247.htm.
[145] Webber, Mark. Hallams, Ellen. Smith, Martin A. (2014). Repairing NATO's motors. International affairs. Vol 90, nr 4, lk 787.
[146] Burton, Joe. (2015). NATO's cyber defence: strategic challenges and institutional adaptation, Defence Studies. Vol 15, nr 4, lk 308.
[147] Kacprzyk, Artur. (2015). NATO Policy on Cyberattacks: Defence and Deterrence. Bulletin. Vol 71, nr 803, lk 2.
[148] NATO. (2014). NATO steps up collective defence, support for reforms in Ukraine. NATO pressiteade. 3. juuni. 2014. Kasutatud 11.04.2017. www.nato.int/cps/en/natolive/news_110609.htm

võimalik esile tuua, kuidas on selline koostöö pärast Walesi tippkohtumist hoogu juurde saanud[149]. Võimalik on välja tuua juba pärast Walesi toimunud NATO poolt korraldatud treeningsessioon parandamaks avaliku- ja erisektori vahelist koostööd[150].

Samas ei ole tegu ainult tehnilise küsimusega, mida saaks koolitusi läbiviies parandada. Seda eriti olukorras, kus aina turvalisematele süsteemidele üleminek on olnud aeglane ning tihti ka kulukas[151]. Seepärast ei liiguta kaasa ei uuemate interneti protokollide ega standarditega rääkimata nendest kasutajatest, kes siiamaani kasutavad aegunud operatsioonisüsteeme, mis ei saa juba ammu vajalikke turvauuendusi[152]. Seda probleemi näeb selgelt ka kriitilise infrastruktuuri puhul ning näiteks USA's on välja toodud, et uue kaitsevõimekuse arendamine või moderniseerimine võib võtta aega 5-10 aastat[153]. Teisalt võivad olla näiteks elektrijaamadel läbimõeldud kriisiplaanid, aga nad ei ole suutelised uuendama viirusetõrjetarkvara olukorras, kus ainuüksi Suurbritannias luuakse igapäevaselt ligi 100 000 uut arvutiviirust[154].

Erasektoriga koostöö saavutamiseks ei peaks NATO tegutsema üksinda, vaid tegema rahvusvahelist koostööd teiste organisatsioonide, nagu näiteks Euroopa Liiduga, kelle eesmärgid on kaudselt sarnased sellele, mis ka NATO'l ehk oma liikmesriikide küberkaitse tagamine. Seda mõistab ka NATO ise, kes selle vajadust Walesi deklaratsioonis tõdes. Teisalt teeb mõlemale osapoolele antud protsessi raskeks see, kui näiteks ainult 15 Euroopa Liidu liikmesriiki on vastu võtnud küberjulgeoleku alased strateegiad ning liikmeskonna kattuvus on üle keskmise[155]. Sellest tulenevalt on võimalik välja tuua, et kuna Euroopa Liidul ei ole ühist küberkaitse poliitikat, siis see nõrgestab ka NATO't ja sellepärast on multilateraalne koostöö vajalik, et mõlemaid organisatsioone tugevdada[156].

Walesi tippkohtumisega on võimalik kokku võtta ühe suure perioodi lõpp küberkaitse strateegiate arendamises, kuna võrreldes 15 aastaga on käesoleva valdkonna olulisus suurenenud nii paberil kui ka tegudes ning see ei ole enam toetusfunktsioonis ning seda

[149] Machi, Vivienne. (2017). Private Sector Plays Bigger Role in NATO Cyber Strategy. National Defense Vol. C1, nr 759, lk 30.
[150] Seal samas
[151] Denning, Dorothy E. (2015). Rethinking the Cyber Domain and Deterrence. Joint Force Quarterly. Nr 77, lk 11.
[152] Seal samas
[153] Seal samas.
[154] Osman, Nazan. (2014). What are the rules of cyber warfare. The Cyber Security Source. 01.09.2014. Kasutatud 03.04.2017. www.scmagazineuk.com/what-are-the-rules-in-cyber-warfare/article/541532/
[155] Sliwinski, Krzysztof F. (2014). Moving beyond the European Union's Weakness as a Cyber-Security Agent. Contemporary Security Policy. Vol 35, nr 3, lk 470.
[156] Seal samas.

