TARTU ÜLIKOOL
SOTSIAALTEADUSTE VALDKOND
ÕIGUSTEADUSKOND
Avaliku õiguse osakond

Sander Pelisaar

Tallinna käsiraamatust rahvusvahelise küberrünnakuid piirava konventsioonini?

Magistritöö

Juhendaja professor *dr. iur.* Lauri Mälksoo

Tartu 2018

SISUKORD

SISSEJUHATUS

Eesti riigi lähiajalugu üheks enimmõjutanud sündmuseks võib lugeda 2007. aasta aprillikuus küberrünnaku ohvriks sattumist. Küberrünnaku käigus rünnati nii Riigikogu, ministeeriumeid, valitsusasutusi, pankasid kui ka meediaväljaandeid teenusetõkestamise rünnaku[1] näol. See sündmus oli murdepunktiks, mis laiendas nii Eesti kui paljude teiste riikide jaoks julgeolekumõistet. Natuke rohkem kui aasta pärast Eestile sooritatud küberrünnakuid asutati just Eestisse NATO küberkaitsekoostöö keskus (*NATO Cooperative Cyber Defence Centre of Excellence*). Sellest ajast on keskendutud nii tehnilise võimekuse tõstmisele küberkaitse osas kui ka juriidiliste lahenduste leidmisele rahvusvahelise õiguse tasandil.

2018. aasta üht suuremat spordisündmust Lõuna Koreas, Pyeongchangis toimunud olümpiamänge jäi varjutama sündmus, kus küberrünnaku näol rünnati olümpiamängude ametlikku kodulehte ning televisiooni- ja internetisüsteeme, peamiseid meediakanaleid spordisündmuse kajastamisel.[2] Hiljem on USA julgeolekuteenistused väitnud, et tegemist oli Venemaa poolse rünnakuga, kus Venemaa proovis rünnaku käigus segada oma jälgi, soovides antud rünnaku süüdlaseks lavastada Põhja-Korea.[3] Sama aasta märtsikuus tuli USA välja süüdistusega, kus väidetakse, et Venemaa ründas 2016. aastal USA energiavõrku, olles katsetanud ka teiste USA kriitiliste infrastruktuuride süsteemide vastupidavust, näiteks tuumaenergia, veevärgi ning lennundusega seotud infrastruktuure ning teenusepakkujaid.[4] 2018. aasta märtsikuus rünnati Saksamaa välisministeeriumi arvutivõrgustikku, mis häirisid valitsusevahelist suhtlust ning tööd.[5] 2017. aastal levis lunavara tüüpi pahavara WannaCry, mis haavas erinevaid andmeid koguvaid teenusepakkujaid, eriti tervishoiuteenuse pakkujaid,

[1] Küberrünnaku liik, mille kaudu toimub arvuti või arvutivõrgu ülekoormamine samal ajal suure hulga päringute

[2] Winter Olympics hit by cyber-attack. 12. veebruar. 2018.
Arvutivõrgus: http://www.bbc.com/news/technology-43030673 (24 märts 2018)

[3] E. Nakashima. Russian Spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say. 24. veebruar. 2018. Arvutivõrgus: https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html?utm_term=.721da7056aff (31 märts 2018)

[4] D. Volz, T. Gardner. In a first, U.S. blames Russia for cyber attacks on energy grid. 15. märts. 2018. Arvutivõrgus: https://www.reuters.com/article/us-usa-russia-sanctions-energygrid/in-a-first-u-s-blames-russia-for-cyber-attacks-on-energy-grid-idUSKCN1GR2G3 (24 märts 2018)

[5] T. Severin, A. Shalal. German government under cyber attack, shores up defenses. 1. märts. 2018. Arvutivõrgus: https://www.reuters.com/article/us-germany-cyber/german-government-under-cyber-attack-shores-up-defenses-idUSKCN1GD4C8 (24 märts 2018)

kellest mõned ka Eestist olid sunnitud küberkurjategijatele maksma krüoptoraha, et lunavara poolt krüpteeritud andmeid taas kasutada saaks.[6] USA julgeolekuteenistused tulid 2017. aasta lõpus, pärast pikka ning põhjalikku juurdlust välja seisukohaga, et WannaCry lunavara taga on Põhja-Koreaga seotud valitsusasutused.[7] Mõned kuud pärast WannaCry rünnakut hakkas levima Petya nimeline lunavara, mille eesmärk oli samuti andmete krüpteerimine ning selle näol ettevõtete ning valitsuste tööd halvata, antud lunavara puhul aga kahtlustatakse, kas antud tegevuse eesmärgiks oli ikkagi majandusliku kasu teenimine. Nimelt arvavad eksperdid, et Petya näol taheti jätta muljet lunavarast, olles tegelikkuses konstrueeritud pahavara tagamõttega. Sellele viitab amatöörlik ning läbimõtlemata tasu teenimise viis, täpsemalt üks bitcoini aadress (tavapäraselt on iga ohvri jaoks unikaalne bitcoini aadress) ning üldine e-mail pahavara loojatega suhtlemiseks, mis andis võimaluse kiirelt e-maili teenusepakkujal konto sulgeda.[8] Kuna viimati nimetatud rünnak sai väidetavalt alguse Ukraina territooriumilt, arvatakse, et rünnaku taga on Venemaaga seotud häkkerid, kuna nii eelnevalt kui ka samal ajaperioodil langes Ukraina ka mitmete teiste küberrünnakute ohvriks tulenevalt Ukraina sõja tõttu. Näiteks 2015. aasta 23. detsembril rünnati Ukraina elektrilevivõrke (arvatakse, et pahavaraga BlackEnergy), mille tulemusena jäi elektrita üle 225 000 kasutaja.[9] Viimaste aastate enim kõneainet pakkunud küberrünnak pandi toime 2016. aasta USA presidendivalimistel, kui Venemaa häkkerid said juurdepääsu väidetavalt 39 osariigi hääletussüsteemile.[10]

Aastast 2015 on muutumatuna püsinud 5 kõige rünnatumat valdkonda, milleks on tervishoiuteenused, finantsteenused, tööstusvaldkond, valitsusvaldkond ning

---

[6] Küberturvalisuse seaduse eelnõu seletuskiri. 26. september. 2017 Arvutivõrgus: https://www.koda.ee/sites/default/files/content-type/content/2017-10/seletuskiri_k%C3%BCberturvalisuse%20seadus.pdf lk 8 (24 märts 2018)

[7] Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea 19. detsember. 2017. Arvutivõrgus: https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/ (24 märts 2018)

[8] O. Solon, A. Hern. Petya ransomware attack: what isi t and how can it be stopped? Arvutivõrgus: https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how (12 märts 2018)

[9] Cyber-Attack Against Ukrainian Critical Infrastructure. veebruar 2016. Arvutivõrgus: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (12 märts 2018)

[10] M. Riley, J. Robertson. Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known. 13. juuni. 2017. Arvutivõrgus: https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections (24 märts 2018)

transpordivaldkond.[11] Majandus kui riigi funktsioneerimise üks peamiseid eksisteerimise tugitalasid, on järjest suurema surve all ning statistikast nähtub, et viie enim rünnatud valdkonna hulgas on kõik enam või vähem riigikorralduse ning riigi kui terviku funktsioneerimisega seotud. Praeguste prognooside kohaselt võib küberrünnakute poolt tekitatud ülemaailmne kahju küündida aastaks 2021 koguni 6 miljardi dollarini.[12]

Need on vaid üksikud näited paljudest küberrünnakutest, mis lähiminevikus riikide vastu toime on pandud, ületamata paljudel juhtudel isegi rahvusvahelist uudiskünnist. Viimaste aastate tendents ei ole kahjuks näidanud küberrünnakute vähenemise märke, pigem on see suurenemas. Ühest küljest on tegemist ühe osaga kuritegevusest, mis on laienenud küberruumi, teisalt proovivad küberrünnakuid enda huvides järjest enam ära kasutada ka riigid, soovides mõjutada seeläbi teiste riikide poliitikat ja majandust ning õõnestada nende julgeolekut.

Tahes-tahtmata tundub, et riigid peavad uue reaalsusega harjuma, leides uute tehniliste võimaluste kõrvale lahendused ka juriidilistele probleemidele, eelkõige laiapinnalise rahvusvahelise lahenduse näol. Julgen väita, et küberjulgeolekust koos küberrünnakutele lahenduse leidmisega võib suure tõenäosusega saada 21. sajandi üheks suuremaks väljakutseks, mis hõlmab pidevat võitlust nii tehnilisel kui juriidilisel rindel.

Eelnevast lähtuvalt tekib küsimus, kas praegune rahvusvaheline õigus on piisav, hoidmaks ära küberrünnakuid riikide vastu ning võtta vastutusele riike, kes on rahvusvahelist õigust eiranud. Kas praegused rahvusvahelise õiguse normid kaitsevad riike ka mitteriiklike organisatsioonide poolt korraldatud küberrünnakute eest?

Küberruumi ning küberrünnakuid reguleerivad rahvusvahelise õiguse normid puuduvad. Seetõttu tuginetakse praegusel hetkel paljuski Ühinenud Rahvaste Organisatsiooni põhikirjale ning teistele rahvusvaheliselt kehtivatele lepingutele ja põhimõtetele. Kuna kehtiva õiguse põhimõtete all ei ole silmas peetud küberrünnakute olemust ning selle spetsiifilisust, jätab kehtiv rahvusvaheline õigus üsna laia tõlgendusvabaduse küberrünnakute kontekstis. Kas taolise tõlgendamisvabaduse näol on üldse praktikas võimalik õigust rakendada? Kas riigid

[11] S. Morgan. 2017 Cybercrime Report. Cybersecurity Ventures. Arvutivõrgus: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf lk 10 (24 märts 2018)

[12] *Ibid.* lk 3

saavad nii laia tõlgendusvõimaluse korral küberruumi asjadest ühte moodi aru või on küberrünnakute ning kübertemaatika kohati liiga kompleksne ning spetsiifiline, kus liiga lai tõlgendusviis ei pruugi viia kõikide probleemide lahenduste tuumadeni?

Kui rahvusvahelise õiguse tõlgendamine küberrünnakute kontekstis kehtiva rahvusvahelise õiguse alusel ei peaks pikas perspektiivis olema jätkusuutlik, siis kas lahenduseks võib olla viimastel aastatel järjest enam arutatud küberkonventsioon? Küberkonventsioon annaks võimaluse keskenduda kübermaailma erisustele ning annaks riikidele konkreetsed käitumisjuhised, lubatu ning lubamatu vahel. Teisalt on selge, et rahvusvahelises õiguses ei ole võimalik konventsioone ilma üldise konsensuseta luua. Seega vajab antud teema lahendamine eelkõige riikidevahelisi kompromisse, mis teeniks nii kodanike kui riikide huve, jätmata samal ajal tähelepanuta ka majandussfääri.

Uurimistöös kasutatakse peamiselt nii süstemaatilis-analüütilist kui ka võrdlevat uurimismetoodikat. Süstemaatilis-analüütilist metoodikat kasutab töö autor eelkõige osas, kus käsitletakse probleeme, mis tulenevad küberrünnaku tõlgendamisest. Millistel juhtudel on küberrünnak rünnak riigi kui suveräänse terviku vastu ning millisel juhul rünnak üksikisiku vastu. Võrreldakse maid, õigussüsteeme ning nende lahendusi. Peamiselt on töös kasutatud Ameerika Ühendriikide, NATO liikmesriikide ning Euroopa õigusteadlaste artikleid, samuti on kasutatud Tallinna käsiraamatut (*Tallinn Manual 2.0*), kui erinevate riikide kübervaldkonna ning rahvusvahelise õigusega tegelevate õigusteadlaste kokkuvõtvaid seisukohti.

Magistritöö eesmärgiks on välja selgitada, millised on vajalikud sammud, tagamaks praktikas rahvusvahelise õiguse kohaldatavus küberrünnakute kontekstis. Magistritöö eesmärgist tulenevad järgmised uurimisküsimused. Esiteks, kas praegune olukord, kus rahvusvaheline õigus reguleerib küberruumi küberrünnakute kontekstis, on praktikas kohaldatav? Teiseks, kui jätkusuutlik on praegune olukord ning kas lahendus võiks olla küberkonventsioon, mis reguleeriks küberruumi just küberrünnakute osas?

Magistritöö ülesehitus lähtub töö uurimisküsimustest. Töö esimeses peatükis analüüsitakse küberrünnaku definitsiooni, tuuakse välja nende erinevused, sarnasused ning probleemid, mis definitsioonidest tulenevad.

Teises peatükis käsitletakse Tallinna käsiraamatus valitsevaid seisukohti ning analüüsitakse, kas antud käsitluse põhjal on võimalik riikidel jõuda kokkuleppele, kuidas rahvusvahelist õigust küberrünnakute korral tõlgendada ning kas selline tõlgendus on piisav rahvusvahelise korra tagamiseks. Samuti käsitletakse antud punktis, kas rahvusvahelises õiguses õigust loov praktika võiks olla olukorra lahenduseks.

Kolmandas peatükis analüüsib autor, kas küberkonventsioon võiks olla kübersfääris valitsevate probleemide lahenduseks. Pakutakse välja võimalikke lahendusi küberrünnakute sfääris ning tuuakse välja, mida võimalik küberkonventsioon endas sisaldama peaks. Samuti lahatakse küberkonventsiooni loomise võimalikkust ning vajalikkust.

Tulenevalt üliõpilastöö kirjutamise ja vormistamise juhendist[13], on järgnevalt loetletud magistritööd enim iseloomustavad märksõnad: kübersõda, sõjaõigus, jõu kasutamine, repressaalid, rahvusvaheline õigus.

[13] J. Sootak jt (koost). Üliõpilastöö kirjutamine ja vormistamine: juhend õigusteaduskonna üliõpilastele. Tallinn: Juura 2016. Arvutivõrgus: https://issuu.com/iuridicum/docs/juhend_2016 (22 märts 2017)

1. KÜBERRÜNNAKU DEFINITSIOON

1.1. Poliitiline taust

Antud teema avamiseks rahvusvahelise õiguse valguses on vajalik käsitleda rahvusvahelise poliitika taustsüsteemi küberruumi ning küberrünnakute kontekstis. Ilmselt ei ole kellelegi üllatuseks, et rahvusvahelist õigust kujundab olulisel määral ka rahvusvaheline poliitika, seda just valdkondade osas, mis on väljakujunemise järgus. Nimelt kujundavad paljuski just poliitilised seisukohad ka rahvusvahelise õiguse võimalikku rakendamist praegu ja tulevikus.

Praegusel hetkel puuduvad küberruumis, sealhulgas küberrünnakute kontekstis rahvusvaheliselt tunnustatud käitumisnormid ja tavad. Puudub ka poliitiline tahe rahvusvahelisel tasandil üksmeele leidmiseks ning nagu järgnevalt selgub, on riikide seisukohad nii küberruumi kui ka küberrünnakute küsimuses üsna erinevad. Rahvusvahelise õiguse edendamiseks küberrünnakute kontekstis on loodud ÜRO liikmesriikide kübereкspertide nõukogu[14], mille eesmärgiks on küberruumi reguleerimine rahvusvahelise õiguse kaudu ning üksmeele leidmine ÜRO liikmesriikide vahel. Antud nõukogu töö on toonud ka märgatava progressi riikidevahelistes suhetes, kuid kahjuks ei ole täielikult loodetud edu saavutanud.

[14] ÜRO liikmesriikide kübereкspertide nõukogu on ÜRO volitusel loodud töögrupp, teabekaitse küsimustes Tänaseks päevaks on antud teemadega tegelenud 5 töögruppi alates aastast 2004. ÜRO liikmesriikide kübereкspertide nõukogu on saavutanud kaks olulist edusammu küberruumis, ülemaailmse küberkaitse protokolli koostamine ning rahvusvahelise õiguse kohaldumise printsiibi toomine kübersfääri konteksti. ÜRO kübereкspertide nõukogusse kuuluvad ÜRO julgeolekunõukogu alalised riigid: USA, Suurbritannia, Prantsusmaa, Venemaa, Hiina ning roteeruvad riigid (sulgudes nõukogus oldud aastad): Saksamaa (2004-2017), Jordaania (2004-2005), Mali (2004-2005), India (2004-2017), Brasiilia (2004-2010, 2014-2017), Valgevene (2004-2015), Mehhiko (2004-2005, 2014-2017), Malaisia (2004-2005, 2014-2015), Lõuna-Aafrika Vabariik (2004-2005, 2009-2010), Eesti (2009-2017), Itaalia (2009-2010), Qatar (2009-2010), Iisrael (2009-2010, 2014-2015), Egiptus (2012-2017), Jaapan (2012-2017), Austraalia (2012-2013, 2016-2017), Kanada (2012-2013, 2016-2017), Indoneesia (2012-2013, 2016-2017), Argentina (2012-2013), Keenia (2014-2017), Hispaania (2014-2015), Kolumbia (2014-2015), Ghana (2014-2015), Pakistan (2014-2015), Soome (2016-2017), Kuuba (2016-2017), Botswana (2016-2017), Kasahstan (2016-2017), Serbia (2016-2017), Holland (2016-2017), Senegal (2016-2017). Loetletud riikide nimekiri näitlikustab soovi leida lai kandepind, mis on vajalik nii poliitilise toetuse huvides kui ka rahvusvahelises õiguses eksisteeriva ühise seisukoha leidmiseks, ehk mida suurem hulk riike aktsepteerib ühte seisukohta ning saavad asjadest ühte moodi aru, seda suurem on tõenäosus konsensuseks ning rahvusvahelise tavaõiguse kujunemiseks.

Poliitiliselt on peamiselt kaks erinevat arusaama küberruumist, moodustades omavahel vastasleerid. Nende kahe leeri vahele jäävad riigid, kelle seisukohad on mingil määral varieeruvad või kellel puudub sootuks konkreetne arusaam ning vaade, mida küberruum endast võiks kujutada või millisel moel peaks seda reguleerima. Lääneriikide ning samameelsete (*like-minded*) riikide huviks on kübersfääri reguleerimine kehtiva rahvusvahelise õiguse läbi. Teine suurem rühm riike on nn Shanghai koostööorganisatsiooni[15] riigid, kelle seas on Hiina, Venemaa, Kasahstan, Kõrgõzstan, Tadžikistan ja Usbekistan, kes sooviksid küberruumi reguleerida küberkonventsiooni näol.

Viimati nimetatud riigid on teinud ka mitmeid küberkonventsiooni loomise ettepanekuid. Esimene vastav ettepanek tehti ÜRO-s 2011. aastal. 2015. aastal korrati sama ettepanekut, muutes teatud määral konventsiooni kavandatavat sisu ja sõnastust. Shanghai koostööorganisatsiooni riikide poolt kavandatav konventsioon kannab nime Rahvusvaheline käitumiskoodeks teabekaitseks (*International code of conduct for information security*). Seega ei lähtu nende riikide arusaam mitte küberruumist või küberrünnakute olemusest, vaid teabe või informatsioon kaitsest.

Venemaa, olles Shanghai koostööorganisatsiooni seisukohtade üheks keskseks kujundajaks, on samuti selgitanud, et nende arusaam ei koosne vaid küberruumist, vaid palju laiemalt, informatsioonist ning informatsiooniruumist. Täpsemalt on seda mõistet käsitletud „Venemaa Föderatsiooni Relvajõudude käitumisjuhisest Informatsiooniruumis“ järgnevalt: „Konflikt kahe või enama riigi vahel informatsiooniruumis eesmärgiga tekitada kahju informatsioonisüsteemidele protsessidele, ressurssidele, kriitiliselt olulistele ning teistele infrastruktuuridele, kahjustada ning rikkuda poliitilist, majanduslikku ja sotsiaalset süsteemi, destabiliseerides massipsühholoogia abil ühiskonda ja riiki ning sundida võimu tegema otsuseid teise riigi huvides.“[16] Antud definitsiooni sõnastus ise näitlikustab ehk kõige

[15] Shanghai koostööorganisatsioon (ingl k. Shanghai Cooperation Organization, SCO) 2001. aastal asutatud piirkondlik julgeolekukoostööorganisatsioon. Liikmeteks on Venemaa, Hiina, India, Kasahstan, Kõrgõzstan, Pakistan, Tadžikistan, Usbekistan.

[16] K. Giles. Russia’s Public Stance on Cyberspace Issues. 2012 4th International Conference on Cyber Conflict. lk 67-69 Arvutivõrgus: https://ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf (30 märts 2018)

“conflict between two or more states in information space with the aim of causing damage to information systems, processes and resources, critically important and other structures, subverting the political, economic

ilmekamalt, kui diametraalne on nende kahe erineva riikide leeri rahvusvahelise õiguse käsitlus küberruumist. Sellise lähenemise taga võib näha Venemaa hirmu vaba internetikeskkonna ees ning soovi allutada internetikeskkond riigi teatava kontrolli alla. Sellise informatsiooniruumi kokkuleppelise mõiste eesmärk on ilmselt vaigistamaks teiste riikide ning ÜRO kriitikat madala internetivabaduse osas. Inimõiguste põhimõtete laienemise küberruumi on heaks kiitnud ÜRO peaassamblee 27. juuni 2016. aasta samasisulise avaldusega.[17] Seega laieneb küberruumi ÜRO Inimõiguste ülddeklaratsioon, mille artiklis 19 sätestatakse, et igaühel on arvamuse- ja sõnavabadus; see õigus kätkeb vabadust sekkumiseta oma veendumustest kinni pidada ja vabadust informatsiooni ja ideid otsida, saada ja levitada igasuguste abinõudega ja riigipiiridest sõltumata.[18] Vene föderatsiooni informatsiooniruumi mõiste annab neile nende endi hinnangul justkui õigustuse tagandada ennast sõnavabaduse põhimõttest, viidates et põhivabaduste propageerimine on teiste riikide soov rikkuda poliitilist ning sotsiaalset süsteemi ning destabiliseerida ühiskonda, sekkudes teise riigi siseasjadesse.

Venemaa seisukohti informatsiooniruumist jagab paljuski ka Hiina, pidades küberruumi asemel silmas samuti laiemalt informatsiooni- või teaberuumi. Lühidalt öeldes räägivad Lääneriigid ning samameelsed tegelikust probleemist ning Shanghai koostööorganisatsiooni riigid kõigest, mis probleemi ümbritseb, välja arvatud rahvusvahelises õiguses valitsevast probleemist enesest. Antud tõlgenduse eesmärgina võib näha soovi tagada suveräänsuse tunnustamine internetikeskkonnas. Teisisõnu tagada Hiina internetitsensuuri tunnustamine ning heakskiit sellele teiste riikide poolt. Hiina seisukohad ÜRO küberekspertide nõukogus on ajas muutunud. Väidetavalt on selle põhjus küberekspertide nõukogu algusfaasis ebapädevate diplomaatide saatmine nõukogusse, kes ei esindanud Hiina õiguspoliitilisi seisukohti. Seetõttu hoidsid Hiina ametnikud nõukogu algsetest aruteludest eemale ning jälgisid selle arengusuundi tagaplaanilt. Samuti oli rahvusvahelise õiguse tendentsi jälgivate inimeste arvates 2013. aastal Hiina nõustumine rahvusvahelise õiguse kohaldamisega küberrünnakute

---

and social systems, mass psychological work on the population to destabilise society and the state, and coercing the government to take decisions in the interests of the opposing side."

[17] United Nations General Assembly. Human Rights Council. The Promotion, protection and enjoyment of human rights on the Internet. 27. juuni 2016. Arvutivõrgus: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf (29 märts 2018)

[18] ÜRO Inimõiguste ülddeklaratsioon. Arvutivõrgus: http://vm.ee/et/uro-inimoiguste-ulddeklaratsioon (12 märts 2018)

kontekstis pigem tahtmatu viga kui läbikaalutletud otsus.[19] Teades viimaseid arenguid antud kontekstis, on selline seisukoht üsna tõenäoline. On selge, et ilma tegeliku tahteta tegutsemine muudab riikidevahelise koostöö ning kompromisside leidmise keeruliseks.

Algselt olid nii Venemaa, Hiina kui ka teised ÜRO liikmesriigid nõus rahvusvahelise õiguse kohaldumisega küberrünnakute kontekstis. Oluline muudatus selles toimus aga viimase, 2017. aasta ÜRO küberekspertide nõukogu koosolekutel. Viimati nimetatud nõukogu koosolekud ebaõnnestusid täielikult ning konsensust rahvusvahelise õiguse rakendamise osas ei õnnestunud küberekspertide nõukogul kokku leppida, mille tõttu ei antud välja ka tavaks olevat nõukogu lõplikku tööraportit. USA esindaja küberekspertide nõukogus ning ekspertgrupi esinaine, Michele G. Markoff on selgitanud, et vaatamata pingutustele jõudmaks mingitelegi kokkulepetele rahvusvahelise õiguse kohaldumise osas küberruumis ning küberrünnakute kontekstis, ei olnud see võimalik, teatud riikide tugeva vastuseisu tõttu. Oli riike, kes ei soovinud enam tunnustada ÜRO üldkogul ühehäälselt 2013. aastal vastu võetud ning 2015. aastal kinnitatud resolutsioone rahvusvahelise õiguse kohaldumise kohta küberruumis.[20] Kuigi Markoff pole selgesõnaliselt riike, kes rahvusvahelise õiguse kohaldumist küberrünnakute osas ei soovi, välja toonud, on eelnevat tausta teades üsna selge, et nendeks riikideks on Shanghai koostööorganisatsiooni liikmesriigid.

Lääneriikide vastuseis küberkonventsioonile on kahetahuline. Esiteks on väga raske eeldada, et küberkonventsiooni osas leitakse üksmeel, kui seisukohad rahvusvahelise õiguses küberrünnakute ja küberruumi osas on niivõrd erinevad. Seetõttu on äärmiselt keeruline jõuda küberkonventsiooni sõnastuse ning sisuni, mis rahuldaks kõiki osapooli sh nii Lääneriike kui ka nn Shanghai koostööorganisatsiooni riike.

Teiseks põhjuseks, miks Lääneriigid ning samameelsed ei soovi küberkonventsiooni sõnastamist, vaid pooldavad rahvusvahelise õiguse otsest kohaldumist kübersfääri, on oht piirata sellega küberruumi innovaatilist arengut. Seades küberkonventsiooni konkreetsed

[19] A. Segal. Chinese Cyber Diplomacy in a New Era of Uncertainty. Hoover Institution. Stanford University. lk 3-8. Arvutivõrgus: https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf (24 märts 2018)

[20] M. G. Markoff. Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security 23. juuni. 2017. Arvutivõrgus: https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm (24 märts 2018)

normid, mida rahvusvahelisel üldsusel tuleb järgida, kardetakse, et selle tõttu ei ole erasektor ning ettevõtjad valmis enam pakkuma ebakonventsionaalseid, nii öelda raamist ning ka õiguses kinnitatud tavadest väljuvaid lahendusi.[21] Üks osa sellest hirmust on põhjendatav ka sellega, et pannes küberruum konventsiooni raamidesse, on oht, et küberruumi arenedes ei suuda normid või konventsioonis kokku lepitud artiklid tehnika arenguga sammu pidada ning seega muutuks konventsiooni normid passiivseteks. See võib tuua kaasa olukorra, kus normid ei suuda reguleerida tegelikkuses ning praktikas toimuvat, tuues kaasa rohkem segadust kui korda, mida õigus vajab.

Kahe eelnevalt nimetatud leeri vahele jäävad riigid, kelle seisukohad on kuskil kahe grupi vahel, toetades kas üht või teist osapoolt ning arengumaad, kelle internetitavad ei ole nii põhjalikult välja kujunenud. Just need riigid, kelle internetitavad alles kujunevad, on mõjutatud sellest, kes neile internetivõimalused ning infrastruktuuri loob, tutvustades sellega tahes-tahtmata ka internetiga kaasnevaid võimalusi. Selline poliitika on üheks osaks nö küberdiplomaatias (*cyber diplomacy*), kus küberinfrastruktuuri loomisel võivad olla tagamõtted. Tutvustades internetikeskkonda, selle tavasid, võimalusi ning vabadusi, mille kaudu tulevikus sellised riigid võivad muutuda poliitiliselt kergemini mõjutatavaks.[22] Seega võib rahvusvahelist küberruumi ning selle tulevikku mõjutada paljuski ka see, kes tutvustab interneti ning selle võimalusi arengumaadele ning milliseks kujuneb sellega nende arusaam küberruumist.

1.2. Küberrünnaku definitsioon

Rahvusvahelise õiguse eksperdid ning riikide esindajad on aastaid rahvusvahelisel tasandil arutlenud küberrünnaku aktuaalseid ohte. Räägitud on nii finants- kui ka väärtpaberiturge kahjustavast rünnakust, tuumareaktori või suure veetammi operatsioonisüsteemi kahjustamisest ning üleujutuse tekitamisest, samuti lennuliiklust korraldava radarisüsteemide ning tarkvarasse häkkimist.[23]

[21] J. A. Lewis. Liberty, Equality, Connectivity: Translatic Cybersecurity Norms. Center for Strategic & International Studies. veebruar 2014. lk 3-5 Arvutivõrgus: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/140225_Lewis_TransatlanticCybersecurityNorms.pdf (30 märts 2018)

[22] A. Segal. Chinese Cyber Diplomacy in a New Era of Uncertainty. Hoover Institution. Stanford University. lk 11-14.

[23] O. A. Hathaway, R. Crootof, P. Levitz, H. Nix, A. Nowlan, W. Perdue, J. Spiegel. The Law of Cyber-Attack. California Law Review. Vol 100, No. 4. August 2012. lk 822-823.

Väidetavalt saab esimeseks riikidevaheliseks küberrünnakuks nimetada 1982. aastal Siberis toimunud gaasitorujuhtme plahvatust. Allikate hinnangul hankis USA, eesotsas CIA-ga luureinfo, mille kohaselt ehitas Nõukogude Liit uut gaasitorujuhet Siberisse ning vajas selle jaoks uut arvutisüsteemi gaastitorujuhtme operatsiooni juhtimiseks (SCADA - *Supervisory Control and Data Acquisition*).[24] Väidetavalt müüdi kontaktide kaudu Nõukogude Liidule vigane arvutitarkvara, mis oli programmeeritud teatud intervalli järel taastama torujuhtme elutähtsate süsteemide algseaded, tuues kaasa gaasitorujuhtmes rõhumuutuse, mille tagajärjel toimus plahvatus, laastades ühe osa Trans-Siberi torujuhtmest.[25]

1991. aastal Lahesõja ajal kasutas USA internetivõrku, edastamaks Iraagi vägedele sõnumeid viimase demoraliseerimise ning alla andmise eesmärgil. Sellele järgnes sõja mõistes konventsionaalne õhurünnak. 2010. aastal toimus Iraanis Stuxnet nimelise pahavaraga küberrünnak, millega tungiti Iraani tuumajaamadesse, pannes uraani rikastamise tsentrifuugid ebakorrapäraselt tööle, lülitades välja kogu süsteemi ning lõpetades Iraani tuumajaamade töö.[26]

Seega ei ole küberrünnakud sugugi uus nähtus rahvusvaheliste suhete ning rahvusvahelise õiguse mõistes. Ometigi puudub rahvusvahelises õiguses üldtunnustatud ning üheselt kokkulepitud definitsioon küberrünnakute osas. Selline situatsioon paneb rahvusvahelise õiguse rakendamise küberrünnakute kontekstis kahtlemata raskesse olukorda. On väga keeruline jõuda kokkuleppele küberrünnakuid puudutavates sisulistes küsimustes, kui puudub üksmeel kõige üldisemas, definitsioonis. Seega algavad rahvusvahelises õiguses küberrünnakutega kokku puutuvate õigusteoreetikute ning praktikute jaoks probleemid juba üsna algses faasis. Kuidas reguleerida ning tõlgendada kehtivat rahvusvahelist õigust, kui puudub kokkulepitu, mis küberrünnaku alla konkreetselt kvalifitseerub? Küberrünnakuid on erineva raskusastmega ning erinevate tagajärgedega, seega on praegusel hetkel endiselt

[24] SCADA ehk Supervisory Control and Data Acquisition on arvutisüsteemide ja sidevõrkude abil toimuv tehniliste protsesside jälgimine ja juhtimine.

[25] Cybereason Intelligence Group. Owning the Battlefield. Fighting the Growing Trend of Destructive Cyber Attacks. lk 3-4 Arvutivõrgus: https://www.cybereason.com/hubfs/Content%20PDFs/Owning%20the%20Battlefield-Fighting%20the%20Growing%20Trend%20of%20Destructive%20Cyber%20Attacks.pdf?t=1516992850438 (6 märts 2018)

[26] M. E. Castel. International and Canadian Law Rules Applicable to Cyber Attacks by State and Non-State Actors. Canadian Journal of Law and Technology. juuni, 2012. lk 3-4

võimatu täie kindlusega öelda, mida riigid loevad õiguslikus mõttes küberrünnakuteks ning mida mitte. Meediaruumiski levinud sõnaühendi küberrünnak lai kasutusviis on kujundanud ka ühiskonnas küberrünnaku mõistest laia ning mitmetimõistetava definitsiooni. Ühest küljest tuleneb see paljuski konkreetse definitsiooni puudumisest, kuid teisalt mängib siin rolli ka teadmatus. Üsnagi laia käsitluse kohaselt võiks küberrünnaku definitsiooni olulisteks märksõnadeks olla ühe või mitme arvuti kaudu sooritatud rünnak teiste arvutite või arvutisüsteemide vastu.

Riigikaitse ekspert Richard A. Clarke on defineerinud küberrünnakut kui „riigi tegevust, mille kaudu tungitakse teise riigi arvutisse või võrku, eesmärgiga tekitada kahju või segadust." Samas artiklis on teine ekspert, endine NSA ning CIA direktor Michael Hayden käsitlenud küberrünnaku mõistet järgnevalt „tahtlik katse vigastada või hävitada teise riigi arvutivõrku."[27] Esimene nendest definitsioonidest käsitleb küberrünnakuna vaid riigi tegevust, piirates samal ajal ka kannataja mõistet riigiga. Seega ei hõlmata antud mõiste alusel küberrünnakuna valitsusväliste osalejate poolt läbi viidud küberrünnakud. Definitsiooni teine pool on teisalt üsna laialt mõistetav, kuna segadust ning kahju on võimalik tõlgendada mitmel viisil. Endise NSA ning CIA direktori Michael Haydeni definitsioon on samuti oma olemuselt päris lai, jättes lahti mõtestamata, kelle poolt peaks küberrünnak olema toime pandud. Teisalt piirdub rünnaku olemus vaid arvutivõrgu näol.

Oxfordi sõnaraamat defineerib küberrünnakut järgnevalt: „Häkkerite üritus kahjustada või hävitada arvutivõrk või süsteem."[28] Eelnevalt nimetatud definitsioon on üsna lai, hõlmates endas häkkeri mõistet, mille alusel tunduvad häkkerid olevat kõik isikud, kes on piisavalt osavad ning pädevad, et arvutisüsteeme kahjustada või rikkuda. Eristatud ei ole riigile omistatavaid rünnakuid ega nö vabakutselistest rühmitustest koosnevaid häkkereid ja indiviide. Puudub täpne selgitus, mida tähendab „üritus" antud kontekstis. Kas igasugune üritus või selline, mis võiks olla piisavalt ohtlik, et potentsiaalselt ka kahju tekitada ning olla seetõttu küberrünnak.

USA ja Venemaa mõttekodade esindajad on kokkuleppeliselt küberrünnakut defineerinud järgnevalt: „Ründaval eesmärgil küberrelva kasutamist, eesmärgiga tekitada määratud

[27] O. A. Hathaway, R. Crootof. The Law of Cyber Attack. lk 823.

[28] Oxford Dictionaries. Arvutivõrgus: https://en.oxforddictionaries.com/definition/cyberattack (24 märts 2018)

sihtmärgile kahju.“[29] Kuigi kõigi terminite osas USA ning Venemaa nimetatud mõttekojad üksmeelt ei leidnud, jõuti selleni küberrünnaku definitsiooni osas. Definitsiooni esimene osa hõlmab küberrelva. Küberrelva definitsiooni on mõttekojad defineerinud kui: „Tarkvara, püsivara või riistvara, mis on kavandatud või rakendatud kahjustama kübervaldkonda.“[30] Antud definitsiooni tugevuseks on küberrelva mõiste kasutamine ning defineerimine, mis konkretiseerib küberrünnaku allikat. Küberrelvade mõiste on autori hinnangul defineeritud viisil, mis lubab küberrelvadena defineerida ka uudsed ja innovaatilised küberrelvad, mida varasemalt kasutatud pole, kuna mõiste ulatus jätab selleks autori hinnangul tõlgendusvõimaluse. Küberrünnaku definitsiooni teine osa jätab aga taaskord üsna laia võimaluse tõlgenduseks, määrates vaid, et küberrünnaku eesmärk on tekitada kahju. Täpsustamata on see, mis liiki peab „tekitatud kahju“ olema. Kas selle all mõeldakse vaid majanduslikku kahju või ka kahju tekitamist inimestele? Samuti jääb selgusetuks kahju ulatus.

Erinevalt USA ning Venemaa mõttekodadest defineerivad USA riigiasutused küberrünnakut järgnevalt: „Rünnak küberruumis, mis on suunatud ettevõtte küberruumi kasutamisele eesmärgiga tegevust häirida, katkestada, hävitada või kuritarvituslikul eesmärgil arvutikeskkonda/infrastruktuuri kontrollida; või andmete kahjustamine/võltsimine või informatsiooni varastamine“.[31] Definitsioon jätab lahtiseks, missuguse olemusega küberrünnakute vorme definitsiooni järgselt käsitleda soovitakse. Mõiste puhul jääb pisut segaseks, mida on konkreetselt „ettevõtte küberruumi“ all silmas peetud ning miks just ettevõtte mõiste on küberrünnakute definitsiooni toodud. Ilmselt on definitsioonis mõeldud mõiste „ettevõtete“ all ka riigiettevõtteid, vastasel juhul käiks antud definitsioon vaid erafirmade kohta. Kuna definitsioonist puudub „*state enterprises*“ oleks autori hinnangul ebaõige mõista „*enterprises*“ all vaid riigile kuuluvaid ettevõtteid. Vaba turumajandust ning majanduskeskkonda väärtustava riigina on ilmselt USA sooviks tõlgendada küberrünnakut laiemalt kui pelgalt rünnakud, mis on suunatud riigiettevõtete vastu. Paljuski võib selle taga olla ka USA vajadus kaitsta oma majanduskeskkonda, sh riigi jaoks olulist rolli mängivat

[29] J. B. Godwin III, A. Kulpin; K. F. Rauscher, V. Yaschenko. East-West Institute. Critical Terminology Foundations 2. Russia-US Bilateral on Cybersecurity. Policy Report 2/2014. lk 44 Arvutivõrgus: https://www.files.ethz.ch/isn/178418/terminology2.pdf (24 märts 2018)

[30] *Ibid.* lk 56

[31] R. Kissel (koost). Glossary of Key Information Security Terms. National Institute of Standards and Technology. US Department of Commerce. 2013. lk 57. Arvutivõrgus: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf (24 märts 2018)

väärtpaberiturgu ning finantsteenuste sektorit. Seega võib definitsiooni puhul näha eesmärgipärast käitumist ning soovi laiendada küberrünnaku mõistet.

Venemaa keskne arusaam ei koosne vaid küberruumist, vaid palju laiemalt, informatsioonist. Täpsemalt on seda mõistet selgitatud „Venemaa Föderatsiooni Relvajõudude käitumisjuhisest Informatsiooniruumis“ järgnevalt: „Konflikt kahe või enama riigi vahel informatsiooniruumis eesmärgiga tekitada kahju informatsioonisüsteemidele protsessidele, ressurssidele, kriitiliselt olulistele ning teistele infrastruktuuridele, kahjustada ning rikkuda poliitilist, majanduslikku ja sotsiaalset süsteemi, destabiliseerides massipsühholoogia abil ühiskonda ja riiki ning sundida võimu tegema otsuseid teise riigi huvides.“[32] Venemaa Föderatsioon on tahtlikult jätnud sõnastamata küberrünnaku definitsiooni. Antud käsitluse põhjust ei ole vaja kaugelt otsida ning tegemist on üheaegselt ilmselt nii poliitilise kui ka juriidilise lahendusega. Antud definitsiooni poliitilist aspekti tutvustas töö autor põgusalt eelmises alapeatükis. Rääkides konkreetsemalt antud definitsioonist, siis käsitletud on informatsiooniruumi. Sellise kontseptsiooni all on mõeldud palju enamat kui lihtsalt küberruum. Informatsioonisüsteemi all võime ilmselt mõista kõiki tänapäevaseid infoallikaid alustades raadioga ning lõpetades internetiga. Samuti tuleb antud mõiste raames kasutusele sotsiaalne aspekt, väljudes küberrünnaku tehnilisest olemusest. Oluline on siinkohal mõista, et poliitiline, majanduslik ning sotsiaalne süsteem tähendab ilmselt ühe konkreetse riigi elukorraldusse sekkumist. Sellele viitab definitsiooni osa, mis käsitleb „destabiliseerides massipsühholoogia abil ühiskonda ja riiki ning sundida võimu tegema otsuseid teise riigi huvides.“ Just eelnevalt mainitud lõigus on eriti selgelt eristuv poliitiline sõnum. Viidates esimeses peatükis käsitletud sõnumile lääneriikide suunas.

Hiina jagab paljuski Venemaa seisukohti ning erinevalt lääneriikidest ei kasuta temagi mõistet „küber“, vaid lähtub „informatsiooni“ mõistest. Kasutatud ei ole ka rünnaku mõistet, vaid kõige lähim mõiste rünnakule on informatsioonisõda, mida töö autor ei ole lugenud

[32] K. Giles. Russia’s Public Stance on Cyberspace Issues. 2012 4th International Conference on Cyber Conflict. lk 67-69 Arvutivõrgus: https://ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf (30 märts 2018)

“conflict between two or more states in information space with the aim of causing damage to information systems, processes and resources, critically important and other structures, subverting the political, economic and social systems, mass psychological work on the population to destabilise society and the state, and coercing the government to take decisions in the interests of the opposing side.”

küberrünnakuga võrdseks mõisteks.[33] Selge on see, et ka Hiina mõistab informatsiooniruumi all palju laiemat kontseptsiooni kui läänemeelsed riigid.

Nigeeria defineerib küberrünnakut järgnevalt: "Pahavaraliste kodeeringute kasutamine digitaalsete või andmete kodeeringute muutmiseks, mille tulemusel võidakse ohustada konfidentsiaalsust ja puutumatust ning mis avab võimaluse andmetega manipuleerimiseks infosüsteemides ja internetivõrgustiku infrastruktuuris."[34] Antud definitsioonis on kasutatud mõistet kodeering, tekitades segadust, mida täpsemalt sellise sõna all on mõeldud. Kas sõnade ühend pahavaraline kodeering tähendab lihtsamalt öeldes häkkimist või on sõna kodeering all mõeldud midagi muud, jääb siinkohal autori hinnangul arusaamatuks. Antud käsitlusel puudub ka täpsustav selgitus, seetõttu jääb antud definitsiooni täpne tõlgendus selgusetuks ilmselt ka teiste riikide jaoks.

Üks põhjalikumaid küberrünnaku definitsioone on valminud Tallinna käsiraamatu vahendusel, mis nimetab küberrünnakut kui küberoperatsiooni, mis on oma iseloomult kas ründav või kaitsev ning mille esilekutsumine võib olla eelduslikult ohuks inimeste tervisele, elule või objektidele, tekitades nende kahjustamist või hävimist.[35] Definitsiooni põhjalikkus tuleneb eelkõige definitsioonile järgnevast selgitusest. Kahjuks ei ole Tallinna käsiraamatus välja toodud definitsioonis kasutatud küberoperatsiooni mõistet. Seega ei ole päris selge, mida on küberoperatsiooni mõiste all täpsemalt mõeldakse - kui lai on kasutatud mõiste ja mida see täpsemalt endas hõlmab.

Erinevalt paljudest teistest küberrünnakute definitsioonidest hõlmab Tallinna käsiraamatu küberrünnaku mõiste enda all ka kaitsvat küberoperatsiooni. Sellise mõttekäigu peamiseks põhjuseks on Genfi konventsioonide (I) lisaprotokoll rahvusvahelise relvakonfliktide ohvrite kaitse kohta, mille artikkel 49 punkt 1 defineerib rünnakut kui vastaspoole vastu suunatud vägivallategusid nii ründefaasis kui kaitses. See tähendab, et riigi poolt vastumeetmena

[33] M. Raud. China and Cyber: Attitudes, Strategies, Organisation. NATO Cooperative Cyber Defence Centre of Excellence. Tallinn 2016. lk 9-10.

[34] Nigerian National Cybersecurity Policy and Strategy – 2015. Arvutivõrgus: https://cert.gov.ng/images/uploads/NATIONAL_CYBESECURITY_STRATEGY.pdf (24 märts 2018) „It usually involves the use of malicious codes to alter digital codes, logic or data, resulting in disruptive consequences that can compromise the confidentiality, integrity, and availability of data and lead to manipulation of information systems and internetwork infrastructure."

[35] M. N. Schmitt, L. Vihul jt (koost). Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations. Cambridge University Press. 2017. lk 415

kasutatav küberoperatsioon võib samuti kvalifitseeruda küberrünnakuks.[36] Antud definitsiooni raames ei kuulu küberrünnakute hulka kõik rünnakud. Näiteks on Tallinna käsiraamatu eksperdid seisukohal, et küberrünnakute hulka ei kuulu rahumeelsed küberoperatsioonid, mille hulka loetakse psühholoogilist küberoperatsiooni ning küberspionaaži, mille hulgas on ka Tallinna käsiraamatus toodud erandid.[37]

Tallinna käsiraamatus käsitletud küberrünnaku definitsiooni täpsemalt lahti seletades on oluline mainida, et sõnaühend „eelduslik oht" tähendab antud kontekstis olukorda, kus oht on mõistlikult ettenähtav. Seega konkreetne rünnak pidi mõistlikule isikule olema ette nähtav kui ohtlik tegevus inimeste elule, inimtervisele või ette nähtav oht asjade vigastamiseks või hävitamiseks. Sealhulgas ei ole rünnaku kontekstis oluline see, et tegemist oleks nö kineetilise ründega, kuna rünnaku vahend ei pruugi olla kineetilise iseloomuga, näiteks küberrünnaku kaudu läbi viidav keemiarünnak vms, mis vastasel juhul antud definitsiooni alla ei mahuks.[38]

Tallinna käsiraamatu küberrünnaku definitsioon võiks rahvusvahelises õiguses olla teoreetiliselt üsna hästi kohaldatav, kuna seos küberrünnaku ning sellele järgnevate tagajärgede vahel tundub olevat lihtsamini tõestatav kui enamik riikide endi poolt välja pakutud küberrünnakute definitsioone. See on ka üks Tallinna käsiraamatu definitsiooni tugevustest, olles praktikas heaks lähtepunktiks riikidele hakates rahvusvahelise õiguse kohaldatavust kokku leppima. Teisalt on autori hinnangul selle sama õiguskindluse taga ka oht, et küberrünnakut defineeritakse ehk liiga kitsalt, jättes kõik olukorrad, mis küberrünnakute alla ei kuulu, kuid rikuvad rahvusvahelise õiguse põhimõtteid käsiraamatus defineerimata küberoperatsioonide alla.

Kui ühelt poolt tekitab küberrünnaku lai tõlgendus kaasa ohu, et riikide vastutusele võtmine on kordades keerulisem. Siis teisalt ei kuuluks antud definitsiooni raames küberrünnaku mõiste alla Venemaa poolt USA presidendivalimiste käigus osariikide hääletussüsteemidesse tungimine. Antud juhul puudus konkreetne oht inimeste elule või tervisele, samuti ei kahjustatud teatavalt otseselt hääletussüsteeme ega hävitatud neid. Samal ajal on selge, et taoline rünnak on rünnak teise riigi suveräänsuse vastu, piirates õigust teostada vabasid valimisi ning tagada poliitiline sõltumatus ÜRO harta artikkel 2 punkti 4 mõistes.

[36] M. N. Schmitt, L. Vihul jt (koost). lk 415.

[37] *Ibid*. lk 415

[38] *Ibid.* lk 415.

Siit võib kerkida küsimus, kas seda on vaja üldse küberrünnaku definitsiooniga siduda, eeldusel, et selline käitumine riigi poolt oleks tõlgendatav keelatud käitumisena ka ÜRO harta artiklite alusel? Autori hinnangul on, seda ka juhul, kui praegune rahvusvaheline õigus on otsekohaldatav ka küberrünnakute kontekstis. Kuigi selliste rünnaku konkreetne tõestamine on üsna keerukas, tooks küberrünnaku mõiste taoline laiendamine kaasa selge sõnumi, et sekkumine riigi valimiste protsessi, riigi suveräänsusesse, ei ole aktsepteeritav ka küberrünnakute vahendusel. Samuti vähendab see niinimetatud halli ala tekkimist, mille võimalusi teatud riigid juba praegugi kuritarvitamas on.