arendatakse samaväärselt traditsiooniliste väeliikidega[157]. Seeläbi on võimalik välja tuua, et pärast Walesi ei ole tegu enam lihtsalt tehnilise küsimusega, vaid võrdväärse väeliigiga ning sellest tulenevalt hakkas NATO pöörama rohkem tähelepanu nii enda kui ka oma liikmete kübervõimekuse moderniseerimisele[158].

[157] Abrial, Stéphane. (2011). NATO Builds Its Cyberdefenses. The New York Times. 27.02.2011. Kasutatud 03.04.2017. www.nytimes.com/2011/02/28/opinion/28iht-edabrial28.html
[158] Machi, Vivienne. (2017). Private Sector Plays Bigger Role in NATO Cyber Strategy. National Defense Vol. C1, nr 759, lk 30.

# KOKKUVÕTE

NATO küberkaitsestrateegiate alguseks saab pidada aastat 2002, kui Praha tippkohtumisel võeti vastu esimesed sisulised otsused, mis olid suunatud NATO, kui organisatsiooni küberkaitse arendamiseks. ühelt poolt on võimalik NATO't esile tuua eeskujuna, kes reageeris varakult küberruumis valitsevatele potentsiaalsetele ohtudele. Teisalt 1999. aastal saadud kogemuste põhjal tehtud otsused olid suunitletud NATO enda võrkude kaitseks ning vähe tähelepanu oli pööratud alliansi liikmetele. Lisaks sellele venis üks suuremaid Prahas algatatud ettevõtmisi, ehk NATO Võrkude Küberkaitse Üksuse tööle rakendamine, veel mitmeid aastaid. Ühtlasi kuigi NATO reageeris ühena esimestest küberruumis valitsevatele ohtudele, siis rauges kiiresti ka tema, mis paistab selgelt silma nii Istanbuli kui ka Riia tippkohtumiste deklaratsioonidest. Kui tõstatada küsimus, miks see pärast 2002. aastat, nii läks, siis tuleb tõdeda, et küberkaitse arendamine antud perioodil ei olnud kindlasti mitte NATO tähtsaim eesmärk ning olulisem oli kohanemine Külma sõja järgses rahvusvahelises kogukonnas.

Kui 2007. aastal toimusid Eesti vastu küberrünnakud ja 2008. aasta augustis algas Venemaa-Gruusia sõda, siis saab õigustatult kutsuda mõlemaid sündmusi NATO jaoks suurteks äratusteks. Esimene tõi välja, et sama oluline, kui enda võrkude kindlustamine, on ka oma liikmesriikide aitamine. Venemaa-Gruusia sõda tõi aga esile, kuidas võib tulevikus välja näha hübriidsõda, kus samaaegselt kasutati kineetilisi- ja küberrelvi. Nende sündmuste põhjal on näha, et igal järgneval NATO tippkohtumisel pöörati aina suuremat tähelepanu küberruumile laiemalt. 2008. aastal kiideti Bukarestis heaks NATO Küberkaitsepoliitika ja Brüsselisse loodi Küberkaitse Juhtimiskeskus, mis tsentraliseeris NATO kaitset ja hakkas samas teistele partneritele abi pakkuma. Üks suuremaid institutsionaalseid samme oli NATO Kooperatiivse Küberkaitse Kompetentsikeskuse rajamine, millest kujunes välja teadus- ja uurimuskeskus. Küberkaitsekeskusest sündis omakorda "Tallinna käsiraamat", mis üritas olukorras, kus enamik rahvusvahelist õigust reguleerivaid seadusi olid kirjutatud enne küberrünnakute ajastut, käesolevat lünka täita tuues välja 95 kommenteeritud rahvusvahelise õiguse punkti, mida raamatu autorite arust saab juba praegu kohandada küberrünnakute puhul.