Küberrünnaku mõistet tõlgendatakse Tallinna käsiraamatus kitsalt peamiselt põhjusel, et sõna „rünnak" all mõistetakse sõja kontseptsioonis relvastatud jõu kasutamist, mis on suunatud inimeste või objektide vastu ning millele *jus ad bellumi* mõistes võib riik kasutada enesekaitse õigust.[39] See tähendab, et sõnaühend „küberrünnak" ei hõlma endas kõiki rahvusvahelist õigust rikkuvaid tegevusi. Kuna Tallinna käsiraamat tuginebki kehtivale rahvusvahelisele õigusele, on antud käsitlus aktsepteeritav ning mõistetav. Siiski leiab autor, et selline käsitlus võib tekitada kübesfääris ka märkimisväärset ebakõla, millele lisab küsitavust ka eelnevalt mainitud küberoperatsioonide mõiste defineerimata jätmine. Ebakõla tekitavatest seisukohtadest rahvusvahelise õiguse mõistes räägib töö autor täpsemalt järgmise peatüki jõu kasutamise, vastumeetmete ning riigi enesekaitse osas.

Ühise küberrünnaku definitsiooni puudumise tõttu on välja pakutud ka tsiviilisikutega seotud rünnete jaoks definitsioon, mis käsitleks nn ebamugavuse (ingl. keeles *inconvenience*) kriteeriumit. Antud vaheaste peaks looma võimaluse teha vahet operatsiooni vahel, mis kvalifitseerub ründeks, ning mis mitte. Seega on jäetud üsna lai abstraktsuse aste, mis võib nn ebamugavuse kriteeriumi alusel tekitada kübersfääris riikidevahelisi konflikte.[40]

Rahvusvahelise Punase Risti komitee on rahvusvahelise humanitaarõiguse kontekstis välja toonud kolm peamist küberrünnaku lahtimõtestamise viisi. Üks seisukohtadest on see, mida käsitleb Tallinna käsiraamat, ehk küberrünnakud on vaid sellised küberoperatsioonid, mis toovad kaasa vägivalla inimeste suunas või füüsikalise kahju või hävimise objektidele. Teine

[39] M. N. Schmitt, L. Vihul jt (koost). lk 4-5

[40] International Humanitarian Law and the Challenges of Contemporary armed conficts Report. 2015. lk 41 Arvutivõrgus: https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts (25 märts 2018)

seisukoht lähtub küberrünnakuteks defineerimisel analüüsipõhisest käsitlusest, mis tugineb vajalikele meetmetele, mida on vaja kasutusele võtta, et antud objekti, võrku või süsteemi taastada. Kolmas lähenemine peab oluliseks rünnaku või operatsiooni mõju antud objekti funktsionaalsusele, mida on rünnatud.[41] Oma olemuselt eristub nendest kõige selgemalt Tallinna käsiraamatuski kasutust leidnud esimene küberrünnaku definitsiooni mõtestamise viis. Teine ning kolmas on oma olemuselt mingil määral sarnased, sõltudes analüüsi käigus kindlaks tehtavast kahjust, mida küberrünnak on tekitanud, olles seega tihedalt seotud mõiste kasutusele võtmiseks teo tagajärjest.

Vahekokkuvõte

Vaadates antud töös käsitletud definitsioone on selge, et kõigil nimetatud mõistetel on omad eelised ning puudused. Enamik definitsioonidest on väga erinevad, omades erinevaid arusaamu ning küberrünnakute definitsioonidesse lisatud mõisteid, mida omakorda lahti seletatud ei ole. Eelnevast lähtuvalt ei olegi niivõrd üllatav, et riikidel puudub ühtne arusaam küberrünnakute definitsioonist ning riigid ei ole kahjuks küberrünnakute definitsioonis kokkuleppele jõudnud. Kuigi viimase kümnendi jooksul on kahtlemata toimunud arenguid positiivses suunas, on endiselt keeruline rääkida rahvusvahelise õiguse kohaldumisest, kui probleemi olemus on selge, kuid puudub üks probleemi jaoks olulistest aspektidest, küberrünnaku definitsiooni selgitus ning käsitluse ulatus. Kui töö lugejale võib jääda mulje, et välja toodud definitsioonid olid antud töösse valitud meelevaldselt, siis tegelikkuses on välja toodud enamik küberrünnakute definitsioone, mida riigid on oma strateegiates või ametlikes dokumentides on välja toonud. Veelgi enam, vaid 38% maailma riikidest on välja töötanud ning avalikustanud küberjulgeoleku strateegia. 12% riikidest on küberjulgeoleku strateegia välja töötamisel. Seega puudub vähemalt pooltel maailma riikidest küberstrateegiad ehk puuduvad ametlikud dokumendid selle kohta, millised on riigi järgmised sammud küberruumi reguleerimiseks ning kuidas nendeni jõuda.[42]

See tähendab ka, et väga suur hulk riike ei ole tegelikkuses küberrünnaku definitsiooni enda jaoks sõnastanud. Küberrünnaku definitsiooni sõnastamine ei ole tavapäraselt ka küberjulgeoleku strateegiate välja töötamisel olulisuse poolest kõrge prioriteetidega

[41] International Humanitarian Law and the Challenges of Contemporary armed conficts Report. 2015. lk 41

[42] Global Cybersecurity Index (GCI)2017. Arvutivõrgus: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf lk 17-18 (25 märts 2018)

definitsioonide hulgas. Tihti ei käsitleta küberrünnakuid, vaid kübersõda, mida autor antud kontekstis ei käsitlenud, kuna nende kahe definitsiooni kontseptsioon on erinev ning see tooks kaasa küberrünnaku definitsiooni veelgi laiema tõlgendusvõimaluse. Küberrünnaku definitsioone ei ole riigid lahti mõtestanud põhjusel, et riik on leidnud, et definitsiooni jaoks ei ole aeg küps, sh puudub piisavalt antud valdkonnas kogenud ning töötavaid õigusteadlasi, kes definitsiooni lahti mõtestaks. Teatud juhtudel võib definitsiooni vältimist põhjendada aga poliitilise seisukohaga, kus selliseid definitsioone ei taheta ametlikes dokumentides sõnastada, seades endale sellega teatud piirid ja kohustused, mida ilmselt soovitakse vältida. Sellisteks näideteks on Venemaa ning Hiina, kellel puudub konkreetne küberrünnaku definitsioon, rääkides kontseptuaalse erinevusena informatsiooni rünnakust ning kübersõjast, mida ei saa tegelikkuses otseselt käsitleda küberrünnakutena, kuna tehnilistele asjaoludele soovitakse lisada sotsiaalne tagamõte.

Antud probleemi lahendus on oma olemuselt lihtsakoeline, kuid praktikas vägagi raskesti saavutatav. Selleks on küberrünnaku osas ühise definitsiooni kokku leppimine vähemalt kehtiva rahvusvahelise õiguse tasandil. Autori hinnangul on väga raske rahvusvahelist õigust praegusel hetkel tõlgendada, kui puudub kokkuleppeline definitsioon küberrünnaku osas. Ainuüksi asjaolu, et definitsioon puudub, ei jäta küll rahvusvahelist õigust kohaldamata, kuid kindlasti muudab see selle kohaldamise keerulisemaks ning loob samal ajal ka riikide tasandil segadust, eelkõige asjaolu tõttu, et puudub konkreetsus ning selgus.

Riikide praegune tõlgendus rahvusvahelisest õigusest võib küberrünnakute osas varieeruda diametraalselt. Mõningal määral tundub, et isegi samameelsed Lääneriigid ei ole küberrünnakute kontekstis päris ühte meelt või ei saa sellest vähemalt ametlikes dokumentides üheselt aru, mida võib mingil määral tingida ka erinevatel aegadel sõnastatud definitsioon. Hetkeseisuga valitseb olukord, kus üks osa riike leiab, et küberrünnak on vaid surmaga või raskete kehavigastuste tekitamine ning objektide kahjustamine või hävitamine, teine osa väidab, et rünnaku mõiste peaks endas hõlmama ka rünnakuid, mis puudutavad näiteks ettevõtteid, millele kahju tekitamine võib mõnel juhul olla riigi majandust või poliitilist olukorda oluliselt mõjutav. Sealhulgas jääb veel erinev seisukoht ka nende seas, kes peavad küberrünnakuks surma ning raskete kehavigastuste tekitamist ning objektide kahjustamist ja hävitamist, vaieldes, kas objektide kahjustamine või hävitamine peab olema vaid füüsilist laadi või on oluline asja funktsiooni kahjustamine või hävimine.

Kolmanda rühma riike moodustavad riigid, kellel puudub veel konkreetne arusaam küberrünnaku mõistest, definitsioonist ning puudub ka konkreetne tegevusplaan küberruumi reguleerimiseks ja korraldamiseks. Seega oleks rahvusvahelise õiguse kohaldamiseks vajalik leida ühine definitsioon. Selle puudumisel on tegelikkuses väga raske edasi minna sisulisemate küsimustega. Kahjuks on näha, et just arusaamade erinevus antud definitsioonis ning ulatus, mida selle all mõistetakse on kategooriliselt erinev.

2. RAHVUSVAHELISE ÕIGUSE KUJUNEMINE KÜBERRÜNNAKUTE KONTEKSTIS

2.1. Rahvusvahelise õiguse kujunemine

Rahvusvaheline õigus on küberrünnakute kontekstis alles kujunemisjärgus. Seetõttu on oluline teada, kuidas rahvusvaheline õigus kujuneb ning millised asjaolud seda kujundada võivad. Rahvusvahelisel õigusel on kolm esmaallikat, milleks on Rahvusvahelise Kohtu statuudi artikkel 38 punkti 1 järgselt rahvusvahelised lepingud, rahvusvaheline tavaõigus ning õiguse üldpõhimõtted. Samuti on teatud juhtudel lisameetmetena rahvusvahelise õiguse allikana lubatud kasutada kohtute lahendeid, erinevate riikide kõige autoriteetsemate ning tunnustatumate õigusteadlaste teoseid.

Rahvusvahelise õiguse kohaldamise teeb keeruliseks riikide ning õigussüsteemide multikultuursus. Tegemist ei ole negatiivse nähtusega, pigem on tegemist paratamatusega, asjaoluga, mis teeb rahvusvaheliste õigusteadlaste ning praktiseerijate töö keeruliseks, kuid millega peab rahvusvaheline õigus kui tervik toime tulema. Rahvusvahelise õiguses on üha enam erinevate õiguslike seisukohtadega riike, mille taga ei ole tihtipeale mitte midagi muud, kui erinev õiguspoliitiline seisukoht. Seetõttu on muutunud ka kompromisside leidmine rahvusvahelist õigust puudutavates küsimustes järjest keerulisemaks ülesandeks.

Kuigi rahvusvahelise õiguse loovad riigid ise, peab rahvusvaheline õigus olema samal ajal riigiülene, olles riikide seisukohtade ning õiguste vahendaja. Leida sellised muutumatud ja universaalsed elemendid riikide seisukohtadest ning praktikast, mis võimaldavad jätta tahaplaanile riikidevahelised erinevused, leides miski, mis kõiki ühendab.[43] Kindlasti ei ole praktikas selline lähenemine kerge, kuid see on ka ainus võimalus, et rahvusvaheline õigus üldse eksisteeriks.

Praegusel hetkel on küberrünnakute tõlgendamine rahvusvahelise õiguse alusel üsna keeruline. Pole päris kindel, mis antud valdkonda - kui üldse reguleerib ning juhul, kui rahvusvaheline õigus on küberrünnakute kontekstis otsekohalduv, siis millised normid ning millisel moel need küberrünnakute valdkonda täpsemalt reguleerivad. Puuduvad ka välja

[43] M. Forteau. Comparative International Law Within, Not Against, International Law. Lessons from the International Law Commission. lk 162-165

kujunenud rahvusvahelised tavad ning valdkonnas kehtiv praktika. Rahvusvahelise õiguse kohaselt ei saa rahvusvaheliseks õigust kujundavaks allikaks tegelikkuses nimetada ka ÜRO peaassamblee resolutsioone. Seega on vähetõenäoline, et ÜRO kübernõukogu poolt välja töötatud raportid ja seisukohad, millest 2013. ning 2015. aasta raportid said peaassamblee toetuse, on muutunud õiguslikult siduvaks ning kujundanud rahvusvahelist õigust.[44] Ometigi on vastu võetud mitmeid dokumente, mis rahvusvahelise õiguse kohaldumist küberrünnakute kontekstis toetavad. Lõpuks taandub küsimus paljuski sellele, kui suur hulk riikidest on valmis rahvusvahelist õigust küberrünnakute kontekstis kohaldama? Paljuski just riikide käitumisest oleneb see, kas rahvusvaheline õigus aktsepteerib kehtivat õigust küberrünnakute kontekstis või mitte. Küsimus, kas rahvusvaheline õigus on küberrünnakute kontekstis konkreetselt antud hetkel otsekohalduv, on ilmselt suureks probleemiks ka näiteks Rahvusvahelise Kohtu jaoks. Rahvusvaheliste küberrünnakute kontekstis on raske leida ka siseriikliku praktikat, mida oleks võimalik rakendada analoogia teel küberrünnakute osas. Kui teatud ulatuses võiks rahvusvahelise õiguse mõttes edasi aidata õiguse üldpõhimõtted, siis on raske näha, et ka see lahendaks konkreetseid probleeme küberrünnakute kontekstis, mis on tihedalt tehnikaga ning tehniliste aspektidega põimunud. Siiski ei saa välistada, et teatud kontekstis võib see õigusteadlaseid ka edasiste kompromisside suunas aidata.

Läbi ajaloo on rahvusvahelist õigust kujundanud ka tunnustatud õigusteadlaste teosed ning publikatsioonid. Eriti oluline oli õigusteadlaste panus rahvusvahelise õiguse kujunemisjärgus, 19. ning 20. sajandi algul, kui väga suures osas tunnustati ka ala ekspertide panust rahvusvahelisse õigusesse. 20. sajandi lõpus vähenes publikatsioonide roll rahvusvahelises õiguses seoses tavaõiguse ning kohtupraktika arenguga.[45] Tallinna käsiraamatu tõlgendus rahvusvahelise õiguse kehtivusest küberruumis võib tulevikus muutuda rahvusvahelise õiguse osaks, sellisele lähenemisele annab lootust rahvusvahelise õiguse eelnev ajalugu. Nimelt on ekspertgrupid ning nende poolt loodud publikatsioonid ka varasemalt kujundanud rahvusvahelist õigust, näiteks 1966. aastal *International Law Associationi* (*ILA*) poolt välja töötatud Helsinki reeglid vee kasutamisest rahvusvahelistest jõgedest (*The Helsinki Rules on the Uses of the Waters of International Rivers*), mida toona liiga uuendusmeelseks peeti ning mida rahvusvahelise õiguse raames oma ajas ei tunnustatud, kuid mis sai hiljem rahvusvahelise tavaõiguse osaks. Näiteks saab tuua ka San Remo käsiraamatu rahvusvahelise

[44] M. D. Evans (koost), Hugh Thirlway. The Sources of International Law. International Law. Oxford University Press. 2003. lk 138-142.

[45] S. Sivakumaran. The Influence of Teachings Of Publicists on the Development of International Law. British Institute of International and Comparative Law. Vol 66. jaanuar 2017. lk 1-4

õiguse kohaldumisest merel toimuvate relvastatud konfliktide osas (*San Remo Manual on International Law applicable to Armed Conflicts at Sea*). Sarnaselt Helsinki reeglitele tunnustatakse ka San Remo käsiraamatut ning selle seisukohti rahvusvahelise õiguse osana.[46] Seega omab ka Tallinna käsiraamat teatavat võimalust, et ühel päeval tunnustatakse seda kui rahvusvaheliselt kehtiva õiguse tõlgendust küberruumis. Juhul kui Rahvusvahelisse Kohtusse peaks jõudma kaasus, mis käsitleb küberrünnakuid ning kohus leiab, et rahvusvaheline õigus kohaldub küberrünnakute kontekstis, võib kohus kehtiva õiguse tõlgendamise vahendina kasutada just Tallinna käsiraamatut. Siiski on reaalsem ning kiirem võimalus Tallinna käsiraamatu laiemaks tunnustamiseks leida riikide toetus käsiraamatus nimetatud käsitlustele. Tallinna käsiraamatu loojad on sõltumatud eksperdid ning praegusel hetkel pole enamik riikidest selle käsitlust avalikult tunnustanud.

Asjaolu, et Tallinna käsiraamatus sedastatu võib ühel päeval saada osaks rahvusvahelisest tavaõigusest, võib see muuta antud teose tähtsaimaks, mis seniajani rahvusvahelist õigust küberrünnakute kontekstis puudutab. Teist nii põhjalikku ning mahukat teost, mis käsitleks kehtivat õigust rahvusvahelise õiguse kontekstis pole. Samuti on Tallinna käsiraamat oma põhjalikkuse tõttu üks enimrefereeritud teoseid rahvusvahelises õiguses, mis puudutab küberrünnakute käsitlust.

2.2. Rahvusvahelise Õiguse Komisjon – selle ajalooline roll õiguse kujunemises (selle roll õiguse kujundajana)

Rahvusvahelise õiguse komisjon (*International Law Commission*) loodi ÜRO peaassamblee otsusega 1947. aastal kooskõlas ÜRO harta artikkel 13 punktiga 1(a), mis sätestab, et peaassamblee algatab uurimusi ja teeb soovitusi, et aidata kaasa rahvusvahelisele koostööle poliitilisel alal ja edendada rahvusvahelise õiguse progressiivset arenemist ja tema kodifitseerimist.[47] Rahvusvahelise õiguse komisjoni artikkel 1 punkt 1 sätestab, et Rahvusvahelise õiguse komisjoni ülesanne on rahvusvahelise õiguse progressiivse arengu edendamine ning kodifitseerimine.[48] Rahvusvahelise õiguse komisjoni töömeetod koosneb erinevate riikide riigikohtute otsuste analüüsimisel viisil, mis aitaks rahvusvahelist õigust

[46] S. Sivakumaran. lk 7-9.

[47] Ühinenud Rahvaste Organisatsiooni põhikiri ning Rahvusvahelise Kohtu statuut. RT II 1996, 24, 95

[48] Statute of the International Law Commission. 21 november 1947. Arvutivõrgus: http://legal.un.org/ilc/texts/instruments/english/statute/statute.pdf (16 aprill 2018)

tõlgendada. Jälgitakse, kuidas erinevad õigussüsteemid õigust teatud küsimuses praktiseerivad. Samuti vaadeldakse, kuidas erinevate riikide rahvusvahelised õigusteadlased õigust tõlgendavad (sh erinevate õigussüsteemide õigusteadlased) ning kas riigid käsitlevad rahvusvahelist õigust sarnastel viisidel.[49] Üha levinum on ka komisjoni praktika küsida aruteldavate teemade osas seisukohti ÜRO liikmesriikidelt endilt.

Näiteks on Rahvusvahelise Õiguse Komisjoni töö kujundanud välja Rahvusvaheliste lepingute õiguse Viini konventsioonini (1969) ning riikide ja rahvusvaheliste organisatsioonide vaheliste või rahvusvaheliste organisatsioonide vaheliste lepingute õiguse Viini konventsiooni (1986).[50] Kuigi Rahvusvahelise Õiguse Komisjoni ning selle traditsioonilist käsitlust loetakse vanamoodsaks ajal, kui rahvusvahelises õiguses valitseb üha enam pehme normistik, võib just Rahvusvahelise Õiguse Komisjon olla üks lahenduste pakkujatest ning rahvusvahelise õiguse kujundajatest küberrünnakute kontekstis.[51]

Nimelt on komisjonil eelnevalt mainitud rahvusvahelise õiguse progressiivse arengu edendamisel ning kodifitseerimisel tähtis roll. Just Rahvusvahelise Õiguse Komisjoni abil oleks võimalik leida ehk riikide vaheline kompromiss või leida vähemasti algsed lähtepunkt diskussiooniks, kust edasi minna. Ilmselt on just antud viis kõige realistlikum, leidmaks riikidevahelist konsensust. Seeläbi oleks võimalik ehk mingis ulatuses jätta tahaplaanile ka poliitilised tegurid, mis küberruumi kujundamist mõjutavad. Ilmselt vajaks sellise rahvusvahelise õiguse suurprojekti teostamisel IT-spetsialistide poolset välist abi ning tunnustatud küberõiguse ekspertide nõu.

[49] M. Forteau. Comparative International Law Within, Not Against, International Law. Lessons from the International Law Commission. Lk 168-170

[50] S. Mathias. The Work of the International Law Commission on Identification of Customary International Law: A View from the Perspective of the Office of Legal Affairs. Chinese Journal of International Law. 2016. lk 19-20.

[51] M. Forteau. lk 166-167

2.3. Rahvusvahelise õiguse kohaldumine küberrünnakute kontekstis Tallinna käsiraamatu näitel

Antud peatükis käsitletakse, kuidas tõlgendada küberrünnakuid ning norme, mis on küberrünnakutega otseses seoses. Autor käsitleb eelkõige Tallinna käsiraamatu reegleid, mis jäävad eelkõige *jus ad bellumi* raamidesse.

2013. aasta ÜRO liikmesriikide ühehäälne otsus oli märgilise tähtsusega, kinnitamaks, et kehtiv rahvusvaheline õigus laieneb ka küberrünnakute kontekstis.[52] Kõik ÜRO liikmesriigid said aru ohtudest, mis varitsevad küberruumi ning probleemidest, mida võivad küberrünnakud riikide julgeolekule valmistada. Oli selge, et antud valdkonna tähelepanuta jätmine annab võimaluse täielikule reguleerimatusele küberruumis. Mingil määral on selline oht olemas praegugi, kuna konkreetseid tõlgendusi, kuidas küberrünnakud rahvusvahelises õiguses kohalduvad, puuduvad. Ometigi oli riikide lahendus ühene ning selge - kehtiv rahvusvaheline õigus laieneb täpselt samamoodi küberruumile kui teistele rahvusvahelise õiguse osadele, et säilitada rahvusvahelise kogukonna rahu, turvalisus ja stabiilsus. Mainiti, et rahvusvahelise õiguse kohaldumine küberrünnakute konteksti vajab täpsemat uuringut ning arusaama.[53] Õiguskindluse ning rahvusvahelise õiguse järjepidevuse hoidmiseks on ÜRO liikmesriigid 2015. aasta raportis taaskord korranud peamiselt 2013. aastal kokku lepitud seisukohti, kinnitades, et rahvusvaheline õigus kohaldub jätkuvalt ka küberrünnakute kontekstis.[54]

Hiina, Kasahstan, Kõrgõzstan, Vene föderatsioon, Tadžikistan ning Usbekistan tegid 2011. aastal ÜRO-le taotluse loomaks küberkonventsioon küberkaitseks.[55] Kui üldiselt võib vaadelda antud situatsiooni ka kui üllast soovi tuua reguleeritus küberuumi ning

[52] United Nations General Assembly Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/69/723. 24. juuni. 2013 Arvutivõrgus: https://disarmament-library.un.org/UNODA/Library.nsf/a45bed59c24a1b6085257b100050103a/2de562188af985d985257bc00051a476/$FILE/A%2068%2098.pdf (30 märts 2018)

[53] United Nations General Assembly. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/69/723.

[54] United Nations General Assembly Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174. 22. juuni. 2015 Arvutivõrgus: http://undocs.org/A/70/174 para 11 (25 märts 2015)

[55] United Nations General Assembly Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/69/723.

küberrünnakute konteksti, siis kahjuks võib selle käsitluse siiruses üha enam kahelda, seda eelkõige 2017. aasta ÜRO ekspertgrupi raporti valguses. 2017. aasta ÜRO grupp riiklikke eksperte kübervaldkonnast, ei jõudnud 2017. aasta lõppraportis kokkuleppele kahjuks isegi varasemate seisukohtade kinnitamise osas, ehk viimases raportis ei leitud konsensust isegi selles, kas rahvusvahelise õigus küberrünnakute kontekstis kohaldub või mitte.[56]

Järgnevas peatükis käsitletakse valdavalt Tallinna käsiraamatu seisukohti rahvusvahelise õiguse kohaldumisest küberrünnakute kontekstis. Põhjus Tallinna käsiraamatu analüüsimiseks on lihte – tegemist on hetkeseisuga kõige põhjalikuma allikaga, mis käsitleb võimalikku rahvusvahelise õiguse kohaldumist küberruumis. Lisaks on Tallinna käsiraamatu koostajad rahvusvaheliselt tunnustatud õiguseksperdid, kes on kursis küberrünnakute kontekstiga ning rahvusvahelise õiguse rakendamise probleemidega praktikas.