2010. aastal toimunud Lissaboni tippkohtumisel võrdsustati operatsioonitasemel küberrünnakud traditsiooniliste väeliikidega tänu vastu võetud "Strateegilisele kontseptsioonile". Küberrünnakute ohtlikkuse tunnustamise seisukohalt oli tegu olulise

sammuga, mis tõi järgnevateks kümnenditeks NATO arengusuundadesse ka küberkaitse arendamise. Kuigi Lissabonis tõstatus arutelu teemal, kas kollektiivkaitsepunkt jõustub eraldiseisva küberrünnaku puhul, siis selgesõnalist vastust ei tulnud ning pigem leiti, et mitte. 2012. aastal toimunud Chicago tippkohtumisel loodi olemasolevatesse struktuuridesse juurde Kiirreageerimise meeskonnad ning NATO Kommunikatsiooni- ja Informatsiooniagentuuri ülesandeks sai ühise kaitse loomine nii NATO'le kui tema liikmetele. 2014. aasta Walesi tippkohtumisel uuendati NATO Küberkaitsepoliitikat, hakati arendama niinimetatud Intelligentne Kaitset, et olemasolevaid ressursse paremini kasutades luua efektiivsem kaitse. Olulise punktina on võimalik välja tuua, et Walesi tippkohtumisel leiti, et küberrünnak iseseisva rünnakuna on piisav, et pöörduda Põhja-Atlandi Nõukogu poole selleks, et ellu kutsuda Washingtoni leppe 5 artikkel. Ühtlasi sai tähelepanu koostöö arendamine erasektoriga, kellele võib kuuluda osa eluks vajalikust või kriitilisest infrastruktuurist.

Walesi tippkohtumisega on võimalik kokku võtta üks pikk periood NATO küberkaitsestrateegiate arendamise ajaloos, kus jõuti punkti, kus küberruumis toimuvat tunnistatakse eraldiseisva väeliigina ning küberrünnaku tagajärge nähakse piisavalt ohtlikuna, et vajadusel on rünnaku alla jääval riigil õigus pöörduda NATO poole, et aktiveerida Washingtoni leppe 5. artikkel. Samas siinkohal tekib küsimus, mida öelda organisatsiooni kohta, kellel võttis peaaegu 15 aastat, pärast esimese suure rünnaku alla jäämist, aega, et jõuda praegusesse punkti. Ühelt poolt on võimalik esile tuua, et demokraatlikud institutsioonid ongi tihtipeale aeglased protsesse ellu viima, aga julgeoleku küsimustes oleks pidanud eeldama, et tähelepanu pööratakse juba enne 2007. aasta küberrünnakut, kuna nii see kui ka 2008. aastal toimunud Venemaa-Gruusia sõda näitasid võimaliku vaenlase võimekust ning pärast seda on NATO paljuski üritanud järgi jõuda. Tulevikus tuleb ainult loota, et NATO on valmis aina kiiremini muutuvas maailmas veelgi kiiremini kohanema selleks, et tagada oma transatlantilise ühenduse julgeolek.