Peamiselt analüüsitakse Tallinna käsiraamatus käsitletud *jus ad bellum*'ist tulenevaid seisukohti, mis hõlmavad endas suveräänsuse (sealhulgas nõuetekohane hoolsus korra tagamisel oma territooriumilt), küberrünnakute omistatavuse, jõu kasutamise ning võimalike vastumeetmete osas, sealhulgas õigust enesekaitsele. Selline teemade valik tuleneb antud magistritöö teemast, mis keskendub eelkõige küberrünnakute õigusvastasusele küberruumis. Teisalt viitavad antud teemadele eraldi tähelepanu ka ÜRO kübervaldkonna riikidevaheliste ekspertgrupi välja töötatud seisukohad 2013. ning 2015. aastast, millega ÜRO liikmesriigid ühehäälselt nõustusid.

2.3.1 Suveräänsus

Rahvusvahelises õiguses keskset rolli omavast suveräänsuse mõistest ei saa mööda minna ka küberoperatsioonide ning küberrünnakute kontekstis. Vaatamata oma interdistsiplinaarsele olemusele omab suveräänsuse mõiste küberrünnakute ja operatsioonide osas samaväärset rolli nagu rahvusvahelises õiguses üldiselt. Suveräänsuse mõistet on tõlgendatud ajaloos mitmeti ning seetõttu puudub selge ning ühene suveräänsuse mõiste.

Suveräänsust võib liigitada nii sisemiseks suveräänsuseks kui väliseks suveräänsuseks. Sisemiseks suveräänsuseks saab nimetada suveräänsuse ühte levinumat definitsiooni, ehk

[56] UNODA. United Nations Office For Disarmament Affairs. https://www.un.org/disarmament/topics/informationsecurity/ (27 märts 2018)

suverääni (valitseja) võimu korraldada elu teatud territooriumil soovitud viisil. Väline aga viitab riigi vabadusele luua suhteid teiste riikidega ning teha koostööd.[57]

Täpsema definitsiooni kohaselt peab riik selleks, et kvalifitseeruda riigiks, täitma kolme peamist kriteeriumit. Omama kindlat, määratletud territooriumi, oma rahvastikku, kes elab sellel territooriumil ning avalikku võimu, kellel on mandaat ning tegutsemisvõime, loomaks suhteid teiste riikidega. Kui riik täidab nimetatud kriteeriumid, kaasnevad sellega õigused, võimalused ning kohustused, mis ühel täisväärtuslikul suveräänsel riigil on.[58]

Rahvusvahelise õiguse allikast võime suveräänsusele viitava artikli leida ÜRO harta artiklist 2 lõikes 1, mis sätestab, et organisatsioon on rajatud kõigi tema liikmete täieliku võrdsuse põhimõttele. [59]

Modernse või tänapäevase suveräänsuse mõiste üheks peamiseks tunnuseks ei ole pelgalt käsitlus, kus riigil on õigus oma territooriumil avaliku võimu kandjate näol otsuseid teha, vaid pigem hõlmab käsitlus riigi õigust teha teiste riikidega koostööd.[60] Seega viitab tänapäevane rahvusvaheline käsitlus varasemast palju rohkem riikide üleriigilisele koostööle ning riikide õigusele omavahel koostööd teha. Just modernne käsitlus on asjakohane ning oluline ka küberrünnakute kontekstis, kuna küberrünnakute riigiülesuse tõttu on vajalik leida riikidevaheline mõistmine ning arusaam. Kübervaldkonna reguleerimine riiklikul tasandil ei täida täielikult probleemi globaalse olemuse tõttu oma eesmärki, seetõttu on järjest olulisem ka rahvusvahelise õiguse raames tehtav koostöö.

[57] E. A. Wilson. People Power and The Problem of Sovereignty in International Law. Duke Journal of Comparative & International Law. Vol 26. No 551.

[58] S. D. Krasner (koost) – Problematic Sovereignty. Contested Rules and Political Possibilities. Columbia University Press. 2001.

[59] Ühinenud Rahvaste Organisatsiooni põhikiri ning Rahvusvahelise Kohtu statuut - RT II 1996, 24, 95

[60] S. Besson. Sovereignty. Max Planck Encyclopedia of Public International Law. aprill 2011. Para 42-45 Arvutivõrgus: http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1472?prd=EPIL (16 aprill 2018)

2.3.2 Suveräänsus küberrünnakute kontekstis

Nagu öeldud omab suveräänsus kübersfääri kontekstis sama tähendust, mida rahvusvahelises õiguses üldiselt. Küberruumil eripärade tõttu on välja toodud aga täpsemad seletused ning tõlgendused, kuidas suveräänsust küberruumi kaudu paremini mõista.

Interneti ning küberruumi mõistetakse järjest enam kui üht põhivabadust ning viiendat domeeni õhu, maa, mere ja kosmose kõrval, mida keegi ei saa omada ning mis on kõigile vabaks kasutuseks.[61] Praktika antud seisukohta aga kahjuks ei kinnita. Freedomhouse'i internetivabaduse uuringu raport 2017. aastast kinnitab, et tendents on pigem vastupidine ning riigid on üha enam internetivabadust piiramas. Koguni 32 riigis oli internetivabaduse tendents negatiivne ning vaid 13 riigis muutus internetikeskkond vabamaks.[62]

Küberruum on oma olemuselt tinglikult jaotatud kolmeks kihiks. Esimene, füüsiline kiht (*The physical layer*) koosneb geograafilisest komponendist ning füüsilistest võrgukomponentidest. Siia kihti kuuluvad eelkõige riistvara ning infrastruktuuriga seotud esemed, mis hõlmavad endas liine, kaableid, raadiolaineid, ruutereid, servereid, arvuteid jne.[63] Teise kihi otsetõlge võiks olla loogiline kiht (*The logical layer)*. See kiht kujutab endas loogilisi võrguelemente, mis oma olemuselt on tehnilised, kuid mis sõlmivad kõik need tehnilised elemendid konkreetsete seadmetega, mille kaudu seadmete kasutajad internetivõrke külastavad.[64] Viimane, kolmas kiht on sotsiaalne kiht (*The Social layer*), antud kiht keskendub inimkomponendile. Siia kuuluvad küberruumi osad, mille kaudu inimene on võrgus identifitseeritav, ehk e-mail, IP-aadress jne.[65]

Taoline jaotus on oluline ka suveräänsuse mõistmisel küberruumis. Riikide suveräänsuse kõige tavapärasema osa moodustab endast füüsiline kiht, hõlmates enda alla riistvara ning

[61] United Nations General Assembly. Human Rights Council. The Promotion, protection and enjoyment of human rights on the Internet. 27. Juuni 2016. Arvutivõrgus: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf (29 märts 2018)

[62] Freedomhouse. Freedom on the Internet 2017. Manipulating Social Media to Undermine Democracy. November 2017. lk 4-5. Arvutivõrgus: https://freedomhouse.org/sites/default/files/FOTN_2017_Final.pdf (29 märts 2018)

[63] The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028. 2010. lk 8 Arvutivõrgus: https://fas.org/irp/doddir/army/pam525-7-8.pdf (25 märts 2018)

[64] *Ibid*.lk 8.

[65] *Ibid*. lk 8.

infrastruktuuride osa. Riigil on õigus hallata ka teist, ehk loogilist kihti. See tähendab, et riigil on õigus kontrollida, et arvutite kommunikatsioon veebiserveritega oleks turvaline. Sotsiaalse kihi rollis on riigil õigus kehtestada teatav kontroll, mis käsitleb, millised tegevused on arvuti ning võrgukasutajatele lubatud ning millised tegevused mitte. Levinud on näiteks lapsporno omamise ning levitamise keeld, mille eesmärgiks on takistada kuritegude toime panemist. Küberruumis valitsev tsensuur ei tohi olla aga vastuolus ÜRO Inimõiguste ülddeklaratsiooniga, mille artiklis 19 sätestatakse, et igaühel on arvamuse- ja sõnavabadus; see õigus kätkeb vabadust sekkumiseta oma veendumustest kinni pidada ja vabadust informatsiooni ja ideid otsida, saada ja levitada igasuguste abinõudega ja riigipiiridest sõltumata.[66]

Riigi õigus suveräänsusele hõlmab endas ka kohustust kaitsta riigisisese õigusega küberkuritegude toime panemist. See tähendab, et riik ei tohi lasta enda territooriumil olevatel isikutel panna toime küberkuritegusid ega küberrünnakuid. Kui ühe riigi territooriumilt on sooritatud küberrünnak teise riigi vastu, ei saa seda kohaselt võrdsustada ühe suveräänse riigi rünnakuks teise riigi vastu. Küll aga võib see riik olla kohustatud andma aru, kuidas sellise rünnaku toime panemine oli võimalik ning millistel põhjustel antud rünnaku läbiviimist ei takistatud. Teatud juhtudel võib rünnaku ohvriks olnud riik kasutada vastumeetmeid ka riigi vastu, kelle territooriumilt rünnak toime pandi.[67] Riiki, kes ei taga korda oma suveräänsel territooriumil, on võimalik mõningatel juhtudel rahvusvahelise õiguse alusel ka vastutusele võtta.

Kuigi vastumeetmeid on loetud teatud juhtudel aktsepteeritavateks ning antud magistritöös on hilisemalt käsitletud ka riigi vastumeetmete võimalusi küberrünnaku korral, tuleks sellistes olukordades olla väga ettevaatlik ning jälgida, millised olid riigi võimalused rünnaku ära hoidmiseks ning kas nende sekkumatus tulenes soovist aidata passiivse käitumise näol rünnakule kaasa või polnud riigi jaoks rünnaku toime panemise avastamine ning takistamine teatud põhjustel võimalik. Tulevikus on oht, et just selliste olukordade tõttu võivad rahvusvahelised konfliktid eskaleeruda ning rünnak, mis on toime pandud riigi osaluseta, võib kaasa tuua halvimal juhul ka riikidevahelise konflikti. Seda olulisem on riikide võimekus kontrollida oma territooriumil asuvat küberruumi ning suveräänsust kübersfääris, siit tuleneb

[66] ÜRO Inimõiguste ülddeklaratsioon. http://vm.ee/et/uro-inimoiguste-ulddeklaratsioon (12 märts 2018)

[67] M. N. Schmitt, L. Vihul jt (koost). lk 11-16

ka peamine vajadus siseriiklikele seadusaktidele, mis antud valdkonda reguleeriksid ning laiemaid konflikte ära hoiaksid.

Suveräänsuse kontekstis on küsitav, kas riigi suveräänsus laieneb sellistele andmetele, mida riik on saatnud teise riigi territooriumile. Enamik Tallinna käsiraamatu koostanud ekspertidest leidis, et andmed, mis on transporditud välisriiki ei saa omada asukohariigi suveräänsuse staatust.[68] Eesti, kes on andmesaatkondade rajamise pioneer, olles kiitnud heaks andmesaatkonna loomise Luksemburgi, on toonud tähelepanu ka antud tegevuse legaalsusele suveräänsuse mastaabis. [69] Kuigi ka Tallinna käsiraamatus tekitas probleem küsitavusi, kas selline tegevus, kus üks riik hoiab valitsuse kriitilistest andmetest varukoopiaid teise riigi territooriumil, ei ole teise riigi suveräänsuse mõistega vastuolus, siis enamik leidis, et kui selleks on poolte nõusolek, siis sellise tegevuse näol ei ole tegemist suveräänsuse rikkumisega.[70]

Antud töö autor leiab, et kuigi antud teema võib tekitada küsitavusi, siis andmete haldamine andmesaatkondadena teistes riikides peaks kuuluma samasse kategooriasse dokumentide haldamisega välissaatkondades. Poolte nõusolekul ning andmesaatkondade kokkulepete jaoks sõlmitud riikidevaheliste lepingute näol on võimalik kokku leppida teatud punktides, mis säilitavad suveräänsuse ning julgeolekutingimused nii andmesaatkonna asukohariigi kui ka andmesaatkonna looja riigi jaoks. Seega ei saa andmesaatkonna asutamist lugeda suveräänsuse rikkumiseks, vaid loomulikuks dokumentide ning riigile vajaliku tarkvara säilitamiseks võimalikeks hädaolukordadeks.

2.3.3 Küberrünnakute eristamine küberkuritegudest

Üks olulistest küsimustest küberrünnakute kontekstis on see, kuidas eristada küberrünnakut kui rünnakut riigi vastu ning millal on toime pandud küberkuritegu üksikindiviidi või ettevõtte vastu. Riigivastastest küberrünnakutest rääkides saab eristada ka majanduslikke küberrünnakuid. Vahetegu on oluline mitmel tasandil. Sellest sõltub paljuski kas üldse ja

[68] M. N. Schmitt, L. Vihul jt (koost). lk 22-29

[69] Valitsus kiitis heaks Eesti andmesaatkonna rajamise Luksemburgi 15.06.2017. Arvutivõrgus: https://www.mkm.ee/et/uudised/valitsus-kiitis-heaks-eesti-andmesaatkonna-rajamise-luksemburgi (15 märts 2018)

[70] M. N. Schmitt, L. Vihul jt (koost). lk 22-29

milliste sanktsioonide näol võib riik küberrünnakule vastata. Sellest, kas ettevõtte ründamisega pannakse toime küberkuritegu või küberrünnak riigi vastu, sõltub sellest, kui laialt mõjutab rünnak riiki kui tervikut ning kas rünnaku motiiviks on rahalise tulu teenimine või riigi kui terviku mõjutamine majanduse kaudu.[71] Kui esimene võiks kuuluda küberkuriteo kategooria alla, siis teine küberrünnaku kategooriasse. Küberkuritegevust reguleerib täpsemalt Budapesti arvutikuritegevusvastane konventsioon.

Küberkuritegude uurimine jääb siseriikliku õiguse raamesse, kuuludes seega iga riigi vastutusalasse, näiteks karistusseadustiku § 206 lg 1 sätestab, et arvutisüsteemis olevate andmete ebaseadusliku muutmise, kustutamise, rikkumise või sulustamise eest karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.[72] Sama seaduse § 207 lg 1 sätestab, et arvutisüsteemi toimimise ebaseadusliku häirimise või takistamise eest andmete sisestamise, edastamise, kustutamise, rikkumise, muutmise või sulustamise teel – karistatakse rahalise karistuse või kuni kolmeaastase vangistusega.[73] Arvutikuriteo ettevalmistamist reguleerib § 216, mis sätestab, et seadme või arvutiprogrammi, mis on loodud või kohandatud eelkõige käesoleva seadustiku §-s 206, 207, 213 või 217 sätestatud kuritegude toimepanemiseks, või kaitsevahendi, mille abil on võimalik hankida juurdepääs arvutisüsteemile, hankimise, valmistamise, valdamise, levitamise või muul viisil kättesaadavaks tegemise eest, et panna ise või võimaldada kolmandal isikul panna toime käesoleva seadustiku §-s 206, 207, 213 või 217 sätestatud kuritegu, – karistatakse rahalise karistuse või kuni kaheaastase vangistusega.[1] Paragrahv 217 sätestab, et arvutisüsteemile ebaseaduslikult juurdepääsu hankimise eest kaitsevahendi kõrvaldamise või vältimise teel – karistatakse rahalise karistuse või kuni kolmeaastase vangistusega. [74]

Neist kaks viimast on sisuliselt siseriiklikud meetmed riigisisese korra hoidmiseks ning tagamaks selle, et riigi territooriumilt küberrünnakuid ei sooritataks. Paragrahvid 216[1] ning § 217 on küberkuritegu reguleerivad paragrahvid, mis kaudselt reguleerivad ka küberrünnakuid. Küberrünnakute sooritamine koosneb paljuski arvutikuriteo toime panemisest ning arvutisüsteemile ebaseaduslikust juurdepääsust.

---

[71] K. Zemanek. Armed Attack. Max Planck Encyclopedia of Public International Law. Oxford Public International Law. oktoober 2013. Arvutivõrgus: http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e241 (14 aprill 2018)

[72] Karistusseadustik[1] - RT I 2001, 61, 364

[73] *Ibid.*

[74] *Ibid.*

Antud normid on karistusseadustikku ning siseriiklikusse õigusesse toodud eelkõige õiguskindluse ning selguse huvides, kinnitamaks, et küberrünnakud ning küberkuritegevus ei ole ühiskonnas aktsepteeritud. Kahjuks on üsna selge, et siseriiklikust reguleeritusest jääb küberruumi kontekstis väheks. Enamik toime pandud küberrünnakuid on kontinentaalse, rahvusvahelise mõõtmega Jälgides reaalajas kasvõi lühikese ajaperioodi jooksul toimuvate küberrünnakute visualiseeringut, näiteks ühe kuulsaima reaalajas küberrünnakuid vahendava veebilehe, Norse kaudu, on näha, et enamik toime pandavatest küberrünnakutest on mandritevahelised.[75] See tähendab omakorda, et kuigi siseriiklike seaduste olemasolu on kahtlemata hädavajalik, ei ole ainult siseriiklike regulatsioonidega antud valdkonda reguleerida võimalik. Küberruumi riigiülesuse tõttu loodi 2001. aastal Budapesti konventsioon, mille eesmärgiks oli siseriiklike õiguste ühtlustumist küberkuritegevuse kontekstis, mille kaudseks eesmärgiks oli ka vähendada küberrünnakute osakaalu. Budapesti konventsioon ei ole aga riikide puuduliku koostöö ning keeruka menetlusabi protsessi tõttu soovitud eesmärki täitnud. Siiski küberrünnakute probleemi tuuma, rahvusvahelisi küberrünnakuid riikide vahel, antud konventsioon reguleerida ei saa. Üheks põhjuseks on siinkohal asjaolu, et konventsiooniga ei ole mitmed olulised rahvusvahelist õigust kujundavad riigid liitunud.[76]

2.4 Küberrünnak kui jõu kasutamine

ÜRO Harta peamiseks lähtepunktiks relvastatud konfliktide vältimiseks on artikkel 2 punkt 4, mis sätestab, et kõik ÜRO liikmed hoiduvad oma rahvusvahelistes suhetes jõuga ähvardamisest või jõu tarvitamisest nii iga riigi territoriaalse puutumatuse, poliitilise sõltumatuse vastu kui ka mõnel muul viisil, mis ei ole kooskõlas ÜRO eesmärkidega.

Kuidas suhestuvad omavahel antud kontekstis arusaam jõu kasutamisest ning esimeses peatükis välja toodud võimalikud küberrünnaku definitsioonid? Kõik oleneb muidugi aluseks võetavast küberrünnaku definitsioonist, mille osas üldine konsensus puudub. Kuna autor keskendub antud töös paljuski Tallinna käsiraamatu analüüsile, lähtutakse ka siinkohal

[75] Norse Corporation Attack map. Arvutivõrgus: http://map.norsecorp.com/ (25 märts 2018)

[76] Näiteks ei ole Budapesti konventsiooni ratifitseerinud Iirimaa, Rootsi, Venemaa, San Marino, India, Hiina, jne. Arvutivõrgus: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (15 aprill 2018)

Tallinna käsiraamatu definitsioonist.[77] Tallinna käsiraamatu reegel 69 sätestab, et küberoperatsioon kvalifitseerub jõu kasutamiseks, kui selle skaala ja mõju on võrreldavad selliste rünnakutega, mis on kvalifitseeritavad küberoperatsioonide välisele jõu kasutuse mõistele.[78]

Antud kontekstis on selge, et küberrünnakute ning jõu kasutamise definitsioonid ei ole samatähenduslikud. Kahe käsitluse peamiseks erinevuseks on küberrünnaku definitsiooni puhul konkreetsus ning võib öelda, et mingil määral ka tagajärjepõhisus ning jõu kasutamise definitsiooni juhul avatud ning laiem tõlgendamisruum. Kui küberrünnaku definitsiooni raames on olulisteks märksõnadeks ründav või kaitsev tegevus, mis võib eelduslikult olla ohuks inimese elule või tervisele ning objektide kahjustamisele või hävimisele, siis jõu kasutamise definitsioonis omab tähtsust skaala ning mõju/tagajärje kriteerium. Tallinna käsiraamatu küberrünnaku definitsioon nõuab üsna konkreetseid tagajärgi, mida jõu kasutamise kriteerium sõnaselgelt ei nõua. Seega võib öelda, et iga küberrünnak kvalifitseeruks Tallinna käsiraamatu mõistes vähemalt jõu kasutamise alla. Vastupidi see ilmtingimata nii ei ole.

Kindlat jõu kasutamise või tarvitamise kriteeriumit ei ole ÜRO harta mõistes välja toodud. Seetõttu on definitsiooni raames välja toodud Rahvusvahelise kohtu lähenemine Nicaragua kaasuses, kus kohus lõi tõlgendamisel välja sõnad skaala ning tagajärjed. Just skaala ning tagajärgede analüüsimisel peaksime saama vastuse, kas küberrünnaku näol on tegemist jõu kasutamisega või mitte.[79] Käsiraamatu reegli kohaselt peab see olema võrreldav sellise jõuga, mida tõlgendatakse jõu kasutamiseks küberoperatsioonide väliselt.[80]

Käsiraamatus on välja toodud rahvusvahelises õiguses valitsev seisukoht, kus poliitilised ning majanduslikud survestamise meetmed, mis võivad mõjutada riigi territoriaalset terviklikkust või riigi poliitilist iseseisvust, ei loeta jõu kasutamiseks. Samuti on toodud välja Nicaragua

[77] M. N. Schmitt, L. Vihul jt (koost). lk 415. Küberrünnak on küberoperatsioon, mis on oma iseloomult kas ründav või kaitsev ning mille esilekutsumine võib olla eelduslikult ohuks inimeste tervisele, elule või objektidele, tekitades nende kahjustamist või hävimist.

[78] *Ibid.* lk 330

[79] I.C.J. Reports. Nicaragua v. United States of America. Military and Paramilitary Activities in and against Nicaragua. 1986. para 195 Arvutivõrgus: http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf (14 märts 2018)

[80] M. N. Schmitt, L. Vihul jt (koost). lk 330

kaasuse käsitlus, kus leiti, et pelk rahaline toetus häkkerite grupile, ei ole piisav ajend kvalifitseerimaks rünnakut jõu tarvitamiseks ÜRO artikkel 2 punkti 4 mõistes. Küll aga kvalifitseerub rünnak jõu kasutamiseks juhul, kui riik tagab väljaõppe või juhised rünnaku läbi viimiseks.[81] Autori hinnangul võib jääda Nicaragua kaasuses välja toodud tõlgendus küberrünnakute kontekstis liiga kitsaks. Täpsemalt tõlgendus, et pelgalt rahaline toetus ei anna alust käsitleda näiteks häkkerite grupi rünnakut jõu kasutamisena riigi poolt. Kindlasti on tegemist probleemse punktiga, kuna ühest küljes on võimalik, et tõlgendus on liiga lai, teisalt võib jällegi tõlgendus jääda kitsaks. Paljuski sõltub see tulevasest praktikast ning sellest, kui iseteadlikud on konkreetsed häkkerite grupid, kes teist riiki rünnanud on. Näiteks kui häkkerite grupp on teadaolevalt ühe riigi vastase käitumismaneeriga, siis justkui piisaks seda rünnakut soosival riigil toetada antud gruppi. Riigil puuduks vajadus ka häkkerite grupi nö „relvastamiseks“ ning väljaõppe sooritamiseks? Täpsemalt on antud probleemi käsitletud töö järgmises peatükis, küberrünnakute omistamise raames.

Kuigi hetkel on rahvusvahelise õiguse raames võetud seisukoht, et poliitilised ning majanduslikud survestusmeetmed, mis võivad riikide territoriaalset terviklikkust ning poliitilist iseseisvust mõjutada, ei hõlma jõu kasutamist, siis kas küberrünnakute kontekstis ei peaks antud seisukohta ümber vaatama? Autori hinnangul peaks seda tegema. Autori seisukohta kinnitab ka Avra Constantinou skaala ning mõju laiendatud käsitlus, kus Constantinou peab jõu kasutamiseks ka seda, kui sihtriigi olulisi elemente on hävitatud sh majanduse- ja kaitsetaristut, kahtluse alla on seatud poliitiline vabadus või kui rünnak on toimunud riigi peamise tööstuse ja majandusliku ressursi vastu, mis tekitab majandusele olulist kahju.[82] Peamine põhjus, miks ka antud töö autor sellist seisukohta pooldab, seisneb küberrünnakute endi olemuses.