# KASUTATUD KIRJANDUSE LOETELU

## Dokumendid


1. Council of Europe. (2001). Convention on Cybercrime. Council of Europe. 23.11.2001. Kasutatud 03.04.2017. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm
2. Council of Europe. (2004). Chart of signatures and ratifications. Council of Europe. 01.07.2004. Kasutatud 03.04.2017. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG
3. Küberjulgeoleku strateegia komisjon. (2008). Küberjulgeoleku strateegia 2008–2013. Kasutatud 03.04.2017. Kaitseministeerium. https://valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf
4. Majandus- ja Kommunikatsiooniministeerium. (2014). Küberjulgeoleku strateegia 2014 – 2017. Majandus- ja Kommunikatsiooniministeerium. Kasutatud 03.04.2017. www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf.
5. NATO Public Diplomacy Division. (2003). The Praegue Summit and NATO's Transformation. NATO Public Diplomacy Division Kasutatud 03.04.2017. www.nato.int/docu/rdr-gde-prg/rdr-gde-prg-eng.pdf.
6. North Atlantic Treaty Organization. (2006). Riga summit declaration. North Atlantic Treaty Organization. Pressiteade (2006) 150. Kasutatud 03.04.2017. www.nato.int/docu/pr/2006/p06-150e.htm.
7. North Atlantic Treaty Organization. (2008). Bucharest summit declaration. North Atlantic Treaty Organization. Pressiteade (2008) 049. Kasutatud 03.04.2017. www.nato.int/cps/in/natohq/official_texts_8443.htm
8. North Atlantic Treaty Organization. (2010). Active engagement, modern defence: strategic concept for the defence and security of the members of the North Atlantic Treaty Organisation adopted by heads of state and government in Lisbon. North Atlantic Treaty Organization. 19.11.2010. Kasutatud 28.03.2017 www.nato.int/cps/en/natolive/official_texts_68580.htm

9. North Atlantic Treaty Organization. (2010). Strasbourg/Kehl summit declaration. North Atlantic Treaty Organization. Pressiteade (2009) 004. Kasutatud 14.05.2017. www.nato.int/cps/en/natohq/official_texts_68828.htm
10. North Atlantic Treaty Organization. (2012). Chicago Summit Declaration. North Atlantic Treaty Organization. Pressiteade (2012) 062. Kasutatud 28.03.2017. www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en
11. North Atlantic Treaty Organization. (2013). The Secretary General's Annual Report 2013. North Atlantic Treaty Organization. Kasutatud 11.04.2017. www.nato.int/cps/en/natolive/opinions_106247.htm
12. North Atlantic Treaty Organization. (2014). NATO steps up collective defence, support for reforms in Ukraine. NATO pressiteade. Kasutatud 11.04.2017. www.nato.int/cps/en/natolive/news_110609.htm
13. North Atlantic Treaty Organization. (2014). Wales summit declaration. North Atlantic Treaty Organization. Pressiteade (2014) 120. Kasutatud 03.04.2017. www.nato.int/cps/cn/natohq/official_texts_112964.htm

**Perioodika**

14. Ashmore, William C. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review. Vol 11, nr 1.
15. Burton, Joe. (2015). NATO's cyber defence: strategic challenges and institutional adaptation. Defence Studies. Vol 15, nr 4.
16. Denning, Dorothy E. (2015). Rethinking the Cyber Domain and Deterrence. Joint Force Quarterly. Nr 77.
17. Dorman, Andrew M. (2012). NATO's 2012 Chicago summit: a chance to ignore the issues once again? International Affairs. Vol 88, nr 2.
18. Ducaru, Sorin D. (2016). The cyber dimension of modern hybrid warfare and its relevance for NATO. Europolity. Vol 10, nr 1.
19. Fulghum David A. Wall, Robert. Butler, Amy. (2007). Cyber-combat's first shot. Aviation Week & Space Technology. Vol 167, nr 21.
20. Gati, Charles. (2002). All That NATO Can Be: To Prague and Beyond. The National Interest. Vol 68.