Küberrünnakute mõjuvahendiks ei ole alati pelgalt nö otsese kineetilise ja objektiliselt tuntava kahju tekitamine. Viimaste tendentside valguses on proovitud küberrünnakuid kasutada ära eelkõige just kaudse mõjutusvahendina. Seda nii majanduslikus võtmes kui ka poliitilise

[81] M. N. Schmitt, L. Vihul jt (koost). lk 330-332

[82] K. Zemanek. Armed Attack. Max Planck Encyclopedia of Public International Law. Oxford Public International Law. oktoober 2013. Arvutivõrgus: http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e241 (14 aprill 2018)

mõjutusvahendina.[83] Küsimus on selles, kas rahvusvaheline üldsus aktsepteerib tulevikus sellist käitumist või mitte. Võib öelda, et praegusel hetkel on tegemist siiski veel üsna uudsete probleemidega ning küberrünnakute näol tõelist poliitilist mõjutamist oleme näinud ehk vaid viimase 5 aasta jooksul. Loomulikult on olnud kaasuseid, mille kaudne eesmärk on segaduse tekitamine ning sellega ka riigi poliitika mõjutamine (näiteks Eesti ning Georgia vastased teenusetõkestusrünnakud vastavalt 2007. ning 2008. aastal). Poliitiliseks mõjutamiseks, mida autori hinnangul peaks taunima ka rahvusvahelise õiguse vahendusel, peaks hõlmama endas näiteks 2016. aasta USA presidendivalimisi tabanud ning sellele sarnanevaid rünnakuid. Siinkohal ei ole autori hinnangul oluline, kas konkreetse kaasuse raames õnnestus reaalselt häältega manipuleerida või mitte. Sellisel tasandil demokraatlike väärtuste kaitse peaks olema juba iseenesest argumendiks ning on oht, et selliseid rahvusvahelise õiguse piiride kompamisi tehakse veel. Majandusliku mõjutamise all peab autor silmas eelkõige olukordi, kus küberrünnak ei ole sooritatud mitte ühe konkreetse ettevõtte vastu, vaid majanduslik mõju hõlmab laiemalt riiki kui tervikut.

Näiteks rünnates USA-s New Yorgis asuvat börsi, ei puuduta oht vaid ühte konkreetset ettevõtet, vaid oht laieneb kogu USA finantssüsteemile, mis olles tihedalt seotud teiste riikide majandusruumiga, tulenedes erineva taustaga ettevõtetest, kes USA börsil kauplevad, võib mõjutada ka teatud määral globaalset majandust. Täpsemalt on antud kontekstis räägitud ohust, kus keskarvutis nakatatakse arvutiviirusega, mis hakkab algoritmide alusel teostama aktsiatega ostu-müügi tehinguid, mõjutades seeläbi aktisaturgu ning hinda.[84] Taoline rünnak mõjutab kaudselt inimeste käitumist aktsiaturul, olles mõjutatud psühholoogilisest faktorist, sh hirm kaotada aktsiaturul raha jne. See, kui suure kahju see võib majandusele tekitada, sõltub paljuski rünnaku eesmärgipäralisusest ning õnnestumisest, mis omakorda sõltub küberkaitsevahenditest.

Jõu kasutamise olemuse hindamiseks on Tallinna käsiraamatu looja, Michael N. Schmitt'i poolt on loodud jõu kasutamise abiskeem. Tegemist ei ole küll juriidiliselt siduva skeemiga, kuid on loodud näitlikustamaks ning abistamaks, kuidas kehtiva rahvusvahelise õiguse alusel

[83] P. Brangetto, M. A. Veenendaal. Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. NATO CCD COE Publications. 2016. lk 117-118. Arvutivõrgus: https://ccdcoe.org/cycon/2016/proceedings/08_brangetto_veenendaal.pdf (14 aprill 2018)

[84] P. Szoldra. Hacker Reveals How Devastating A Cyberattack On The Stock Market Could Be. 21. august. 2013. Arvutivõrgus: http://www.businessinsider.com/hacker-reveals-how-devastating-a-cyberattack-on-the-stock-market-could-be-2013-8 (13 aprill 2018)

jõu kasutamise olemuse võiks kindlaks teha. Tõsidus (*Severity*), Vahetu (*Immediacy*), Otsesus (*Directness*), Invasiivsus (*Invasiveness*), Mõõdetavus (*Measurability*), Sõjalne iseloom (Military character), Riigi seotus (*State involvement*), Õiguspärasuse eeldus (*Presumptive legality*).[85] Järgnevalt on autor lahendanud Stuxneti kaasuse näitel jõu kasutamise skeemi. Stuxneti kaasus on võetud näiteks eelkõige selle tõttu, et tegemist on kaasusega, mida peetakse esimeseks ning teadaolevalt ainsaks küberrünnakuks, mida saaks käsitleda jõu kasutamisena rahvusvahelise õiguse mõistes.

2.4.1 Jõu kasutamine Stuxneti näitel

Stuxneti näol on tegemist viirusega, mis loodi väidetavalt USA ning Iisreali poolt eesmärgiga pärssida Iraani tuumaprogrammi. Viirus hävitas pahavaraga uraani rikastamise tsentrifuugid. Algselt ei olnud teada, et tegemist on küberrünnakuga, selgus saabus alles siis, kui Iraani teadlased pöördusid probleemiga Valgevene arvutitehnikute poole. Väidetavalt levis viirus operatsioonisüsteemidesse töötaja mälupulga kaudu. [86]

Schmitti jõu kasutamise abiskeem.

(1) Tõsidus (*Severity*): Inimvigastused ning eelduslik oht sellele teadaolevalt puudub. Küll aga hävitati mitmeid uraani rikastamise tsentrifuuge. Väidetavalt hävitas Stuxneti viirus 984 uraani rikastamise tsentrifuugi. Tuues kaasa uraani rikastamise programmi efektiivsuse vähenemise 30% võrra.[87]
(2) Vahetu (*Immediacy*): Seda, kui kiiresti küberrünnaku mõju oli tunda, ei ole täpselt teada. Antud kontekstis on mõeldud ka seda, kas rünnak oli nii vahetu, et sellele oleks võinud rakendada vastumeetmeid. Pigem tuleks siinkohal vahetuse aspekti eitada, kuna iraanlased said küberrünnakust teada alles siis kui valgevene arvutiteadlased olid operatsioonisüsteeme uurinud.
(3) Otsesus (*Directness*): On põhjust eeldada, et just Stuxneti viirus on otseseks põhjuseks, mis hävitas uraani rikastamise tsentrifuugid. Seega on Stuxneti viiruse ning uraani rikastamise tsentrifuugide hävimise vahel põhjuslik seos.

[85] M. N. Schmitt, L. Vihul jt (koost). lk 333-337

[86] M. Holloway. Stuxnet Worm Attack on Iranian Nuclear Facilities. Stanford University. 16. juuli 2015. Arvutivõrgus: http://large.stanford.edu/courses/2015/ph241/holloway1/ (15 aprill 2018)

[87] *Ibid.*

(4) Invasiivsus (*Invasiveness*): Küberrünnaku objektiks olnud *SCADA* juhtpult, oli suure tõenäosusega turvatud. On teada, et *SCADA* süsteemidel puudus juurdepääs internetivõrgule. Seega oli juba antud faktor iseenesest üks kaitsemehhanismidest, on põhjust eeldada, et rünnatud operatsioonisüsteem oli turvatud. Rünnak tabas eeldatavalt sihtmärki, kuna väidetavalt oli operatsiooni eesmärgiks peatada Iraani tuumaprogramm.
(5) Mõõdetavus (*Measurability*): Rünnaku tagajärjel langes uraani rikastamise programmi efektiivsus väidetavalt 30% võrra, samuti hävitas 984 uraani rikastamise tsentrifuugi.[88]
(6) Sõjaväeline iseloom (*Military character*): Operatsiooni sõjaväeline iseloom on täpselt teadmata, kuid võib eeldada, et sellise rünnaku läbi viimiseks oli vajalik luureandmete (andmed kasutatavatest arvutisüsteemidest ning nende täpsemast olemusest) olemasolu, mis viitab vähemalt kaudselt sõjaväelisele seotusele antud küberrünnakuga.
Kas kannataja pooleks oleva riigi rünnatud objektil on sõjaväeline iseloom? Ilmselt oleneb see paljuski käsitlusest, kuid pigem võiks eeldada, et Iraani tuumaprogramm, mida rünnati, oli sõjaväelise iseloomuga.
(7) Riigi osalus (*State involvement*): Kindlad ning otsesed tõendid, mis viitaks USA või Iisraeli seotusele antud küberrünnakuga puuduvad.
(8) Eeldatav õiguspärasus (*Presumptive legality*): Tegemist ei ole lubatud tegevusega rahvusvahelise õiguse mõttes ning sellise rünnaku näol oleks tegemist ka jõu kasutamisega juhul, kui tegemist ei oleks küberrünnakuga ehk ka küberoperatsioonide väline taoline rünnak oleks kvalifitseeritav jõu kasutamisena.

Antud skeemi kasutamine aitab kindlasti jõu kasutamise kvalifitseerimisel. Ometigi on näha, et ka antud skeemi raames tekivad teatud küsitavused. Kuigi skeem ei ole siduv ning võib väita, et skeem peab olema täidetud näiteks vaid teatud ulatuses väitmaks, et jõudu on kasutatud, tekitab ebakindlust asjaolu, kuidas leida konkreetseid tõendeid selliste rünnakute läbi viimise kohta. Antud juhul tegi asjaolu ehk keerukamaks see, et viirus avastati hilja ning operatsioonisüsteemi isoleerituse tõttu internetivõrgust, oli väga raske kindlaks teha ka allikat, kust küberrünnak alguse sai. Teisalt peaks rahvusvaheline õigus olema ka teisteks sarnasteks kaasusteks valmis ning juhtunust omad järeldused tegema.

Tuginedes Tallinna käsiraamatus välja toodud definitsioonile, käsitletakse jõu kasutamist küberoperatsioonina, kui selle skaala ja mõju on võrreldavad selliste rünnakutega, mis on

[88] M. Holloway. Stuxnet Worm Attack on Iranian Nuclear Facilities. Stanford University. (15 aprill 2018)

kvalifitseeritavad küberoperatsioonide välisele jõu kasutuse mõistele.[89] Skaala ja mõju kontseptsiooni on lahti mõtestanud Avra Constantinou, kes on öelnud, et relvastatud rünnak tähendab toimingut või mitmeid toiminguid, mis omavad märkimisväärset suurust ja intensiivsust (skaala) ning mille tagajärjed (mõju) on tekitanud sihtriigi oluliste elementide hävimise, sealhulgas selle inimestele/rahvale, majanduse- ja kaitsetaristule, riigi autoriteedi murendamisele, poliitilise vabaduse ning riigi füüsilisest elemendist ilmajäämine eelkõige selle territooriumi kaotamise näol. Constantinou on maininud oma käsitluse raames ka jõu kasutamist riigi peamise tööstuse ja majandusliku ressursi vastu, mis tekitab majandusele olulist kahju.[90]

Järgnevalt vaatleb autor põgusalt ka Constantinou poolt välja pakutud nö laiendatud skaala ja mõju kontseptsiooni järgides Stuxneti kaasust.

Skaala (*Scale*) – Stuxneti küberrünnaku skaala hindamisel tuleks vaadelda asjaolu, et rünnak toimus sisuliselt arvutiviiruse koodi paljunemise näol, mis kumuleerumise näol muutis rünnaku järjest intensiivsemaks ning suurendas rünnaku skaalat. Kuigi algselt ei tundunud rünnak olevat oma olemuselt intensiivne ning märkimisväärset suurust omav, siis ajaperioodi vältel, mil viirus laienes, muutus ka rünnaku skaala suuremaks ning seeläbi on autori hinnangul jõu kasutamise skaala jaoks vajalikud omadused kvalifitseeritud.

Mõju (*Effect*) - 984 uraani rikastamise tsentrifuugi rünnak on ilmselt arvestatava mõjuga, seda enam, et väidetavalt vähendas see kogu töö efektiivsust 30% võrra ehk pea 1/3 võrra. Seega oli rünnakul oluline mõju ilmselt ka riigi majandusele ning kaitsetaristule.

Eelnevast selgub, et jõu kasutamise skeemide järgi lahenduseni jõudmine vajab oluliselt määral informatsiooni rünnaku detailidest ning sellest, kui reaalsed ning otsesed on tõendid konkreetse rünnaku kohta. Seega ei ole antud skeemidest väga palju kasu olukordades, kus jõu kasutamisele soovitakse vastata vastumeetmetega, kuna paljuski on mõlemad skeemid tagajärjepõhised ning vajavad olulist infot rünnaku olemusest.

Selliste rünnakute kvalifitseerimisel jõu kasutamiseks võib oleneda otsus isegi väikestest detailidest, mis võivad viidata kaudsele seotusele või rünnakut mõjutanud asjaoludele.

[89] M. N. Schmitt, L. Vihul jt (koost). lk 330

[90] K. Zemanek. Armed Attack. Max Planck Encyclopedia of Public International Law. (14 aprill 2018)

Michael N. Schmitt'i käsitlus annab oluliselt parema raamistiku konkreetse kaasuse jõu kasutamise üle otsustamisel. Teisalt võib selle raamistiku lahenduskäigu lahendamine olla informatsiooni puudulikkuse tõttu väga keeruline. Teisest küljest toetab töö autor Constantinou seisukohta, kes pooldab ka olulise majanduskahju ning poliitilise sekkumise aktsepteerimist jõu kasutamisena.

2.5 Küberrünnaku omistamine konkreetsele riigile

Tallinna käsiraamatu reegel number 14 sätestab, et riik kannab rahvusvahelist vastutust kübertegevusele, mis on omistatav riigile ja kujutab endast rahvusvahelise õigusliku kohustuse rikkumist.[91] Küberrünnakute omistamine mängib keskset rolli selles, kas ja millised on tagajärjed rünnakule ning kuidas võib kannatada saanud riik käituda. Samuti on see oluline määramaks, kas riik, kes küberrünnaku toime pani, on üldse tegelikkuses rünnaku taga või on küberrünnak sooritatud ilma riigipoolse heakskiiduta.

2.5.1 Riiklikud küberrünnakud

Riiklikeks küberoperatsioonideks saab Tallinna käsiraamatu reegli 15 mõistes nimetada selliseid operatsioone, mis on riigiorgani poolt läbi viidud või selliseid operatsioone, mis on siseriikliku õiguse alusel volitatud tegutsema riigi nimel.[92] Kõige lihtsam on riigiga seostada selliseid rünnakuid, mis on viidud läbi riigiorgani enda poolt. Tallinna käsiraamatus mõistetakse selliste rünnakute all eelkõige rünnakuid, mis on läbi viidud riigi sõjaväe või kaitseväe poolt või selle küberüksuse poolt. Rõhutatud on, et „riigiorganit" tuleks käsitleda laia tõlgendusena selleks, et vältida võimalikke kontseptsioone, mis välistaksid otsese riigi vastutuse. Pelgalt asjaolu, et riik omab firmat või korporatsiooni ei ole käsiraamatu mõistes aluseks nimetada firmat riigiorganiks. Siseriikliku volituse alusel riigi nimel tegutsevad asutused on valitsuse või riigi funktsioone ellu viivad asutused. Viimati nimetatud konteksti raames on silmas peetud taaskord laia käsitlust. [93]

[91] M. N. Schmitt, L. Vihul jt (koost). lk 84

[92] *Ibid.* lk 87

[93] *Ibid.* lk 87-89.

2.5.2 Mitteriiklikud küberoperatsioonid

Tallinna käsiraamatu reegel nr 17 toob välja valitsusväliste tegutsejate poolt läbi viidud küberoperatsioonid, mida saab riigile omistada juhul kui:

a) Need on läbi viidud kooskõlas riigi juhistele ning kontrollile
b) Riik tunnustab ja võtab rünnaku omaks.[94]

Antud käsitluse üldise reegli kohaselt ei ole üksikindiviidide ning rühmituste poolt toime pandud küberrünnakud ja küberoperatsioonid riigile omistatavad. Siiski saab indiviide ja rühmitusi vastutusele võtta, sellisel juhul on oluline see, et indiviid või rühmitus, kes viis rünnaku läbi, on saanud rünnakuks juhiseid ning instruktsioone riigilt või on riigi kontrolli all. Rünnakut ei saa riigile omistada pelgalt selle eest, et riik on valitsusvälist tegevust toetanud üldisel viisil või seda julgustanud. Siiski on käsiraamatus mainitud, et asjaolu, et rünnak ei ole riigile omistatav, ei tähenda, et riik ei võiks kanda vastutust rahvusvahelise õiguse rikkumise toetamise eest.[95]

Autori hinnangul loob Tallinna käsiraamatus selgitatud kontseptsiooni üsna keerulise situatsiooni küberrünnakute rakendamise ümber rahvusvahelises õiguses, kus puudub täielik õigusselgus, mis piirini on tegemist riigile omistatava operatsiooniga, millisel juhul vastutab riik nö õiguse rikkumise toetamise eest ning millisel juhul on tegemist üksikindiviidide ning rühmituste poolt iseseisvalt läbi viidud küberrünnaku või küberoperatsiooniga. Rahvusvaheline õigus jätab sellisteks situatsioonideks autori hinnangul väga laia tõlgendusvõimaluse, mida saaks kitsendada ning konkretiseerida rahvusvahelise õiguse praktika tekkimise käigus küberrünnakute kontekstis, kuid mille tekkimisest ei ole riigid ka ise huvitatud, kartes situatsioonide eskaleerumist.

Küsitav on, kas rahvusvahelise õiguse nii lai tõlgendamine on küberrünnakute praktikas asjakohane. Suurema skaalaga küberrünnakud vajavad enamasti finantsvõimekuse kõrval ka instrueerimist ja tehnilist väljaõpet, kuid täielikult ei saa välistada ka olukordi, kus algselt tundunud väikse võimekusega rühmitus paneb toime laastava tagajärjega küberrünnakuid. Ilmselt annab ka sellele, kas rahvusvaheline õigus nii laia tõlgenduse läbi oma eesmärki

[94] M. N. Schmitt, L. Vihul jt (koost). lk 94-95.

[95] *Ibid.* lk 95-99.

täidab, praktika. Seega on tegemist mingis mõttes olukorraga, kus praktika oleks vajalik, kuid mida kõik riigid samaaegselt luua ei soovi.

Rahvusvahelise õiguse seisukohalt võib üsna keeruliseks osutuda just mitteriiklike organisatsioonide ja indiviidide poolt läbi viidud küberrünnakud. Tallinna käsiraamatust tuletatud praktika ning reeglid on hõlmanud endas konventsionaalseid relvastatud rünnakuid. Teisalt on autori hinnangul riigi ning organisatsioonide sidemeid märkimisväärselt lihtsam avastada konventsionaalsete relvarünnakute osas, keeruliseks võib see kujuneda aga küberrünnakute kontekstis. Kahtlemata on raskemate tagajärgedega küberrünnakud tihti spetsiifilisemad, vajades teatud juhtudel ka luureandmeid süsteemidesse tungimiseks ning küberrünnaku sooritamiseks, mis annab ehk suurema võimaluse leida sidemed teatud riigi, tema julgeolekuteenistuste ning küberrünnaku sooritaja vahel. Samas olukorras, kus on teada häkkerite grupi ebasümpaatia teatud riigi vastu, piisab rünnata sooviva riigi finantsilisest toetusest, andmata spetsiifilisi juhiseid ega täpsemat informatsiooni ning juhul, kui on teada, et just tänu rahalise võimekuse paranemisele sai häkkerite grupp läbi viia rünnaku palju laiahaardelisemalt kui see seni oleks võimalik olnud. Kas sellistes olukordades ei peaks mitte ka riik siiski rünnaku eest vastutama, olles taganud küll vaid rahalise toe, kuid kaudselt andes sellega võimekuse, mida grupil varasemalt polnud? Käsiraamatus on küll öeldud, et riiki võib siiski vastutusele võtta rahvusvahelise õiguse rikkumise toetamise eest, kuid kas see ei võiks olla nii otsese mõjuga toetuseks, mis kvalifitseerub ka näiteks jõu kasutamiseks?

Kõige olulisem küsimus on aga ehk see, kes suudab selliste küberrünnakute läbi viimise ning sidemed riikide ja häkkerite vahel tõestada ja tuvastada. Konventsionaalsete rünnakute korral jääb oluliselt rohkem materiaalseid jälgi riigi ja organisatsiooni vahelistest sidemetest isegi kõrge konspiratsioonitaseme korral kui küberruumis. Loomulikult jääb ka küberruumis maha iga tegevust hõlmanud jälg, kuid vastavate tehniliste oskuste korral on võimalik oma jälgi edukalt ka varjata. Kõrge konspiratsioonitaseme korral on riikidel väga keeruline leida, kes on rünnakute autor ning kas need sidemed viitavad ka riigi toele. Võib üsna kindlalt väita, et enamikul maailma riikidest puudub selliste rünnakute uurimiseks kompetents ning vahendid. Seda nii tehnilisel tasandil kui ka inimressursside näol. Seega kui õiguslikul tasandil on analoogia kasutamine valitsusväliste tegutsejate ning riikide vaheliste sidemete omistamine teostatav, siis seda, kas antud süsteem laiemalt praktikale vastu peab, näitab aeg. Autor pakub antud probleemile lahenduse 3. peatükis, küberkonventsiooni kontekstis, pakkudes lahenduseks ÜRO juurde kuuluvat Rahvusvahelist küberkaitse keskust.

2.6 Võimalikud vastumeetmed küberrünnakule Põhja-Atlandi lepingu artikkel 5 ning Tallinna käsiraamatu alusel.

Tallinna käsiraamatu alusel koosnevad riigi võimalikud vastumeetmed kahest osast. Vastumeetmed, mida võib kasutada vastuseks teise riigi poolt jõu kasutamise vastu ning enesekaitse, mis on lubatud vastuseks sellisteks jõu kasutamist hõlmavateks rünnakuteks, mis kvalifitseeruvad relvastatud rünnakutele.

Tallinna käsiraamatu reegel number 20 annab riigile õiguse kasutada nii küberalaseid kui muud laadi vastumeetmeid, kui mõni riik, kes omab tema ees rahvusvahelist juriidilist kohustust, seda rikub.[96] Seega ei sea käsiraamat riikidele piiranguid, millisel moel võib riik jõu kasutamisele vastata ning küberrünnakutele ei pea vastama pelgalt küberoperatsiooni või küberrünnaku näol. Käsiraamatu reegel number 21 sõnastab, et vastumeetmed, oma olemuselt kas küberalased või muud laadi, võib võtta kasutusele vaid vastutava riigi kuuletuma kutsumiseks kannatanud riigi poolt.[97]

Tallinna käsiraamat rõhutab, et vastumeetmete kohaldamise eesmärgiks on selle näol lõpetada ründava riigi ebaseaduslik tegevus. Nagu reeglite sõnastusest nähtub, on jäetud väga lai tõlgendusviis, milline vastumeede olla võiks. Küberrünnaku vastumeetmeks ei pea antud reegli järgi olema ilmtingimata vastus kübersfääris või küberrünnaku näol. Enamik eksperte leidsid, et rünnaku vastus peab olema selline, mille kasutusele võtmise meede lõpetaks rünnaku toime panemise ründava riigi poolt. Teisalt ei tohiks vastumeede kasutada ära ründava riigi nõrkuseid, vaid olema kantud tõelisest soovist rünnaku ning konflikti lõpetamiseks. Samuti soovitati ennetavalt teavitada riiki ebaseadusliku ründe eest ning mõned ekspertidest leidsid, et enne vastumeetme kasutamist peab riik otsima rahumeelset lahendust läbirääkimiste läbi.[98]

Mitmed vastumeetmete kohaldumise seisukohad Tallina käsiraamatus leidsid ekspertide poolt lahknevaid arvamusi. See tähendab, et just vastumeetmete osa on ehk Tallinna käsiraamatu raames kõige problemaatilisem. Autori hinnangul tekitab probleeme ka see, et vastumeetmeid võib kasutada sisuliselt kõigi riigi vastu suunatud rahvusvahelist õigust rikkuvate rünnakute

[96] M. N. Schmitt, L. Vihul jt (koost). lk 111.

[97] *Ibid.* lk 116.

[98] *Ibid.* 116-122.

vastu. Siinkohal ei ole mõeldud vaid küberrünnakuid, vaid kõiki küberoperatsioone, mis rikuvad rahvusvahelist õigust. Autori hinnangul nõrgendab just vastumeetmete osa ehk Tallinna käsiraamatu üldist käsitlust. See ei näita mitte käsiraamatu nõrkust, vaid pigem seda, kui erinevad on arusaamad vastumeetmete osas ka õigusteadlaste hinnangul. Kui teistes osades on rahvusvahelist õigust proovitud tõlgendada üsna kitsalt, näiteks riigile olulise majandusliku kahju tekitamise lugemist ei loeta rünnakuks riigi vastu (peamiselt sõna „rünnaku" kui sõjalise relvastatud rünnaku mõiste tõttu ning rahvusvahelise kehtiva praktika tõttu), siis vastumeetmete kohaldamisel on jäetud väga suur tõlgendusruum ning riikidel on laias laastus ise võimalik otsustada, millistel juhtudel vastumeetmeid kasutada ning millised need vastumeetmed oma olemuselt peaksid olema. Piirang on loodud reegliga number 22, mis sätestab, et vastumeetmed, oma olemuselt küberruumi kuuluvad meetmed või teised meetmed ei tohi hõlmata endas tegevust, mis seaks ohtu fundamentaalsed inimõigused, sõjategevust kättemaksu näol või peremptoorseid norme rikkuvaid meetmeid. Riik, kes kasutab vastumeetmeid, peab täitma oma kohustusi tunnustades diplomaatilist ning konsulaarõigust. [99]

Peremptoorseid norme ja fundamentaalseid inimõiguseid ei ole konkreetsetesse kataloogidesse paigutatud, kuid üldiselt on levinud arusaam, et peremptoorsed normid sisaldavad endas selliseid olulisi väärtuseid ja printsiipe, mis on fundamentaalselt olulised rahvusvahelisele kogukonnale. Peremptoorse normi olulisus sõltub sellest, milline on olulisus ning väärtus selle normi taga, mida ta endas kannab. Rahvusvahelise Õiguse Komisjon on Viini konventsiooni artikli 53 kavandis peremptoorsete normide all välja toonud genotsiidi, orjastust ning elementaarseid põhiõiguseid ja õigust enesemääramiseks.[100] Konkreetse kataloogita ei ole küll päris selge, mis normid täpsemalt peremptoorsed normide ning fundamentaalsete inimõiguste alla kindlasti kuuluvad, mis küberrünnakute vastumeetmetena keelatud on, kuid nagu eelnevalt mainitud, saab antud kataloogi või keelatud vastumeetmed kindlaks teha sellega, millist rahvusvahelisele kogukonnale olulist väärtust rikutakse ning peremptoorse normiga kaitsta soovitakse. Antud asjaolu ei tohiks muuta üleliia keeruliseks arusaamist vasturünnakute lubatuse ning lubamatuse piiri ulatusest. Tähele tuleb panna ka seda, et kõikide keelatud vastumeetmete näol, mil tegemist on nö piiripealsete vastumeetmetega, on kaheldavad nende kasutamise eetilisus ning siirus.

[99] M. N. Schmitt, L. Vihul jt (koost). lk 122-123.

[100] A. Orakhelashvili. Peremptory Norms in International Law. Oxford Scholarship Online. jaanuar 2009.

Tallinna käsiraamatu eksperdid nõustusid, et vastumeetmed ei või olla kvalifitseeritavad relvastatud rünnakuteks (käsiraamatu reegel 71). Samaaegselt ei jõutud kokkuleppele, milline võib olla vastumeetme ulatus „jõu kasutamise“ lävendit ületavate vastumeetmete ning „relvastatud rünnaku“ mõiste künnise vahele jäävate vastumeetmete osas.[101] Antud seisukoht tähendab, et nii riigid kui eksperdid on väga erinevatel seisukohtadel, milline võib vastumeede rünnakule olla. Jõu kasutamise ning relvastatud rünnaku vahele jäävata meetmete võimalik ulatus on üsna lai ning seetõttu võib see tekitada päris palju probleeme.

2.7 Võimalik relvastatud sekkumine vastuseks küberrünnakule

Õigus enesekaitseks tuleneb rahvusvahelises õiguses ÜRO Harta artiklist 51, mis sätestab, et relvastatud kallaletungi puhul organisatsiooni liikmele ei piira käesolev põhikiri mingil määral võõrandamatut õigust individuaalsele või kollektiivsele enesekaitsele, kuni Julgeolekunõukogu ei võta rahvusvahelise rahu ja julgeoleku säilitamiseks vajalikke meetmeid.[102]

Tallinna käsiraamatu reegel number 71 sätestab enesekaitse reegli relvastatud rünnaku vastu. Riiki, keda on tabanud küberoperatsioon, mida saab kvalifitseerida relvastatud rünnakuks, võib kasutada oma õigust enesekaitsele. Seda, kas küberoperatsioon kvalifitseerub relvastatud rünnakuks, sõltub selle skaalast ning mõjust.[103]

Seega tuleb ka võimaliku enesekaitse kasutamiseks lähtuda jõu kasutamises käsitletud skaala ja mõju arusaamast. Asjaolu teeb keeruliseks vahetegemine jõu kasutamise ning relvastatud sekkumise vahel. Kui lähtuda Tallinna käsiraamatu küberrünnaku definitsioonist ning sellise definitsiooni loomise tagamõttest, mis on loodud eesmärgiga käsitleda sõna „rünnak“ all vaid selliseid küberrünnakuid, mis kvalifitseeruvad relvastatud rünnakuteks *jus ad bellum*’i mõistes ning tekitavad kahju inimeste tervisele või elule ning kahjustavad või hävitavad objekte ning mille vastuseks on õigus kasutada enesekaitset.[104] Antud punkti raames pole eksperdid siiski nõus, et õigus enesekaitsele on lubatud vaid selliste rünnakute korral, mis on ohuks inimeste tervisele või elule või kahjustavad või hävitavad objekte. Samuti oli eksperte, kes on seisukohal, et rünnak rahvusvahelisele aktsiaturule on kvalifitseeritav relvastatud

[101] M. N. Schmitt, L. Vihul jt (koost). lk 124-126.

[102] Ühinenud Rahvaste Organisatsiooni põhikiri ning Rahvusvahelise Kohtu statuut - RT II 1996, 24, 95

[103] M. N. Schmitt, L. Vihul jt (koost). lk 339.

[104] *Ibid.* lk 4-5.

rünnakuks. Enamik eksperdid leidsid, et ka valitsusvälise terrorirühmituse vastu võib kasutada enesekaitset.[105]

Jõu kasutamise aspekti ning enesekaitse vahetegu on äärmiselt keeruline. Kui jõu kasutamise raames leiab praegune rahvusvaheline õigus ning Tallinna käsiraamatu eksperdid, et majanduslikud ning poliitilised rünnakud ei kvalifitseeru jõu kasutamise alla, siis küberrünnaku kontekstis on siiski eksperte, kes leiavad, et rahvusvahelise aktsiaturu ründamine võiks kaasa tuua õiguse enesekaitseks, mis vajab rünnaku kvalifitseerumist mitte pelgalt jõu kasutamiseks, vaid relvastatud rünnakuks riigi vastu. Sama võib väita ka terroriakti poolt valitsusvälise terrorirühmituse poolt. Seega võib väita, et käsiraamatu ning kehtiva rahvusvahelise õiguse käsitlused jõu kasutamise ning relvastatud rünnaku vahetegemisel on üsna arusaamatud ning nendes puudub järjepidevus ja õigusselgus. Antud analüüs viib järeldusele, et praeguste seisukohtade järgi oleks teatud rünnakute kvalifitseerumine relvastatud rünnakuks kergem kui jõu kasutamiseks, mis on antud kontekstis täielikult õigusliku loogika vastane.

On üsna tõenäoline, et küberrünnakutele võib enesekaitse raames vastata ka konventsionaalselt tuntud relvastatud jõu näol. Selliseks seisukohaks annab aluse nii NATO liikmesriikide kaitseministrite koosolekul jõutud seisukoht, mida NATO on ka peasekretäri vahendusel kinnitanud. Küberrünnak võib oma olemuselt kvalifitseeruda relvastatud rünnakuks, millele liikmesriigid võivad vastata Põhja-Atlandi lepingu artikkel 5 rakendamisega.[106] Täpsemad tõlgendused, milline rünnak peaks olema, et artikkel 5 rakendataks, puuduvad. Siiski on avalikes seisukohtades öeldud, et igasugune rünnak kindlasti relvastatud rünnakuks ei kvalifitseeru.

Samalaadse seisukoha on USA kaitseministeerium välja öelnud oma käsiraamatus, avaldades toetust põhimõttele, et juhul kui küberrünnaku tagajärjed on füüsikaliselt samasugused, mida tooks kaasa endaga pommirünnak või raketirünnak, käsitletaks seda kui iga teist samasugust rünnakut.[107] Antud seisukohaga sisuliselt kinnitatakse, et küberrünnakuid, mis tekitavad

[105] M. N. Schmitt, L. Vihul jt (koost). lk 340-343.

[106] NATO Affirms that Cyber attacks may trigger collective defense obligations. American Journal of International Law. jaanuar 2015.

[107] USA Department of Defense Law of War Manual. Office of General Counsel Department of Defense. mai, 2016. Arvutivõrgus: https://www.defense.gov/Portals/1/Documents/DoD_Law_of_War_Manual-June_2015_Updated_May_2016.pdf (8 aprill 2018) lk 987-988

inimestele kehavigastusi või surma või kahjustavad või hävitavad objekte, loetakse võrdseks pommi- või raketirünnakuga, millele vastatakse ka samaväärselt, sealhulgas ei välistata kineetilise jõu kasutamist.

Kõik Tallinna käsiraamatu eksperdid leidsid, et rünnakule, mis ületab oma olemuselt relvastatud rünnaku, võib enesekaitse käigus vastata kineetilise jõu kasutamisega. Antud seisukoht on tuletatud analoogia korras olukorrast, kus kineetilist jõudu on enesekaitsena lubatud kasutada näiteks biorünnakute ja keemiarünnakute vastu.[108]

Seda, milline võib riigi õigus enesekaitsele olla, käsitleb Tallinna käsiraamat reeglite 72 ning 73 näol. Esimene nendest paneb enesekaitset teostavale riigile kohustuse, et vastus peab olema vajalik ning proportsionaalne. Rünnak peab olema vajalik selleks, et lõpetada ründava riigi rahvusvahelise õiguse rikkumine ning muud mõistlikku vahendit rünnaku lõpetamiseks pole. Proportsionaalsus peab olema vastav rünnakule, mida kannataja riik talus ning mis on vajalik selleks, et rünnak ja oht riigi julgeoleku vastu lõppeks. Reegel 73 ütleb, et õigus enesekaitsele on riigil, kes on langenud küberrünnaku alla või selleks on vahetu oht. Antud kontekstis leidsid riigid, et vahetu oht on selline, kus on arusaadav, et riik on tegemas otseseid jõupingutusi ründamiseks ning on piisav alus arvamaks, et see rünnak viiakse ka ellu.[109]

Vajalikkuse kriteerium tähendab, et see peab kvalifitseeruma nö viimaseks võimaluseks, et katkestada relvastatud rünnak riigi vastu. Samuti peab olema veendunud, et rünnak pandi toime eesmärgipäraselt ning mitte õnnetusena. Vasturünnak (enesekaitse) peab olema sellise proportsionaalsusega, et lõpetaks rünnaku, olles samal ajal vajalik ning mitte liigselt kahjustav. Proportsionaalsuse hindamise muudab küberrünnakute kontekstis keeruliseks nende kiirus ja peitlik iseloom.[110]

Viimati nimetatut iseloomustas ka Stuxneti küberrünnak, mida Iraani ametnikud ei pidanud küberrünnakuks, vaid tehniliseks veaks, saades küberrünnakust teada alles arvutitele tehnilist kontrolli sooritades. Seega on ilmselt ka tulevikus raske teha kindlaks küberrünnaku ulatus ja iseloom, kuna viirused võivad olla algselt peitliku iseloomuga, paljunedes seejärel kiiresti arvuti tarkvaras, tekitades seeläbi ka suuremat kahju, kui algselt tundus.

[108] M. N. Schmitt, L. Vihul jt (koost). lk 340

[109] *Ibid.* lk 348-353

[110] M. Roscini. Cyber Operations and the Use of Force in International Law. Oxford Scholarship Online. 2014.

Vahetust ohust rääkides ei tohiks käsitleda vahetust kui võimalust rünnanud riigile kätte maksta, vaid kasutama seda kui võimalust rünnaku tõrjumiseks. Kuigi üldiselt ollakse seisukohal, et enesekaitse peab olema vahetu iseloomuga, siis küberrünnakute kontekstis, kus rünnaku avastamiseks ning selle lokaliseerimiseks kulub rohkem aega, võiks „vahetut“ tõlgendada ehk pisut laiemalt.[111] Tuues taaskord näite Stuxneti kaasusest, siis ilmselt juhul, kui antud rünnak oleks kvalifitseerunud relvastatud rünnakuks, oleks olnud lubatav vasturünnak enesekaitse eesmärgil sooritada ka pärast paari nädala möödumist viirusega nakatumisest. Siinkohal tuleks pigem hinnata seda, millisel ajaperioodil hakkas rünnak esimesi uraani rikastamise tsentrifuuge hävitama ning mis faasis sellest teada saadi ehk kui saadi teada paari nädala möödudes nakatumisest ning rünnak kestis ning „paljunes“ sellel hetkel veel edasi, kas sellisel juhul võiks veel rääkida vahetust ohust? Autori hinnangul ilmselt võiks. Antud näide oli siinkohal illustreeriv ning on küsitav, kas Stuxneti küberrünnak kvalifitseeruks relvastatud rünnakuks või peaks antud rünnakut kvalifitseerima pigem jõu kasutamisena. Seni kuni puuduvad konkreetsed rahvusvahelised kokkulepped, tuleks praegusel hetkel küberrünnakutele kineetilise jõuga vastamise osas olla pigem ettevaatlikul seisukohal.

Vahekokkuvõte

Rahvusvahelise õiguse kohaldamise ning analüüsimise panuse osas on kahtlemata kõige suurem töö ära tehtud Tallinna käsiraamatu kontekstis. Teised nii mahukad ning põhjalikud teosed kehtiva rahvusvahelise õiguse kohaldumisest küberkontekstis puuduvad. Ometigi puudub Tallinna käsiraamatul suurem kandepind ning seega on selgusetu, kas sellised seisukohad võetakse kunagi ka rahvusvahelises õiguse osas eeskujuks.

Rahvusvahelise õiguse kohaldumine küberrünnakute osas on kahtlemata äärmiselt keeruline. Tallinna käsiraamat toonud sellisesse võimalikku tõlgendamisse oluliselt rohkem selgust, kuid jääb endiselt küsitavaks, kui reaalne on selle rakendamine praktikas. Tooksin esile, et küberrünnaku definitsioon käsitleb sisuliselt vaid selliseid olukordi, kus tagajärjeks on rünnak inimeste elule või tervisele ning objektide kahjustamine ning hävitamine. Antud seisukohta on selgitatud põhjendusega, et sõna „rünnak“ mõistetakse sõja kontseptsioonis suunatuna inimeste või objektide vastu, millele *jus ad bellumi* mõistes saab riik kasutada enesekaitse õigust. Ometigi on vastumeetmete osas lähtutud üldisest arusaamast, mille kohaselt võib

[111] M. Roscini. Cyber Operations and the Use of Force in International Law. Oxford Scholarship Online. 2014.

vastumeeteid kasutada juhul, kui rikutud on rahvusvahelise õiguse kohustusi, täpsemalt jõu kasutamist. Vastumeetmete viisid on jäetud üsna lahtiseks ning suur otsustusõigus antakse antud tõlgenduse kohaselt riigile endale, kuidas sellises situatsioonis käituda. Probleemiks on ka käsiraamatu käsitlus õigusele enesekaitseks, kus kohati on ekspertide hinnangul relvastatud rünnakuks sellised juhtumid, mida tavapäraselt ei kvalifitseerita ka jõu kasutamiseks. Selline lähenemine ei ole õiguslikult vaadates loogiline, kuna iga relvastatud rünnak peab omama vähemalt jõu kasutamise tunnuseid. Iga jõu kasutamiseks kvalifitseeritud rünnak ei pea omama aga relvastatud rünnaku tunnuseid. Seega on vastumeetmete osas veel rahvusvahelise õiguse kohaldumise tasandil palju selgusetust.

Taoline käsitlus tekitab mingil määral vastuolulise olukorra ka Tallinna käsiraamatu kui terviku osas. Kui teistes käsiraamatu osades on laia tõlgendusviisi enamasti välditud, siis vastumeetmete ning riigi enesekaitse kontekstis on lähtutud üsna laiast tõlgendusviisist. Lisaks on eksperdid olnud antud teemade kontekstis üsna erinevatel seisukohtadel, mis ongi antud laia tõlgendusviisi ning suurema selgusetuse antud teema osas kaasa toonud. Taoline käsiraamatu tõlgendus tekitab küsitavuse, kas rahvusvahelise õiguse kohaldumine küberrünnakute konteksti on üks-ühele võimalik. Tuleb nentida, et sellisteks ebamäärasteks seisukohtadeks on paljuski andnud aluse rahvusvahelise õiguse enda praktika. Näiteks õigusele enesekaitseks terrorirühmituse vastu annab aluse 9. septembri terroriakt kaksiktornide vastu ning sellele järgnenud Afganistani sõda. Seega võib öelda, et rahvusvahelise õiguse arengus omab endiselt suurt rolli see, millist praktikat riigid ise kujundavad. On küsitav, kas kogu rahvusvahelise õiguse praktikat on võimalik küberrünnakute kontekstis siiski üle võtta või vähemasti tuleks teha tööd selle nimel, et praktika käsitlused koostaksid terviku rahvusvahelise õiguse ning küberrünnakute mõistes.

3. KÜBERKONVENTSIOON

Kuigi küberrünnakuid reguleeriv ühtne konventsioon puudub, on üks küberruumi reguleeriv konventsioon 2001. aastast siiski kehtiv. Tegemist on Euroopa Nõukogu eestvedamisel loodud Budapesti arvutikuritegevusvastane konventsiooniga. Praeguseks on antud konventsiooni ratifitseerinud 56 riiki, kellest 13 on Euroopa Nõukogusse mitte kuuluvad riigid.[112]

Olgugi, et konventsiooniga liitunud riikide arv ei olegi nii väike, on konventsiooni nõrkuseks asjaolu et konventsiooni ei ole ratifitseerinud mitmed küberruumi kujundavad riigid, ei Hiina ega Venemaa. Lõplikku versiooni ei ole allkirjastanud ka Brasiilia ja India.

Kuna konventsioon on keskendunud küberkuritegevusele, siis antud konventsioon ei reguleeri täpsemalt riikidepoolseid küberrünnakuid. Murelikuks teeb asjaolu, et seitsmeteistkümne aasta möödudes on huvi konventsiooni vastu küll jätkuvalt olemas, kuid ratifitseerinute arv ei ole oluliselt suurenenud. Ometigi oli antud konventsioon edasiminek just rahvusvahelise koostöö poolest küberkuritegevuse raames ning riikidevahelise menetluse mõttes, millega kaasnes ka teatav seaduste ühtlustumine riikide küberruumides.

Eelnevast lähtuvalt on selge, et ka konventsioon küberrünnakute valdkonnas ei pruugi lahendada koheselt kõiki kübermaailmas ning küberrünnakute kontekstis olevaid probleeme. Ometigi on mitmeid argumente, mis toetaksid konventsiooni loomist küberrünnakute kontekstis.

3.1 Konventsiooni loomine

Peamiseks probleemiks konventsiooni loomisel on vastuseis poliitilisel tasandil, täpsemalt puudub poliitiline tahe ning valitseb usaldusmatus rahvusvahelise kogukonna seas. Küberkonventsiooni kasuks räägib võimalus sõnastada terminid konkreetselt ning anda tehnilisel tasandil täpsemaid kirjeldusi ning lahendusi küberrünnakute kontekstis.

[112] Council of Europe. Convention on Cybercrime. Chart of Signatures and ratifications of Treaty 185. Status as of 30.03.2018. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=LwUpff4y (30.03.2018)

Võimalik, et rahvusvahelise õiguse kohaldamine küberrünnakute kontekstis on hetkelises olukorras parim lahendus, kuna poliitiline tahe enamaks puudub. *Soft law* peamiseks eeliseks peetaksegi just asjaolu, et reguleeritus kasvõi nõrgemal tasandil, on parem kui täielik reguleerimatus ning kokkulepete puudumine.[113] Sellele, et täpsemate kokkulepeteni viimine on äärmiselt keeruline protsess, viitab ka viimane ÜRO kübervaldkonna ekspertgrupi koosviibimine, kus definitsioonide sõnastamiseni ning rahvusvahelise õiguse normide rakendamiseni küberruumis ei jõutud. Kas pikas plaanis on rahvusvahelise õiguse kohaldumine küberrünnakute kontekstis hea lahendus, seda on praegusel hetkel raske öelda. Põhjus on lihtne, rahvusvahelist õigust küberrünnakute kontekstis ei ole kordagi rakendatud ning kuidas seda kohtutasandil teha ning kui reaalne ja teostatav saab see praktikas olema, on endiselt ebaselge. Tegelikkuses on ju küsitavaid kaasuseid praktikas ka esinenud, kuid rahvusvahelise kogukonnal on senimaani puudunud tahe ning valmisolek antud teemat sellisel tasandil arutleda.

Tallinna käsiraamatut ning rahvusvahelise õiguse kohaldumist selle valguses on kritiseeritud, kui olles liiga kitsa ringi riikide pool tunnustatud, täpsemalt riikide poolt, kes Tallinna käsiraamatu väljaandmist toetasid. Mis tähendab, et Tallinna käsiraamatus välja toodud seisukohad ei ole leidnud üldist tunnustamist riikide poolt. Samuti seatakse kahtluse alla rahvusvahelise õiguse tunnustamise küberrünnakute kontekstis, viimase ÜRO ekspertgrupi nõukogu koosviibimise valguses. Samuti valitseb skepsis praktika kujunemise osas küberrünnakute kontekstis praeguse rahvusvahelise õiguse alusel.[114]

Rahvusvahelise õiguse kohaldumise näol peaksime olema olukorras, kus küberrünnakute korraldamise eest saab võtta riiki vastutusele ning potentsiaalselt võtta kasutusele ka vastumeetmed. Kuna praktikas ei ole ühtegi sellist juhtumit olnud, on eelnevalt mainitud skepsisel ka teatud alus. Nagu eelnevalt mainitud, on esinenud teatavaid kaasuseid, kus võiks tekkida põhjendatud ootus konkreetsete küberrünnakute või küberoperatsioonide aruteluks ÜRO julgeolekunõukogus. Sellisel tasemel aga arutelud praegusel hetkel puuduvad. Juhul kui julgeolekunõukogu võtaks sellise kaasuse arutelule, annaks see kindlasti esimesed vihjed, kuidas riigid ise taolist käitumist lahendada proovivad ning kuidas võiks küberrünnakuid rahvusvahelises õiguses käsitleda.

[113] J. Klabbers. The Concept of Treaty in International Law. Developments in International Law. 1996. Springer.

[114] M. Eilstrup-Sangiovanni. Why the World Needs an International Cyberwar Convention. 18. juuni 2017. Arvutivõrgus: https://link.springer.com/content/pdf/10.1007%2Fs13347-017-0271-5.pdf (8 aprill 2018)

Praegune olukord viitab autori arvates selgelt sellele, et rahvusvahelise õiguse rakendamine kehtiva õiguse alusel on väga keeruline. Taolises olukorras on ehk liigselt entusiastlik loota ka rahvusvahelist õigust kujundavale praktikale. Teisalt on tegemist suletud ringiga, kui puuduvad kaasused, mida rahvusvaheline üldsus oleks huvitatud küberrünnakute kontekstis arutama, ei saa tekkida ka rahvusvahelist õigust kujundavat praktikat. Olukord tõstatab õigustatud küsimuse. Mis garanteerib selle, et järgmine rünnak, mida saaks käsitleda rahvusvahelise õiguse raames küberrünnakuks, selleks ka kvalifitseerub ning võimaldab tuua kaasa rahvusvahelise õiguse alusel lubatud sanktsioonid? Praegusel hetkel puudub tegelikkuses kindlus, et rahvusvahelist õigust küberrünnakute kontekstis aktsepteeritakse, samuti puuduvad konventsioonid, mis käsitleks küberrünnakuid.