21. Georgescu, Constantin. Tudor, Monica. (2015). Cyber terrorism threats to critical infrastructures NATO's role in cyber defense. Knowledge Horizons / Orizonturi ale Cunoasterii. Vol 7, nr 2.
22. Harašta, Jakub. (2013). Cyber security in young democracies. Jurisprudencija. Vol 20, nr 4.
23. Journal of International Affairs. (2016). Is cyber defense possible? Journal of International Affairs. Vol. 70, nr 1.
24. Kacprzyk, Artur. (2015). NATO Policy on Cyberattacks: Defence and Deterrence. Bulletin. Vol 71, nr 803.
25. Laasme, Häly. (2011). Estonia: Cyber window into the future of NATO. JFQ: Joint Force Quarterly. Vol 63, nr 4, lk 61.
26. Laasme, Häly. (2012). The Role of Estonia in Developing Nato's Cyber Strategy. Cicero Foundation Great Debate Paper. Vol 12, nr 8.
27. Machi, Vivienne. (2017). Private Sector Plays Bigger Role in NATO Cyber Strategy. National Defense Vol. C1, nr 759.
28. Mirkovic, Jelena. Reiher, Peter. (2004). A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. ACM SIGCOMM Computer Communication. Vol 34, nr 2.
29. Noetzel, T. Schreer, B. (2012). More flexible, less coherent: NATO after Lisbon. Australian Journal of International Affairs Vol 66, nr 1.
30. Schmitt, Michael N. (2015). The law of cyber targeting. Naval War College Review. Vol 68, nr 2.
31. Shakarian, Paulo. (2011). The 2008 Russian Cyber Campaign Against Georgia. Military Review. Vol 91, nr 1.
32. Sliwinski, Krzysztof F. (2014). Moving beyond the European Union's Weakness as a Cyber-Security Agent. Contemporary Security Policy. Vol 35, nr 3.
33. Szentgáli, Gergely. (2013). The NATO Policy on Cyber Defence: The Road so Far. Academic & Applied Research in Military & Public Manageme. Vol 12, nr 1.
34. Stephen Herzog. (2011). Revisiting the Estonian Cyber Attacks: Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security. Vol 4, nr 2.
35. US Department of Defense. (2010). Quadrennial Defense Review Report. Washington DC: US Department of Defense. Veebruar 2010.

36. Wallander, Celeste. A. (2000). Institutional assets and adaptability: NATO after the Cold War. International Organization. Vol 54, nr 4.
37. Webber, Mark. Hallams, Ellen. Smith, Martin A. (2014). Repairing NATO's motors. International affairs. Vol 90, nr 4.
38. Yost, David S. (2010). NATO's evolving purposes and the next Strategic Concept. International Affairs. Vol 86, nr 2.

**Internetiviited**

39. Abrial, Stéphane. (2011). NATO Builds Its Cyberdefenses. The New York Times. 27.02.2011. Kasutatud 03.04.2017. www.nytimes.com/2011/02/28/opinion/28iht-edabrial28.html
40. Corbin, Kenneth. (2009). Lessons from the Russia-Georgia Cyberwar. Real time IT News. 12. 03. 2009. Kasutatud 20.03.2017. www.internetnews.com/government/article.php/3810011/Lessons-From-the-Russia-Georgia-Cyberwar.htm
41. Danchev, Dancho. (2008). Coordinated Russia vs. Georgia Cyber Attack in Progress. ZDNet. 11.08.2008. Kasutatud 03.04.2017. www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/
42. Geers, Kenneth. (2010). Valmistume kübersõjaks. Diplomaatia. September nr. 85. Kasutatud 28.12.2016. www.diplomaatia.ee/artikkel/valmistumine-kubersojaks/
43. Hughes, Rex B. (2009). NATO and Cyber Defence. Mission Accomplished. Atlantische Commissie. Kasutatud 03.04.2017. www.atlcom.nl/ap_archive/pdf/AP%202009%20nr.%201/Hughes.pdf
44. Joshua Davis. (2007). Hackers Take Down the Most Wired Country in Europe. Wired Magazine. 21.09.2007. Kasutatud 14.05.2017. www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=1
45. McLaughlin, Daniel. (2008). Lithuania accuses Russian hackers of cyberassault after collapse of over 300 websites. Irish Times. 02.07.2008. Kasutatud 24.04.2017. www.irishtimes.com/news/lithuania-accuses-russian-hackers-of-cyber-assault-after-collapse-of-over-300-websites-1.942155
46. Meikar, Silver. (2013). Sõda internet pärast. Diplomaatia. September, nr. 121. Kasutatud 28.12.2016. www.diplomaatia.ee/artikkel/soda-interneti-parast/