Selleks, et luua küberkonventsioon, on määrava tähtsusega riikide endi soov luua rahvusvahelist õigust kujundav konventsioon, mis oleks poolte jaoks ka õiguslikult siduv. Siinkohal on oluline välja tuua, et konventsioonil pole konkreetseid tunnuseid või kindlat vormi.[115] Eelnevalt nimetatu viitab asjaolule, et riikidele ei tehta ettekirjutusi, kuidas konventsiooni luua, vaid tegemist on vaba protsessiga. Pole ka ettekirjutust, milline peaks täpne konventsiooni sõnastuse kujundamise protsess välja nägema. Küll aga on oluline, et konventsiooni loomise protsessis lööks kaasa riigi esindaja, kellel on selleks riigi poolne selge esindusõigus.[116] Olulised faasid konventsiooni loomisel on selle lõplikule sõnastusele nõusoleku andmine kahe kolmandiku riikide poolt, kes on ka konventsiooni kujundamisel ise kaasa löönud. Samuti on oluline konventsiooni koostamises kaasa löönud riigi esindaja allkiri, mis kinnitab, et antud seisukohad on riigi jaoks vastuvõetavad. Viimase sammuna toimub konventsiooni ratifitseerimine riigi seadusandliku võimu poolt, mille järel konventsioon jõustub.[117] Konventsiooniga on võimalik liituda hilisemas faasis ka siis, kui konventsiooni väljatöötamises pole osaletud. Sellisel juhul nõustub ning annab konventsioonile heakskiidu, ratifitseerides ning aktsepteerides välja töötatud konventsiooni.[118] Seega on teoreetiliselt võimalik konventsioon luua ka kitsa ringi riikide poolt, kes on konventsiooni eesmärkide ning sõnastuse osas sarnastel seisukohtadel, kutsudes hiljem teisi riike antud konventsiooniga liituma. Antud käsitlus pole aga praktikas perspektiivikas, kuna konventsioon ei ole

[115] M. D. Evans (koost), Malgosia Fitzmaurice. The Practical Working of the Law of Treaties. International Law. Oxford University Press. 2003. lk 174

[116] J. Crawford (koost). Brownlie's Principles of Public International Law (8th edn). Oxford University Press. 2012. lk 371-373.

[117] M. N. Shaw. International Law. Cambridge University Press. 2008. Lk 909-912.

[118] J. Crawford (koost). lk 374.

kolmandatele riikidele siduv ning toetuse leidmine kitsa ringi poolt koostatud konventsioonile on äärmiselt keeruline.

Lähtudes autori poolt välja pakutavast küberkonventsiooni loomise võimalusest, kus konventsiooni kavandi kujundab välja Rahvusvahelise Õiguse Komisjon, on vajalik komisjoni vastav ettepanek ÜRO peaassambleele Rahvusvahelise Õiguse Komisjoni statuudi artikli 18(2) alusel.[119] Seejärel valmistab komisjon ette omapoolse kavandi vastavalt statuudi artiklile 20, mis sätestab, et komisjon peab töötama välja konventsiooni artiklid ning saatma need omapoolsete kommentaaridega ÜRO peaassambleele.[120] Komisjonil on võimalik oma töösse kaasata ka eksperte ning teadlasi, samuti on võimalik küsida riikide seisukohti vastavalt statuudi artiklile 21 lõigetele 1 ja 2.[121] Rahvusvahelise Õiguse Komisjon saadab oma lõpliku konventsiooni versiooni ÜRO peasekretäri kaudu ÜRO peaassambleesse vastavalt Rahvusvahelise Õiguse Komisjoni statuudi artiklile 22.[122] Seejärel on ÜRO peaassambleel võimalus konventsioon vastu võtta või pakkuda välja omakorda muudatusi, mida Rahvusvahelise Õiguse Komisjon võiks sisse viia. Seega on Rahvusvahelise Õiguse Komisjoni kaudu võimalik Küberkonventsiooni luua. Seda nii teoreetiliselt kui ka praktikas. Autori hinnangul oleks selline lahendus, kus küberkonventsiooni arutatakse eelkõige õiguslikul tasandil ning ÜRO vahendusel parem lahendus, kui see, et konventsioon loodaks ühe kitsa ringi riikide poolt.

3.2 Küberkonventsiooni sisu

Küberkonventsiooni vajadus seisneb eelkõige just õigusselguse huvides. Küberkonventsiooni üheks oluliseks rolliks peab olema tulevikus kübersfääris kasutatavate definitsioonide kokku leppimine. Lähtudes seisukohast, et tulevane küberkonventsiooni loomine algatatakse Rahvusvahelise Õiguse Komisjoni poolt, on sellise protsessi käigus definitsioonide kooskõlastamine kindlasti tõenäolisem, kuna poliitiline faktor ei tohiks komisjoni töös nii suurt rolli mängida, kui riikidevahelise eestvedamise käigus loodud konventsiooni korral. Ometigi on definitsioonides kokku leppimine oluline just probleemide üheses mõistmises.

[119] Statute of the International Law Commission. 1947. Arvutivõrgus: http://legal.un.org/ilc/texts/instruments/english/statute/statute.pdf (22 aprill 2018)

[120] *Ibid.*

[121] *Ibid.*

[122] *Ibid.*

Esimeses peatükis autori poolt analüüsitud situatsioon, mis viitas küberrünnakute osas konkreetse definitsiooni puudumisele ning riikide erinevaid käsitlusi, mida kvalifitseerida küberrünnakutena, peab leidma küberkonventsioonis lahenduse. Situatsioon, kus küberrünnak on defineeritud küll üheselt, kuid hiljem analüüsi käigus selgus, et konkreetsetes situatsioonides eksperdid sellega siiski ei nõustunud, tuli välja just Tallinna käsiraamatu puhul, kus enesekaitse õiguse kasutamise raames oleksid paljud eksperdid küberrünnaku mõistet siiski laiendanud selleks, et riikidel oleks antud olukordades õigus enesekaitseks. Selline situatsioon tekitab rahvusvahelise õiguse seisukohast pigem rohkem segadust kui selgust. Olukord, kus puudub konkreetne küberrünnakute definitsioon, teeb mingil määral ka selle eest vastutusele võtmise keerulisemaks, kuna riikidel endil puudub ühtne ja konkreetne arusaam lubatust ning lubamatust. Autori hinnangul võiks küberrünnaku definitsioon hõlmata endas ka jõu kasutamist puudutavat. See looks autori hinnangul ühtse käsitluse terminist küberrünnak ning konkretiseeriks oluliselt küberruumi terminoloogiat. Selline lahendus looks ühtsema seisukoha küberrünnakutest, luues samaaegselt ka süsteemsema käsitluse.

Küberkonventsioonis peaksid kindlasti olema täpselt reglementeeritud küberrünnakute omistamise võimalused riigile ning see, milliste küberoperatsioonide/küberrünnakute näol on tegemist jõu kasutamisega. Küberrünnakute kvalifitseerumiseks oleks ehk mõistlik luua küberrünnakute mõistes mitmetasandilised käsitlused. Näiteks 1. tasandi küberrünnakud kattuks Tallinna käsiraamatu mõistega küberrünnakutest. Autori hinnangul oleks mõistlik tasandite loomine selleks, et oleks õiguskindlus, millised küberrünnakud mis kategooriatesse kuuluvad ning millised on erinevate tasandite küberrünnakute tagajärjed (sh rahvusvahelise õiguse mõistes) 2. tasandi küberrünnak võiks kattuda jõu kasutamise mõistega jne. Seega toimuks kaasuse nn lahendamisel objektiivne hindamine, millisesse küberrünnaku kategooriasse rünnak kuulub ning lähtuvalt antud objektiivsest hinnangust ning rünnaku kategooriast oleneb, millised on riigi võimalused küberrünnakule vastamiseks ehk vastumeetmeteks.

Siinkohal toob töö autor välja, et toetab ka küberkonventsiooni kontekstis tõlgendamist, mida praegune rahvusvaheliselt kehtiv õigus ei toeta ehk küberrünnak (jõu kasutamine), mis on toime pandud riigi peamise tööstuse ja majandusliku ressursi vastu, tekitades majandusele olulist kahju ning ka poliitilise vabaduse ohtu seadmine peaks kvalifitseeruma autori hinnangul välja toodud käsitluse järgi 2. tasandi küberrünnakuks ehk praeguse mõiste alusel jõu kasutamiseks. Autor rõhutab, et ei toeta nn Shanghai koostööorganisatsiooni riikide kontseptsiooni, mis räägib samuti põgusalt poliitilisest mõjutamisest, rääkides samal ajal

täiesti erinevatest arusaamadest küberrünnaku kontekstis. Autor jagab oma arusaama pigem kontseptsiooniga, mida on välja pakkunud ka näiteks Avra Constantinau ning mida autor on varasemalt oma töös peatükis 2.4 ning 2.4.1 analüüsinud.

Tallinna käsiraamatu üheks nõrgimaks osaks võiks nimetada ehk vastumeetmete ning riigi enesekaitseõiguse osa, mida autor on käsitlenud teises peatükis. Antud osas tuleb välja ka küberrünnakute kohaldamise keerukus ning mitmetahulisus rahvusvahelise õiguse kontekstis. Kui rahvusvahelise õiguse eksperdid, kes on ühel meelel rahvusvahelise õiguse otsekohaldumise pooldamisel küberrünnakute kontekstis, jäävad sisulistes seisukohtades antud küsimuses üsna suurele erimeelsusele, siis on konsensuse leidmine veel raskem olukorras, kus mängu tulevad poliitika ning erinevad seisukohad ka põhiterminites. Leian, et vastumeetmete ulatus tuleks määrata kindlaks konkreetsemalt ning küberkonventsioonis võiks seda teha näiteks autori poolt eelnevalt mainitud küberrünnakute kategoriseerimise näol. Loomulikult peab riikidele jääma võimalus erinevates olukordades rakendada erinevaid vastumeetmeid, sest vastumeetmete kasutamine sõltub paljuski sellest, milline oli konkreetne rünnak ning milline vastumeede on sobilik just selle rünnaku lõpetamiseks. See on ka üks põhjustest, miks ei saa vastumeetmete võimalused liiga kindlalt raamidesse suruda. Näiteks ei ole alati võimalik küberrünnaku vastumeetmena kasutada küberrünnakut, on olemas nii teoreetiline kui reaalne võimalus, et küberrünnaku tagajärjel puudub kannatada saanud riigil võimalus oma kübervaldkonnaga seotud infrastruktuuri kasutada (sh näiteks võrguteenuseid) ning seega on üheks võimaluseks vastumeetmena kineetilise jõu kasutamine. Teisalt on selge, et iga küberrünnaku vastu ei saa kasutada kineetilist jõudu, seega on äärmiselt oluline, et vastumeetmete ulatus oleks konkreetsemalt kindlaks määratud, et vältida olukorda, kus küberrünnakute jaoks kasutatud vastumeetmete kasutamise käigus on oht konflikti eskaleerumiseks, mitte pooltevahelise lahenduse leidmiseks.

Küberkonventsiooni raames oleks vajalik luua ka reaalne ning praktikas tõhusam majanduse ning ettevõtjate kaitse küberrünnakute kontekstis. Praegusel hetkel on ettevõtjad ühed suurimad küberrünnakute ohvrid ning autori hinnangul ei võeta küberrünnakuid ettevõtete ning firmade vastu piisavalt tõsiselt ning asja vaadeldakse justkui paratamatust, kus ettevõtjad peavad iseseisvalt looma võimekuse oma infrastruktuuri kaitsmiseks. Kindlasti ei saa ka küberkaitse tehnilist poolt tähelepanuta jätta, kuid teisalt puudub kõikidel firmadel põhjalikuks küberkaitse süsteemi loomiseks raha. Arvates, et väiksemaid firmasid ei rünnata või neil puudub olulisus suuremas plaanis riigi julgeolekusse, on autori hinnangul lühinägelik. WannaCry rünnak, mis haavas mitmeid firmasid ning tegi kahju ka Eesti tervishoiusüsteemile

oli praegusel hetkel veel pelgalt hoiatus sellest, kui haavatavaks võib muutuda riik küberruumis ning seda palju laiemalt, kui vaid sõjalises kontseptsioonis. Teadmata detailselt kui heal tasemel ning turvaline on eesti kübervõimekus e-tervise ning digiloo valdkonnas, võib näiteks WannaCry sarnane info blokeerimine ja krüpteerimine tuua kaasa olukorra, kus inimesele võib olla keeruline anda erakorralise meditsiini näol abi, kuna puudub eelnev teave haigusloost. Tegemist on kindlasti pigem äärmiselt teoreetilise väljapakutud kontseptsiooniga, kuid hoiatuseks selle teoreetilisest võimalusest saab välja tuua ka antud töös mainitud juhtumit, kus Eesti tervishoiuteenuse pakkujad pidid lunavara kätte saamiseks küberkurjategijatele tasu maksma. Seega võib väita, et ka pahavara ning lunavara rünnakud on äärmiselt tõsised juhul, kui need tabavad süsteemi nõrkuseid, eriti olukorras, kus riigid sõltuvad üha enam olulistest andmebaasidest, mida hoitakse pilveteenustes ning teistes analoogsetes küberruumi pakutavates võimalustes.

Üheks olulisemaks aspektiks küberrünnakute avastamisel on tõhusam riikidevaheline koostöö. *Computer emergency response team - CERT*'ide[123] suurema koostöö vajadus on välja toodud nii ÜRO küberekspertide nõukogus. Samamoodi on Eesti järjekindlalt antud seisukohta toetanud.[124] Autor nõustub täielikult koostöö suurendamise vajadusega ning autori hinnangul oleks küberkonventsiooni raames vajalik asutada ÜRO juurde kuuluv Rahvusvaheline küberrünnakute keskus (Sisuliselt rahvusvaheline *CERT*), mis tegeleks eranditult küberrünnakute allikate kindlaks tegemise ning rünnakute omistamisega. Argument, miks rahvusvahelise küberrünnakute keskuse loomine oleks vajalik, on eelkõige seotud tehnilise, finantsilise ning inimressursside võimekuse parandamise tõttu. Praegusel hetkel puudub enamikel riikidest reaalne võimekus rünnaku täpseks tuvastamiseks.[125] Taoline keskus motiveeriks riike ka konventsiooniga liituma, kuna pikas perspektiivis oleks taolisesse organisatsiooni panustamine oluliselt soodsam, kui olukord, kus igal riigil on endal taoline keskus. Infosüsteemiametid ning *CERT*-id oleksid riikidel jätkuvalt olemas, kuid nende esmaülesandeks oleks tegeleda eelkõige riigi turvasüsteemide parandamise ning arendamisega

[123] CERT viitab organisatsioonile, kes tegeleb turvaintsidentidega CERT tegevuse raamistikus. CERT organisatsioone eksisteerib üle maailma ja nad on omavahel tihedas koostöös, jagades informatsiooni infoturbeintsidentide kohta ja teavitades turvaohtudest. Selgitus RIA kodulehelt. Arvutivõrgus: https://www.ria.ee/ee/cert.html (14 märts 2018)

[124] M. Kaljurand. United Nations Group of Governmental Experts: The Estonian Perspective. International Cyber Norms: Legal, Policy & Industry Perspectives, NATO CCD COE Publications. 2016 Arvutivõrgus: https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_Ch6.pdf (14 märts 2018)

[125] M. Eilstrup-Sangiovanni. lk 16-17

ja seetõttu ei peaks antud ametid tegelema niivõrd suures mahus kübervaldkonna kriminalistikaga.

Samuti oleks vajadus küberrünnakutele spetsialiseeruva kohtu järele. Autori hinnangul ei ole olukord, kus riik peab ennast ise Rahvusvahelisele kohtule allutama küberrünnakute kontekstis jätkusuutlik. Rahvusvahelise õiguse maksmapanemiseks ei ole kohus küll ainsaks vahendiks, ometigi tundub enamike küberrünnakute lahendamine mõistlik just kohtu vahendusel. Usun, et sellisel moel oleks võimalik minimaliseerida ka küberrünnakute kontekstis kitsaskohaks olevate vasturünnakute kasutamist ning konfliktide eskaleerumist. Autor ei kahtle Rahvusvahelise Kohtu kohtunike pädevuses, ometigi tuleb arvestada, et küberrünnakud on oma olemuselt üsna spetsiifilised. Viimati nimetatud probleemi saaks lahendada ka Rahvusvahelise Küberkaitsekeskuse ning Rahvusvahelise Kohtu tiheda koostöö läbi, mis looks ühest küljest küll võimekuse, kuid teisalt võib seada kahtluse alla kohtumõistmise erapooletuse ning sõltumatuse. Ometigi oleks võimalik nende kahe asutuse koostöö ulatus kokku leppida.

Olles realist, on küberkonventsiooni jaoks hetkeline rahvusvahelise poliitiline maastik üsna killustunud ning kokkulepete sõlmimine äärmiselt keeruline. Teisalt ei ole lahendus ka praegune olukord, kus puudub täielik kindlus, kas ja kuidas on küberruum reguleeritud. Ilmselt on riikide huvi leida kompromisse seda suurem, mida suuremaks muutub oht riikidele endile. Ajalugu on näidanud, et riikidevahelised kokkulepped ning konsensus sünnivad kahjuks hõlpsamini pärast seda, kui praktikas on toimunud esimene reaalne konflikt ning kitsaskohad on esile kerkinud ka praktikast.

Vahekokkuvõte

Küberkonventsiooni loomine on protsess, mis nõuab aega ning kindlasti ei täida konventsiooni eesmärki olukord, kus luuakse konventsioon, mis ei suuda reaalsuses lahendada praktikas asetsevaid probleeme ning ei rahulda enamike riikide seisukohti küberrünnakute osas. Konventsioonil saab olla mõtet vaid siis, kui selle näol on võimalik tõesti luua rahvusvahelisse õigusesse rohkem selgust. Vastasel juhul on mõistlik leppida kokku kehtiva rahvusvahelise õiguse normid küberrünnakute kontekstis. Kui suudetakse kokku leppida vähemalt kehtiva rahvusvahelise õiguse kohaldumises, oleks vajaduse korral võimalik selle pinnalt luua tulevikus ka konventsioon, mis küberruumi ühtselt reguleeriks.

Isegi kui küberkonventsiooni vastu jääb riikide poolne huvi leigeks, leian, et antud peatükis pakutud ideid võiks kasutada ka juhul, kui rahvusvahelise õiguse pinnalt luuakse normid, mis reguleerivad küberruumi. Näiteks oleks autori hinnangul võimalik Rahvusvahelise küberkeskuse loomine ka sellisel juhul, kui konventsioonis kokku leppida ei suudeta. Samuti oleks võimalik Rahvusvahelise Kohtu juurde loodava erikohtu loomine küberrünnakutega seotud kaasuste lahendamiseks. Mõlema institutsiooni loomiseks on vajalik nii ÜRO kui ka ÜRO liikmesriikide heakskiit ning üldine ja laiem huvi selliste institutsioonide loomiseks.

Praeguste rahvusvaheliste suhete tasandil on keeruline ette kujutada konventsiooni küberünnakute kontekstis, mis rahvusvahelise õiguse praktikas oma eesmärki täidaks. Seda põhjusel, et isegi kui konventsioon loodaks, puuduks sellel suure tõenäosusega vajalik laiapinnalisus, kus konventsiooniga liituks ning konventsiooni aktsepteeriks enamik kübersfääri kujundavatest suurriikidest. Näiteks juhul, kui konventsiooni looks nn lääneriigid ja samameelsed, on vähetõenäoline, et sellele leitaks toetus Shanghai organisatsiooni liikmesriikide poolt ning vastupidi. Selline konventsioon tähendaks aga, et praktikas sellest palju kasu ei oleks, kuna konventsioon on siduv vaid riikidele, kes selle on allkirjastanud.[126] Rahvusvaheline tavaõiguse eeliseks on aga see, et tava saab olla praktikas siduv ka riikide jaoks, kes nö rahvusvahelise tava kujundamises pole ise konkreetselt kaasa löönud. Oluline on see, et nimetatud tava oleks praktikas suure enamuse riikide poolt aktsepteeritud käitumine.[127] Seega räägib rahvusvaheline olukord praegu selgelt rahvusvahelise õiguse otsekohaldumise kasuks. Ometigi võivad praktikas tekkivad probleemid rahvusvahelise õiguse kohaldumise kontekstis tuua kaasa vajaduse reguleerida küberrünnakute kontekst spetsiifilisemate reeglite alusel kui praegune kehtiv õigus seda võimaldab. Autor on seisukohal, et juhul kui konventsiooni loomiseks peaks tekkima suurema osa riikide heakskiit, oleks seda mõistlik teha Rahvusvahelise Õiguse Komisjoni vahendusel. Usun, et sellisel juhul on kokkulepete sõlmimine märkimisväärselt reaalsem, kui juhul, kui riigid proovivad konventsiooni loomist iseseisvalt algatada.

[126] M. D. Evans (koost), Hugh Thirlway. lk 121-123

[127] *Ibid*. lk 124-125.

KOKKUVÕTE

Magistritöö eesmärgiks on välja selgitada, millised on võimalikud vajalikud sammud, tagamaks rahvusvahelise õiguse muutumine küberrünnakute kontekstis praktikas kohaldatavaks. Sellega seoses oli käesoleva töö uurimisküsimuseks, kas praegune olukord, kus rahvusvaheline õigus reguleerib küberruumi küberrünnakute kontekstis, on praktikas kohaldatav. Kui jätkusuutlik on praegune olukord ning kas lahendus võiks olla küberkonventsioon, mis reguleeriks küberruumi just küberrünnakute osas.

Küberrünnakute ühtse definitsiooni puudumine on üks rahvusvahelise õiguse tasandil olevatest probleemidest küberrünnakute kontekstis. See tähendab, et küberrünnaku näol toimuvaid rünnakuid hinnatakse ning käsitletakse erineval tasandil. Riigid ei pruugi mõista küberrünnaku tõsisust ning raskusastet, mis antud teema käsitlemisel on äärmiselt oluline, kuna riikidepoolse ühtse hukkamõistuta, ei ole võimalik olukorda lahendada. Lisaks erinevatele küberrünnaku mõistete tõlgendamistele, on ka riigid, kes mõistavad kogu küberrünnaku konteksti täielikult erineval tasandil. Kui Lääneriigid ning nendega samameelsed mõistavad küberrünnakuid kui puhtalt tehnilisel tasandil olevaid rünnakuid, siis Shanghai koostööorganisatsiooni kuuluvad riigid räägivad informatsioonirünnakutest, mis hõlmavad endas lisaks tehnilisele tasandile ka sotsiaalset tasandit, mille hulka kuulub näiteks mõjutamine. See tähendab, et need kaks osapoolt mõistavad probleemi täiesti erinevalt ning räägivad ka mõistete kontekstis totaalselt erinevatest asjadest.

Üks töös tõstatunud küsimustest küberrünnakute kontekstis on, kas rahvusvaheline õigus kohaldub ka küberrünnakute kontekstis. ÜRO liikmesriigid on kaks korda kinnitanud ÜRO küberekspertide nõukogu ettepanekut, et kehtiv rahvusvaheline õigus laieneb ka küberruumi. Siiski on praegusel hetkel küsitav, kas sellised ÜRO liikmesriikide seisukohad on muutnud selle rahvusvahelise tavaõiguse osaks ning riigid on tunnustanud seda justkui käitumist, mida kõik riigid aktsepteerivad ning tavaks peavad. Kuigi lääneriigid on sellele tuginenud, ei saa autori hinnangul seda täieliku veendumusena väita, et taoline praktika on muutunud rahvusvahelise õiguse tavaks. Antud seisukohta murendab viimane ÜRO küberekspertide nõukogu seisukoht, kus samu seisukohti enam ei tunnustatud ja üle ei korratud. See ei tähenda automaatselt välistatust, et rahvusvaheline õigus ei võiks küberrünnakute kontekstis hetkel kehtida, kuid autori hinnangul vajab see siiski ka rahvusvahelises praktikas suuremat kandepinda ning tunnustamist, et see nii oleks. Vajalikud oleks riikide seisukohad

konkreetsete küberrünnakute kontekstis ÜRO julgeolekunõukogus või koguni Rahvusvahelise Kohtu lahendid ja seisukohad.

Selgust võiks luua ka töös mainitud Rahvusvahelise Õiguse Komisjoni poolne teemaga tegelemine. Usun, et sellisel tasemel teemaga tegelemine võiks anda rahvusvahelise õiguse kohaldumise kohta kindlamaid seisukohti kui pelk õigusteadlaste arutelu. ÜRO küberekspertide nõukogu, mis viis kindlasti antud valdkonna arutelu uuele tasandile on mingil määral ammendunud ning seda just poliitiliste seisukohtade taha, mis antud nõukogu tööd oluliselt mõjutasid, seda just viimaste nõukogu koosseisude töös.

Teiseks suureks probleemiks rahvusvahelises õiguses seonduvalt küberrünnakutega on selle rakendamine juhul, kui praegu kehtiv rahvusvaheline õigus on otsekohalduv küberrünnakute kontekstis. Lisaks sellele, et puudub täielik kindlus, kas rahvusvaheline õigus rakendub, on küsimus, kui edukalt ning kuidas seda rakendama ning tõlgendama peaks? Praegusel hetkel puuduvad riikidevahelised kokkulepped ka selles osas, kuidas rahvusvahelist õigust küberrünnakute kontekstis rakendada. Siinkohal on autori hinnangul peamisteks variantideks eelnevalt nimetatud Rahvusvahelise Õiguse Komisjoni poolne töö rahvusvahelise õiguse kujundamisel näiteks Tallinna käsiraamatu abil või leida Tallinna käsiraamatule laiem rahvusvaheline tunnustus, mis on äärmiselt keeruline, kuid võib viia ka potentsiaalselt kõige otsesemate ning kiiremate lahendusteni. Tallinna käsiraamatus on endiselt ka teatud küsitavusi, millele autor on eelnevalt oma töös tähelepanu pööranud näiteks vastumeetmete kasutamise ulatus.