47. Messmer, Ellen. (1999). Kosovo cyber war intensifies: Chinese hackers targeting U.S. sites, government says. CNN. 12.05.1999. Kasutatud 21.04.2017. http://edition.cnn.com/TECH/computing/9905/12/cyberwar.idg/
48. Mälksoo, Lauri. (2013). "Tallinna käsiraamat" kui rahvusvahelise elu sündmus. Diplomaatia. August nr. 120. Kasutatud 28.12.2016. www.diplomaatia.ee/artikkel/tallinna-kasiraamat-kui-rahvusvahelise-elu-sundmus/
49. Nakashima, Ellen. (2012). With Plan X, Pentagon seeks to spread U.S. military might to cyberspace. Washington Post. 30.5.2012. Kasutatud 14.05.2017. www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-tospread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html.
50. Osman, Nazan. (2014). What are the rules of cyber warfare. 01.09.2014. The Cyber Security Source. Kasutatud 03.04.2017. www.scmagazineuk.com/what-are-the-rules-in-cyber-warfare/article/541532/
51. Ottis, Rain. (2013). Kübersõja küsimärgid ja eripärad. Diplomaatia. September, nr. 121. Kasutatud 28.12.2016. www.diplomaatia.ee/artikkel/kubersoja-kusimargid-ja-eriparad/
52. Spillius, Alex. (2011). US could respond to cyber-attack with conventional weapons. Daily Telegraph. 01.06.2011. Kasutatud 27.03.2017. www.telegraph.co.uk/news/worldnews/northamerica/usa/8550642/ US-could-respond-to-cyber-attack-with-conventional-weapons.html
53. Zmijewski, Earl. (2008). Georgia Clings to the Net. Reneysys: The Internet Intelligence Authority. 10.08.2008. Kasutatud 20.03.2017. http://dyn.com/blog/georgia-clings-to-the-net/
54. Tiirmaa-Klaar, Heli. (2010). Rahvusvaheline koostöö küberjulgeoleku tagamisel. Diplomaatia. September nr. 85. Kasutatud 28.12.2016 www.diplomaatia.ee/artikkel/rahvusvaheline-koostoo-kuberjulgeoleku-tagamisel/

**Artiklite kogumikud**

55. Rantapelkonen, Jari. Salminen, Mirva. (2013). The Fog of Cyber Defence. Tampere. Juvenes Print Oy.

**Muud allikad**


56. Bumgarner, John. Borg, Scott. (2008). Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008. U.S. Cyber Consequence Unit Special Report. August 2009.
57. Rasmussen, Anders. F. (2014). Press conference following the meeting of the North Atlantic Council at the level of Heads of State and Government during the NATO Wales Summit. North Atlantic Treaty Organization. Kasutatud 28.03.2017. www.nato.int/cps/en/natohq/opinions_112871.htm

## Summary – "NATO Cyber Defence Strategies during 2007-2015"

The North-Atlantic Treaty Organization (NATO) has given since its creation a huge impact to today's political system in Europe. After the collapse of the USSR, NATO might have lost its main opponent, but since then new dangers have emerged, one of them being different asymmetrical threats, for example, terrorism, biological and chemical weapons of mass destruction and cyber-attacks. All these threats have the potential to be a danger to the security of nation-states. Besides that, the even growing dependences on different communication devices, internet networks, and digital infrastructures mean that it would make no sense for potential threats not to use those digital opportunities to benefit from them. Taking into consideration the rapid development of those fields it means, that also NATO must be one step ahead to be able to create security in the North-Atlantic region. The problem is that cyberattacks, like many other asymmetrical threats, cannot be treated like traditional kinetical weapons. For example, with a cyber-attack it can be done from anywhere in the world and because of its anonymity and global nature it's no wonder if it might become one of the main arsenals for different non-country groups around the world. This paper aims to give an overview how NATO has done during the period of 2007-2015 with the challenge and what kind of institutional and political changes have been made to benefit the transatlantic union.