Kindlasti on üks asjaolu, mis raskendab kehtiva õiguse kohaldamist praktika puudus. Leian, et kõiki kehtiva rahvusvahelise õiguse tavasid ei saa küberruumis küberrünnakute kontekstis rakendada. Küberrünnakud on siiski piisavalt spetsiifilised, et erineda konventsionaalsetest rünnakutest, samuti on küberrünnakute näol tegemist üheaegselt nii pehmema mõjuga rünnakust (demokraatia ning poliitika mõjutamine ning majanduse halvamine) kui ka potentsiaalselt väga raskete mõjudega rünnakust (rünnakud, mis hävitavad objekte või nõuavad inimelusid). Ometigi peaks Tallinna käsiraamatu näol kaaluma tõsiselt seda, et olles praegusel hetkel ainulaadne teos just selle põhjalikkuse tõttu küberruumi ning küberrünnakute kontekstis, peaks Tallinna käsiraamatut käsitlema kui baasmaterjali rahvusvahelise õiguse normide välja töötamise protsessis ning õiguse kohaldamisel.

Võimalikul küberkonventsiooni loomisel on omad eelised ning puudused. Autori hinnangul on küberkonventsiooni eeliseks selle konkreetsus ning täpsus. See annab küberrünnakute spetsiifilisuse tõttu konventsioonile rahvusvahelise õiguse rakendamisel eelise nn *soft law* ees. Võimalik, et seda isegi juhul, kui lepitakse kokku kehtiva rahvusvahelise õiguse tõlgendamise osas. Praegusel juhul jääb küsimus õhku, kui reaalne on praktikas kehtiva rahvusvahelise õiguse kohaldamine küberrünnakute kontekstis. Samuti on mingil määral ootus, milline kaasus oleks rahvusvahelise kogukonna hinnangul piisavalt tõsine, et kaalutakse selle arutamist näiteks ÜRO julgeolekunõukogus, mis tooks selguse, kas kehtivat rahvusvahelist õigust aktsepteeritakse rahvusvahelisel tasandil või mitte või oleks vajalik siiski küberkonventsiooni olemasolu? Üks piiripealsetest kaasustest on näiteks töös mainitud väidetavalt USA ning Iisraeli poolt läbi viidud Stuxneti nimelise pahavaraga rünnak Iraani tuumareaktorite vastu, mis toimus küll enne 2013. aastal ÜRO liikmesriikide poolt kujundatud seisukohta, et kehtiv rahvusvaheline õigus kohaldub küberruumis. Siiski oleks juba siis oodanud riikide poolt teatud reaktsiooni ehk kõrgemal tasandil. Seni kuni puuduvad kehtiva rahvusvahelise õiguse tõlgendusnormid ning praktika, annaks konventsioon kindlasti ka selgemad tegevuspiirid riikide tegevuseks küberruumis. Küberkonventsiooni peamine puudus seisneb selle kokkuleppimise keerukuses ning asjaolus, et riigid mõistavad küberruumi ning küberrünnakutega seonduvat diametraalselt erinevalt. See muudab ühisosa leidmise äärmiselt keeruliseks ning seetõttu ei pruugi loodav konventsioon lahendada praktikas valitsevaid probleeme, kuna asjaoludes, mille järgi on vajadus kokkuleppeks, ei leita laiapõhjalist toetust ning konsensust. Välja on toodud ka asjaolu, et konventsioon piirab ühiskonna ning tehnoloogia innovaatilist arengut. Autor nõustub teatud määral küll antud argumendiga, kuid leiab, et see ei ole kindlasti ületamatuks probleemiks, mis välistaks küberkonventsiooni loomise. Oht jäämaks innovatsioonile jalgu oleneb paljuski konventsiooni sõnastusest ning sellest, kuidas konventsiooni soovitakse tõlgendada.

Küberrünnakute avastamisel ning uurimisel omab olulist rolli riikidevaheline koostöö. Rahvusvaheline kommuun peab seisma oluliselt rohkem riikide eest, kellel puudub küberrünnakute tõrjumiseks tehniline võimekus või ressurss, sealhulgas inimressurss. Praegusel hetkel ei ole paljud riigid küberrünnakute ennetamiseks ning toime tulemiseks piisavalt valmistunud. Samuti puudub paljudel neist ka võimekus küberrünnaku allika kindlakstegemiseks ning ka rünnaku tõrjumiseks. Seetõttu on hädavajalik riikide suurem koostöö. Leian, et just tehnilise võimekuse olemasolust sõltub paljuski see, kas küberrünnakute allikaid on võimalik kindlaks teha või mitte ning kas rahvusvahelist õigust saab rakendada ning riiki vastutusele võtta. Nagu näha töö raames lahendatud Stuxneti

abiskeemist, on raske öelda, millised peavad olema kaudsed asjaolud, mis viitavad küberrünnaku läbi viimisele ning millisel juhul ollakse selliste asjaolude esinemise korral seisukohal, et küberrünnaku taga on konkreetne riik. Seetõttu on oluline, et oleks ka konkreetsemaid tõendeid küberrünnaku läbi viimiseks, et objektiivsete faktide näol oleks võimalik küberrünnaku läbi viijad kindlaks määrata.

Autor pakkus oma töös välja ühe koostöö edendamise lahendusena ÜRO juurde Rahvusvahelise küberkeskuse loomise, mis tagaks kiirema ning tõhusama küberrünnakute uurimisprotsessi. Kaaluma peaks ka Rahvusvahelise erikohtu loomist küberrünnakute jaoks. Praegusel juhul ei ole rahvusvahelisel tasandil küberrünnakutega seonduvaid kaasuseid Rahvusvahelisel Kohtul lahendada tulnud, kuid probleem võib tekkida riikide vähesest huvist allutada ennast kohtulikule uurimisele. Antud kontekstis soovib autor välja tuua ka asjaolu, et riigid peaksid rahvusvahelisel tasandil leppima kokku ka oluliselt paremad meetmed majanduslike küberrünnakute tõkestamiseks ning teatud ulatuses ka vastutusele võtmises, vähemalt selliste rünnakute osas, kus majanduslike küberrünnakute taga on võimalik näha riikide osalust (näiteks WannaCry). Küberrünnakud ei ole vaid teatud kitsa ringi riikide probleem, vaid rahvusvaheline probleem, mis ületab riigipiire ning mis oma ohupotentsiaalilt võib teatud kontekstis olla võrreldav keemiarelvade ning tuumarelvadega, millesse rahvusvaheline üldsus suhtub märksa tõsisemalt.

Töö autor pooldab praegust nn *soft law* käsitlust ning seda, et rahvusvaheline õigus on küberrünnakute kontekstis otsekohalduv, seda peamiselt põhjusel, et ka nõrgem reguleeritus on parem, kui täielik reguleerimatus. Teisalt on antud töö toonud välja mitmeid võimalikke probleeme, mis rahvusvahelises õiguses võivad küberrünnakute kontekstis tekkida. Näiteks küberrünnakute omistamise keerukuse ning vastumeetmete kasutusele võtmise kontekstis. Küberrünnakute tõlgendamine rahvusvahelise õiguse kontekstis on võimalik, kuid autor leiab, et päris üks-üheselt see praktikas ei toimi. Selle probleemi võiks lahendada küberrünnakute endi praktika tekkimine rahvusvahelise õiguse tasandil, mis on lähtunud küberrünnakute spetsiifikast ning iseäraisusest, kuid autori hinnangul ei saa päris üks-ühele käsitleda ka siis konventsionaalsete relvade poolt läbi viidud rünnakuid ning küberrünnakuid. Siiski ei välista autor täielikult küberkonventsiooni loomise vajadust. Paljudele nimetatud küsimustele, mis töö käigus tekkisid, annab täpsema selguse korduvalt mainitud küberrünnakute valdkonnas tekkiv praktika. Kindlasti on praktika kujunemine üks aspektidest, mida mingil määral riigid ise ning ka rahvusvaheline kogukond ootab, teisalt selliste konfliktide tekkimist ei soovita. Just esmased kaasused võivad anda vihje, kui efektiivne on rahvusvaheline kehtiv õigus

küberrünnakute kontekstis ning kas teoorias käsitletu toimib ka praktikas. Küberruumi reguleerimiseks on peamiselt kaks võimalust, mida autor lahendaks Rahvusvahelise Õiguse Komisjoni kaudu. Nendeks on kehtiva rahvusvahelise õiguse normide kokku leppimine või küberkonventsiooni loomine. Praegune olukord, kus valitseb selgusetus kehtiva õiguse üle, on kahjuks soodsaks pinnaseks tõsiste rahvusvaheliste konfliktide tekkimiseks.

ABSTRACT

From Tallinn Manual to restrictive International Cyber Convention?

One of the most influential events in Estonia's recent history is the cyber attack which happened in 2007. During this the Estonian parliament, ministries, government agencies, banks and media was under a denial-of-service attack. This event was the breakpoint which made Estonia and many other countries rethink their national security in cyberspace. About one year later the NATO Cooperative Cyber Defence Centre of Excellence was founded in Estonia. Since then the focus on advancing the technical and legal solutions in the field of cyber security in international level has been increasing.

Although cyber security has become a bigger part of countries' national security, the tendency of recent years shows the increasing number of cyber attacks. There are more cyber attacks being committed each year and most of these are not even known by the international community. On one side, the regular crime has been moving to cyberspace, but more critical are the cyber attacks which have been carried out to influence country's politics, economy and to undermine the national security.

Currently there are no laws created for the regulation of cyberspace. In previous years the United Nation's Group of Governmental Experts (GGE) have agreed upon that international law applies in cyberspace activities. This means that countries agreed not to interfere with each other's infrastructure, help other nations to investigate the origins of the cyber attack and to be responsible for the actions if they have originated from their country. However, in 2017 when the fifth edition of the cyber norms was developed by the GGE's, it failed to be accepted. The countries involved could not find a consensus especially in the part which indicated that international law applies in cyberspace. Therefore, the international order in cyberspace is still officially undefined.

The current situation regarding to cyber attacks means that there are no norms that regulate international law in the context of cyber attacks. Thereof, cyber attack sphere is mostly relied on the existing United Nations Charter and other international treaties and principles. Hence, the current international law leaves quite a broad margin of interpretation for the definition of cyber attack. It is a question whether this margin leaves too much freedom in understanding the definition and its regulation. It is not certain that different countries understand the

definition of cyber attack the same way. This may indicate that the topic of cyberspace is too complex and the margin of interpretation makes it too hard for countries to overcome the violations being conducted in cyberspace.

In this thesis mainly systematic-analytical and comparable analytical methods are being used. Systematic-analytical methods are mostly used in the parts where the author describes problems that are caused by the interpretation of cyber attack definition. For example, when can the attack be accounted as an attack against country's sovereignty or when is it accounted as an attack against an individual. Comparable analytical method is being used to compare countries, various legal systems and cases. In this thesis different legal scholars' articles and viewpoints have been used for the analysis. Also, many standpoints are based on Tallinn Manual 2.0, which is still currently the only in-depth manual that describes cyberspace in the context of cyber attacks.

The aim of this thesis was to explain whether the situation where international law regulates the cyberspace in the context of cyber attacks can also be applied in practice. If this is not the case then what are the necessary steps to continue with. This thesis brings out how different countries understand the definition of cyber attack. In addition, it is analysed whether international law would be enough to regulate the actions in cyberspace and if not then could the International Cyber war Convention be the solution in defining the cyber norms between countries.

One of the main flaws in understanding and creating the norms in cyberspace is the missing one-to-one definition for cyber attacks in international law. This means that cyber attacks can be defined, handled and judged differently. In the first part of the thesis the author brings out how cyber attack has been defined in different countries and how much these definitions differ from each other. The comparison of these definitions shows that countries do not understand the severity of the attack and the degree of difficulty exactly the same way.

The question that is under the analysis in this thesis is whether international law is enough to regulate the cyberspace and anything else related to cyber security. The latest proposal from UNGGE's failed to reach consensus among the UN member countries. But previously in 2013 and 2015 the countries have approved the proposition of GGE's that international law applies for regulating cyberspace. Therefore, the author believes that applying international law in regulation cyberspace needs more agreed upon definitions, terms and practice on international

level which would help to get the required recognition from the countries. For example, it would be necessary to have the viewpoints of the countries in the context of specific cyber attacks in the UN Security Council or even the International Court of Justice. The topic of cyber attacks would be clearer if the International Law Commission would take the responsibility of the subject. This would give regulating the cyber attacks with international law a more firm position. The current discussion would need new and fresh standpoints since the current views have been lagging behind the same political opinions.

If cyber attacks would be regulated by international law then this raises a question on how this should be interpreted and implemented in practice. Currently there are no international agreements between countries on how international law should be applied in context of cyber attacks. One of the solutions for this would be that the International Law Commission takes the responsibility of designing the international law around the cyberspace using Tallinn Manual as basis for this. Although Tallinn Manual might still have some questionable solutions which the author has previously described, it is still currently the only in-depth manual that describes cyberspace in the context of cyber attacks.

One of the solutions to avoid the uncertainty of regulating and defining cyberspace would be to create an International Cyber war Convention. This however has its advantages and disadvantages. The advantage of the convention would be its specific legal basis which would mean that everyone will have the same understanding of how cyberspace is regulated and how cyber attacks are defined, handled and judged. However, the main issue with this is the complexity on how to make countries agree with the convention whose opinion of cyberspace and definition of cyber attacks is diametrically opposite. This makes finding a common practise very difficult and may end with the support of only a few countries. Also, it is important to emphasize that this kind of convention may restrict the innovative growth of technology and economy. But the author finds that this problem can be overcome by keeping some regulations more broad when defining the convention.

The infrastructure of countries is becoming more dependent on information technology. Therefore, discovering and researching cyber attacks should be a transnational co-operation. The international community should more firmly stand up for countries that do not have the technical capabilities or resources to defend themselves from a cyber attack. Currently there are too many countries who do not have sufficiently prepared themselves to prevent and overcome a cyber attack. The author has brought out as one of the solutions to create an

International Cyber security centre which would assure a faster and efficient research process for cyber attacks. Also, it should be taken into consideration to create an international tribunal for cyber attacks. In this context it is important to bring out that countries should already improve their methods on blocking the economic cyber attacks and find better solutions on how to tackle those who are responsible. Cyber attacks are not just one country's problem, but an international affair which crosses borders and can be as dangerous as chemical and nuclear weapons which the international community regards with much more severity.

KASUTATUD MATERJALID

Kasutatud kirjandus

1. A. Orakhelashvili. Peremptory Norms in International Law. Oxford Scholarship Online. jaanuar 2009.
2. A. Segal. Chinese Cyber Diplomacy in a New Era of Uncertainty. Hoover Institution. Stanford University. Arvutivõrgus: https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf
3. Cyber-Attack Against Ukrainian Critical Infrastructure. veebruar 2016. Arvutivõrgus: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 (12 märts 2018)
4. D. Volz, T. Gardner. In a first, U.S. blames Russia for cyber attacks on energy grid. 15. märts. 2018. Arvutivõrgus: https://www.reuters.com/article/us-usa-russia-sanctions-energygrid/in-a-first-u-s-blames-russia-for-cyber-attacks-on-energy-grid-idUSKCN1GR2G3 (24 märts 2018)
5. E. A. Wilson. People Power and The Problem of Sovereignty in International Law. Duke Journal of Comparative & International Law. Vol 26. No 551.
6. E. Nakashima. Russian Spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say. 24. veebruar. 2018. Arvutivõrgus: https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html?utm_term=.721da7056aff (31 märts 2018)
7. Freedomhouse. Freedom on the Internet 2017. Manipulating Social Media to Undermine Democracy. November 2017. Arvutivõrgus: https://freedomhouse.org/sites/default/files/FOTN_2017_Final.pdf (29 märts 2018)
8. Global Cybersecurity Index (GCI)2017. Arvutivõrgus: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (25 märts 2018)
9. I.C.J. Reports. Nicaragua v. United States of America. Military and Paramilitary Activities in and against Nicaragua. 1986. para 195 Arvutivõrgus: http://www.icj-cij.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf (14 märts 2018)

10. International Humanitarian Law and the Challenges of Contemporary armed conficts Report. 2015. Arvutivõrgus: https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts (25 märts 2018)
11. J. A. Lewis. Liberty, Equality, Connectivity: Translatic Cybersecurity Norms. Center for Strategic & International Studies. veebruar 2014. Arvutivõrgus: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/140225_Lewis_TransatlanticCybersecurityNorms.pdf (30 märts 2018)
12. J. B. Godwin III; Andrey, Kulpin; Karl Frederick, Rauscher, Valrey, Yaschenko. East-West Institute, Critical Terminology Foundations 2, Russia-US Bilateral on Cybersecurity. Policy Report 2/2014. Arvutivõrgus: https://www.files.ethz.ch/isn/178418/terminology2.pdf (24 märts 2018)
13. J. Crawford (koost). Brownlie's Principles of Public International Law (8th edn). Oxford University Press. 2012.
14. J. Jones, N. Shashidar. Ransomware Analysis and Defense Wannacry and Win32 environment. International Journal of Information Security Science. Vol 6. No 4.
15. J. Klabbers. The Concept of Treaty in International Law. Developments in International Law. 1996. Springer.
16. J. Sootak (koost). Üliõpilastöö kirjutamine ja vormistamine: juhend õigusteaduskonna üliõpilastele. Tallinn: Juura 2016. Arvutivõrgus: https://issuu.com/iuridicum/docs/juhend_2016 (13 märts 2017)
17. K. Giles. Russia's Public Stance on Cyberspace Issues. 2012 4th International Conference on Cyber Conflict. Arvutivõrgus: https://ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf (30 märts 2018)
18. K. Zemanek. Armed Attack. Max Planck Encyclopedia of Public International Law. Oxford Public International Law. oktoober 2013. Arvutivõrgus: http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e241 (14 aprill 2018)
19. Küberturvalisuse seaduse eelnõu seletuskiri. 26. september. 2017 Arvutivõrgus: https://www.koda.ee/sites/default/files/content-type/content/2017-10/seletuskiri_k%C3%BCberturvalisuse%20seadus.pdf (24 märts 2018)
20. M. D. Evans (koost), Hugh Thirlway. The Sources of International Law. International Law. Oxford University Press. 2003.

21. M. D. Evans (koost), Malgosia Fitzmaurice. The Practical Working of the Law of Treaties. International Law. Oxford University Press. 2003.
22. M. Eilstrup-Sangiovanni. Why the World Needs an International Cyberwar Convention. 18. juuni 2017. Arvutivõrgus: https://link.springer.com/content/pdf/10.1007%2Fs13347-017-0271-5.pdf (8 märts 2018)
23. M. Forteau. Comparative International Law Within, Not Against, International Law. Lessons from the International Law Commission.
24. M. G. Markoff. Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security 23. juuni. 2017. Arvutivõrgus: https://www.state.gov/s/cyberissues/releasesandremarks/272175.htm
25. M. Holloway. Stuxnet Worm Attack on Iranian Nuclear Facilities. Stanford University. 16. juuli 2015. Arvutivõrgus: http://large.stanford.edu/courses/2015/ph241/holloway1/ (15 aprill 2018)
26. M. Kaljurand. United Nations Group of Governmental Experts: The Estonian Perspective. International Cyber Norms: Legal, Policy & Industry Perspectives, NATO CCD COE Publications. 2016 Arvutivõrgus: https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_Ch6.pdf (14 märts 2018)
27. M. N. Schmitt, L. Vihul jt (koost). Tallinn Manual 2.0 On the International Law Applicable to Cyber Operations. Cambridge University Press. 2017.
28. M. N. Shaw. International Law. Cambridge University Press. 2008.
29. M. Riley, J. Robertson. Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known. 13. juuni. 2017. Arvutivõrgus: https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections (24 märts 2018)
30. M. Roscini. Cyber Operations and the Use of Force in International Law. Oxford Scholarship Online. 2014.
31. NATO Affirms that Cyber attacks may trigger collective defense obligations. American Journal of International Law. jaanuar 2015.
32. Nigerian National Cybersecurity Policy and Strategy – 2015. Arvutivõrgus: https://cert.gov.ng/images/uploads/NATIONAL_CYBESECURITY_STRATEGY.pdf (24 märts 2018)

33. Norse Corporation Attack map. Arvutivõrgus: http://map.norsecorp.com/ (25 märts 2018)
34. O. Solon, A. Hern. Petya ransomware attack: what isi t and how can it be stopped? Arvutivõrgus: https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how (12 märts 2018)
35. Oxford Dictionaries. Arvutivõrgus: https://en.oxforddictionaries.com/definition/cyberattack (24.03.2018)
36. P. Brangetto, M. A. Veenendaal. Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. NATO CCD COE Publications. 2016. Arvutivõrgus: https://ccdcoe.org/cycon/2016/proceedings/08_brangetto_veenendaal.pdf (14 aprill 2018)
37. P. Szoldra. Hacker Reveals How Devastating A Cyberattack On The Stock Market Could Be. 21. august. 2013. Arvutivõrgus: http://www.businessinsider.com/hacker-reveals-how-devastating-a-cyberattack-on-the-stock-market-could-be-2013-8 (13 aprill 2018)
38. Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea 19. detsember. 2017. Arvutivõrgus: https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/ (24 märts 2018)
39. R. Kissel (koost). Glossary of Key Information Security Terms. National Institute of Standards and Technology. US Department of Commerce. 2013. Arvutivõrgus: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf (24 märts 2018)
40. S. Besson. Sovereignty. Max Planck Encyclopedia of Public International Law. aprill 2011. Arvutivõrgus: http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1472?prd=EPIL (16 aprill 2018)
41. S. D. Krasner (koost) – Problematic Sovereignty. Contested Rules and Political Possibilities. Columbia University Press. 2001.
42. S. Morgan. 2017 Cybercrime Report. Cybersecurity Ventures. Arvutivõrgus: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf (24 märts 2018)
43. T. Severin, A. Shalal. German government under cyber attack, shores up defenses. 1. märts. 2018. Arvutivõrgus: https://www.reuters.com/article/us-germany-

cyber/german-government-under-cyber-attack-shores-up-defenses-idUSKCN1GD4C8 (24 märts 2018)

44. The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028. 2010. Arvutivõrgus: https://fas.org/irp/doddir/army/pam525-7-8.pdf
45. United Nations General Assembly Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/69/723. 13. jaanuar. 2015 Arvutivõrgus: http://undocs.org/A/69/723 (25 märts 2015)
46. United Nations General Assembly Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174. 22. juuni. 2015 Arvutivõrgus: http://undocs.org/A/70/174 (25 märts 2015)
47. UNODA. United Nations Office For Disarmament Affairs. Arvutvõrgus: https://www.un.org/disarmament/topics/informationsecurity/
48. USA Department of Defense Law of War Manual. https://www.defense.gov/Portals/1/Documents/DoD_Law_of_War_Manual-June_2015_Updated_May_2016.pdf
49. Valitsus kiitis heaks Eesti andmesaatkonna rajamise Luksemburgi 15.06.2017. Arvutivõrgus: https://www.mkm.ee/et/uudised/valitsus-kiitis-heaks-eesti-andmesaatkonna-rajamise-luksemburgi (15 märts 2018)
50. Winter Olympics hit by cyber-attack. 12. veebruar. 2018. Arvutivõrgus: http://www.bbc.com/news/technology-43030673 (24 märts 2018)

Kasutatud õigusaktid

51. Karistusseadustik[1] - RT I 2001, 61, 364

Rahvusvahelised lepingud

52. Council of Europe. Convention on Cybercrime. Chart of Signatures and ratifications of Treaty 185. Status as of 30.03.2018. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=LwUpff4y (30 märts 2018)

53. Statute of the International Law Commission. 1947. Arvutivõrgus: http://legal.un.org/ilc/texts/instruments/english/statute/statute.pdf (22 aprill 2018)
54. Ühinenud Rahvaste Organisatsiooni põhikiri ning Rahvusvahelise Kohtu statuut. RT II 1996, 24, 95
55. ÜRO Inimõiguste ülddeklaratsioon. Arvutivõrgus: http://vm.ee/et/uro-inimoiguste-ulddeklaratsioon (12 märts 2018)

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, **Sander Pelisaar**,

(sünnikuupäev: **24.11.1992**)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose

„**Tallinna käsiraamatust rahvusvahelise küberrünnakuid piirava konventsioonini?**“, mille juhendajaks on *dr. iur.* Lauri Mälksoo,

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, 23.04.2018.