Although one of the most famous cyber-attacks is 2007 on against Estonia, then the roots of NATO's cyber defence strategies go back to 1999 when NATO involved itself in the Kosovo crisis and because of that came under a cyberattack. Besides that, attacks were carried out against the participating NATO members. This is many ways opened the eyes for NATO against the potential threats and in the following Prague Summit in 2002 NATO took its first steps in building up its cyber defence strategies. The NATO Cyber Defence Program was accepted and one of the first actions was the launching of the NATO Computer Incident Response Capability. With that, a bigger emphasis was put on defending its own networks against emerging new threats like cyber-attacks. Although it can be brought out as a fast reaction against new threats, then during the Istanbul and Riga summits minimal or nothing was done to improve upon the decisions taken in Prague and many initiatives like Computer Incident Response Capability were not fully operational. Likewise, the decision made in Prague focused mainly on protecting the infrastructure of NATO itself and not the ones of

its allies. This policy ended after the cyber-attack in 2007 when Estonia came under a cyberattack and when in 2008 for the first time openly kinetical and cyber weapons were used during a combat operation in Georgia in the Russo-Georgian war.

Since then every following NATO summit has focused on cyber defence related topics and has improved year by year and a bigger emphasis has been put on the defence of NATO's member states. Starting with the Bucharest summit in 2008 a bigger promise to cyber defence can be brought out beginning with the confirmation of the NATO Policy on Cyber Defence and creation of the Cyber Defence Management, which was located Brussels. Also in 2008, it was accepted that the NATO Cooperative Cyber Defence Centre of Excellence will be launched in Estonia. Since its creation, it has turned out to be a science- and education centre which organizes different training sessions and cyber defence exercised like Cyber Coalition and Locked Shields. Furthermore, it started the project "Tallinn manual" to help clear the fog what is related to cyber-attacks and international law.

The biggest steps were taken in Lisbon in 2010 when NATO accepted its new Strategic Concept and for the first, it included the cyberspace as an operation theatre. Although Lisbon's summits declaration lacked the notion of cyber deterrence which meant, that the Washington Treaty Article 5 was not triggered turning cyber-attacks. This was made a lot clearer during the next years when the discussion started about throughout the Chicago summit in 2012 and in Wales 2014 it was finally decided, that a cyber-attack alone against a NATO member is enough to ask the North-Atlantic Council for help. In Chicago, it was also agreed upon to creation of the Rapid Reaction Team's to be ready at a moment notice to react to different cyber-attacks and to forestall different attacks the NATO Communications and Information Agency was founded. NATO Computer Incident Response Capability came also active after the Wales summit. In Wales, the Smart Defence concept, NATO Defence Planning Process, and the Enhanced Cyber Defence Policy were agreed upon. As a new political move upon Wales a bigger attention was put into cooperation with private sector who might own critical or vital services to help those services to be up to date.

During the period of 2007-2015 NATO has been considerable improvements to its cyber defence related strategies and upon Wales, an important period in NATO's history can be concluded. On the other, it must be asked why it took NATO that long to realize the potential threat of cyberattacks and action was taken after 2007 because the first contact was already

made in 1999. This meant, that for the following years NATO was catching up on the field of cyber defence in a situation where potential threats were openly concluding hybrid warfare. This had the potential to create a lack of security if there were threats who would have wanted to exploit it. Because of that, it is important for NATO to continue being active in the field of cyberspace and improving its cyber defence to combat potential dangers.

**Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks**

Mina, **Henry Narits** (sünnikuupäev: 03.12.1992)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose **"NATO Küberkaitsestrateegiad aastatel 2007-2015"**, mille juhendaja on dotsent Vahur Made.

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

1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.
3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, 19.05.2017